MINISTRY OF FINANCE
Finland

Effective Information Security

A Summary of General Instructions on Information Security Management

The Government Information Security Management Board

5/2009
VAHTI

MINISTRY OF FINANCE

Effective Information Security

A Summary of General Instructions on Information Security Management

The Government Information Security Management Board 5/2009 VAHTI

MINISTRY OF FINANCE
PO Box 28 (Snellmaninkatu 1 A) FI-00023 GOVERNMENT
FINLAND
Tel. +358 9 16001
Internet: www.financeministry.fi
Layout: Pirkko Ala-Marttila

ISSN 1455-2566 (print)
ISBN 978- 951-804-982-4 (print)
ISSN 1798-0860 (pdf)
ISBN 978-951-804-983-1 (pdf)

Edita Prima Plc
Helsinki 2009

Introducing the organisation – VAHTI'S task

The Ministry of Finance is responsible for the steering and development of central government information security in Finland and has set up the Government Information Security Management Board (VAHTI) as the body responsible for cooperation, steering and development in the area of central government information security. In its work, VAHTI supports the Government and the Ministry of Finance in decision-making and in the preparation of decisions relating to central government's 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 management.

VAHTI handles all the significant central government information security policies and the steering of information security measures. VAHTI also handles central government information security statutes, instructions, recommendations and targets. All areas of information security are subject to VAHTI's scrutiny.

VAHTI's work has improved central government information security, and the effectiveness of its work is evident not only in the central government but also in companies and internationally. The result is a very comprehensive set of general information security instructions (www.vm.fi/VAHTI). Led by the Ministry of Finance and VAHTI, a number of joint information security projects have been implemented with ministries and agencies. VAHTI has prepared, managed and implemented the central government information security development programme, in which significant development work has been achieved at a total of 26 development locations by 300 people appointed to the projects.

VAHTI promotes the development of networked operating practices in public administration information security work.

In addition to the central government, the results of VAHTI's work are also widely utilised in local government, the private sector, international cooperation and everyday life. For three years in succession, VAHTI has been recognised with an award for exemplary work in improving Finland's information security.

Executive summary

The Government Information Security Management Board (VAHTI) has produced for the central government's use comprehensive instruction and recommendation material over the entire field of information security. These summarised instructions serve as a manual and as a link to the more extensive instructions and present their main elements in condensed form. Moreover, these instructions emphasise the management perspective, management and supervisor responsibility as well as information security planning. Their purpose is to give the management of central government organisations, and particularly their senior information management staff and security and information security personnel, together with people otherwise working in the said tasks, instructions for managing information security as part of their own work.

These instructions have been written primarily for central government use, but they are for the most part also applicable to other organisations. Information security has been described as an entity that includes operational processes and people as well as the security and safeguarding of information material and information systems. The main elements are people, processes, information material, information technology and availability of information. Policy, instructions, training and the consequent common understanding and operating practices that arise are the cornerstones of an organisation's good information security culture.

An organisation's internal data processing, production and customer service depend on the confidentiality, integrity and availability of the information behind them, namely on information security. A breach of information security can undermine an organisation's operational reliability and interrupt or prevent the provision of services used by both internal and external services. Without information security measures as well as backup measures created in advance, the electronic services and activities provided by society cannot be guaranteed in a normal situation nor, in particular, in the event of serious disruptions or emergency conditions.

It is the task of the management, as part of their own management work, also to ensure the information security of their organisation's operations. Part of the management process should be to ensure that the level of information security and risk management corresponds to the targets set for them and that

sufficient maintenance and development resources have been allocated to information security functions. Attention should also be paid to the wellbeing of employees, because a high level of security can be achieved only by an organisation where employees are well motivated in their work.

The management develop and strengthen the principles of their organisation's information security and risk management. In addition, measures should be taken to ensure that management receive regular reports on the organisation's information security situation and events as well as on any corrective measures arising from them.

This publication gives an overall picture of what an information security management system created on the basis of an information security and risk management system, and supporting good information management practice, should be like and how it should operate. With the aid of an information security management system, an organisation can ensure the achievement of both its own and the Government's targets in accordance with the resolution on central government information security and other guidelines, general information principles and statutes, as well as instructions given by the Ministry of Finance. The most important objective of VAHTI activity and instructions is to enhance central government information security.

The VAHTI instructions support organisations in the planning, implementation and maintenance of information security as well as in preparing the necessary documents.

Structure

The introduction to these instructions describes the general principles and justification of information security from a central government perspective.

Chapter 2 deals with the fundamentals of information security as well as the organisation, monitoring and reporting of information security, including risk management.

Chapter 3 examines the organisation of information security, its incorporation into processes as well as its implementation and practical evaluation.

The main details of the elements of information security are discussed from Chapter 4 onwards on the basis of a traditional eight-element subdivision. Chapter 11 examines the principles of continuity and emergency conditions planning and Chapter 12 the classifications used in information security.

Appended to these instructions is a set of document models relating to the building of an organisation's information security management system.

Appendix 1 presents model policies and planning frameworks.

Appendix 2 is a list of information security responsibilities and related roles.

Contents

1 Introduction

1.1 Introduction to the concept of information security

The term information security means the protection and back-up of information and services as well as systems and telecommunications in order to manage the risks directed at them. Protection and back-up are achieved in both normal and emergency conditions through administrative, technical and other measures.

The objective of information security is to safeguard the confidentiality, integrity and availability of information from threats and accidents arising from hardware and software faults, natural events and wilful, negligent or accidental actions.

Central government information, information systems and services are essential for Finnish society; they are also economically irreplaceable and vital in terms of the nation's security and functions. For society to function, an adequate level of information security is required.

Efficiency requirements in a rapidly developing and internationalising society have made information technology vital in all activities in society. Our engagement with information technology as well as our dependence on its reliability and the continuous availability of information and technology are placing an increasing significance on information security. Information security is of key importance in managing and safeguarding all of an organisation's activities, whether in normal conditions, during disruptions or malfunctions, in emergency conditions or in possible special situations. Information security is a fundamental prerequisite of the quality and operational reliability of central government as a whole as well as of good information management practice.

A high standard and quality of information security are important for citizens as well as for central government activities and openness. A low level of information security may jeopardise the security and economic interests of the central government and citizens, cause additional work and costs as a consequence of damage and loss of information, and weaken the credibility of the authorities' activities.

The key statutes governing central government information security work are:

- The Archives Act (Arkistolaki 831/1994)
- The Personal Data Act (Henkilötietolaki 523/1999)
- The Act on Electronic Services and Communication in the Public Sector (Laki sähköisestä asoinnista 13/2003)
- The State Budget Act (Talousarviolaki 423/1988)
- The State Budget Decree (Talousarvioasetus 1243/1992)
- The Act on the Openness of Government Activities (Julkisuuslaki 621/1999)
- The Decree on the Openness of Government Activities (Julkisuusasetus 1030/1999)
- The Act on the Protection of Privacy in Working Life (Työelämän tietosuojalaki 759/2004):
- The basic rights and freedoms provisions of the Constitution (Perustuslaki 731/1999)
- The Act on the Protection of Privacy in Electronic Communications (Laki yksityisyyden suojasta sähköisessä viestinnässä 516/2004)
- The Emergency Powers Act (Valmiuslaki 1080/1991)
- The State Civil Servants Act (Virkamieslaki 750/1994)

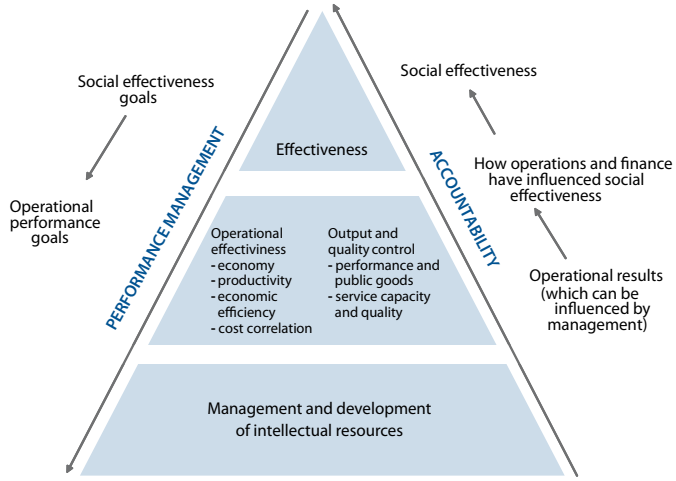
Each authority is individually responsible for implementing the statutes and the resolution on central government security as well as promoting information security development.

The Government resolution on central government information security relates to:

- ministries, government agencies and public bodies
- data processing, information management and data transfer services acquired by them from external parties or outsourced to unincorporated government enterprises founded by them and
- state-owned enterprises handling official functions of the state.

An organisation should conduct its activities in accordance with good administrative practice. Good information management practice requires performance responsibility and accountability as well as a commitment to efficiency and transparency. The performance prism is also applicable to information security management.

Figure 1. Performance prism



Information security and its productive management require the commitment of management to the development of information security. The management must also ensure the allocation of the resources required by information security. The organisation must develop the ability to integrate information security into its management activity and culture. Through an open and transparent management model it is possible to involve all personnel in developing information security. This creates for the organisation a secure operating and services environment that fulfils its operational needs. An advanced management system and a high information security culture create the conditions for cost-effective risk management and thereby an effective information security management system.

Senior management commitment is essential for systematic work to succeed. The management decide the desired information security level (maturity level) and its significance for their organisation. The desired strategic intent and position are presented regularly in up-to-date operating strategy and policy documents (information security and risk management policy). Based on these, the organisation prepares and strengthens the practical information security instructions that govern the practical information security and processes of the organisation's personnel.

In particular, the importance of the secure handling of information (information capital) should be emphasised as part of both the employees' and the organisation's activities.

Regular information security training effectively maintains the information security expertise and information security awareness of personnel.

Quality, cost-effective provision of services also means secure services.

The level of information security should also be measured. Indicators linked to the performance management process will ensure the achievement of information security targets both on an annual basis and over a longer period. The fulfilment of the information security level and the management of related risks should also be evaluated by the organisation's internal auditing or corresponding function. The task is to confirm that management are complying with laws, statutes and standards, and to supervise the implementation of management's plans.

Information security management means in practice the implementation of risk management. Daily operating processes must include methods by which risks can be reduced, or their impact lessened, in an orderly manner. In well-managed organisations, information security and other security tasks, the responsibilities of those performing these tasks and reporting practices are properly defined.

The provision of electronic services requires the trust of users. Information security aspects relating to the provision of services must be reviewed when examining an organisation's opportunities to provide new services. Use of information technology services requires a connection between the user and the system. The information security of the connection depends on the classification of the information moving on the information network. The information security of the connection must correspond to the information security level of the information transferred in the network. Linked data warehouses must be accessible, consistent and up-to-date, and the confidentiality of the information obtainable from them must be ensured.

1.2 Good information management practice

Good governance in public administration means the quality, efficiency, transparency and accountability of operating practices and structures. An essential element of good governance in public administration is a citizen- and customer-oriented way of operating. This requires clarity of organisational structures and roles at different levels of management and operating according to these roles.
Definition: Financial Controller

Good information management practice is a way of operating that includes a high standard and good quality of work. The good quality requirement relates above all to the documents and information processed by the public administration. The characteristics required of these are accessibility and availability, integrity and accuracy, and confidentiality. The quality of documents and information is ensured with the aid administrative practice and information systems.
Ministry of Finance definition of information management practice 11/2000

Good information management practice must be included in the normal work of every employee and it should also be taken into account in processes. Targets in accordance with the Act on the Openness of Government Activities should be fulfilled through the appropriate organisation, resourcing, planning and direction of operations.

The first practical prerequisite for the implementation of good information management practice is that the authority has detailed, up-to-date descriptions of its own tasks, including what information and documents are created in the handling of the said tasks as well as how long the information and documents should be kept. These descriptions are needed for document and information management. The descriptions not only serve the organisation itself, but also external parties who need the information. Those seeking information can then ascertain which public documents and information exist in the organisation and where they can be found.

Another prerequisite is that the organisation's individual issues are under control. Lists of individual issues that are being, and have been, processed should be obtainable in records, various information systems, registers and archives.

A third prerequisite for good information management practice is that the authority's information management and archiving as well as its communications and information service are appropriately resourced and organised, and that responsibilities for tasks as well as mutual division of labour are clearly specified. This means that all functions and work stages related to information processes are significant. A quality system is achieved only if all areas of information work cooperate effectively and appropriately.

A fourth prerequisite for good information management practice is that operations are governed by instructions. Instructions help ensure operational continuity, transparency and quality. Common ground rules should ensure that employees act in the same way in the same situations, in which case good information management practice goals and principles will be fulfilled. Instructions can help safeguard operational continuity, because then operating practices can be transferred from one person to another and taught to new employees. The Act and Decree on the Openness of Government Activities require that personnel are trained to act in accordance with instructions, and that compliance with instructions is supervised and monitored.

1.3 Coordination of information security work in central government

In December 2008, the Government issued a resolution on a national information security strategy. The resolution's objectives are to promote national and international information security cooperation, enhance national competitive-

ness and the operational environment for Finnish ICT companies, improve information security risk management and safeguard the fulfilment of fundamental rights and national information capital, and increase information security awareness and expertise.

The Government resolution on central government information security steers development policies. According to the Government's rules of procedure, the Ministry of Finance directs and reconciles development activities. Each ministry is responsible for advancing information security activities in its own administrative branch. It is the task of the Government Information Security Management Board (VAHTI) to prepare and harmonise the information security policies of the Government and the Ministry of Finance.

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 government activity, steering and performance management. VAHTI handles central government information security statutes, instructions, recommendations and targets. 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 it promotes the development of networked operating practice in public administration information security work.

The Management Board participates when necessary in the work of cooperation groups developing national and international information security. The key central government organisations in terms of information security work are represented on the board.

Each ministry is responsible for directing and monitoring information security in its own administrative branch.

The Data Protection Board and the Data Protection Ombudsman promote the development of and adherence to good data processing practice according to the provisions of the Data Protection Act. They monitor the protection of privacy and issue instructions on the protection of personal data records from use by third parties.

The National Audit Office of Finland performs audits of central government IT and electronic administration functions. Information security is one aspect to be taken into account in these audits.

The National Archive Service issues document management orders and instructions on the retention, preservation and destruction of data materials.

The Finnish Treasury issues instructions on the fulfilment of obligations under the Budget Decree (administrative and payment traffic systems).

The Communications Regulatory Authority supervises telecommunications activities and, when necessary, issues technical orders on the operation of telecommunications companies and on the provision of telecommunications equipment, networks and services with a sufficient level of security. The Com-

munications Regulatory Authority also acts as the national information security authority, and it maintains and provides the services of the national Computer Emergency Response Team (CERT-FI). In addition, the Communications Regulatory Authority's duties include communications security (COMSEC) tasks.

The information system department of the National Board of Economic Defence and its data transfer, data processing and mass communications committee, together with the National Emergency Supply Agency, direct and develop in cooperation with the responsible administrative branches the emergency planning of the data transfer, data processing and electronic mass communications of government agencies, public bodies and businesses as well as contingency planning for emergency conditions.

1.4 A changing, globalising operating environment

Finnish public administration, through a tightening of international cooperation and the accelerating globalisation of the operating environment, is to an increasing extent bound by, and dependent on, constraints relating to data processing of other countries and international organisations. Cooperation takes place via electronic networks, and therefore data exchange requires not only mutual trust but also common procedures and, in the case of agreements, evaluation practices.

The international practices that bind Finland apply mainly to the handling of data and, of these, European Union directives and the partnership agreements between Finland and the West European Union (WEA) and between Finland and NATO bind the central government directly. International information security cooperation may give rise to investment in human resources and associated costs.

In addition, the Organisation for Economic Cooperation and Development's (OECD) recommendation on security principles guides the central government's information security practices and defines good information management practice.

1.5 Working group

These instructions were prepared by an inter-ministerial working group established in 2006 by the Government Information Security Management Board and were translated into English in 2009.

1.6 Chapter guide to the instructions by target group

The Government Information Security Management Board (VAHTI) has produced for central government use comprehensive instruction and recommendation material over the entire field of information security.

This publication is intended to serve as a manual and as a link to the more extensive instructions, presenting their main elements in condensed form. These instructions emphasise the management perspective, management and supervisor responsibility as well as information security planning. Their main target group are senior management and directors of central government organisations and information management and security personnel and information security management in particular. Moreover, individuals working in central government tasks other than those mentioned above may find guidelines for their own work in these instructions.

This publication also gives to those working outside central government and to those interested in the development of information security an opportunity to acquaint themselves with the body of instructions and recommendations on the continually changing management and development of information security created under VAHTI's direction.

Chapter guide by target group

Role - task	Ch 2	Ch 3	Ch 4	Ch 5	Ch 6	Ch 7	Ch 8	Ch 9	Ch 10	Ch 11	Ch 12
Senior Management	X	X								X	
Administrative Management	X	X		X							
Security Management	X	X	X	X	X	X	X	X	X	X	X
Information Security Management	X	X	X	X		X	X	X	X	X	X
Subunit Management, Sector Management	X	X	X	X	X					X	X
Information Technology Management	X	X	X	X		X	X	X	X	X	X
Information Security Experts, Security Experts		X	X	X	X		X	X	X	X	X
Individuals working in supervisor roles	X		X	X							
Information System Owner	X	X	X	X		X	X	X	X	X	X
System Experts, IT Support	X		X	X		X	X	X	X		
Emergency Preparedness Manager/ Secretary	X	X	X	X	X	X	X	X	X	X	X
Internal Auditing, System Auditing	X	X	X	X	X	X	X	X	X	X	X
Individuals responsible for document management and archives	X		X							X	
Individuals responsible for information service	X		X							X	
Information System Main User	X		X		X	X	X		X	X	X
Standard Users, employees	X		X		X				X		
Procurement personnel	X									X	
Individuals handling personal data records	X		X	X							
Premises management personnel	X				X					X	X
Information Security Group	X	X	X	X	X	X	X	X	X	X	X
Security and Emergency Preparedness Group	X	X	X	X	X	X	X	X	X	X	X
Risk Management Co-ordination Group	X	X	X	X	X	X	X	X	X	X	X
Individuals responsible for contracts and agreements	X				X					X	
Occupational Safety Director, Occupational Safety Supervisor	X	X		X			X			X	X
Consultants and Service Companies	X		X		X			X	X	X	X

2 Information security fundamentals

2.1 Risk management policy

The reports on operations included in the financial accounts of a accounting offices shall comprise the following:

An assessment of the appropriateness and adequacy of internal control and of the risk management entailed therein and a statement prepared on the basis of it on the status and the most essential development needs of internal control (assessment and statement of assurance of internal control).
State Budget Decree (1243/1992) Section 65, Paragraph 7

Information security risks are diversifying while completely new risks and threats are arising. A prerequisite of national security is the preventive identification and management of risks. When risks are reliably recognised, their adverse effects can be minimised by developing information security. Operations should focus on prevention, not on reaction after the fact. Risk management also calls for adequate, up-to-date monitoring of the national situation.
National Information Security, 2002, Chapter 3.1

Management of information security risks is part of an organisation's comprehensive risk management. Integration of risk management into management systems substantially improves an organisation's ability to respond to various information security, and other, threats. The principles of risk management include the introduction, maintenance and updating of the management system.

Effective risk management reduces and alleviates losses and other damage that threaten an organisation. It involves systematic, continuous development to identify, evaluate and control threats. Risk management is based on the organisation's operational goals and strategy, development, safeguarding of service processes, and the expertise of personnel and management of human resources.

Risk management policy formulates management as a whole and creates policies for its handling and development. To provide for systematic risk management in the policy, procedures and tools are agreed by which information on the most important risk factors is supplied to management. The procedures described in the policy specify the identification of risks, their management planning, implementation and monitoring, and agreements are made on the organisation and continuous implementation of risk management work.

With the aid of risk management policy, risk management is integrated into the management system and its annual schedule. The policy does not necessarily need to be a separate document; it may be included, for example, in operating and financial plans.

The risk management policy is approved by the organisation's senior management and it is based on statutes and ministerial instructions. Management also determines the coverage, responsibilities and internal organisation of risk management.

2.2 Information security policy

> The senior management of a ministry, agency or institute approve and confirm the security and contingency planning principles to be adhered to in their organisation and determine the internal organisation handling the issue. Individual units and their managers are responsible for the implementation and monitoring of security and contingency planning principles in accordance with the principles of performance management. Operating principles should include information security targets and procedures.
> *Government Resolution on Central Government Information Security (11.11.1999)*

With the aid of information security policy, management specifies the objectives, responsibilities and operating guidelines of information security.

For the establishment of an information security culture, it is essential that the significance of information security and the general principles of information security work are explained to every employee. Information security policy serves as a foundation on which various information security plans and instructions are built.

The formulation of information security is directed by the purpose and strategy of an organisation's activities, risk analysis, laws and regulations. If an organisation is committed to adhering to certain standards, and especially if one of the organisation's objectives is certification according to a standard, the information security policy must fulfil the requirements of these standards.

Senior management approve an organisation-specific information security policy, confirm the security and contingency planning principles, and specify responsibilities and the activities the internal information security organisation. Heads of units are responsible for the implementation and monitoring of security and contingency planning principles in accordance with the principles of performance management.

Responsibility for the preparation and maintenance of information security policy is often assigned to the individual responsible for information security. The management ensure that the document is reviewed or updated regularly,

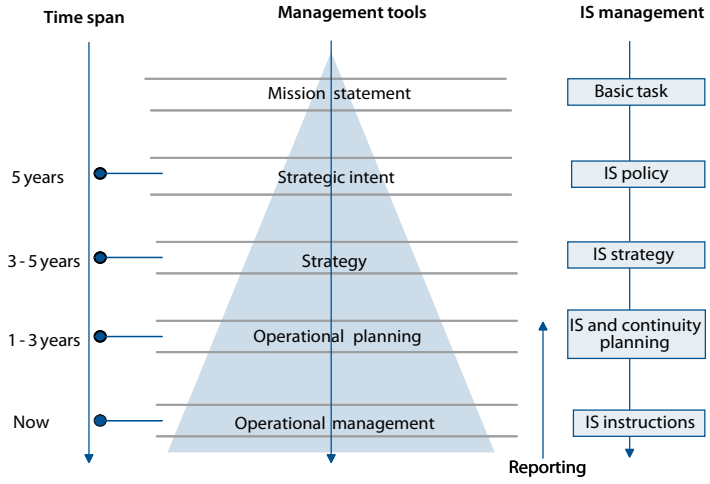
at least every three years and when there are operational and organisational changes.

2.3 Information security management

> In order to create and implement good information management practice, the authorities shall see to the appropriate availability, accessibility, protection and integrity of documents and information systems and the information contained in them as well as other factors affecting the quality of information.
> *Act on the Openness of Government Activities, Section 18*
>
> Information security management is an integral part of the operational management of an organisation. It should therefore be included in the responsibilities of every individual working in management positions. Information security is best implemented when it is built into the organisation's planning processes (operational development), quality and other monitoring system (assessment, measurement), and achievement of targets of routine operations.
> *Information Technology Security and Safeguarding Operations, National Board of Economic Defence, 2002*

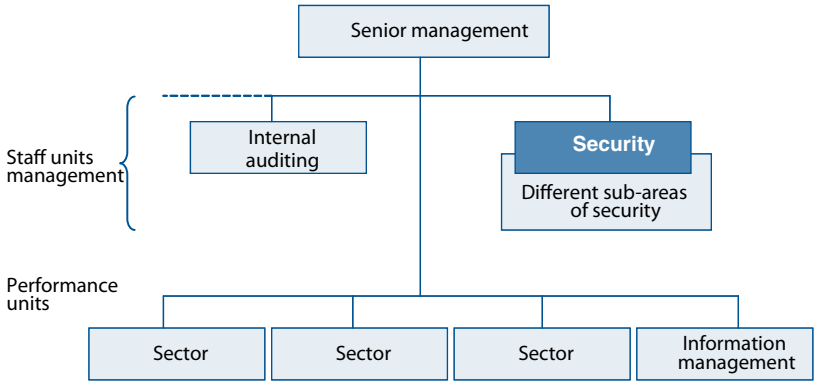
Information security management is therefore part of all management activity. In addition to the management, attending to information security is part of the responsibilities of everyone employed by an organisation. Only the commitment of management to the development of information security will enable the achievement of targets set for an organisation's activities.

Figure 2. The relationship between the management system and information security



To enable effective planning and resourcing of information security activities and to assign responsibilities by means of regular risk analysis, the management need an overall view of the functions, processes and staff expertise at different levels of their organisation, and of the key risks associated with the organisation's activities.

Figure 3. Example of an information security organisation model



Information security management must be arranged so that the set objectives are in the right proportion to an organisation's overall security and so that they support the various security objectives in strategies. Security is often part of the management functions of senior management while information security is one of its subareas, but other organisational approaches are also possible. The selected organisation model affects the focus of information security management tasks. An organisation should be structured in such a way that security is closely related to auditing, with the security function reporting directly to management. Implementation and monitoring (evaluation/auditing) should be operationally differentiated.

Information security management draws on an up-to-date information security policy. In an organisation, information security takes shape in the form of, for example, regular risk assessment and management measures, determining the information security level of new systems and attending to it throughout the entire life cycle of the system.

Information security responsibilities are included in the management system, management rules, rules of procedure and job descriptions, and in human resources performance management. Job descriptions should specify responsibilities, information security management, authorisations and actions in the event of serious incidents, as well as monitoring and reporting obligations. In addition to general responsibilities, special expertise and nominated security

experts are also required in an organisation's information security management tasks.

The information security responsibility specification must follow organisational and operational changes. Information security arrangements depend on an organisation's maturity level. Depending on the organisation, a number of the information security responsibilities can be included in the duties of the same individual. It is essential that arrangements are made for the handling of these tasks.

A list of essential responsibilities and roles is presented in Appendix 2, where the responsibilities of individuals working in different roles for information security implementation and development are described.

No separate law has been enacted on information security, rather elements of it can be found in selected legal provisions.

2.4 Information security as an element of performance management

> The information on performance shall include comparisons with performance targets in accordance with Section 11 as well as repots on deviations and the main reasons for the deviations.
> *State Budget Decree, Section 65*
>
> For example, an adequate level of information security is an absolute prerequisite of the operational continuity and credibility of an agency.
> The Ministry of Finance recommendation Information Security and Performance Management (VAHTI 1/2005) presents the main principles of information security and their connection with performance management, the management of agencies and operational assessment.
> *Handbook on Performance Management (Ministry of Finance 2/2005, Chapter 7.4)*

It is the task of every organisational level and all performance areas to attend to the information security of their own activities and services they purchase, specify the required principles, and when necessary prepare regulations and detailed instructions.

Clear and measurable information security targets should be specified for each organisational level in performance target negotiations. It is recommended that information security targets for large development projects be agreed on an individual project basis in order to ensure their cost-effectiveness. Performance targets should be closely linked to actual activity, thereby ensuring the achievement of results.

In performance management, an organisation must:

- attend to the performance management of information security
- agree with its performance units the concrete implementation of information security work
- attend to information security procedures when outsourcing and acquiring services on a subcontracting basis or when procedures cover several parties
- attend to the information security training of its personnel, and
- attend to continuity and emergency preparedness planning as well as contingency planning for emergency conditions and related contractual procedures.

Information security tasks are included in the job descriptions of all employees. They apply to both organisation management and standard users. Performance units determine performance targets all the way to the information security targets of individual employees.

Table 1. Information security targets and period

Targets based on an organisation's own characteristics for different time intervals	
Time interval	**Target areas**
Strategic planning period	Operational productivity, quality, uninterrupted service provision.
Operating and financial planning period	Specification of desired information security level (maturity level) and implementation of development programme in accordance with it. Achievement of maturity level as specified in the management system.
Annual targets	Measurable targets that show that the security level has been met. Targets from the development programme.
Constraints Compliance of statutory information security level. Management statement on risk management.	

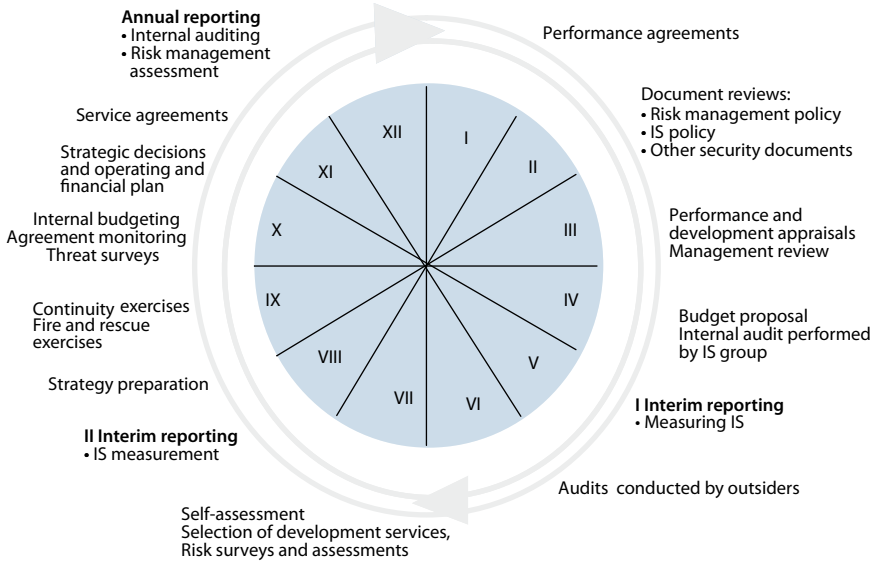
When setting targets, indicators should also be specified. Possible indicators may be, for example, fulfilment of development targets, the trend in the number of information security anomalies, and the imputed savings to be achieved through information security measures in the event of serious incidents (person years and the corresponding value in euros).

To monitor the security situation and results, performance agreements should also specify monitoring responsibilities as well as reporting to senior

management, the organisation's operational and key support function management, key individuals in positions of responsibility and supervisors. Performance management target-setting directs the planning and implementation of practical security measures. Information security tasks, responsibilities and reporting obligations can also be recorded in other documents in addition to performance agreements.

Information security is included in the annual planning process. Annual and longer period targets are incorporated into performance management. Costs arising from information security measures are normal operating expenditure and they are taken into account when planning activities and preparing budget proposals.

Figure 4. Donut dial for annual planning



The budget takes into account information security development investments, cost items in plans, and operational expenditure such as personnel expenses and maintenance agreement costs. The budget must also make provision for expenditure caused by risks as well as information security assessment and measurement costs.

When developing operational activities, adequate resources must be allocated to information security in new processes and systems. When information security investments are made, a payback period in proportion to the estimated risk is calculated.

2.5 Information security as part of operational strategic planning

> Government agencies shall plan their operations and finances, and their performance, several years ahead. Ministries shall plan the effectiveness of operations and operative performance in their sector several years ahead.
> *State Budget Act (423/1988), Section 12*
>
> The national information security strategy is a key element of the Government information society policy. The strategy assists in combating information threats and exploiting related opportunities in both normal and emergency conditions. The strategy provides a common direction to the information security efforts of the Government, businesses, organisations and individual citizens. The strategy does not, however, affect the division of responsibility relating to information nor existing organisational structures.
> *Explanatory Memorandum on the Government Resolution on National Information Security Strategy*

Information and its utilisation play a key role in the strategies of organisations today. At the same time, information security has become a strategic question. Information society development provides an opportunity to reform operating practices, improve customer service and save resources.

An information security strategy is a management policy on information security targets and the means by which the organisation aims to achieve these targets. Information security is primarily included in the strategic plans. The security guidelines contained in strategic plans are linked to operations and thereby directly to any changes that occur. Information security is also included in an organisation's other strategies (for example human resources and information management strategies). An information security strategy supporting the implementation of the organisation's strategic plans can also be specified separately.

Strategic decisions and plans are also reviewed in terms of information security when operating guidelines change or, for example, new electronic services are introduced. Function-specific information security strategy priorities are included in strategic plans and information security guidelines formulated for new services.

Table 2. Relationship of planning documents to time

Effectiveness	Planning document
Strategic planning period	Information security strategy, risk management policy, information security policy
Operating and financial planning period	Development plans, information security instructions, continuity plans
Year	Risk analyses, risk management plans, action plans

2.6 Information security and quality

Features common to all quality systems are customer-orientation, description of processes, responsibilities and tasks, and measurement and continuous development of operations. Information security is an essential element of the operational and service features and characteristics by which established or expected needs are fulfilled. It is therefore an operational quality factor. Information security is part of an organisation's quality system.

Security requirements have already been covered for some time in standards, for example in information security standards such as ISO19977 and ISO27001 and their predecessors. A standard can be applied both as a checklist of information security measures and as a certification option. Alongside standards, however, additional requirements resulting from Finnish statutes, for example in relation to preparedness for emergency conditions, should be taken into account. Assessment, particularly of operationally critical systems and software, is absolutely necessary.

An information security and quality platform for new information systems and the services based on them is created in connection with system development in the preliminary assessment stage or in the specification of an outsourced service when it is acquired. Addressing information security only after development work or the purchase of a ready-made product is generally very expensive or virtually impossible. Information security is therefore a key component of system development already from its initial stages.

Public image, protection of privacy and equal treatment of customers are core values for the quality of information security. Requirements for information security measures also necessitate extensive, networked cooperation between organisations.

The European Foundation for Quality Management (EFQM) quality system applied in central government, moreover, sets quality criteria for organisations' activities to which information security requirements are also clearly related.

The Common Assessment Framework (CAF) linked to EFQM is a European public administration quality self-assessment method. The following table

describes the main information security criteria of the CAF, divided into assessment areas:

Table 3. Main criteria of the CAF method

Assessment area	Information security assessment criteria
Leadership	Information security leadership practice
Strategies and planning	Security policy, information security policy and security in operating strategies as well as their translation in operations
People	Information security expertise and its inclusion in operating practices
Partnerships and resources	Information security management in cooperative relationships, technology, the management of information and knowledge, and the management of the physical operating environment Outsourcing and security management Information security in the procurement of services
Processes	Information security management as part of process development, planning and systematic management in own and partner-related processes as well as the continuous development of information security processes
Customer/citizen oriented results	Information security indicator and monitoring of results from the perspectives of the customer and performance
People results	Motivation, satisfaction and performance, information security work expertise, commitment
Social results	Responsibility for social effectiveness. Monitoring secure development. Detecting events that jeopardise security and preventively influencing them.
Key performance results	Results of agreed development projects

Wide-ranging information security work requires comprehensive documentation and a systematic approach. The existence of operating principles and plans alone does not produce quality; this depends on the actions performed in practice and the results achieved with them.

A quality operating practice requires clear targets and their achievement, the benchmarking of methods against the best practices of external organisations, improvements in performance and results, as well as results recognised based on benchmarking. Good quality also requires performance and process management, but so that achieved results are traceable from the operating practices specified as a consequence of such management.

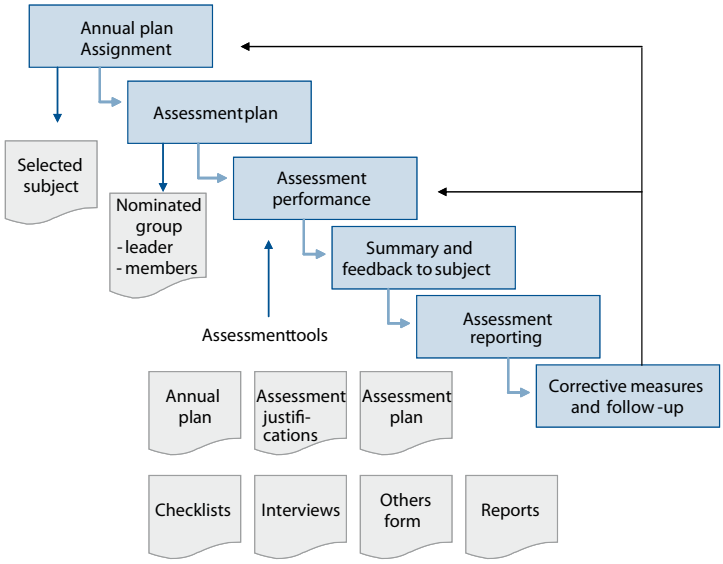
2.7 Assessment and monitoring

> The reports on operations included in the financial accounts of accounting offices shall comprise the following:
>
> An assessment of the appropriateness and adequacy of internal control and of the risk management entailed therein and a statement prepared on the basis of it on the status and the most essential development needs of internal control (assessment and statement of assurance of internal control).
> *State Budget Decree (1243/1992), Section 65, Paragraph 7*

Information security assessment is part of risk management according to an organisation's planning cycle. Assessment produces data on operational results and development needs, and supports the fulfilment of responsibility and accountability for results. Information security assessment should begin by first assessing the information security management system and its coverage. In addition to the management system, it should cover the various subareas of information security.

The evaluation process has clear main stages: appoint an assessment group, plan the process and select the method, conduct the assessment, collect and analyse the data obtained, and finally report the results, justifications, and proposals for further measures. After the assessment, responsibilities are assigned for the presented proposals on further measures and their implementation scheduled.

Figure 5. Evaluation process



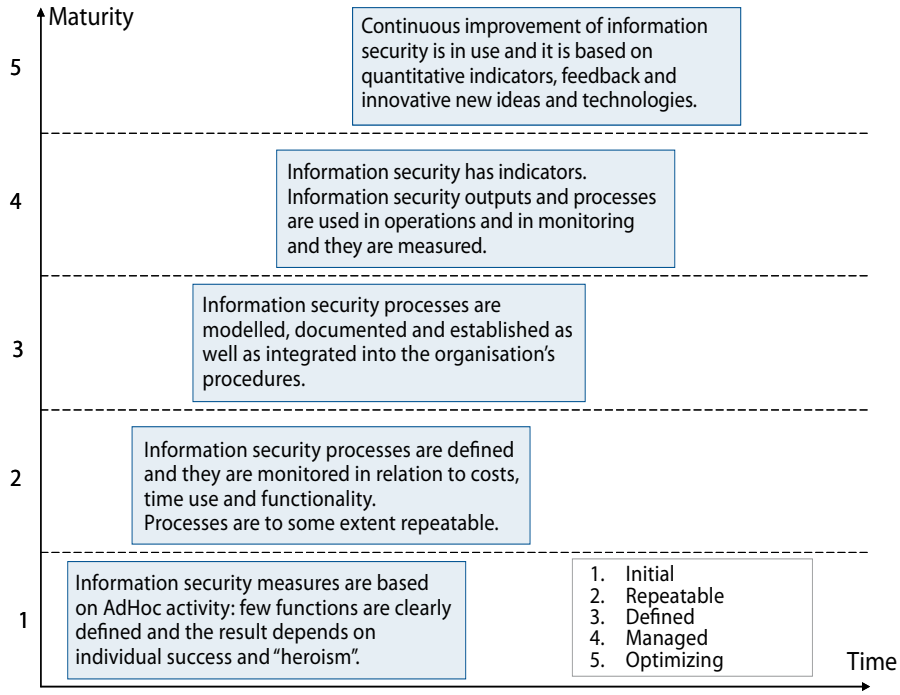
3 Organisation of information security

3.1 Process thinking as the basis of information security

> The senior management of a ministry, agency or institute approve and confirm the security and contingency planning principles to be adhered to in their organisation and determine the internal organisation handling the issue. Individual units and their managers are responsible for the implementation and monitoring of security and contingency planning principles in accordance with the principles of performance management. Operating principles should include information security targets and procedures.
> *Government Resolution on Central Government Information Security (11.11.1999)*

Information security must be included as part of an organisation's operating processes to ensure that it is implemented in practice. Its incorporation into processes requires good cooperation from information security management, personnel responsible for information security, information system owners and service providers. Measures that increase information security should be taken into account when processes are planned to ensure that security requirements are fulfilled.

Figure 6. Information security maturity levels (ISO 21827 Systems Security Engineering - Capability Maturity Model)



When secure processes are maintained and developed, due attention should also be paid to the maturity level set as a target for the organisation's processes and to the constraints this sets for development.

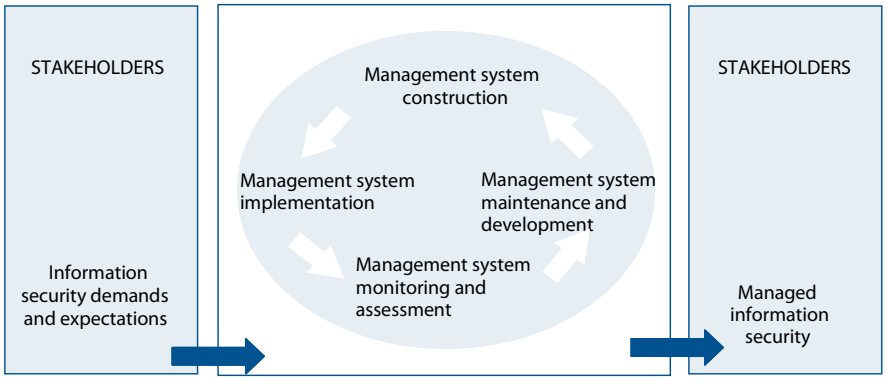
Tasks included in the PDCA (Plan, Do, Check, Act) process model based on the ISO 27001 information standard can be divided into four parts:

- at the planning stage (Plan), the process is initiated, business impact and risk analyses are made and a continuity strategy formulated based on them
- at the implementation stage (Do), planned solutions are implemented and training begins
- at the checking stage (Check), data on the state of the process is produced by means of monitoring, testing, reviewing, auditing and reporting
- at the development stage (Act), solutions are improved based on the data collected.

The management and development cycle of the PDCA model for information security processes includes planning and construction of the management

system (Plan), implementing and operating it (Do), monitoring and assessment (Check), and maintenance and development (Act). The cycle calls for continuous activity and its purpose is to lead to the continuous improvement of operations.

Figure 7. Application of the PDCA model in an information security management system (ISO/IEC 27001:2005)



An information security management process, i.e. a process for the development and maintenance of information security, also describes in its essential aspects what is required in terms of information security of an organisation's management. The objective of the process is to produce a managed information security package that facilitates the fulfilment of an organisation's targets and the reliability of its operations.

3.2 Information security management system

> Information system and network security policies, practices, measures and procedures should be coordinated and integrated to create a coherent system of security.
> *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*

An information security management system is a framework consisting of the following operating models and documents:

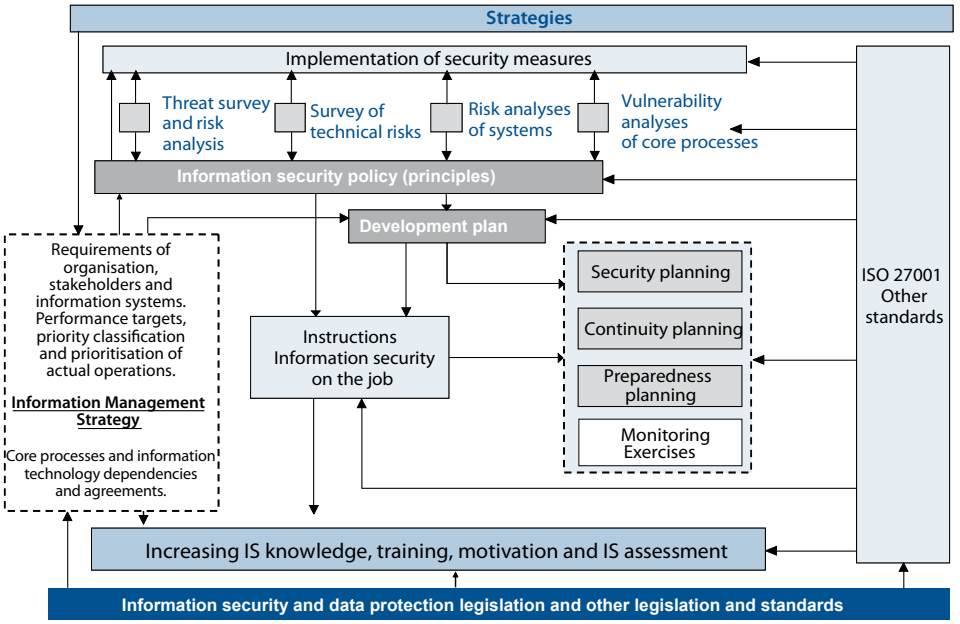
- information security policy and strategy
- information security practices and principles describing the security practices in use
- information security development plan

- basic and supplementary instructions for information security
- information security architectures (topology and framework descriptions of solutions)
- information security reporting to management
- fire and rescue plans
- continuity plans
- contingency plans
- operational information security processes
- auditing plan.

An information security management system is used to implement an organisation's strategy.

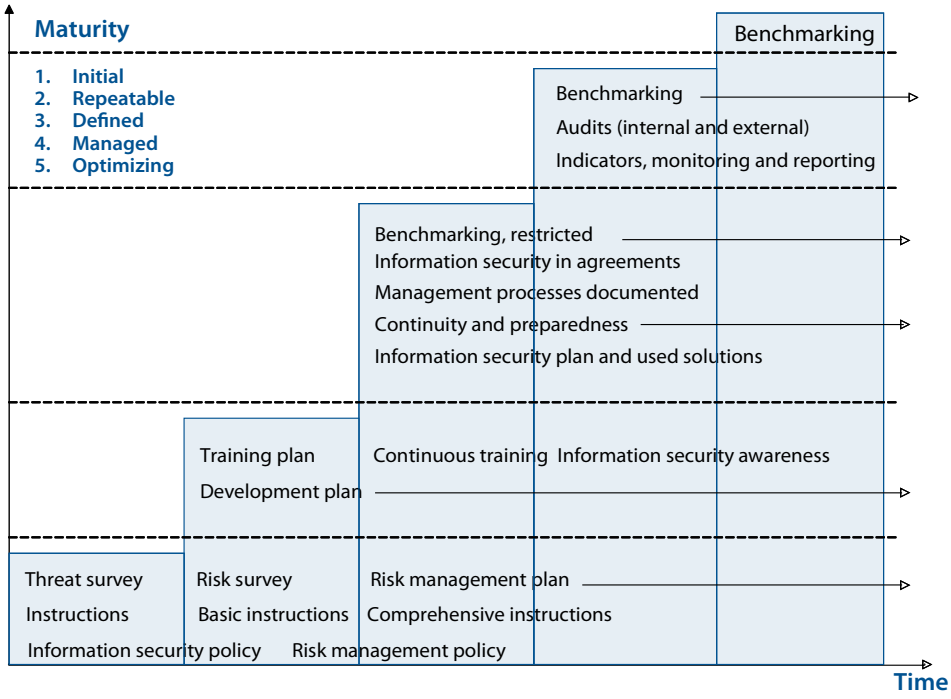
An organisation's strategy is managed by means of a management system, which covers the detailed organisation of information security as well as information security policies, planning, responsibilities, procedures, processes and the necessary resources. A management system assists in monitoring and assessing the effectiveness and appropriateness of information security measures. By continuously developing the system, it is possible to improve the organisation's preparedness to systematically manage its information security.

Figure 8. Information security management system model



The key components of an information security management system are an up-to-date information security policy and related documents as well as regular risk management, applying to both current activities and planned changes. Based on these, an information security strategy as well as information security plans are prepared, which help to implement information security solutions in accordance with existing information security requirements. Management systems regularly measure and assess the effectiveness and appropriateness of information security activities.

Figure 9. An example of the application of the maturity concept in a central government organisation



Various maturity models can be used to assist in developing a management system. With their help, the existing state of information security can be determined and a target level for its development set which will implement the requirements laid down for the organisation's information security. An organisation can also adhere to management models described in information security standards.

The achievement of the target level is generally a long-term development project whose objectives are described in operating and financial plans and spread over several years. In addition, the project should be divided so that measurable targets can be set for development activities on an annual basis and the necessary resources allocated to achieve the targets.

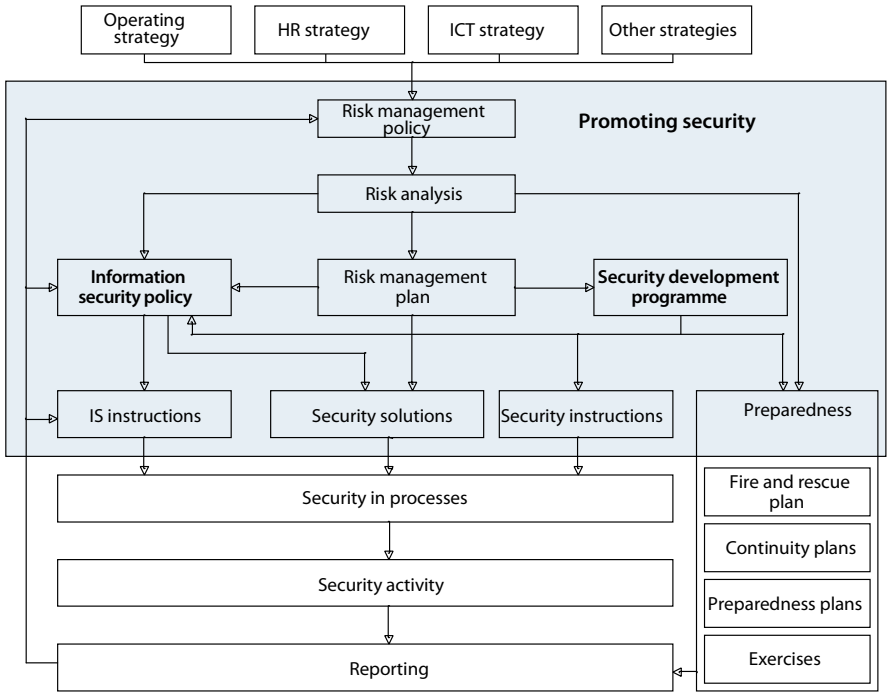
3.3 Information security planning and development

Security planning translates the security measures that follow from the organisation's operating policies and strategies into targets for individuals in positions of responsibility and for the whole organisation. Plans are therefore the basis for the implementation and comprehensive development of information and other security and they must be taken into account in performance management in connection with performance appraisals as well as when implementing ICT services and extensive development projects.

Systematic information security development calls for synchronisation of the information security management system. Information security requirements arising from strategies and the operational demands of development projects must be harmonised. Development plans assess the information security risks caused by operational requirements and seek appropriate solutions to reduce and eradicate risks. In this way the desired level of information security is achieved.

Plans are used to direct information security work and its implementation in practice. They are prepared at all organisational levels. They take into consideration continuity and contingency plans and measures.

Figure 10. Relationship between information security plans and security plans



In addition to planning, attention should be paid to the implementation of plans as well as their assessment, control and monitoring. The division of responsibility for control and monitoring must be clear, and activities need to be efficient and appropriate. An information security management system can be of assistance in implementing systematic control and monitoring as well as assessment of plans.

Meeting the set targets according to the plans requires that the necessary resources, schedules and links with other activities are taken into consideration in the planning phase.

Sufficient time and resources are required for planning, and planning must be linked to the whole organisation's operating and financial planning.

It is often possible to find cost-effective information security solutions in an earlier stage of projects but which can no longer be implemented later. Information security costs can therefore be better controlled the earlier in the process the information security perspective is considered.

3.3.1 Planning fundamentals

Information security planning draws on legal statutes and the Ministry of Finance's VAHTI instructions, and builds on safeguarding and quality control of an organisation's operations.

Measures are directed at the different elements of information security. Plans should take into account an assessment of an organisation's information risks, dependence on information technology, and other threats connected with the use of technology as well as the specification of measures required by risk management and implementation plans.

An organisation should prepare:

- information security practices and principles designed to protect operations from internal and external damage directed at information and information technology describing the means by which information security is ensured,
- a continuity plan that enables important services and functions to continue when normal information processing has been blocked for technical or other reasons during normal conditions,
- an emergency preparedness plan, prepared irrespective of the priority classification of the organisation (information processing) as a contingency for emergency conditions,
- a development plan for the systematic development of information security.

The various elements of information security should be adequately taken into account at the different stages of planning.

3.3.2 Information security practices and principles (an information security plan)

For the overall management and control of information security, an organisation must have an up-to-date description of the solutions and principles already in use. This document is also known as an information security plan. The content, however, is not that of a plan. Solutions to be adopted at a later date are described in the information security development plan. The information security plan describes the organisation's information security management solutions.

The document:

- describes the information security solutions, tasks and responsibilities in use and their level, and the manner in which they are implemented within the organisation
- describes the solutions for the protection, correct processing and confidentiality of data
- specifies the security technology that supports operations as well as the measures connected with the continual development of security and their monitoring points
- specifies the procedures for reporting on information security activity and its results to the organisation's management, if not described in other documents.

The basic premise for information security maintenance and development is the specification of the organisation's main functions as well as a risk survey conducted within the organisation. This risk survey includes information systems that support the main functions.

Information security practices and principles aim to fulfil information security needs under normal circumstances. In addition, the organisation should also take into account the basic factors that influence continuity planning and emergency preparedness planning for emergency conditions, even if these plans are made separately.

3.3.3 Information security development plan

The information security development plan is generally linked to the information security practices and principles document. In addition, together with

the information security policy and the information security assessment, the development plan forms a logical package that describes the systematic development work.

The development plan serves as a guide for implementing the measures by which shortcomings perceived in an information security assessment are rectified and by which efforts are made to develop the information security maturity level to its target level. Progress in the implementation of the development plan is described as part of the organisation's reporting.

3.4 Information security implementation

In order to create and implement good practice in information management, the authorities shall:

Plan and implement their document and information administration and the information management systems and computer systems they maintain in a manner allowing for the effortless realisation of access to the documents and for the appropriate archiving or destruction of the documents, the information management systems and the information contained therein, as well as for the appropriate safeguarding and data security arrangements for the protection, integrity and quality of the documents, the information management systems and the information contained therein, paying due attention to the significance of the information and the uses to which it is to be put, to the risks to the documents and the information management systems and to the costs incurred by the data security arrangements
Act on the Openness of Government Activities, Section 18 Paragraph 4

It must be appropriate and justified to process personal data in the operations of the data controller. The purpose of the processing of personal data, the regular sources of personal data and the regular recipients of recorded personal data shall be defined before the collection of the personal data intended to be recorded in the file or their organisation into a personal data file. The purpose of the processing shall be defined so that those operations of the data controller in which the personal data are being processed are made clear.
Personal Data Act, Section 6

In information security, more consistent and interoperable operating instructions are needed than in other functions. Instructions can be divided into general, organisation-specific, and special instructions covering some restricted area. Instructions in the central government include the Ministry of Finance's instructions on information management development as well as the VAHTI instructions. They are suitable as such for the basis of information security work in central government organisations.

Organisation-specific instructions outline dedicated information security practices so that they are suitable for an organisation's own operating practices and processes. Such instructions include information security instructions that serve as the basis for in-house personnel training, for example. The commitment of personnel to secure operating practices is seldom achieved through instructions that are general in nature. For this reason, actual instructions must consist of information security instructions adapted to the individual organisation and its operating practices and must be based on its own information security policy. Information security operating procedures are included as part of the organisation's normal operating processes, which are properly documented and covered by clear instructions.

Special instructions are primarily an organisation's own instructions, relating for example to a restricted field of activity or specific information system. They are intended for the information management's and security personnel's own use or relate to individual services, functions, projects, technical security solutions or continuity, emergency preparedness and recovery plans. As a rule, these documents are security classified.

General and organisation-specific information security instructions can form a distinct entity in an organisation's collections of instructions and standing rules. Information security instructions relating to individual services and functions can be situated in the quality assurance system next to the functions in question. Instructions intended for all personnel are distributed to the entire organisation. Special instructions are situated according to their required use either in the instructions collection or in the quality assurance system and distributed in an appropriate way to their target groups.

It is important to note that expertise in information security measures cannot be required of personnel if confirmed and approved information security instructions and the training and familiarisation required for compliance with them are not available. Instructions should be made readily available, and everyone should be familiar with their content.

3.4.1 Procurement

The procurement of services, information technology equipment or an information system includes the specification of information security requirements and an assessment of information security features. Key requirements are specified and clearly presented at the invitation to tender stage, and information security factors in the tender comparison and selection criteria. Implementation of information security requirements may be an absolute precondition of any purchase.

In the procurement of information technology services and equipment, central government instructions issued on the subject shall be adhered to. Where

resources are scarce in a public organisation, it is possible to acquire shared information security resources from a public sector partner instead of purchasing them from the private sector.

In the central government's general terms of public procurement contracts, information security is not a special subject of attention. In connection with a purchase there might be a need to enter into a separate security agreement specifying the protection principles and confidentiality periods to be observed by the parties to the agreement. Through agreements, an effort should be made to prevent leaks and thefts of information in connection with deliveries or thereafter. Security clearances may be made on suppliers, depending on the safety critical nature of the project or service.

3.4.2 Outsourcing

Outsourcing requires that the supplier of the outsourced services has access to the procedures derived from the organisation's information security requirements. The procedures are included in the Ministry of Finance's information security recommendations for the outsourcing of information management functions. Requirements and targets must be agreed at the beginning of the outsourcing process.

Outsourcing of functions and services requires a division of obligations between the organisation and the supplier, a task specification and a plan to ensure that the desired level of information security can be achieved and maintained throughout the entire outsourcing process. Overall responsibility for functions remains with organisations, even though the service supplier is responsible to the organisation for the services it supplies.

Organisations must have sufficient expertise to ensure that the security issues raised during outsourcing are handled professionally and that the service supplier's security situation can be monitored as part of the acquired services. In connection with the procurement of services, information security needs should, depending on their content, be reviewed and, if necessary, a confidentiality agreement and a security agreement prepared.

3.4.3 Training

> In order to create and implement good practice on information management, the authorities shall:
>
> See to it that their personnel are adequately informed of the right of access to the documents they deal with and the procedures, data security arrangements and division of tasks relating to the provision of access and the management of information, as well as to the safeguarding of information, documents and information management systems, and that compliance with the provisions, orders and guidelines issued for the realisation of good practice on information management is properly monitored.
> *Act on the Openness of Government Activities, Section 18 Paragraph 5*

An organisation's information security culture is characterised in either its careful or careless approach to handling information and to planning and acquiring its systems. As information security is connected in one form or another to all activities, the commitment of personnel to information security plays a key role. As a result, the information security awareness of personnel must be continually developed.

The Government resolution on the development of central government information security requires that personnel working in a central government organisation have sufficient information security expertise and knowledge. An organisation's management provide guidelines on information security training in connection with performance management. On the basis of management guidelines, the human resources management or a corresponding training organisation incorporates the training plans into information security training for the organisation's management, supervisors, personnel or specialised personnel. The outcome and coverage of training are monitored regularly.

Risk awareness and accountability are maintained by specific training and in other training contexts. A supervisor's own example has an impact on whether information security instructions are adhered to in practice.

3.4.4 Communications

Information security instructions specify internal and external responsibilities, rights and obligations relating to security and information security as well as restrictions in respect of communications.

Detailed information security arrangements should not be actively made public. Due to public image, to foster trust in electronic communications or services, and to guide customers there might be a need to communicate in a

general way about information security procedures. Such communication must be carefully planned.

In internal communications and instructions, employees should be informed of what personal data is collected for use from information systems, what rules are applied to the private use of e-mail, what activities not related to work are permitted, and what the consequences are of unauthorised use.

Successfully surviving a crisis is influenced in a crucial way by how well an organisation has prepared for crisis communications. Successful communication is ensured by a clear division of roles between those responsible for communications and other contact personnel as well as by proper planning so that communications and the channels used are clearly specified and that crisis communications exercises are held in advance.

3.5 Practical assessment and reporting

Management is responsible for the assessment process as part of regular management as well as performance management. This includes management-approved information security indicators. Line management should adopt assessment operating models and promote the information security philosophy at all levels of the organisation.

Information security monitoring includes reporting on the information security situation and level as well as on anomalies and incidents. Monitoring and reporting of the organisation's information security is part of performance management and it is discussed in performance target negotiations on an annual basis. Like all monitoring, reporting covers the whole of information security, not only information technology.

Information security must be monitored continuously and actively. Monitoring is planned so that human resources are directed to the most significant areas in terms of information security, such as the most important processes, information systems, data warehouses, and compliance with information security instructions.

To monitor information security, control procedures and a reporting method are developed for reporting essential achievements, information security anomalies and information security assessment results to senior management. The performance reporting procedure for information security is agreed in connection with performance target negotiations. In addition, senior management should receive regular reports of the information risks produced by the management system and how they are controlled.

Regular reports must also be obtained from partners and service suppliers on information security areas connected with the supply of the services provided. Outsourcers cannot transfer responsibility; all activity and related risks must be monitored regularly.

Table 4. Events and their reporting period

An example of information security reporting practices:

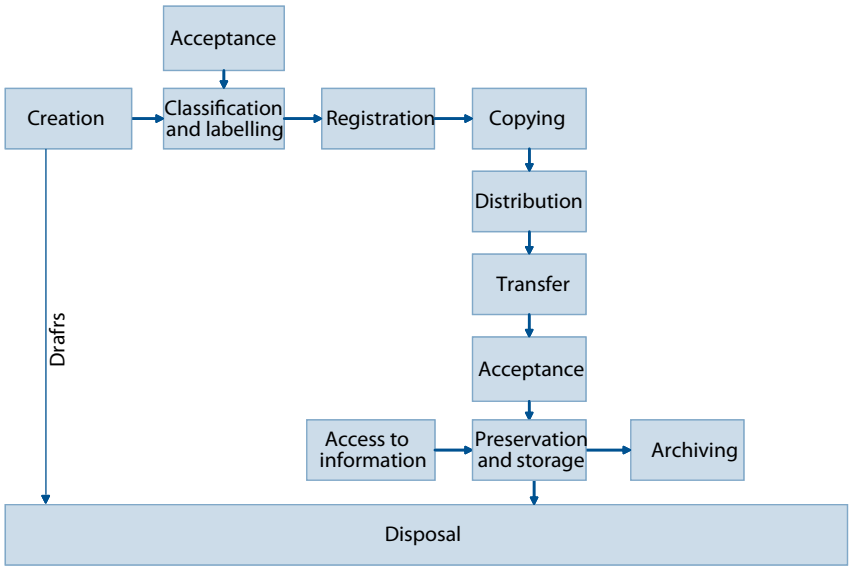
	Reporting period	Subject
1	Immediate reporting to management, operational management, key supervisors	A momentary event jeopardising operations: serious threat, serious damage requiring immediate action to rectify, new risk or 'close-shave' event
2	Weekly reporting to key individuals responsible for systems	Events of the week, automatically and according to requirements
3	Monthly snapshot to security management	Monthly summary of events and measures by which an incident can be prevented in future or the risk reduced.
4	Four-monthly review to senior management in accordance with the risk management policy	Security situation report (possibly as part of other reporting) as well as information on new threats, a survey of the information security of services.

4 Security of information material – information capital management

Security of information material concerns the protection of information in different storage formats. It covers paper documents, optical and magnetic information storage media, microfilms, recordings and other corresponding technical devices. Security of information material also covers processing rules from the creation of the information material to its disposal.

Organisation-specific instructions are required for the processing of information material. Government authorities should particularly take into account the Act and Decree on the Openness of Government Activities. The organisation's management are responsible for familiarising personnel with instructions on the processing of information material. Safeguarding the information security of such material concerns all personnel and the entire life cycle of the material.

Figure 11. Life cycle of information material



Government authorities must have an up-to-date archive formation plan covering all information material, detailing information material processing rules as well as safeguarding the integrity and accessibility of the material at the different stages of its life cycle. Handling of classified information should take into consideration the protection measures required by the security class in question.

5 Personnel security

Personnel security is a system of policies and procedures, which seeks to manage the risk of staff or contractors exploiting their legitimate access to an organisation's assets or premises (facilities) for unauthorised purposes.

Personnel security is based on competent and committed personnel whose information security responsibilities and tasks have been described in their job descriptions. In addition, adequately specified human resources management processes are needed, as are other processes that describe tasks so precisely that the emergence of risks related to key personnel is avoided.

Key issues are processes associated with entry into employment, essential changes to job descriptions and termination of employment, and an agreed operating model on these, used by all parties, is required. Depending on the competence requirements and confidentiality of tasks, the background, suitability and expertise of individuals being recruited should be vetted before they are employed.

When managing key personnel risks, key individuals are identified for each function and their availability in the service of organisation is ensured in different situations. When plans are made, adequate forward provision must be made for holidays, absences, job rotation and temporary arrangements, and personnel training for emergency conditions. Hazardous job combinations should be identified and removed so that methods designed to protect the organisation's operations cannot be circumvented undetected.

Adequate staff numbers, their job satisfaction and motivation also have a significant impact on the realisation of information security. Provisions for exemptions from military service in time of war are part of ensuring sufficient personnel resources in connection with preparedness planning for emergency conditions.

6 Physical security

The purpose of physical security is to ensure organisations' uninterrupted operation in all circumstances taking their special needs and risks into account. Each organisation is responsible for its physical protection.

This element of information security includes, among other things, access control, camera surveillance, other technical monitoring and guarding as well as prevention of fire, water, electrical, ventilation and burglary damage. Minimum requirements for measures and systems that enhance the security of premises should be determined on the basis of the security needs of the area, building, group of facilities or facility. In connection with new buildings or renovations, facilities are protected or protection is improved in line with their security classification.

Facilities management and the implementation of security arrangements are often the task of real-estate management or the building's owner. The security needs of functions and the information technology they use are known best by the management of the organisation in question, who decide on security solutions. Facilities security development needs are taken into account when preparing annual plans.

7 Security of telecommunications services

An organisation's telecommunications functions and the different network systems that implement them should be planned and constructed according to good information management practice so that the chosen architecture supports contingency plans for different threats. Telecommunications security includes, among other things, the assembly, cataloguing and maintenance of telecommunications equipment, monitoring of changes, logging of incidents, access control, network management, encryption and back-up of communications, examination, recording and investigation of information security anomalies, and testing and approval of telecommunications software.

8 Hardware and equipment security

Hardware and equipment security means the protection, installation, maintenance and removal of equipment as well as related administration in which the owner and security class of the equipment, as well as the monitoring of equipment and its capacity planning are determined. Generally, hardware and equipment security is employed to safeguard equipment over its life cycle, and it includes, in addition to installation, security and maintenance, various support services and agreements as well as the safe disposal of the hardware and equipment at the end of their life cycle.

The agreement of restrictions and response times determining the level of service agreements over the hardware and equipment's life cycle may have a significant impact on the maintainability of the information security level and reaction to information security anomalies.

Relying on service agreement response times can reduce the amount of back-up equipment but dependency on the supplier's ability to act within the framework of response times grows. It is particularly important to specify by agreement the response times of an acquired service in those cases where the entire service plus equipment is located with the provider or part of the organisation's equipment is located on the premises of the supplier of the operating service. In such cases, it is necessary to pay attention to the arrangement of the physical security of individual items of equipment on the premises of the other party and on access control to the premises in the event of incidents. Moreover, service agreements should cover to the entire system and sufficiently precise clarifications of network connections and of physical access to the system outside working hours are required, if the system has to be continuously available to customers.

In respect of hardware and equipment maintenance, it is important to ensure that all information on them can be restored at any time when recovering from an anomaly. This means that back-up copies must exist of operating systems, software and their settings. Similarly, the operational data contained within them is also required, of course.

It must be possible to monitor equipment continuously using software, and to monitor the development of equipment utilisation rates regularly. Clear instruc-

tions are required for system information security updates and they should be tested before the installation of a production system. The reversal of updates should be possible in the event of problems being perceived in an update.

9 Operations security

Operations security creates and maintains the operating conditions required for the secure use of information technology. This is implemented by attending to, for example, functionality monitoring, access rights management, monitoring of use and logs, information security measures relating to software support, maintenance, development and service functions, back-up copying and incident reporting. The protection of all information systems from malware (such as e-mail viruses or worms) is part of operations security. The operations security level of a system is based on the classification of the information on the system.

9.1 System maintenance

Expert maintenance of information systems implements and improves information security by keeping systems up-to-date and recognising their normal state. This prevents in advance unwelcome incidents and minimises their impact.

Good maintenance practice is systematic, responsible and professional. It is covered by clear instructions, and responsibilities are assigned for system maintenance tasks. The systems being maintained, related procedures and measures should be documented, and the documentation updated as required.

There must be a clear agreement between the maintaining party and the system owner on each party's responsibilities and the level on which the maintenance service is implemented. The agreement should include any restrictions defining the service level and response times. The content of outsourced services, particularly information security services, including response times in different situations as well as escalation and actions in the event of disruptions, or even emergencies, must be precisely specified. Maintenance personnel responsible for systems are required to have sufficient training, and their knowledge of system components must be up to date.

9.2 Information security of telework and remote access

An organisation's management personnel have management and monitoring responsibility for the secure arrangement of telework. Telework should always be agreed in writing and information security instructions corresponding to the special characteristics of the work prepared for it. The employees' and management's preparedness for telework must be ensured through increased security awareness, motivation and training. Confidentiality of information is emphasised in remote access; information is only available to those authorised to access it.

Devices used for work, such as laptop computers as well as mobile phones and smart phones, set particular challenges for securing the information they contain and transfer. Particular attention should be paid to logging in to devices, and the confidential information they contain should be encrypted. In addition, means are required to protect and restrict telecommunications, if devices are connected to an insecure network or connected via an insecure network. Users should be instructed to exercise special care when handling equipment, so that the loss or theft of devices or information can be avoided. In telework it should be noted that the organisation's opportunity to supervise the physical security of a remote workstation located at home is generally poor.

9.3 Information technology monitoring

Information technology monitoring consists of the monitoring of system facilities and access. It may be real-time observation (for example whether a certain service is continuously available) or observation of anomalous events based on event log data recorded by hardware and equipment and systems.

Monitoring should be take place to the extent required by the information classification and the critical nature of the services. For example, services whose continuous accessibility has been classified as critical should also be monitored around the clock. Others are monitored during working hours and automatic alerts call duty personnel to the site, if necessary, also outside working hours.

Various software can be used to detect information security anomalies within a huge mass of operating events. To facilitate monitoring, monitoring systems can generate real-time snapshots of the entire information system and collect data and issue alerts on events that exceed approved threshold values.

Log data are utilised in the detection of information security anomalies. The collection and saving of logs is arranged so that they cannot be changed or deleted in connection with data cracking. Some of the data in the logs is confidential by statute and should be protected from unauthorised processing. Monitoring of personnel activity and processing of monitoring data is regulated by

law. Technical monitoring of employees is agreed with personnel in the cooperation procedure.

Operating instructions specify the parties whose warnings about information security threats should be followed. The Finnish Communications Regulatory Authority CERT-FI is the national actor which observes and monitors information security threats and communicates about them.

9.4 Management of access rights

Up-to-date management of access rights and authorisations based on the work roles of information system users is an absolute prerequisite of information security. Various measures are employed to ensure that authorised users can gain access only to the information to which they have access rights according to their duties and related responsibilities.

10 Software and software development security

Software security means protection features and identification, monitoring and log procedures of operating systems, system software and software tools as well as other software and applications, together with security measures connected with the maintenance and updating of software.

Software security depends on the processes used in software development, software operating settings and the settings of the software's service platform (operating system and possible middleware or auxiliary software) as well as the training and instructions received by users.

Software security can also be influenced by using other technical security means. Access of users and other programmes to the information contained in a programme can be restricted by isolating an information network and by improving the security of the software environment, for example by installing security updates and programmes and by using systems' security features.

10.1 Security of electronic services

The security of electronic services is a manifestation of software security, among other things. The security of software used for the provision of electronic services is a key prerequisite for secure electronic communications.

10.2 System development security

When new information systems are being developed and procured, information security must be included in the project. Information security is an integral part of all changes and development of information systems throughout their entire life cycle. The security of a system's technical and administrative interfaces must also be ensured. A risk assessment made at the beginning of a project is used to direct information security according to the nature of the system that is the subject of development work.

The priority classification, security needs and security level, and IT security requirements are determined at the preliminary study stage of the information system. The testing of the information system should be planned on both an administrative and technical level. Tests can be directed either on a one-off basis to a part or all of the system or regularly to the production environment, in which case minor changes that take place in the system can be tested gradually. Administrative information security checks include various requirement specification and plan reviews as well as the certification of solutions using information security experts. Technical checks include code reviews, particularly for critical software functions.

11 Continuity and special situations management

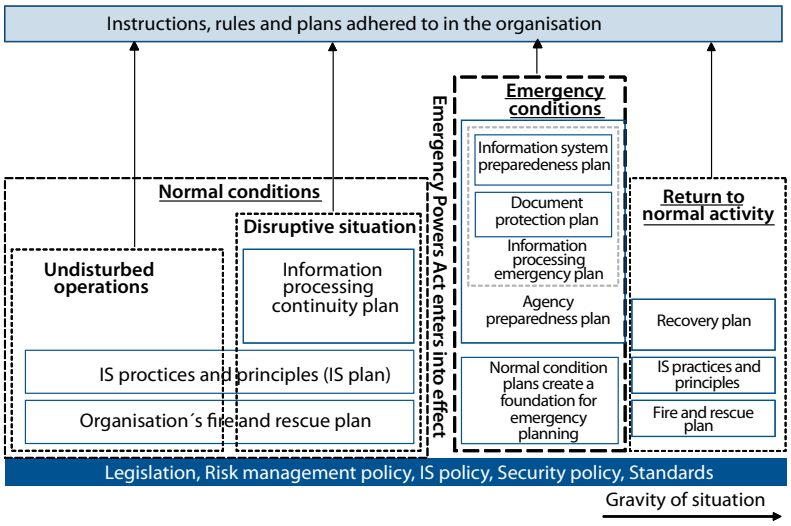
Emergency conditions mean regionally or nationally adverse operating conditions whereby regular powers can no longer be relied on to control the situation. Emergency conditions have been defined in the Emergency Powers Act (Valmiuslaki /1999) and the State of Defence Act (Puolustustilalaki 1083/1991).

11.1 Ensuring operational continuity

An organisation should be able to prepare itself so that operating capacity is maintained according to plan during emergency conditions as well as during disruptive incidents in normal circumstances. These situations are defined as surprising or sudden events that may paralyse the organisation or the security of key functions and the operation of the vital systems it maintains. For society, vital information systems implement or support functions whose absence would jeopardise the society significantly in financial or other ways. The functions may also be such that their absence or disruption as well as inaccuracy or disclosure of information would have a paralysing effect on society or would adversely affect an organisation's activities or the security of individuals.

Every organisation must identify for itself the information systems that are essential in terms of central government activity. Key systems must be implemented so that their operational continuity is safeguarded in all circumstances. During disruptive incidents, special measures must be instigated to restore the normal situation. Incidents may cause a significant need to redirect resources.

Figure 12. Operational security arrangements



A continuity plan, emergency preparedness planning, other advance preparations and related exercises form the basis of preparedness for emergency conditions. Government authorities are obliged to make contingency plans for serious incidents and emergency conditions during normal circumstances. Organisations must maintain operational security plans for these situations.

The emphasis of contingency planning should be on identifying and preventing threats as well as on safeguarding essential information processing. Plans are used to ensure that operations continue in exceptional conditions primarily with the existing organisation and resources.

11.1.1 Continuity plan

Contingency planning for interruptions to operations, information systems, communication systems and services is increasingly important. The effects of interruptions, moreover, are more widely directed at an organisation's own user groups, other public authorities, customers and partners as well as society as a whole. An interruption in one part of an extensive system configuration might restrict or even prevent information processing over the entire network.

For information security management and control, public authorities must have an operational continuity plan in case of incidents. This plan should make contingencies for serious accidents directed at local operations or information processing facilities that could be affected by fires, water damage, explosions and gas leaks, as well as for extensive damage to the information technology infrastructure itself or other external threats directed at them, such as cyber incidents and attacks.

Contingency planning requires preparedness for maintaining the integrity of databases and real-time processes, the construction of a fault tolerant system, reliable back-up and safe copying, as well as ready-made back-up system plans, and even back-up equipment working in parallel in the most important parts of the system.

Some of the main factors when reviewing the continuity assurance of services and the information technology supporting them include:

- specification of key functions and services
- specification of information processing essential for key functions
- situation assessments of events leading to serious interruptions
- the impact of interruptions on production, services, customers and deliveries
- the information processing dependencies of functions
- the indirect dependencies of other parties on the interruption of services
- the points at which down-times become critical
- critical times of a periodic nature
- assessments of financial losses arising in each interruption, by application
- when restricting the use of information technology, the priorities of the applications being maintained and the measures taken to ensure their operation.

The continuity plan should include all the measures needed to continue operations in the event of interruptions until operations can be restored to their original operating level.

Planning includes:

- a plan to back up systems
- planning the back-up system's operating environment, covering hardware, software, connections and operating functions
- a recovery plan.

Continuity plan preparation and related back-up systems planning are pointless if the functionality of the plan has not been ensured. For this reason it is essential for the continuity plan to be tested and to know if it will also work in the event of a serious disruption. Senior management need information about the level of contingency planning at any given time.

11.1.2 Emergency preparedness plan

Among the most important factors when reviewing the planning of services and the information technology supporting them for emergency conditions are:

- up-to-date threat scenarios
- the impact of emergency conditions on operations
- the paralysis and disconnection of international telecommunications links
- the supply of equipment and spare parts
- exemptions from military service in time of war of reservists and other individuals important for the organisation
- the significance of information processing for the organisation and customers in emergency conditions
- the significance of the organisation's operations, production or service for the livelihood of citizens and society in different situations
- emergency production requirements set by the Government and the maintenance of information processing thereby required
- the restriction of information technology use and the reduction of dependencies and
- security measures.

The emergency conditions preparedness plan adapts information processing to the level permitted by crisis situations. The emergency preparedness plan aims to safeguard or replace an operation that has been agreed in advance and decided by the organisation.

The National Emergency Supply Agency has founded a service operator, Huoltovarmuusdata Oy, to safeguard the operation of critical information systems. Huoltovarmuusdata Oy offers high-security computer rooms and data-material storage, saving and back-up copying services for central government and private sector organisations that are critical for security of supply. With these services, customers can safeguard the continuity of their operations also in emergency conditions and in the event of incidents during normal conditions. Huoltovarmuusdata Oy provides services in cooperation with the sector's leading service providers.

11.1.3 Recovery plan

A recovery plan is used to prepare for recovery from an operational disruption or from emergency conditions to normal operations. The plan describes how

operational systems are restored from back-up systems and what checks have to be performed so that services can be restarted without risk.

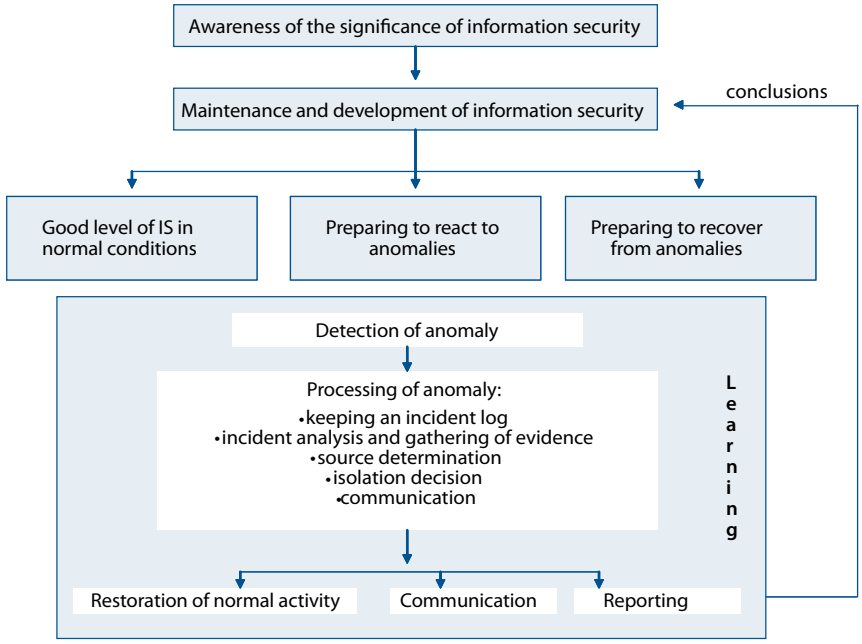
Recovery plans are system-specific.

11.1.4 Fire and rescue plan

An organisation must prepare fire and rescue plans for its premises, if the number of individuals present on the premises at the same time exceeds 20 or if the computer rooms have been furnished with automatic extinguishing equipment or fire detectors required by statute or the decision of an authority. The fire and rescue plan must be kept up to date and communicated to employees. Individuals assigned responsibilities in the plan should be trained in normal conditions at the workplace for fire and rescue actions.

11.1.5 Information security anomaly management

Figure 13. Information security anomaly management



Situations that give rise to anomalies in information security may be intentional or unintentional. An organisation must prepare systematically in advance for the greatest risks and plan corrective measures, recovery and crisis communications. An anomaly management process is part of the information security management system and an element of risk management. Processing of anomalies is part of normal activity and and it involves a specified process.

An organisation must take steps to prevent information security anomalies arising, but also to ensure that it has the capacity to detect different kinds of anomalies and to react to them. The information security practices and principles (information security plan) document describes the various means and methods of protection used in the organisation to maintain information security.

12 Classification used in information security

Appropriate classification is instrumental in managing information requirements. Data materials, tasks, individuals, processes, systems, premises and organisations are classified into groups that differ from each other in terms of their information security needs; information security requirements in accordance with the classification are then formulated for them.

In addition to specified requirements, unequivocal classification criteria are defined for each class. These take into account, among other things, the life cycle of the classified factor and the requirements set for operational preparedness and continuity. Based on the classification, it is easy to identify the requirements to be applied at any given time.

In assessing information security levels, a Capability Maturity Model (CMM) can be utilised, as described in the instruction entitled An assessment of information security in the central government VAHTI 8/2006 – Tietoturvallisuuden arviointi valtionhallinnossa (available only in Finnish).

12.1 Classification of organisations

Organisations can be classified according to whether they or their parts provide vital services in emergency conditions. The central government's instructions in force are utilised in this priority classification. Using a priority classification of an organisation or parts thereof, information security measures can be targeted so that the organisation's critical functions are protected appropriately and effectively.

12.2 Classification of facilities

Classification of areas, buildings and facilities may be built on up-to-date classification models, including, for example, the Ministry of Finance classification or the EU security classification.

Table 5. Premises security classification models

The security classification consists of four levels:

Premises security - zone class	EU classification	Traditional premises classification	Description of classification
Security zone 1 (special zone)	(Technically protected area)	Class 4, full protection	Access to premises discloses confidential and secret information. Premises are EMP and HMP protected. Premises are clearly defined and delineated. Access is controlled and permitted only to those authorised to do so. Access control, camera surveillance.
Security zone 2 (isolation zone)	Security area I	Class 3, special protection	Access to premises discloses confidential and secret information. Premises are clearly defined and delineated. Access is controlled and permitted only to those authorised to do so. Access control, camera surveillance.
Security zone 3 (restriction zone)	Security area II	Class 2, enhanced basic protection	Processing and storage of confidential and secret information. Access is controlled and permitted only to those authorised to do so, others are chaperoned. Access control, camera surveillance.
Security zone 4 (surveillance zone)	Administrative area	Class 1, basic protection	In general use for meetings and visiting, access control, camera surveillance.

Most of the central government's operations, buildings and the property kept in them are such that their protection should be arranged with at least Class 4 measures. The grouping of government agency premises into Class 2 – 4 is based on their operational importance. For entities belonging to Classes 3 and 4, a statement from the Security Police on the special risks and protection measures of the entity should be requested at the planning stage.

Based on a priority classification, each organisation has a premises security zone class, which dictates the minimum requirements for the whole of premises security. Based on a security survey, a protection class differing from this can be specified for areas, buildings, groups of facilities, premises and individual entities. These include, for example, computer rooms and archives. A security survey takes into consideration the information kept on the premises and its classification as well as the activity that takes place on the premises and the risks directed at them. The protection classification of organisation premises and the detailed requirements of the classes as well as the position of various

organisations in the classification have been specified in a Ministry of Finance recommendation.

A statute on information security under preparation will specify protection requirements for closed premises intended for the storage of classified information. The premises are equipped with appropriate electronic locking, access control and measures preventing unauthorised access to the information material kept in them. A possible additional requirement is that access to information is controlled and documented and that those working on the premises have personal identifiers.

12.3 Classification of personnel

In terms of personnel, the purpose of classification is to identify critical key individuals for an organisation's activities. By the actions of these key individuals, activities can be continued in the event of various disruptions and in emergency conditions, or with their aid the continuation of operation can be safeguarded in all situations.

Key individuals include those who have knowledge, expertise and experience that is essential to the organisation. This can manifest itself, for example, as important personal relationships or as special expertise in systems that support operations, or it can be based on the status of key individuals or the knowledge they possess.

12.4 Classification of tasks

The classification of tasks specifies tasks that are critical in the event of serious disruption to operations and in emergency conditions. This is closely linked to the classification of personnel, security reports and the implementation of various plans as well as to processes that the organisation must handle in all situations.

12.5 Priority classification of systems

Factors influencing the priority classification schemes include the priority classification of the information they contain and the availability requirements of each system.

Systems should be classified in an organisation according to consistent principles:

- those whose integrity, availability and confidentiality are important
- those whose integrity and availability are important
- those whose integrity and confidentiality are important

Another way of classifying systems is based on the classification of the National Board of Economic Defence:

> Group 1 includes important information systems, whose information security and recovery preparedness must be on a high level. These are, for example, logistics systems, ERP systems, service chains and important data warehouses as well as nationally important and other key administration systems and e-mail.
>
> Group 2 includes information systems important for an organisation's internal operating environment, such as financial management and customer service systems as well as management information systems, whose availability in normal conditions must be ensured.
>
> Group 3 includes information systems whose temporary suspension of use does not cause direct damage. These are, for example, human resources management, planning and marketing systems as well as statistics.

12.6 Classification of information material

Information material can be divided into material that contains public information and material that contains confidential information. Confidential information can be unclassified or it can be classified, in which case it can be classified as restricted, confidential, secret or top secret.

Table 6. Equivalent classification terms for confidential information material

Classification	Traditional class	Traditional classification	EU classification
Top Secret	Security Class I	Top Secret	EU Top Secret
Secret	Security Class II	Secret	EU Secret
Confidential	Security Class III	Confidential	EU Confidential
Use restricted	Security Class IV	Official use	EU Restricted

A decree on good information management practice pursuant of the Act on the Openness of Government Activities is currently being prepared, and instructions on the handling of information material are being updated.

Appendix 1: Model policies and planning frameworks

Information Security Policy

1. Introduction
2. Objective of information security policy
   - 2.1. Concept and significance of information security
   - 2.2. Definitions
3. Factors guiding information security
4. Threats directed at information security
5. Significance of information security for an organisation
   - 5.1. Service tasks vital for operations
   - 5.2. Information security principles
   - 5.3. Practices supporting the implementation of information security
6. Prioritising security measures
7. Information security management system
8. Information security responsibilities
   - 8.1. Information security responsibilities of an organisation
   - 8.2. Responsibilities of an organisation's partners
9. Information security training and instructions
10. Information security communications
11. Monitoring the implementation of information security
12. Actions in emergency situations and conditions

Risk Management Policy

1. Introduction
2. Risk management targets
3. Risk management principles and terminology
4. Risk management organisation
   - 4.1. Organisation and responsibilities
   - 4.2. Coverage

5. Risk management implementation
    5.1. Risk management process
        5.1.1. Risk identification
        5.1.2. Risk assessment
        5.1.3. Risk management
6. Instructions
7. Monitoring, supervising and reporting the effectiveness of risk management
8. Communication
9. Training

Appendix 1: Terminology
Appendix 2: Risk areas

Model Plan Frameworks

The following is an example of the content of an information security development plan. In specifying the content of elements of the plan, use of the Ministry of Finance information security instructions and Chapter 4-10 of these instructions is recommended. The precise content of elements of the plan is organisation-specific.

Information Security Development Plan

1. Analysis and selection of information security needs and development areas
    1.1. Gap analysis (analysis of shortcomings, in which the differences between the current state and the target state are assessed)
    1.2. Selection of developmental priority areas
2. Classification development
3. Management system development
    3.1. Policy development
    3.2. Instructions development
    3.3. Risk management development
    3.4. Development of indicators and monitoring
4. Development of processes
    4.1. Raising the maturity level
5. Security culture development
    5.1. Increasing security awareness
    5.2. Information security communications development

Information Security Principles and Practices (formerly entitled Information Security Plan)

1. Administrative security measures and management
   1.1. Purpose and objectives of security
   1.2. Management-approved principles and policies
   1.3. Implementation idea
   1.4. Responsibilities, organisation and management of operations
   1.5. Functions and systems to be secured
   1.6. Agreements
2. Information security measures and procedures
   2.1. Personnel security
   2.2. Information material security, backup and safe copying
   2.3. Physical security
   2.4. Hardware security
   2.5. Software security
   2.6. Telecommunications security
   2.7. Operations security, protection from malware
3. Security of outsourced data processing functions
4. Securing key development areas (for example electronic communications service, telework)
5. Implementation of information security measures in connection with procurement
6. Information security monitoring, supervision, auditing and testing
7. Instructions
8. Preparedness and procedures in the event of damage
9. Training
10. Plan updating and measures maintenance
11. Reporting to management

Emergency Preparedness Plan

1. Basic concept (describes how special situations are prepared for and managed)
   1.1. Supply of information
   1.2. Formation and dissemination of situation awareness
   1.3. Prevention
   1.4. Contingency planning for situation management including advance preparations
   1.5. Crisis management
   1.6. Communications
2. Threat analysis
3. Implementation of tasks

   3.1. Necessary measures
   3.2. Specification of responsibilities
   3.3. Required resources
   3.4. Operating conditions
   3.5. Legislative foundation
4. Compatibility assessment
   4.1. Cooperation with other administrative branches
   4.2. Cooperation with the rest of society
5. Plan maintenance, contingency training and preparedness exercises

Continuity Plan

1. Specification of vital functions, information systems and applications, services to be safeguarded
2. Maximum permitted down-times specified for vital functions
3. Safeguarding electronic services
4. Descriptions of events leading to serious down-time
5. Back-up system solution
   5.1. Hardware
   5.2. Back-up facilities
   5.3. Repair and delivery of new hardware
   5.4. Data transfer
   5.5. Electronic and telecommunications connections
   5.6. Safeguarding of essential manual measures
6. Emergency preparedness organisation
   6.1. Responsibilities for initiating continuity plan and necessary measures
   6.2. Alerting individuals in positions of responsibility
   6.3. Contact people (equipment supplier, maintenance, back-up system owner, insurance company)
7. Measures
   7.1. Back-up and safe copying, and safeguarding use
   7.2. Instructions on the saving of hardware, software, files and accessories
   7.3. Other damage limitation procedures
   7.4. Back-up system boot order
   7.5. Performance of back-up copying and software transfer
   7.6. Transfer plan for transfer to back-up facility or back-up system
   7.7. Back-up system security measures
   7.8. Agreements
8. Recovery plan

9. Down-time insurance
10. Training
11. Continuity plan maintenance, testing and updating
12. Reporting to management

System Recovery Plan

The recovery plan includes a detailed plan of how the production system will be restored

1. Recovery arrangements
2. Emergency preparedness organisation
   - 2.1. Responsibilities for initiating continuity plan and necessary measures
   - 2.2. Alerting individuals in positions of responsibility
   - 2.3. Contact people (equipment supplier, maintenance, back-up system owner, insurance company)
3. Measures
   - 3.1. Back-up and safe copying, and restoration of use
   - 3.2. Instructions of the restoration of hardware, software, files and accessories
   - 3.3. Other damage limitation procedures
   - 3.4. Acquisitions, repairs and deliveries required for restoration to normal system
   - 3.5. Communications and customer-related measures
   - 3.6. Restarting of operations and repair of information systems
   - 3.7. System testing after recovery
4. Training
5. Recovery plan maintenance, testing and updating
6. Reporting to management

Appendix 2: Information security responsibilities by role

Information security management and implementation tasks by role

Role	Responsibility
Senior management	• approves risk management and information security policy and related principles • decides the main information security and risk management policy outlines • is responsible for the implementation of information security and risk management • integrates risk management as part of management activity • includes information security as part of risk management • requires the information security prioritisation of functions as well as the prioritisation of risk management • creates conditions and guarantees the resources needed by information security and risk management • sets requirements for reporting and • sets requirements for the taking of information security and risk management into account in operations.
Administration management	• specifies tasks relating to the processing of personal data and their areas of responsibility, particularly those relating to information and data protection • attends to fire and rescue activities as well as other security systems when responsibility for them has not been assigned to any specific individual • is responsible for arranging orientation and information security training for personnel • is responsible for specifying and maintaining the content of personnel management processes • supervises information security matters according to the donut dial for annual planning as part of operating and financial planning.
Security management	• participates in the specification of risk management, security policy and principles, and information security policy • develops overall security functions, including information security in accordance with risk management and security policy • directs the implementation of security practice to safeguard personnel, operations and property and to manage the risks associated with them • monitors risks and the state of their management • arranges risk management training and • reports to senior management on security, risks and threats.

Information management	• preparation and presentation of information security policy relating to information management and information technology • direction of information security development measures of the administrative branch or organisation • information security performance management within information management • ensuring the implementation of information security within information management and • monitoring the implementation of information security in procured ICT services • assists management and units in implementing risk management • in accordance with performance management targets, monitors and develops risk management with proposals and • arranges risk management monitoring and management information.
Information security management	• participates in the specification of risk management policy and principles as well as information security policy and principles • develops information security in accordance with security policy • is responsible for increasing personnel's security awareness and arranging information security training • directs the practical implementation of information security and related risk management, and reports to senior management on information security, risks and threats.
Subunit management, sector management	• implementation of information security development measures in their sector • organising security situation monitoring • appointing information system owners and • performance management of information security in their sector.
Individual working in a supervisory role	• implements information security in accordance with set information security targets • monitors compliance with central government and own information security instructions and • reports on risks and information security as well as perceived information security anomalies.
Information security expert, security expert	• assists management and units in implementing information security • in accordance with performance management targets, monitors and develops information security with proposals and • arranges information security monitoring and management information.
Person responsible for document management	• implements information security in information services and in document management according to good information management practice.

Information system owner	• maintains information system descriptions • implements the relevant security measures for own information system • monitors information security in the information system and • reports on information security as well as on perceived information security anomalies.
Information technology experts, system expert, IT support person	• applies and implements the organisation's information security policy utilising own special expertise • is responsible for taking information security measures into account in own area of responsibility • adheres to good information security practice and • reports on information security.
Information system main user	• maintains information security procedures in information systems • monitors system operation in terms of information security • prepares for anomalous events and for the counter-measures required for them and • reports events and incidents that jeopardise security.
Standard user, employee	• knows the instructions given on information security and complies with them and • reports on observed problems, threats and procedures contrary to instructions.
Emergency preparedness manager, Emergency preparedness secretary	• takes contingency measures into account in the organisation's operations • develops the administrative branch's preparedness for emergency conditions • reviews and proposes operations to be safeguarded in emergency conditions and • develops preparedness of vital systems in cooperation with senior information management personnel and other management.
Internal auditing, System auditor	• monitors implementation of approved principles and plans • audits information security and risk management • assesses the adequacy of risk management and information security measures in relation to the organisation's responsibilities and obligations, and • reports the audit results to management.
Procurement personnel	• take information security into account as part of procurement criteria.
Personal data record handlers and information service personnel	• take information security into account in handling and managing documents.
Agreement and real estate management personnel	• take information security requirements into account in premises, surveillance and access control • take information security into account in agreements
Information Security Group	• represents the information security perspectives of the organisation's different parties • reconciles information security measures and security level • directs information security measures at the interfaces of services provided by the organisation.

Security and Emergency Preparedness Group or Risk Management Coordination Group	• cooperation body developing, planning and coordinating risk management, security and emergency preparedness issues.
Occupational safety personnel	• ensures the effectiveness of fire and rescue plan as part of personnel safety and fire and rescue issues
Consultants and service companies	• adhere to good data processing and information security practice • maintain and monitor in their work the general instructions on central government information security and other information security instructions in central government projects and • report on the information security of projects and services as well as factors influencing information security

Appendix 3: Valid VAHTI publications

VAHTI 5/2009	Effective Information Security
VAHTI 4/2009	Information Security Instructions for Personnel
VAHTI 3/2009	Logging instructions *
VAHTI 2/2009	General instructions on ICT contingency planning *
VAHTI 1/2009	VAHTI annual report 2008 *
VAHTI 9/2008	General instructions on information security in projects *
VAHTI 8/2008	Information security terms *
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen **
VAHTI 6/2008	Report by IS training in the central government *
VAHTI 5/2008	24/7 information security services in the central government *
VAHTI 4/2008	General instructions on information security auditing in the central government *
VAHTI 3/2008	Encryption technologies in the central government *
VAHTI 2/2008	Personnel security as a part of information security *
VAHTI 1/2008	VAHTI annual report 2007 *
VAHTI 3/2007	Summary of general instructions on information security management *
VAHTI 2/2007	Information security in modern mobile phones *
VAHTI 1/2007	Challenges in international information security work *
VAHTI 12/2006	Electronic identification in the central government services *
VAHTI 11/2006	Instructions for information security trainers *
VAHTI 10/2006	Security instructions for the personnel *
VAHTI 9/2006	Best practises in access control and management *
VAHTI 8/2006	Assessment of information security in the central government *
VAHTI 7/2006	Change and information security, from regionalisation to outsourcing – a controlled process *
VAHTI 6/2006	Setting and measuring information security targets *
VAHTI 5/2006	Records management information security instructions *

VAHTI 4/2006	Review of the arrangement of round-the-clock information security in the central government *
VAHTI 3/2006	Review of the distribution of central government information security resources *
VAHTI 2/2006	Electronic-Mail Handling Instruction for State Government
VAHTI 1/2006	VAHTI annual report 2005 *
VAHTI 3/2005	Management of information security anomalies *
VAHTI 2/2005	Electronic mail handling instructions for central government *
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Securing the state administration's key information systems *
VAHTI 4/2004	Datasäkerhet och resultatstyrning **
VAHTI 3/2004	General instructions on protection against malware *
VAHTI 2/2004	Information Security and Management by Results
VAHTI 1/2004	Government Information Security Development Program 2004-2006
VAHTI 7/2003	Risk assessment instruction to promote government information security *
VAHTI 3/2003	Assessment of information security management systems *
VAHTI 2/2003	Secure remote access from insecure networks *
VAHTI 1/2003	Secure use of the Internet *
VAHTI 4/2002	Instructions for processing sensitive international data *
VAHTI 3/2002	Information security instructions for telework *
VAHTI 1/2002	Information security recommendation for ICT rooms *
VAHTI 6/2001	Information security checklist for ICT procurement *
VAHTI 4/2001	General instructions on the information security of electronic services *
VAHTI 2/2001	Information security recommendation on government local area networks *
VAHTI 3/2000	General recommendation on information system development *
VAHTI 2/2000	Information security instructions for processing government data material (revised) *

* (only available in Finnish)
** (Swedish publication)

Revised and supplementary instructions can be found on the VAHTI website (www.vm.fi/vahti) and instructions can also be ordered from the printing house Edita.

MINISTRY OF FINANCE
Snellmaninkatu 1 A
P.O. BOX 28, 00023 GOVERNMENT
Tel. (09) 160 01
Fax (09) 160 33123
www.vm.fi

5/2009
VAHTI
June 2009

ISSN 1455-2566 (print)
ISBN 978- 951-804-982-4 (print)
ISSN 1798-0860 (pdf)
ISBN 978-951-804-983-1 (pdf)