

**THE EXPLANATORY NOTE OF
REGULATION 47 ON INFORMATION
SECURITY MANAGEMENT OF
TELECOMMUNICATIONS OPERATORS**

MPS 47

CONTENTS

CONTENTS 1

1 LEGISLATION 2

1.1 LEGISLATIVE BASIS FOR REGULATION 2

1.2 OTHER RELEVANT STATUTES..... 2

2 PURPOSE AND VERSION HISTORY OF THE REGULATION 2

2.1 PURPOSE OF THE REGULATION 2

2.2 KEY AMENDMENTS AND VERSION HISTORY 3

2.3 DEFINITIONS..... 3

3 PARAGRAPH-SPECIFIC EXPLANATIONS AND APPLICATION INSTRUCTIONS 6

3.1 §1 SCOPE OF APPLICATION 6

3.2 §2 ORGANISATION OF INFORMATION SECURITY 7

3.3 §3 INFORMATION SECURITY CONTROL DOCUMENTATION 8

3.4 §4 RISK MANAGEMENT..... 10

3.5 §5 INFORMATION SECURITY MEASURES..... 22

3.6 §6 MONITORING OF INFORMATION SECURITY MANAGEMENT 25

4 REFERENCE LIST 25

5 ANNEXES 27

5.1 SIMPLIFIED EXAMPLE OF RISK ASSESSMENT 27

1 LEGISLATION

The objective of this chapter is to provide regulation users with an overview of the statutes on which the regulation is based. Moreover, the chapter lists other relevant legislation within this area.

1.1 Legislative basis for regulation

FICORA's proposal for the regulation is based on sections 19 and 20 of the Act on the Protection of Privacy in Electronic Communications [1].

Under section 19(4) of the Act on the Protection of Privacy in Electronic Communications, FICORA may issue more detailed regulations to telecommunications operators regarding the information security of services referred to in subsections 1–3. Under subsection 1, telecommunications operators and value-added service providers must maintain the information security of their services. Under subsection 3, telecommunications operators are responsible to their subscribers and users for the information security referred to in subsection 1 also on behalf of any third party that wholly or in part provides a network service or communications service.

1.2 Other relevant statutes

This chapter describes the other statutes issued by FICORA that fall under the theme of this regulation. The objective of this chapter is to provide regulation users with a better opportunity to form an overall understanding regarding the regulations relating to communications networks and services.

Regulation 54 on priority rating, redundancy, power supply and the physical protection of communications networks and services [2]. The objective of this regulation is to ensure the operational reliability, data protection and information security of communications networks and services under normal circumstances, in disruptive situations under normal circumstances and in exceptional circumstances. Correspondingly, the regulation lays down the minimum requirements for telecommunications operators regarding, for instance, securing the power supply for equipment used in communications networks and services, the physical protection of equipment, and ensuring equipment and connections.

2 PURPOSE AND VERSION HISTORY OF THE REGULATION

The objective of this chapter is to provide regulation users with information on the goals and purpose of this regulation. The most significant amendments to the regulations and recommendations preceding this regulation are also detailed in this chapter.

2.1 Purpose of the regulation

Information security management has been comprehensively described in, for instance, the ISO 27001 (Information Security Management - Specification with Guidance for Use) standard [3].

Comprehensive conformance to this standard may prove too arduous, particularly for small telecommunications operators in Finland.

The regulation describes the minimum requirements for information security management that all telecommunications operators must implement in their operations. These requirements are intended to ensure a basic level of information security for the telecommunications operations undertaken by telecommunications operators. This basic level acts as the foundation for ensuring the information security of communications networks and services. In particular, the requirements focus on the continuous development of information security management, planning, implementation and assessment. The regulation also attempts to reduce the adverse effects of information security risks on telecommunications operations.

2.2 Key amendments and version history

Since the regulation's previous version entered into force, FICORA has issued service-specific regulations such as those on the information security and functionality of e-mail services (M11) [4] and Internet access services (M13) [5]. The requirements set forth in the service-specific regulations have overlapped to an extent with the requirements determined in the previous version of this regulation. An attempt was made to eliminate this overlap through an amendment to the regulation. Simultaneously, the requirements for, for instance, risk management relating to information security management were specified.

2.3 Definitions

This chapter describes the definitions employed in the regulation.

2.3.1 Telecommunications

Telecommunications is defined in the Communications Market Act. According to this Act, telecommunications refers to a network service or communications service. Public telecommunications refers to providing a network or communications service to a set of users that is not subject to any prior restriction.

In the Communications Market Act, network service refers to a service provided by a network operator, and communications service refers to a service provided by a service operator. Network operator refers to an operator that provides a communications network in its ownership or for other reasons in its possession, for the purposes of transmitting, distributing or providing messages. Service operators, on the other hand, refers to an operator that transmits messages over a communications network in its possession or obtained for use from a network operator or distributes or provides messages in a mass communications network.

Typical network and communications services include call services, broadband services, e-mail services and mass communications services.

2.3.2 Information security

Information security is determined in the Act on the Protection of Privacy in Electronic Communications. According to this law, information security refers to the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it, that data can only be modified by those who are entitled to do so, and that data and information systems can be used by those who are entitled to use them.

2.3.3 Information security risk

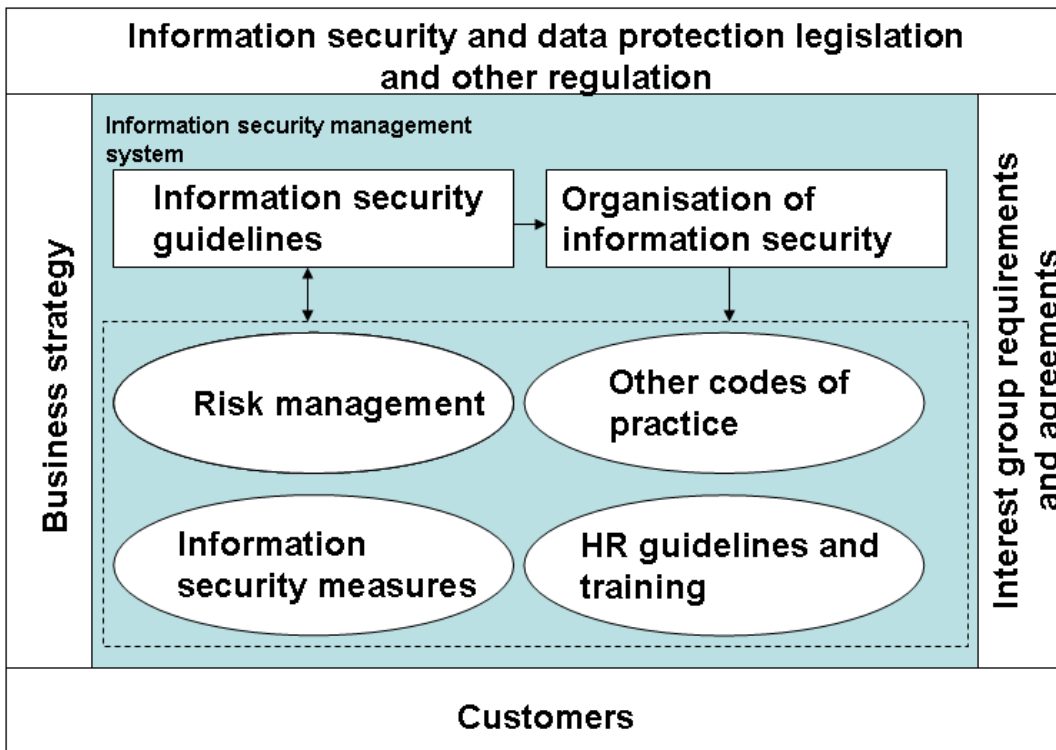
Under this regulation, information security risk refers to an inadvertent or intentional factor that compromises the confidentiality, integrity or availability of telecommunications operations. Information security risks differ from information security threats in that their likelihood and impact has been assessed.

Causes of information security risks include:

- human errors
- deficiencies in or failure to follow personnel instructions
- theft
- capacity deficit
- device breakdown
- application errors
- spread of malware
- communications traffic disruptions
- vandalism
- fire, and
- errors or negligence on the part of subcontractors or members of the partnership network.

2.3.4 Information security management system

Under this regulation, information security management system refers to a part of a telecommunications operator's management system that is based on risk assessment and control. Telecommunications operators are required to know their operating environment and take its special characteristics into account with regard to the development of their information security management system. In addition to business strategy, management system requirements are usually derived from information security and protection legislation, the regulations issued by FICORA, other statutes as well as the requirements and agreements of customers and interest groups.



Requirements for telecommunications operators' information security are derived from information security and protection legislation and other regulations, including:

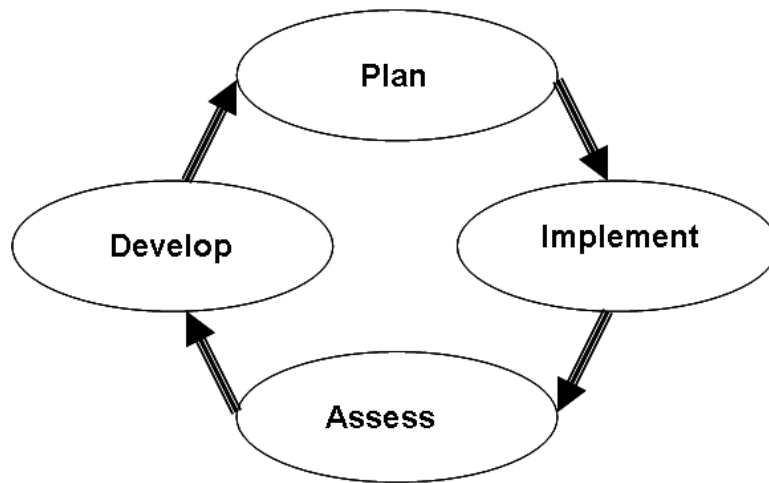
- Communications Market Act
- the Act on the Protection of Privacy in Electronic Communications
- FICORA regulation 47/2009 M.

Other information security-related requirements may apply to telecommunications operators' operations, including:

- customer requirements
- ISO 27000 standard family
- PCI DSS
- HIPAA
- SOX
- EuroSOX
- VAHTI instructions, and
- other countries' legislation.

The objective of the management system is to provide support for the development, planning, implementation and assessment of information security.

An information security management system is described, in general terms, as a four-phase process:

**Planning phase:**

The planning phase is used for creating the policies as well as defining the goals, targets and required functions with regard to information security.

Implementation phase:

In the implementation phase, the information security policies, controls and functions are applied.

Assessment phase:

The assessment phase is used for measuring the impact of the procedures on the goals, policies and practical experiences determined in the planning phase.

Development phase:

During the development phase, the information security management system is developed on the basis of the assessment phase results. Development targets may include elements such as information security policies and information security functions.

3 PARAGRAPH-SPECIFIC EXPLANATIONS AND APPLICATION INSTRUCTIONS

This chapter covers paragraph-specific explanations and application recommendations.

3.1 §1 Scope of application

This regulation is applied to operations that are related to the implementation of telecommunications operators' public network and communications services. The regulation's scope of application covers the provision of, for instance, internet connection services, e-mail services and voice services as determined by the Communications Market Act. The regulation is also applied to insignificant telecommunications operations [6].

This regulation does not apply to authorities' activities in a public authority network as determined in the Communications Market Act, or any other communications network that has been built to ensure public order and security, national defence, rescue operations, civil defence, or the safety of land, sea, rail or air transport. Similarly, the regulation cannot be applied to the temporary provision of communications networks or services. In this case, temporary means an uninterrupted period of no more than two months in length.

This regulation's scope of application is limited to telecommunications operations, not covering activities that have no direct impact on the functionality of communications services and networks and end users' information security and data protection.

3.2 §2 Organisation of information security

Explanations:

Safeguarding information, information systems and operational preconditions requires that operators efficiently organise their information security matters. The basic prerequisite is that responsibilities and obligations relating to information security matters are defined.

Application:

An information security management system must include the executive management's view on how information security responsibilities are allocated in the organisation. Information security responsibilities and obligations may include both administrative and operative responsibilities. Information security responsibilities should particularly be assessed when organisational changes take place. These include changes in personnel or a change effected in the operating environment by an organisational restructuring.

It is possible to divide information security responsibilities into groups. The information security group can be used as an example with regard to administrative responsibility. Similarly, abuse and cert/csirt groups are examples of operative groups.

Examples of administrative information security responsibilities include the development of the information security management system and control documentation, the maintenance of a monitoring system displaying the company's information security situation, the observation of information security issues in risk management and continuity planning, the maintenance and development of relevant information systems, the correctly sized resourcing of information security functions and investments, and the observation of information security issues in the training of key functions in particular.

Since these responsibilities are connected to various parts of an operator's management system, the control and monitoring of the realisation of information security responsibilities in a

co-ordinated manner is recommended. The importance of efficient co-ordination increases in significance as the extent to which the company's information security responsibilities are decentralised increases. Depending on the company's size, one or more persons in charge of information security must be made responsible for the development and monitoring of information security issues. Information security issues must be processed as part of normal management reporting.

The terms CERT (Computer Emergency Response Team) and CSIRT (Computer Security Incident Response Team) operations are in some cases used to refer to co-ordinated first-response activities and info contact point maintenance in cases of information security violations. A function intended as the contact and service point during violations of customers' and external interest groups' information security, in connection with the provision of internet services, is traditionally called an Abuse function.

The capacity to process information security violations relating to individual telecommunications services will be determined separately, if required. However, telecommunications operators must have the basic capacity to manage information security violations and risks that concern their operations and substantially affect their customers.

Administrative responsibilities may cover the following:

- information security planning
- planning information security training for personnel
- monitoring the information security level of the telecommunications company
- risk management planning and organising, and
- processing and planning projects that enhance information security.

3.3 §3 Information security control documentation

Explanations:

Information security is an element in the quality of the telecommunications operations provided by a telecommunications operator. Information security control documents are basic information security documents used by the company's management to indicate the strategic intent and general principles of information security. These documents create the basis for systematic information security development and management, while also assisting in the allocation of information security investments.

Application:

A telecommunications operator must plan information security control documents in accordance with its own risks and needs. The telecommunications operator's information security team or some other requisitely large group of representatives from the company prepares the documents

for approval by the management. The party that has prepared the documents may also handle their publication and appropriate communication to all organisation employees. The control documents must be easily available to all employees, through, for instance, the organisation's intranet site. Moreover, the control documents must be part of the orientation programme for new employees. The telecommunications company must ensure that conformance with the main principles of information security, as determined in the documents, is monitored.

The information security control documentation must indicate the following matters with regard to the company's telecommunications operations:

- information security goals
- responsibilities for ensuring information security
- information security organisation, and
- methods for the maintenance and development of the organisation's information security in relation to, for instance, internal audits.

Telecommunications operators must keep written documents on how the following special areas have been taken into consideration to the extent that they apply to the telecommunications operator's own telecommunications operations:

- Personnel safety
 - Personnel's information security-related responsibilities and obligations.
 - Personnel's information security competence and its development.
 - Analysis of key person risks, with possible background checks.
 - Avoidance of sets of responsibilities and tasks that are dangerous with regard to telecommunications operations.
 - Instructions on the procedures followed when employment is terminated.
- Hardware and software security
 - Sufficient documentation for correct focusing of the repair of a detected vulnerability.
 - Spare part supply.
 - General system change management process.
- Communications security
 - Requirements regarding communications security are discussed in more detail in the service-specific regulations, such as the regulations on information security and the functionality of e-mail services (M11) [4] and Internet access services (M13) [5].
- Information material security
 - Ensuring the confidentiality, integrity and availability of information: how information is classified, and how personnel are instructed on information handling.
- Safety of use
 - Maintenance responsibilities for user right register: allocation, changing and deletion of user rights.
 - Prevention of the accumulation of user rights.

- Prevention of unauthorised persons from accessing the management and configuration information related to the implementation of communications services as well as the invoicing, subscriber and log data of the telecommunications operator's customers.
- Interference in information security violations and misuse.
 - Responsibilities for the detection of and intervention in incidents which are significant with regard to information security.
 - Instructions and processes for recovery from information security problems.
 - Assessment of severity.
 - Notifications to the authorities.
 - Communicating deviations.
 - Post-deviation activities.
 - Misuse and actions, contrary to instructions, on the part of personnel.

Physical safety issues have been regulated in more detail in regulation FICORA M54. The obligation to report information security incidents as well as fault and disturbances in public telecommunications has been determined in regulation FICORA M9 [7].

Moreover, telecommunications operators must draft sufficiently detailed instructions for individual procedures that are relevant to information security. In practice, this means drafting detailed instructions for, for instance, processing identification data.

In the case of subcontracts and outsourcing contracts, it must be ensured that the limits of information security responsibilities between the telecommunications operator and the subcontractor are defined in sufficient detail. However, the overall responsibility for information security always lies with the telecommunications operator, regardless of whether or not functions have been outsourced.

References to the statutes governing telecommunications operations as well as the sanctions applicable when these statutes have been violated should be included in subcontracts.

The National Emergency Supply Agency has issued recommendations [8] that can be referenced in contracts, with regard to the management of operational continuity. These recommendations concern:

- management
- ERP
- personnel and HR management
- partnerships, and
- assessment of operational continuity management.

3.4 §4 Risk management

Explanations:

One of the key components of an information security management system is efficient risk management. This usually refers to the identification of risks related to a company's business operations as well as post-identification risk assessment, control measures, and the monitoring of the implementation of these measures. The primary objective of a management system is to protect the organisation and its capacity to perform its tasks under normal circumstances, in disruptive situations under normal circumstances and in exceptional circumstances, taking financial factors into account. Risk management may form part of a company's preparedness or continuity planning.

The preparedness obligation for telecommunications operators is determined in sections 90 and 128 of the Communications Market Act [9].

Section 90 of the Communications Market Act places an obligation on telecommunications operators to prepare for exceptional circumstances. By means of contingency planning and preparations for exceptional circumstances, telecommunications operators must ensure that their activities will continue with the minimum disruption even in the exceptional circumstances referred to in the Emergency Powers Act [10] and in disruptive situations under normal circumstances.

According to paragraph 128 of the Communications Market Act, public communications networks and services as well as the connected communications networks and services must be planned, built and maintained in such a manner that they function as reliably as possible, even in the exceptional circumstances referred to in the Emergency Powers Act and in disruptive situations under normal circumstances, and that access to emergency services is secured as reliably as possible even in the event of network disruptions.

The objectives of risk management include:

- expediting recovery from information security problems related to telecom operations
- reducing the costs and damage resulting from information security problems related to telecom operations
- focusing investments that improve the information security of telecom operations
- improving the quality and productivity of telecom operations
- financial optimisation of telecom operations risks, and
- prevention of the realisation of telecom operations risks.

Risks management requirements aim at ensuring that the telecommunications operator is aware of the repercussions should the risks be realised, and whether risk-reducing measures are sufficient.

Application:

Risk management standards and publications include the following:

- ISO/IEC TR 13335-3, Information technology - Guidelines for the management of IT Security - Techniques for the management of IT Security. [11]
- ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management [12]
- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology [13]
- Enisa: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools [14]
- COSO ERM (Enterprise Risk Management - Integrated Framework (2004)) [15]
- BS 31100:2008, Risk management. Code of practice [16]
- ISO 31000 Risk management -- Principles and guidelines [17]
- The Institute of Risk Management (IRM), Risk Management Standard [18], and
- PK-RH's Risk Management in SMEs [19].

This regulation does not include an obligation to comply with a certain standard. Risk management models vary on a company-specific basis, and there is no single model that would fit every company. The fundamental issue is to tie the goals of the risk management system to the operative goals of the company, while ensuring the support of the management.

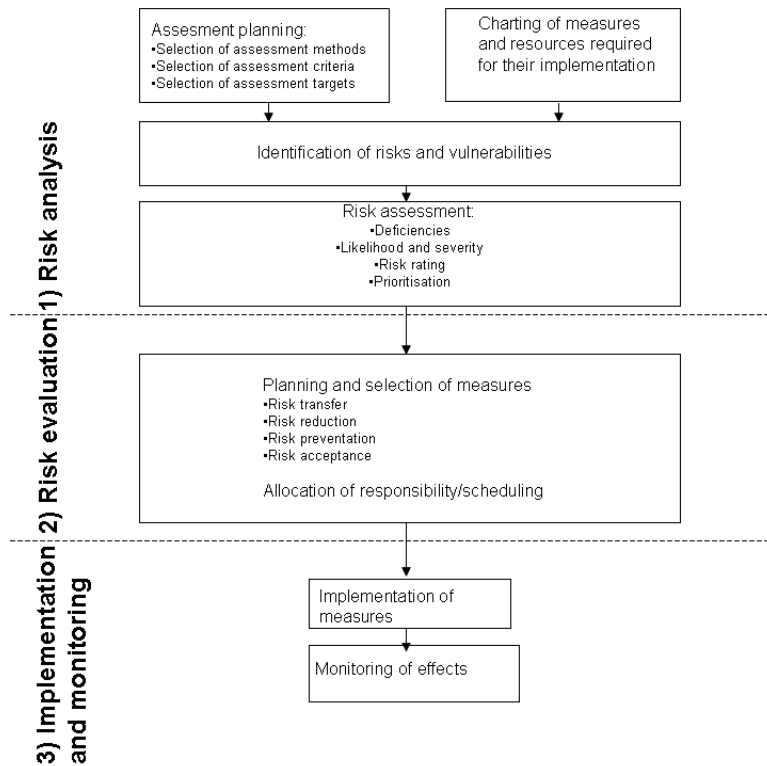
The minimum requirements for risk management are:

- The telecommunications operator has classified the functions, processes and systems that are most crucial with regard to telecommunications operations.
- The information security risks related to telecommunications operations have been analysed.
- The telecommunications operator regularly monitors the information security level of its telecommunications operations. This information security level can be monitored by means of, for instance, random inspections, information security checks and information security audits.

FICORA's regulation 54/2008 M includes provisions concerning the priority rating of the functionality of communications networks and services. Telecommunications operators may use priority rating, drafted on the basis of regulation 54, with regard to the analysis of the availability risks of services experienced by end users.

Information security risks relating to telecommunications operations must be analysed with regard to the most significant and critical functions, processes and systems related to telecom operations, and measures for the reduction, elimination or transfer of these risks must be documented.

Risk management can be roughly divided into three phases:



3.4.1 Risk analysis

Risk analysis means the systematic measures used to identify information security threats and vulnerabilities that endanger telecommunications operations, and to forecast the consequences of potentially realised threats. Risk analysis must be planned, implemented and documented in a high-quality fashion. It should be performed on an object as per the predetermined target level. This may mean, for instance, an availability requirement for the communications service determined by a FICORA regulation or a customer contract. In particular, risk analysis is used to target threats that endanger the fulfilment of the objective set for the target.

Risk analysis comprises five areas which are:

- assessment planning
- identification of information security threats endangering telecommunications operations
- identification of exposed systems and functions
- assessment of the severity and likelihood of risks, and

- prioritisation of risks.

Risk analysis answers the following questions with regard to the analysed target:

- What might happen? (Threats)
- Why a certain threat may be realised? (Vulnerabilities)
- What is the likelihood of the threat being realised, and what are the consequences of its realisation with regard to telecommunications operations? (Likelihood and severity)
- How great is the resulting risk? (Risk number), and
- What are the greatest risks? (Prioritisation)

The key objectives of risk analysis are:

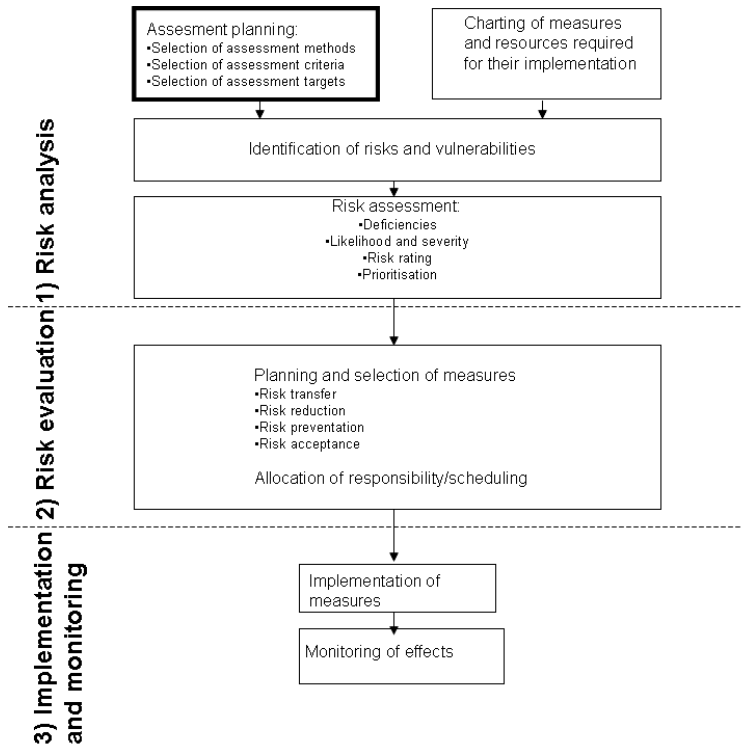
- bolstering information security leadership and allocation of investments
- improving information security, and
- identifying information security risks related to telecommunications operations as well as their severity.

Due to the objectives of risk analysis, implementers of risk analysis should be very familiar with the operations, operational goals and related requirements of the risk analysis target.

3.4.1.1 Risk assessment planning

The assessment of information security risks forms a crucial part of the systematic development of telecommunications information security. Such an assessment is used for identifying the functions, information and systems that are essential to telecommunications operations.

The foundation for effective risk analysis is laid down in the risk analysis planning and preparation phase, during which the operational goals of the analysed target are identified, the areas falling outside the analysis are determined, and the most suitable analysis method is selected. Careful planning and preparation are used to ensure the efficient use of the resources reserved for risk assessment, the realisation of risk analysis goals, and the achievement of the best attainable operational benefits.



Risk assessment planning must include the risk assessment methods to be used, the risk assessment criteria, the assessment objectives, and the subject matter on which assessment focuses. For instance, the methods most suited to the assessment of personal risks are not necessarily those that should be applied to assessing information system risks.

Prior to starting the assessment, the objective of assessment, the operational goals of the target, the implementation method of the assessment, and the schedule should be determined. Risk assessment objectives can be tied to the number of assessments, the schedule, or the improvement measures identified by the assessment.

The extensiveness of telecommunications operations as well as the organisation’s possibilities should be taken into consideration in assessment planning. For instance, if a telecommunications operator's business operations only comprise small-scale e-mail services, the risk assessment methods can be dramatically scaled-back. The minimum requirement for risk assessment planning, however, is that even scaled-back assessment methods are documented.

Sources such as previous information security reviews, information on “near-miss” situations, and other material related to information security, should be utilised in risk assessment.

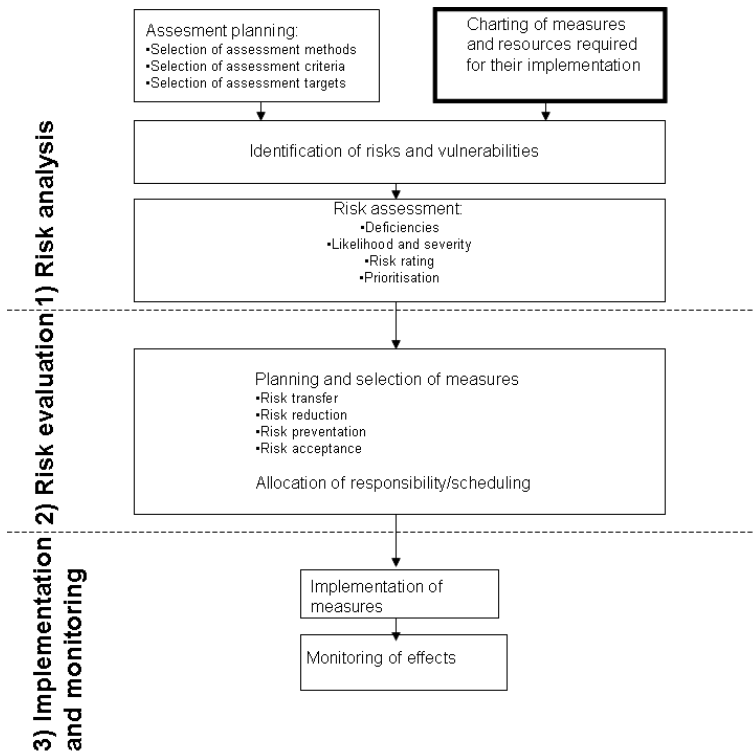
Telecommunications operators should ensure that the people participating in risk assessment have a proper understanding of the risk assessment method used.

Risk assessment documentation, recording, and the processing of assessment results should also be determined in the planning phase.

3.4.1.2 Determining the resources required for functions and their implementation

The basic prerequisite for identifying systems and functions is that the systems and functions that are essential to telecommunications operations have been determined, at least with regard to the following areas:

- equipment rooms
- hardware and software
- communications connections
- information material, and
- system maintenance and support personnel.



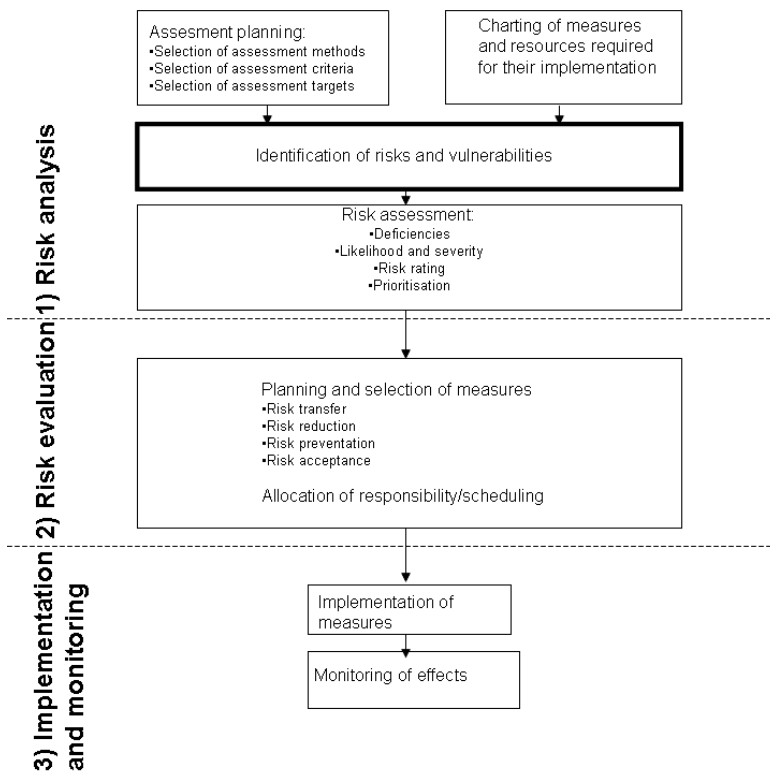
Telecommunications operators may use importance classification, drafted on the basis of regulation 54, with regard to the analysis of the availability risks of services experienced by end users. Moreover, regulation 47 requires that telecommunications companies determine risks from the perspective of information material security for systems processing confidential information.

These systems include invoicing, telecommunications interception and telecommunications monitoring systems.

This analysis improves the telecommunications operator's chances of assessing the criticality, confidentiality and required resourcing of the information systems and processed information. Moreover, the analysis provides help in focusing measures that improve information security.

3.4.1.3 Identification of threats

In this context, threat means a telecommunications operations-endangering situation, the likelihood or severity of which has not been assessed. The definition of threats is dependent on the selected risk assessment target and its restriction. Results from previous information security audits of the risk analysis target as well as previously realised risks or information security deviations should be utilised in the determination of risks. Information security audits can be implemented as inhouse audits or outsourced to an external provider. Audits should be performed, depending on the criticality of the target, at an interval of 6 months to 2 years, and every time significant changes are made to the assessment target.



In every case, some vulnerability, i.e. exposure to a factor threatening telecommunications operations, is related to the realisation of a threat. Vulnerabilities can either be technical or non-technical, relating to, for instance:

- hardware and software
- processes, and

- personnel.

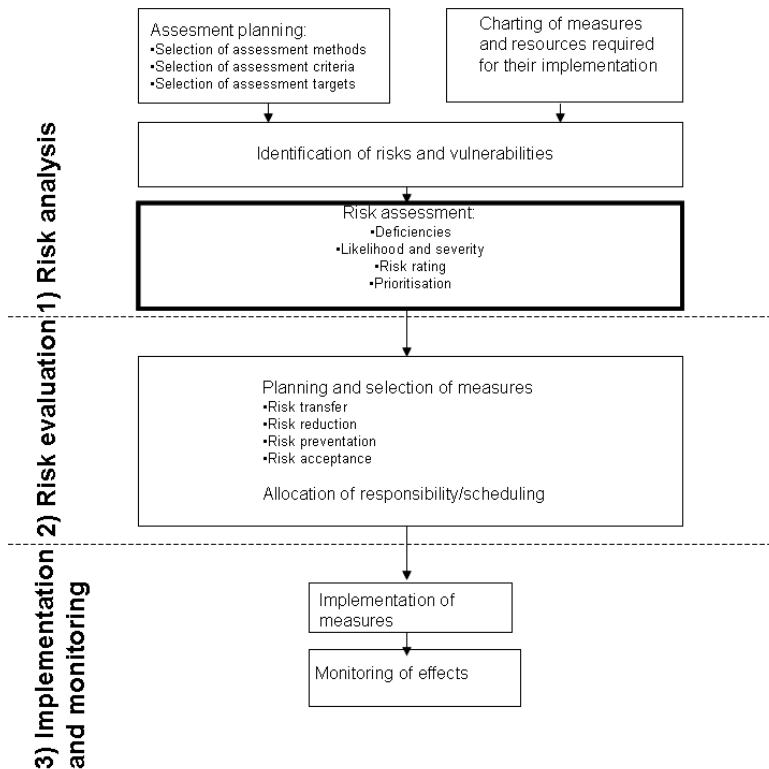
A software- and hardware-related threat entails that, for instance, malware is inhibiting the operation of the device or software in question.

A process-related threat means, for instance, that the recovery from the aforementioned malware infection is delayed. Vulnerabilities may include such items as the lack of agreed operating methods.

A personnel-related threat may comprise, for instance, a certain service lacking a person responsible for it. The related vulnerabilities include the person responsible falling ill or terminating his or her employment.

3.4.1.4 Risk assessment

Risk assessment means assessing the severity of the identified threat and assessing the likelihood of its realisation.



Severity:

Severity refers to the consequences of the realised threat for the function to which it is related. Severity may increase over time, meaning that the level of severity attached to a service’s temporary lack of availability may be lower than that considered appropriate in the event of the service’s prolonged unavailability.

Likelihood:

Likelihood refers to the likelihood of a threat being realised.

When assessing likelihood, all previously performed measures aimed at preventing the threat’s realisation should be taken into account.

Severity and likelihood can be indicated by means of, for instance, numbers on a scale of 0 to 3, in which 0 corresponds with no impact or likelihood, and 3 corresponds with a very significant impact or likelihood of realisation.

Risk rating:

Risks are usually indicated by means of a risk rating that can be formed by, for instance, multiplying the threat’s severity by its likelihood. Based on this risk rating, risks can be priority classified on the basis of the threat’s severity and likelihood.

Risk classification:

Analysed risks can be classified on the basis of their risk rating, among other things. Prioritising risks with regard to their impact on business operations is a widely used method in the biggest companies in particular. The most important thing, however, is that detected risks are classified in some manner in order to focus available resources on the most severe risks.

Risk classification serves as a recommendation that supports decision-making when planning and focusing corrective measures. At its simplest, risk classification can appear as below, with a threat likelihood and severity scale of 0 to 3:

| Risk rating | Recommendation |
|--------------------|---|
| [0-1] | Insignificant risk. No measures required. |
| [2] | Acceptable risk. The decision on the approval of this risk must be documented. |
| [3-4] | Moderate risk. The risk can be temporarily accepted. Initiation of measures to reduce the risk is recommended within the available resources. |
| [6] | Significant risk. Initiation of measures to reduce the risk is recommended as soon as possible. |

- [9] Unacceptable risk. Immediate initiation of measures to reduce the risk is recommended.

Documentation:

Documentation must include information that can be used retrospectively for assessing the realisation of risk management, and the adequacy of the risk assessment and measures.

Documentation must include at least the following:

- Risk analysis
 - Risk analysis objectives
 - Risk analysis restrictions
 - Risk analysis results
 - Final risk analysis report.
- Risk evaluation
 - List of the greatest risks
 - List of the most critical deficiencies.

3.4.2 Risk evaluation

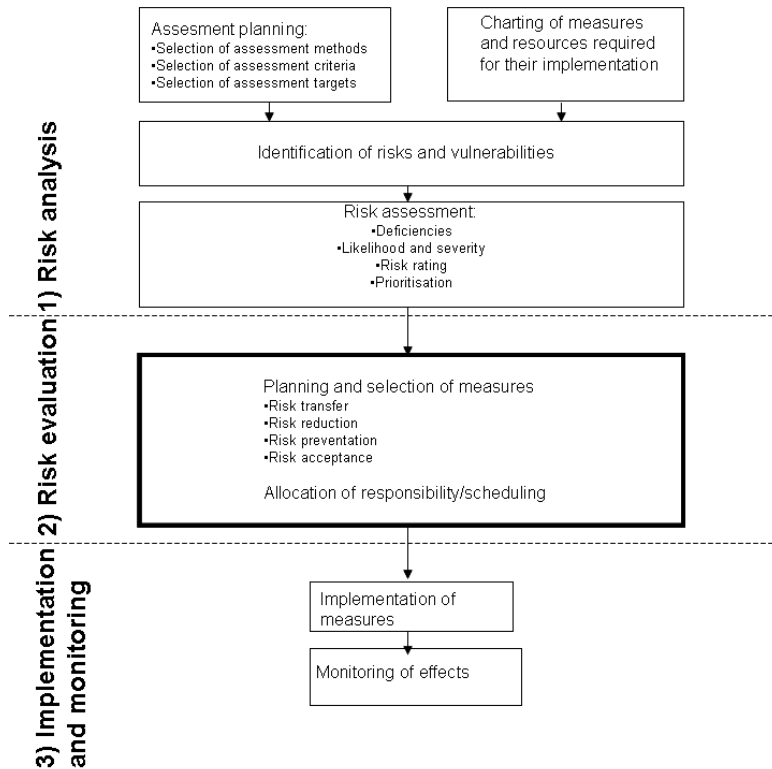
Risk evaluation is used for highlighting key development needs on the basis of the risk assessment results. This risk assessment summary indicates, for instance:

- greatest risks
- most critical deficiencies, and
- targets for further investigation.

3.4.2.1 Planning and selection of measures

The requirements of binding regulations, the costs of solutions, human resources, the operator's willingness to take risks, and the losses resulting from the realisation of a risk should be taken into account when selecting information security measures based on the risk analysis. These refer to measures aimed at:

- transferring risks
- reducing risks
- avoiding risks
- accepting risks
- preventing risks, and
- improving the detection of risks.



If a significant risk cannot be entirely removed, the telecommunications operator must draw up a recovery plan in anticipation of the realisation of the risk.

Transferring risks means passing on the costs resulting from the realisation of the risk to a third party by means of instruments such as an insurance or contract. If the risk is realised, overall responsibility for the information security of telecommunications operations remains with the telecommunications operator regardless.

Reducing risks refers to the prevention of damage and sharing of the risk.

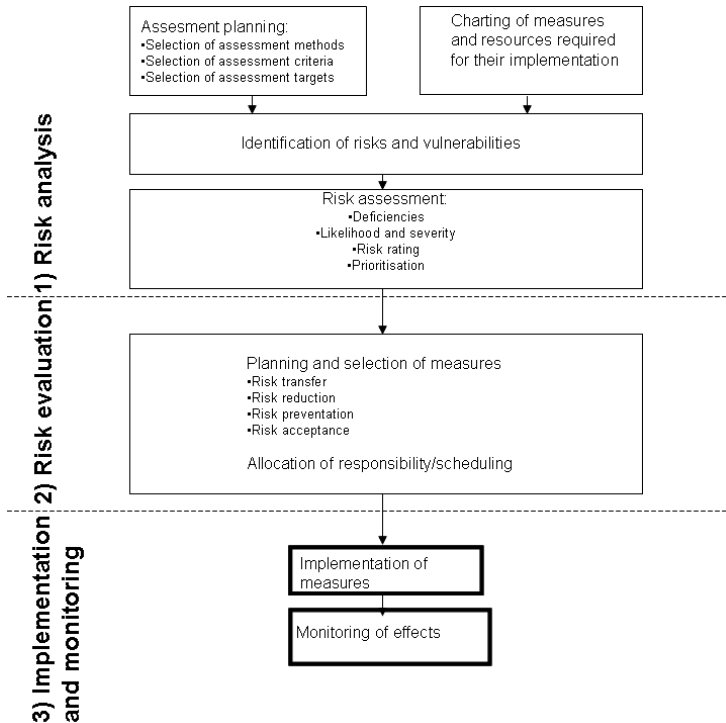
Avoiding risks means shedding a product, service, contractual partner or activity that comprises too great a risk.

Risks that entail only minor consequences can be accepted, if the risks are not contrary to legislation and regulations. However, the simultaneous realisation of multiple minor risks may substantially change the situation with regard to, for instance, the quality of telecommunications operations. When decisions on the acceptance of risks are made, one should consider on a case-specific basis to whom and under what conditions the risk is acceptable, while also taking account of the consequences and costs resulting from the realisation of the risk.

The owner of a function or service must ensure that risks are accepted. Risk acceptance decisions are performed in accordance with the company hierarchy.

3.4.2.2 Allocation of responsibility and scheduling of measures

This section is related to paragraph 5 of the regulation, and is covered in section 3.5 of this document.



3.5 §5 Information security measures

Application:

A plan should be drafted for selected information security-improving measures, detailing such matters as the persons responsible for the determined measures and implementations as well as their monitoring schedule.

Information security-improving measures relating to the transference of risks include:

- avoiding certain products, protocols or measures
- avoiding dubious contractual partners, and
- abandonment of operations entailing too great a risk.

Information security-improving measures relating to the reduction of risks include:

- personnel training in matters of information security
- operational instructions
- adoption of products that improve information security
- backup systems
- regular information security updates
- up-to-date backup copies
- security classification for documentation, and
- access control.

Advance detection of risks can be improved by measures such as conducting regular target audits, integrating risk management into product development at as early a stage as possible, improving the personnel's awareness of information security, and providing instructions for reporting problematic situations.

Personal risks can be prevented by means of, for instance, alternates, and information system risks can be prevented by means of backup systems.

Telecommunications operators must draft sufficiently detailed instructions for individual procedures that are relevant to information security. These instructions may refer, for instance, to the following areas:

- visitor protocols
- management of access rights
- remote use of telecommunications systems, and
- processing of confidential information material (e.g. identification, invoicing and customer information).

3.5.1 Information material security

Telecommunications operators must have processing instructions for information material that is vital to telecommunications operations. These instructions must cover the following matters, among others:

- general principles for assessing the security class and confidentiality of information material, and keeping information material confidential
- processing and modification rights to the allocation of information material reading rights, modification rights and the allocation of these rights
- determination of confidentiality
- publicity for information or document: for instance, speaking publicly on an issue

- document features: paper, stamp and other markings
- storage and concealment
- printing and copying
- reception, distribution, sending and transportation
- documentation of information and document processing, and
- document archiving, processing, or termination of processing rights, disposal of document.

User- or user group-specific processing rights must be separately determined for all security classified information material. It must also be ensured that inappropriate people do not have access to security classified information. However, security classified information material must be available to persons who have processing rights to this material.

Processing instructions for telecommunications operators' information material may be based, as applicable, on the Information Security Instructions for State Administration's Information Material [20], prepared by the Ministry of Finance.

The telecommunications operator must ensure that up-to-date backup copies exist of all information material that is relevant to the availability of communications networks and services, and that these backup copies are stored in a locked facility and separate from the equipment in question. It must be possible to take the backup copies into use if the original information material is damaged due to a reason such as a software defect, equipment failure, or an accident in the equipment room. This information material includes user information and configuration information.

3.5.2 Interference in misuse and information security problems

A telecommunications operator must be able to react to information security violations and threats that, on the one hand, affect the company's capacity to provide telecommunications services and, on the other, fundamentally endanger the information security of the company's customers.

Intervention in cases of misuse and information security problems related to network and communications services must occur in an organised manner and comprise at least the following functions:

- Drafting of instructions and processes concerning intervention in cases of misuse and information security problems.
- Reporting on misuse and information security problems.
- Responsibilities and functions for the investigation, submission for preliminary investigation and assessment of the severity of misuse and information security problems.

- Responsibilities and functions for damage limitation, elimination of misuse or information security problem, and briefing of executive management.
- Notifications to the authorities.
- Responsibilities and functions for recovery from misuse or information security problem.
- Functions for preventing the recurrence of the incident.

3.6 §6 Monitoring of information security management

Explanations:

New technologies and services entail new challenges for the information security of communications networks and services. As a normal part of a company's operations from the planning of communications services and networks to maintenance, information security management is a continuous process that must react to changes.

Application:

An organisation's management must ensure that sufficient resources exist for the planning, implementation, assessment and maintenance of the information security management system.

The information security management system must be regularly serviced and updated as required. Change needs must be reviewed once per year and always when required. The need to alter the management system may arise in connection with, for instance, organisational restructuring or changes to the company strategy.

4 REFERENCE LIST

[1] Act on the Protection of Privacy in Electronic Communications (516/2004 with amendments), <http://www.finlex.fi/fi/laki/ajantasa/2004/20040516>
<http://www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf> (amendments up to 1328/2007 included)

[2] M54 Regulation on priority rating, redundancy, power supply and physical protection of communications networks and services
<http://www.ficora.fi/attachments/suomiry/5vB4GW4xt/Viestintavirasto542008M.pdf>
<http://www.ficora.fi/attachments/englantiav/5wJbOLb5P/FICORA542008.pdf>

[3] Information Security Management - Specification with Guidance for Use
<http://www.iso.org/iso/home.htm>

[4] M11 Regulation on information security and functionality of e-mail services
<http://www.ficora.fi/attachments/suomiry/5AWLwAxxQ/Viestintavirasto11A2008M.pdf>
<http://www.ficora.fi/attachments/englantiav/5B37cMfzM/FICORA11A2008M.pdf>

[5] M13 Regulation on information security and functionality of Internet access services
<http://www.ficora.fi/attachments/suomiry/5AWLt8K4m/Viestintavirasto13A2008M.pdf>
<http://www.ficora.fi/attachments/englantiav/5B37hthyt/FICORA13A2008M.pdf>

[6] Government decree (Nr. 675) on telecommunications of minor significance
<http://www.finlex.fi/fi/laki/kokoelma/2003/20030106.pdf>

[7] M9, Regulation on obligation to report information security incidents and faults and disturbances in public telecommunications

<http://www.ficora.fi/attachments/suomiry/5hw8uQW3c/Viestintavirasto09C2009M.pdf>

<http://www.ficora.fi/attachments/englantiav/5hw9MAxqr/FICORA09C2009M.pdf>

[8] National Emergency Supply Agency: Contract-based preparedness in the information society sector

http://www.huoltovarmuus.fi/documents/3/SOPIVA_julkaisu.pdf

[9] Communications Market Act (393/2003 with amendments),

<http://www.finlex.fi/fi/laki/ajantasa/2003/20030393>

<http://www.finlex.fi/fi/laki/kaannokset/2003/en20030393.pdf> (amendments up to 119/2008 included)

[10] Emergency Powers Act (1080/1991 with amendments),

[http://www.finlex.fi/fi/laki/ajantasa/1991/19911080?search\[type\]=pika&search\[pika\]=valmiuslaki](http://www.finlex.fi/fi/laki/ajantasa/1991/19911080?search[type]=pika&search[pika]=valmiuslaki)

<http://www.finlex.fi/fi/laki/kaannokset/1991/en19911080.pdf> (amendments up to 696/2003 included)

[11] ISO/IEC TR 13335-3, Information technology - Guidelines for the management of IT Security - Techniques for the management of IT Security

<http://www.iso.org/iso/home.htm>

[12] ISO/IEC 27005:2009 Information technology - Security techniques - Information security risk management

<http://www.iso.org/iso/home.htm>

[13] NIST Special Publication 13-800, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology

<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

[14] Enisa: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools

http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf

[15] COSO ERM (Enterprise Risk Management - Integrated Framework [2004])

<http://www.coso.org/-ERM.htm>

[16] BS 31100:2008, Risk management. Code of practice.

<http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=00000000030191339>

[17] ISO 31000 Risk management -- Principles and guidelines

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170

[18] The Institute of Risk Management (IRM), Risk Management Standard

<http://www.theirm.org/publications/PUstandard.html>

[19] PK-RH's Risk Management in SMEs

www.pk-rh.fi/riskilajit/tietoriskit/tietoriskit

[20] Ministry of Finance: Information Security Processing Instructions for Information Material

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3386/3388_fi.pdf

5 ANNEXES

5.1 Simplified example of risk assessment

This simplified and limited example describes the risk management process of a small e-mail services provider in accordance with the model in section 3.4. The company in question provides e-mail services to some 750 customers. In the example, the risk assessment of the e-mail service has only been described with respect to a single risk. Typically, e-mail services are subject to numerous other risks that must also be assessed.

5.1.1.1 Risk analysis

Risk analysis objectives:

In this case, risk assessment is used for determining the business effects of the e-mail service in a situation in which competent maintenance personnel are unavailable. The financial impacts of the situation are also taken into account in the assessment. The assessment is based on interviews conducted with the current persons in charge and the supervisor.

Risk analysis restrictions:

The risk analysis target is an e-mail service provided by the operator to its customers, totalling around a third of the company's cash flow. This analysis concentrates on the maintenance of the e-mail service. The objective of maintenance is to ensure the uninterrupted functioning of the e-mail system in all situations. Personnel availability and competencies are prerequisites for the maintenance and development of the e-mail system.

Risk analysis results:

The so-called potential problem analysis is used as the assessment method.

The threat's severity is assessed on a scale of 0 to 3, in which:

- 0 means the threat does not impact on the company's business operations
- 1 means the threat has a minor impact on the company's business operations
- 2 means the threat has a significant impact on the company's business operations
- 3 means the threat has a very significant impact on the company's business operations.

A similar scale is used in assessing the likelihood of a threat's realisation.

Risks are prioritised using the so-called risk rating, i.e. the result of multiplying the likelihood of the threat's realisation by its severity. The risk rating scale is 0 to 9, in which:

- 0–1 refer to an insignificant risk
- 2 refers to an acceptable risk
- 3–4 refer to a modest risk
- 6 refers to a significant risk

- 9 refers to an unacceptable risk.

Two people are currently responsible for the maintenance of the e-mail service. One of these persons' fixed-term employment contracts will end after three months, and this person has indicated that he will move abroad to study after the termination of employment.

The primary threat is the disruption of system operations due, for instance, to a sudden spike in the amount of spam. End customers experience disruptions of operations as delays caused to incoming e-mail that, if prolonged, may result in substantial financial losses to the company. Prolongation is likely if competent personnel are unavailable.

Vulnerabilities:

- The temporary employee's employment ends after three months.
- The only maintenance operator falling ill or being absent for other reasons.

Severity of threat: The e-mail service comprises around a third of the company's cash flow. The functionality of the e-mail service is very important to the company's business operations, giving a threat severity rating of 3.

Likelihood of threat: The approaching summer holiday season increases the likelihood, since the current maintenance person spends three weeks on holiday in July. Significant flaws in the e-mail system have been detected around once per month. Employing the aforementioned criteria, 2 was determined as the threat's likelihood rating.

Risk rating: severity of threat * likelihood of realisation of threat = 3 * 2 = 6.

Final risk analysis report:

Based on the risk analysis, a major risk was identified in e-mail service maintenance, and this risk should be reduced as soon as possible.

The effects of the maintenance personnel's short-term temporary unavailability are not necessarily significant, if no malfunctions occur during their absence. As the absence becomes prolonged, the effects markedly increase. Consequently, the likelihood of malfunctions increases as well. Since the e-mail system cannot be rendered operational without the maintenance personnel's expertise, any absence of maintenance personnel that coincides with a malfunction impacting on service functionality will cause significant financial losses, and have a negative impact on the company's image.

In this assessment, the unavailability of maintenance personnel during malfunctions causes a significant risk based on the effects and likelihood of the risk's realisation. The risk is clearly related to the company's core operations.

5.1.1.2 Risk evaluation

Measures:

The functionality of the e-mail service is listed among the company's primary business goals. In order for these business goals to be achieved, the assessed risk requires risk reduction measures. As a reduction measure, a second maintenance technician is appointed for the e-mail system in good time before the departure of the current employee, thus avoiding a situation in which only one person is responsible for maintenance. A training plan is drafted for maintenance personnel in order to ensure the necessary expertise in the future.

Allocation of responsibility and scheduling:

The closest supervisor of the maintenance personnel is responsible for the measures; he will immediately initiate the required in-house recruitment process.

5.1.1.3 Implementation and monitoring

The closest supervisor of the maintenance personnel reports on the performance of the determined measures, while reporting on progress to his supervisor.

Monitoring the effects of measures:

The maintenance personnel's resources and expertise are monitored in the future as part of the annual risk analysis of the e-mail service environment and as part of daily supervisor work.