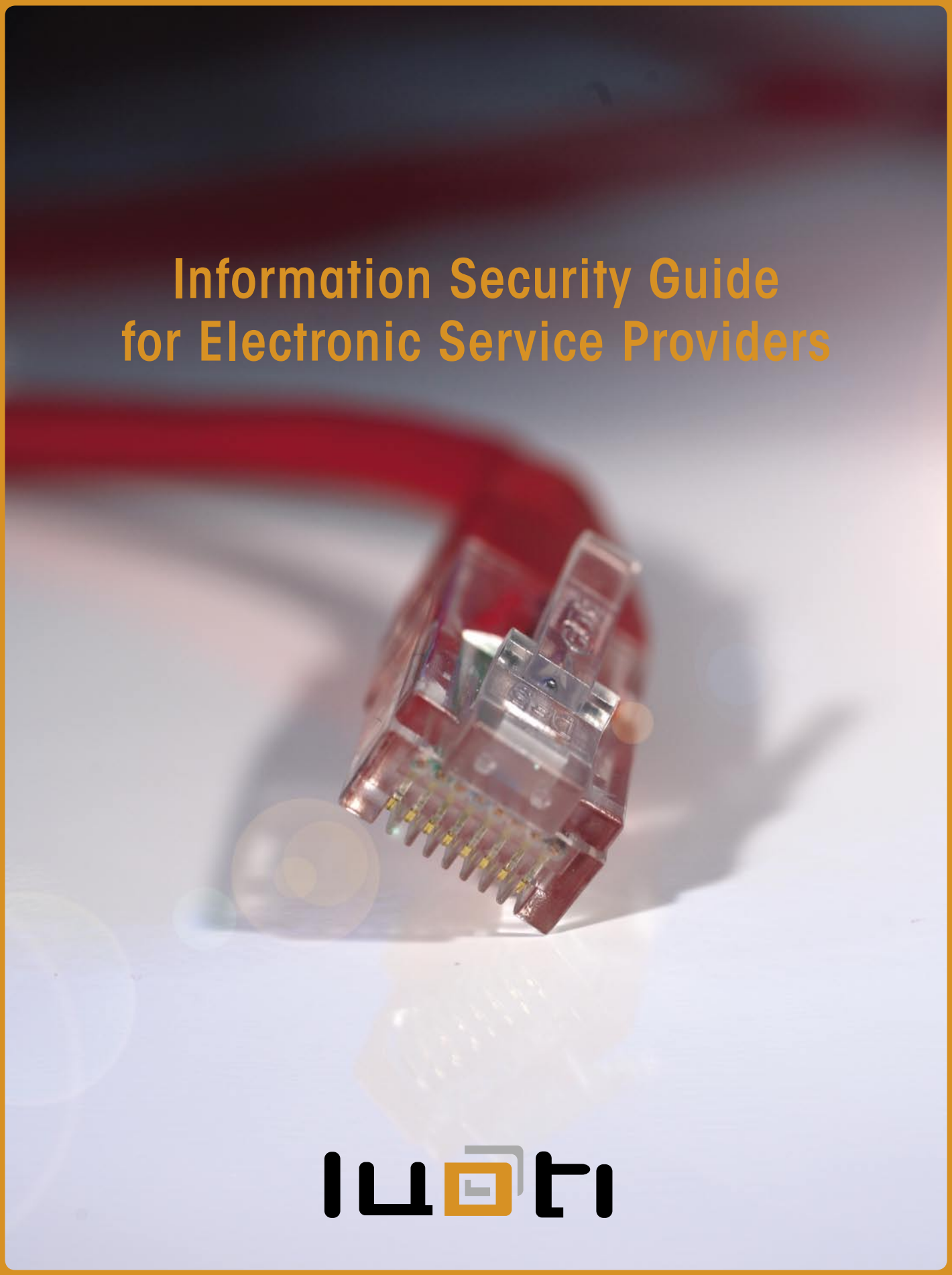
Information Security Guide for Electronic Service Providers



Information Security Guide for Electronic Service Providers

ISBN 952-201-786-8, ISBN 952-201-787-6 (electronic version), Luoti-publication 8/2006, Helsinki 2006

Preface

This Information Security Guide for Electronic Service Providers has been prepared as part of the Finnish Ministry of Transport and Communications' Development Programme on Trust and Information Security in Electronic Services (LUOTI). During 2005-2006, the LUOTI programme has promoted the information security of new electronic services. The programme's central objective has been to increase service providers' awareness of the role of information security in the development and provision of electronic services. Progress has been made towards this objective through practical project work, conducting background studies into the information security of different technologies, and by considering the need for research and development as well as legislation in the field of information security. This guide contains the key results of the programme.

Ensuring adequate information security is part of good business practice and a prerequisite for reliable service provision. Information security should be taken into account at all stages of the service development process, as this will help in maintaining the quality and usability of the service and in earning consumers' trust. The most significant policy lines in terms of information security are decided at the service planning stage.

The purpose of the guide is provide service providers with advice on information security at the different stages of service development. A task list has been prepared for each development stage, together with a list of questions that service providers should ask themselves to ensure the information security of services under development. The guide does not cover everything, rather it highlights the key information security questions for service provision so that service developers and providers can assess them for themselves.

The guide has been written by Karri Tomula, Mika Laaksonen and Harri Metso of KPMG Oy Ab. The work has been supervised by Kimmo Lehtosalo of Eera Finland Oy and Päivi Antikainen of the Ministry of Transport and Communications. In addition, a number of people have commented on different versions of the guide in connection with its preparation.

The Ministry of Transport and Communications expresses its thanks to everyone who contributed to making the publication of this guide possible.

Helsinki, 27 November 2006

Päivi Antikainen
Ministerial Adviser


WORLD WIDE

1
Purpose of the Information Security Guide for Electronic Service Providers

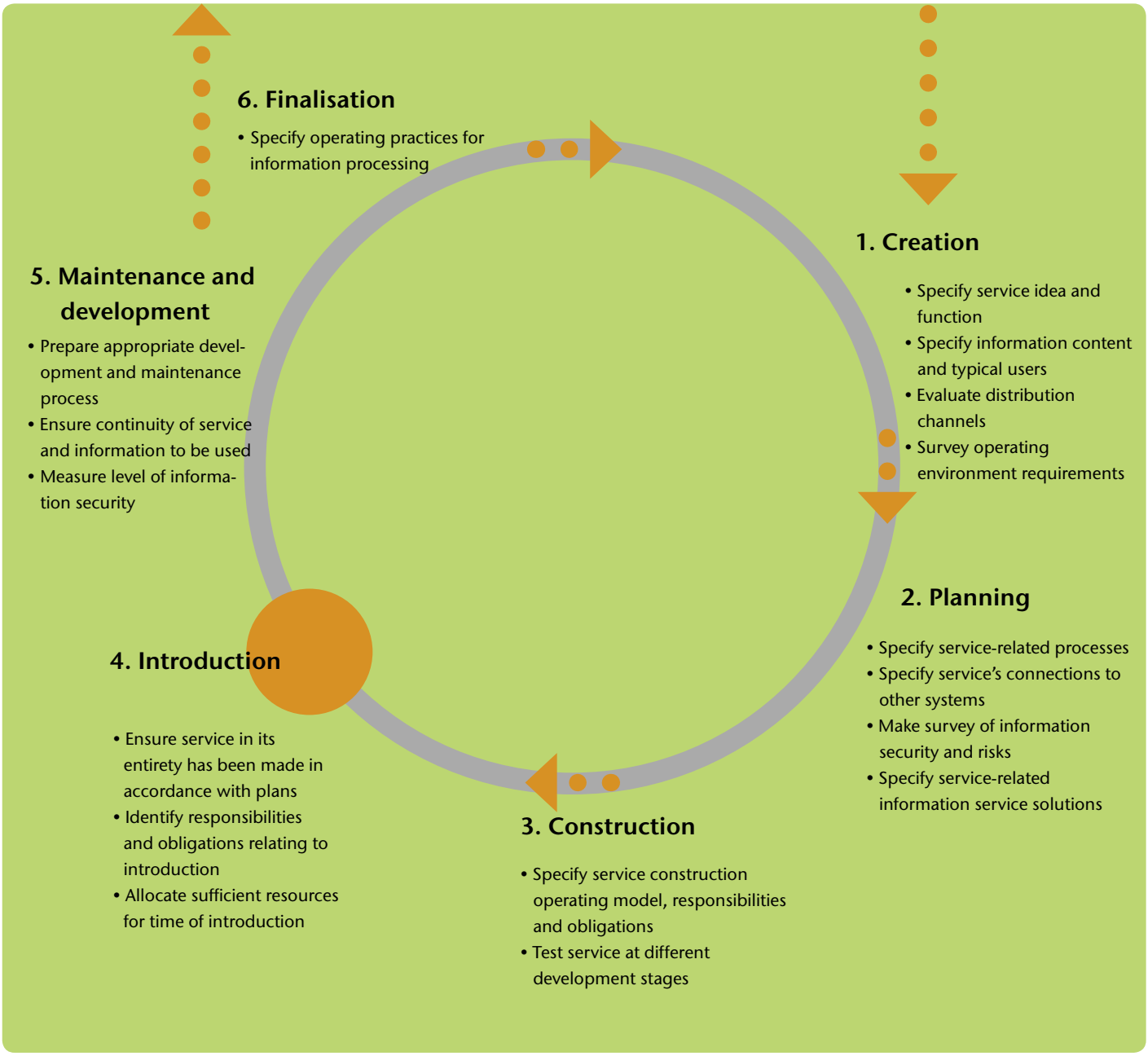
Information security plays an important role in electronic services. Effective information security ensures the trust of users and the quality of services. Nowadays, electronic services can utilise numerous functions, such as transmitting moving pictures or locating users. Often services are designed in a multichannel environment, enabling them to be used on a number of terminal devices. Combining different functions, distribution channels and software platforms sets numerous challenges for information security planning. Simultaneous requirements for expertise in different technologies and information security have grown, and the various, and increasingly more professional, information security threats have increased.

By a secure electronic service is meant a service developed by a reliable party whose content and operation is reliable and which is available in accordance with agreed terms and conditions. In addition, the payment of services must be secure and the personal information of users must remain confidential. One prerequisite for a secure service is that it can be used only by those who have the right to use the service. The misrepresentation of users by external parties should be difficult in a secure electronic service. For customers to be offered secure services, information security should be a key part of the development of services and due attention should be paid to information security at all stages of service development.

This information security guide for electronic service providers will help service providers and developers ascertain how information security can be used to support the objectives of an electronic service. The guide will help in identifying the key issues that ought to be taken into account at the various stages of service development to make the service secure. In addition, the guide attempts with the aid of task lists, for example, to present effective solution models for the development of secure electronic services. The guide does not go deeply into individual technical solutions nor, for example, the requirements set by different standards.

The guide is aimed at companies that provide electronic services and at individuals who are responsible for service development, quality and security. The latter include, in particular, developers of business operations and services, project managers, and all who are responsible for information security. Readers of the information security guide do not, however, need a deep knowledge of information security or the related technology.

The guide has been divided into six segments, following the different stages of electronic service production. The guide covers significant information security issues connected with the different stages. These stages are presented in the figure below, and are discussed in more detail in the following chapters of the guide.



Implementing good information security demands goal-directed project management. The most significant policy lines in terms of information security are formulated when the service is planned. Without thorough planning, information security requirements will not cover the needs of the service, nor will it be possible to assess or develop appropriately the realised level of information security. Before planning begins, the service provider should prepare a project timetable, allocate the necessary resources and establish guiding principles for implementing the service. Resourcing should take into account, in addition to other measures and requirements, the demands set by information security, because otherwise many important issues vital for information security may fail to be realised due to lack of time and other resources.

1.1
Definition of information security

By the term information security is meant the administrative tasks and technical solutions employed to ensure the confidentiality and integrity of information, access to the information held by the electronic service, and the availability of the information, service or system.

• ***Confidentiality*** ensures that the information can only be used by individuals who have permission to do so. The information is not disclosed or otherwise made available for the use of third parties.

• ***By integrity*** is meant that the information used in the service is not changed when it is transferred or stored. Information whose integrity is secured remains as its owner intends it to be, and it is not changed our destroyed by hardware or software errors, natural events or unauthorised acts.

• ***Availability*** means that the information is available to those individuals who need the information and are authorised to use it.

The concepts of non-repudiation, authentication and access control are also often connected with information security.

• ***Non-repudiation*** means that it can be verified that a certain individual or party has sent or received certain information, and that the individual or party therefore cannot deny that they have sent or have received the information. Non-repudiation is a prerequisite for the implementation of many electronic services, such as business conducted on the internet.

• ***Authentication*** ensures that the parties are who they claim to be. Where individuals are concerned, the term identification is often used. For example, in e-commerce and official services as well as in communications between individuals it is often important to know for sure who the other party is and where the information originates.

• ***Access control*** is used to restrict the use of an electronic service only to those parts of the service that the customer is authorised to use. The objective of access control is partly to safeguard the confidential and integrity of information.

Information security and data protection are not synonyms, but they are closely related. Data protection cannot be guaranteed without good information security. By data protection is meant the protection of an individual's identity in connection with the handling of personal data. Personal data used in electronic services must be protected from unauthorised or damaging use. It is the electronic service provider's duty to ensure that data is protected, and this is an absolute prerequisite for the implementation of a secure electronic service.


2
◀
+ 0
9 WXYZ
8 TUV
* ▶
6 MNO
5 JKL
3 DEF
2 ABC
C

2
Service creation

The aim of this chapter is to present what the creation stage of a service should include and how information security factors can be taken into account already at the creation stage. This section discusses the information handled by the service, the content of the service and the surveying of users as well as the significance of external and internal information security requirements. In addition, the chapter considers alternative ways of producing a service as well as distribution channels for the development of a secure service.

Service creation and the development of an idea, in which the concept of the service originates, are often informal processes, situations or events. The creation stage focuses mainly on the question of whether there is a need for the service, how the service could be produced and whether sufficient users of the service can be found. The creation stage sets out guiding principles for information security, its implementation and its significance during the entire life cycle of the service. The most significant part of information security planning and specification, however, only takes place at the service planning stage.

Creation stage task list

1. Consider the kind of information that the service will handle.

2. Determine the typical users of the service (age, level of expertise).

3. Analyse the distribution channels suitable for implementing the idea.

4. Assess the scope of the organisation needed to produce the service as well as the required partners and service production methods.

5. Survey the legal provisions and other requirements relating to the service.

Creation stage questions:

How will the service be used?

Who will use the service?

What kind of equipment will be required for implementing and using the service?

What information and skills will a user of the service need in order to use the service efficiently and securely?

Will the service provider have sufficient resources or a suitable network to deliver the service?

2.1
Defining the information content and users of the service

The information to be used in the electronic service may in terms of its content be such that its protection is necessary e.g. for commercial or legal reasons. The information may be the users' personal data or otherwise sensitive information, for which reason its protection from external users or unauthorised changes is important. The information may also be valuable from a business standpoint, because it may provide, for example, a competitive advantage in the market, or the business idea of the service may be based on the dissemination of information for a fee to paying customers.

The information necessary for using the service and to be stored in the service must be identified at the creation stage, because the planning and development of the information security of the entire service is aimed at protecting this information. Such information has a different protection need, which must be reflected in the structure of the service to be implemented. The information's protection need can be determined through a classification of the information. The classification can at its simplest be a division into public and confidential information. In terms of information security it is also important to identify the information's location and information streams, because the protection methods to be used are different, for example, in information transfer and storage, even though encryption may be used in both. It is a good idea to attempt to classify information according to the kind of protection need assigned to it. A person register is created in connection with a number of electronic services.

By the term person register is meant a data set containing personal data which is processed partly or completely with the aid of automatic data processing or which is organised as a card index, list or in some corresponding way. As far as the application of the Personal Data Act is concerned, it is essential to define the purpose of the processing of personal data so that it is clear for which duties of the data controller the personal data is being processed. Personal data can be processed only for a certain specified purpose. Based on the specification, it can also be assessed which personal data are necessary for the purpose of the processing.

The following types of information are generally connected with electronic services:

- Customer or user information, such as names, addresses, e-mail addresses and credit card data.
- Service authentication information, such as passwords, encrypted forms of passwords, and certificates.
- Service production information, such as the configuration and definition files of web servers, operating systems, databases and applications.
- The service's information content, which may be provided free of charge or for a fee. In terms of free information, it is worth noting that this also needs protecting, at the very least so that it remains correct.
- Service maintenance and production information.

In the creation stage it is also necessary to evaluate the potential users of the service, because users' level of information technology know-how may vary significantly with respect to both service use and information security. Taking the service's target group into account is important, for example, in devising service log-in and user identification solutions. There is always good reason to be attentive to the usability, ease-of-use and user-friendliness of the service, but particularly when the service's target group are e.g. children, the elderly or special needs groups. A survey of service users is also significant in the later stages of service development, when users are instructed in using the service and when instruction is planned.

2.2
Internal and external information security requirements

Requirements relating to electronic service information security can come both from within an organisation and from external parties. By internal information security requirements is meant those operating practices dictated by an organisation's information security policy as well as the operating guidelines that affect the operation of the electronic service. By external requirements is meant information security measures dictated by the operating environment, such as legislation, standards, partners and information security threats.

This guide focuses particularly on information security issues relating to the provision of electronic services, taking into account service security demands arising from the needs of end-users. The guide also covers, however, an organisation's internal information security requirements, because an organisation's own information security is also a prerequisite for the implementation of a secure electronic service.

2.2.1
Internal requirements set by an organisation

An electronic service can be part of an organisation's wider service package. An electronic service must comply with the information security requirements set by the organisation for its own operations. Electronic service development should comply with the organisation's information security programme, policy and operating guidelines.

At the creation stage of an electronic service, any of the organisation's internal plans and guidelines that affect the information security of the service should be taken into account.
These are, for example:

- Business requirements and goals.
- Architecture, continuity and recovery plan requirements.
- The organisation's information security policy.
- Information security guidelines, operating practices and training.
- Operating models relating to information security monitoring and measurement.

2.2.2
External requirements set by the operating environment

Finland has no specific information security act that exhaustively prescribes the information security obligations and rights of organisations and individual computer users. Information security provisions are contained in several laws that are currently valid. In addition, information security is also covered in the national legislation of other countries. At the electronic service creation stage, it is necessary to specify the countries in which the service will be offered and to review the information security legislation of these countries.

Finnish legislation

This section considers the Finnish legislation relating to a service provider's information security.

• The objective of the Act on the Protection of Privacy in Electronic Communications 516/2004 is to ensure confidentiality and protection of privacy in electronic communications and to promote information security in electronic communications and the development of electronic communications services. The Act attempts to clarify rules governing the processing of confidential identification data and they are extended to the corporate or association subscriber. In addition, the objective of the Act is to clarify information security implementation options and provide guidelines for the use of cookies and the processing of location data. The Act is aimed at increasing the information security and data protection of electronic communications, and increasing users' confidence in it. Compliance with the Act and any provisions issued under it is supervised mainly by the Finnish Communications Regulatory Authority, while compliance with statutes relating to e.g. the processing of location data and direct marketing by means of automated systems are supervised by the Data Protection Ombudsman.

• The Personal Data Act 523/1999 defines the conditions on which personal data can be processed. The Act also prescribes requirements for the information security of systems that contain personal data, for example the data controller must carry out the technical and organisational measures necessary for securing personal data against unauthorised access, accidental or unlawful destruction, manipulation, disclosure and transfer, and other unlawful processing. Compliance with the Act is supervised by the Data Protection Ombudsman, who also issues directions and guidelines on the application of the Act.

• The Act on the Provision of Information Society Services 458/2002 prescribes on matters relating to the provision of information society services, particularly on electronic

commerce in the Europe Economic Area. The Act requires that service providers must make available to recipients of the service information about themselves and their activities as specified in the Act, must give guidelines and information about the service to recipients of the service before an electronic order is made, and must arrange, for the use of consumers, procedures by which possible errors in orders can be noticed and corrected in advance. Compliance with the Act is supervised by the Finnish Communications Regulatory Authority and the Consumer Ombudsman, taking into account the provisions of the Consumer Protection Act on the supervisory authority of the Consumer Ombudsman.

• The Act on Electronic Signatures 14/2003 prescribes on the provision of certificates and their use in electronic signatures and identification. Its purpose is to promote the use of electronic signatures, to establish their position and to increase trust in the provision and use of qualified certificates. Compliance with the Act is supervised mainly by the Finnish Communications Regulatory Authority, while compliance with the personal data provisions given in this Act is supervised by the Data Protection Ombudsman.

• The Act on Electronic Services and Communication in the Public Sector 13/2003 applies to public sector bodies, which must ensure an adequate level of information security both in their services to customers and in communication between each other. The Act applies to the initiating of administrative, judicial, prosecutional and enforcement matters and to the consideration and service of decisions of such matters by electronic means. The Act does not apply to preliminary investigations and police inquiries or to electronic services and communication in the Evangelical Lutheran Church of Finland. In information systems, parties must identify themselves using reliable methods. More detailed regulations, guidance and recommendations on the application of the Act are given by the National Archive Service and the Ministry of Finance.

• The Communications Market Act (393/2003) (quality requirements for communications networks and communications services) relates mainly to the general information security obligations laid down for telecommunications operators. The aim of the Communications Market Act is to ensure that communications networks and services are high quality, secure, inexpensive and fairly available. Compliance with the Act and any provisions issued under it is supervised by the Finnish Communications Regulatory Authority.

• The Act on the Openness of Government Activities (621/1999) prescribes on the right of access to official documents in the public domain. In order to create and realise good administrative practice, the authorities must see to the appropriate availability, usability, protection and integrity of documents and information systems as well as the information contained in them. Under the Act, a secret official document must not be shown or given to a third party or made available to a third party by means of a technical interface. The Act contains a comprehensive list of secret official documents.

• The Consumer Protection Act applies to offering, selling and other marketing of consumer goods and services by businesses to consumers. The Act comprehensively prescribes on marketing, adjustment and interpretation of terms of contract, consumer credit and consumer service contracts. Compliance with the Act is supervised by the Consumer Ombudsman.

The Acts and their content are not examined more deeply here, but already at the creation stage service developers should consider the kind of requirements and rights that the national legislation of different states sets for their service.

Other external requirements

At the service creation stage it is also worth identifying other possible external requirements. For example, when developing services for which a fee will be charged, due attention should be paid to the requirements of different means of payment and their operators. These include, among others, the credit card companies' Payment Card Industry Data Security Standard (PCI-DSS), which sets requirements for service log systems, authentication meth-

ods, data encryption and many other factors relating to information security. The standard also applies to parties who receive and process credit card payment data.

Electronic services are also associated with various value chains and networks in which several companies and private individuals participate in developing and providing the service. Networks are characterised by contracts between actors in which responsibilities and obligations should be determined also with respect to information security. Service-related cooperation agreements and agreement-related information security requirements are discussed in section 2.3.

Requirements, orders and recommendations can also be issued by official bodies, such as the Finnish Bankers' Association, the Financial Supervision Authority or the Finnish Communications Regulatory Authority. Service developers should therefore acquaint themselves with norms in their own field as well as with regulations relating to the planned service elsewhere than in the legislative sphere. Moreover, many information security standards can be useful during electronic service development work, and an organisation's own requirements may require compliance with these standards.

By standardisation is meant the drawing up of common operating practices. This helps service providers and consumers act in accordance with generally perceived good practice. In terms of information security, electronic services are linked to standards that direct an organisation's activities, standards that direct the technical realisation of the service and standards that increase consumer confidence.

The most important information security standards relating to an organisation's activities are the ISO standards. These cover information security as a whole, focusing on the administration of information security in the organisation. In addition, various frameworks prepared by official bodies and organisations (COBIT, ITIL, VAHTI) can be utilised in the administration of organisations' information security.

Standards directing the technical implementation of a service depend to a large extent on the distribution channels, hardware platforms and terminal devices used for producing the service. Moreover, technical solutions have their own standards, which also cover information security.

The level of an organisation's information security and the prevailing information security culture create the foundation for the information security of the new service. Consumer confidence is increased by various quality standards and by information security certificates that require compliance with certain standards (for example, ISO 27001).

Standards and various security-enhancing frameworks are discussed in more detail in the appendix to this guide.

2.2.3 Information security threats to an electronic service

Service providers must monitor their operating environment and the changes happening within it. An electronic service must answer threats arising in the operating environment.

The severity of information security threats may be different from the perspectives of the service provider and service user. Typical information security threats affect both the provider and users. Information security threats realised from the service provider's perspective might compromise the reputation of the electronic service as well as the service provider's reputation more widely. On the other hand, an electronic service's good information security may serve as a competitive advantage in the service market.

Typical information security threats:

- Malware (Trojan horses, viruses, worms, spyware, spam mailing programs).
- Phishing (falsifying a service, eavesdropping telecommunications, acquiring information through social means).
- Penetration of the electronic service (unauthorised use of information, staining the reputation of the service).
- Denial-of-service attacks (hijacking communications links, consuming resources, exploiting vulnerabilities).

Malware, such as viruses, is the most common information security threat to an electronic service. In the future, as intelligent viruses increase, the information security

threats caused by malware will grow further. Many attacks are already tailored to target certain organisations or services. Furthermore, communications eavesdropping, unauthorised use of information, and service blocking are information security threats that affect both users and service providers.

At the creation stage, the service provider should survey the information security threats and protection methods in collaboration with value network actors. Wide-scale and distributed denial-of-service attacks affect the functioning of the entire internet, so each electronic service must adhere to the principles of information security in its operations. Various forums, such as the Finnish Communications Regulatory Authority's CERT team, disseminate information on these principles and information security threats. Threat impacts, risk analyses and protection methods are discussed in more detail in sections 3.6 and 3.7.

2.3 Alternative ways of producing an electronic service

An assessment of factors affecting the information security of a service should consider the alternative ways of producing the service. An electronic service can be produced entirely within an organisation itself or it can be constructed from various components produced, for example, by subcontractors. When the service needs resources from outside the organisation, there is good reason to draw up a cooperation agreement that specifies the parties' responsibilities, obligations and information security requirements. Purchasing components of the service from outside does not eliminate the service provider's responsibility. If information security shortcomings are perceived in a service component purchased from outside, more often than not it is the electronic service provider who suffers the consequences, not the party from whom the service component was purchased.

Various options for producing a service are presented below.

Working alone

The service provider should invest particularly in project management, to ensure that information security is appropriately taken into account at all stages of the work and that the various measures are documented with the required precision.

Working alone, the service provider should survey their organisation's own information security expertise and if necessary acquire additional expertise for the organisation.

Purchasing the necessary components of the electronic service from other organisations

Components to be used in the electronic service can be purchased on a subcontracting basis. For example, the maintenance of servers required in the service can be purchased from outside one's own organisation. When purchasing components, information security requirements should be expressed when the contract is prepared. In terms of functions purchased from outside, the appropriateness of their information security should be checked as if they were from one's own organisation.

Network building

A value network is built around the service creator, who assembles the products or services supplied by different manufacturers and developers into one service configuration. The service provider coordinates the work of users and content providers.

When creating and planning the service, the value network must be clear, so that responsibilities and obligations for different parts of the service can be specified exactly. Presenting concrete information security requirements to all members of the value network at the contract stage is important.

2.3.1 Information security requirements to be specified in a contract made with outsiders

In the contract, the service provider should set out clear and concrete information security requirements, with which a subcontractor or other partner, such as a network service supplier, application developer and maintenance services supplier, must comply. The following list outlines various requirements that ought to be highlighted when entering into a contract.

Information security requirements with which a subcontractor or other partner must comply:

1. Operational and maintenance practices must be documented and made known to all employees who need them. In addition, the appropriateness of the above-mentioned practices should be checked by maintaining them regularly in a manner agreed and documented in advance.
2. Changes relating to the service must be performed and documented in accordance with a change management procedure agreed and documented in advance.
3. Risky job combinations connected with the operation and maintenance of network and systems and with the supervision of the practices mentioned above (for example a job in which the same person develops a program, tests it and finally put the program into production) should be identified and if necessary divided between different individuals.
4. The service provider should be able to supervise and check a service purchased as well as the practices, reports, documents and log files associated with the service (the right to audit).
5. Service resources and their utilisation rates should be monitored to ensure an adequate level of service. Safeguarding the performance of the network and systems requires that the service supplier also assesses future capacity requirements regularly in a manner agreed and documented in advance.
6. New information systems, hardware and software connected with the service, as well as new versions of existing systems, hardware and software, should be tested in accordance with instructions specified and documented in advance and should be approved before they are taken into use.
7. Critical service data must be backed up appropriately and the restoration of back-ups tested regularly in accordance with back-up and test procedures specified and documented in advance. In addition, the installation media of all software must be stored so that the software in question can be reinstalled at any time.
8. The network and systems must be monitored, operated and maintained so that the security and availability of the service can be appropriately guaranteed. This applies to both saved data and data that moves on the network.
9. For the exchange of information between organisations connected with the project, the parties should agree and document in advance operating principles, procedures and controls to safeguard the information's confidentiality, availability and integrity in connection with its transfer, regardless of the means of transfer.
10. The network's active hardware and servers must compile logs at least of maintenance and information security events agreed in advance. The logs should be stored securely for a period agreed and documented in advance. Ideally the network should have a centralised log server to which only a very restricted number of people have access. This enables any information security breaches to be studied.
11. Log data about service errors should also be collected. In addition, log data should be analysed and reacted to appropriately. Log files should be protected from unauthorised changes and unauthorised access.
12. To ensure service continuity, the service supplier must have continuity management processes and plans which are constantly maintained. Such plans should identify and document service-critical processes and infrastructure.
13. Statutory and other officially imposed requirements that apply to the service, together with contractual requirements, should be identified and documented. Changes in requirements should be monitored regularly.

2.4
Electronic service distribution channels

The selected electronic service distribution channels and the technology they require have a great influence on how the service's information security should be implemented and on the requirements set for it. The most common electronic service distribution channels are the internet, the mobile network and the digital television network. This section presents the advantages and disadvantages of these distribution channels from the standpoint of information security.

2.4.1
Internet

Electronic services are implemented as a rule via the internet because on the internet many kinds of services that extend beyond national frontiers can be built. Furthermore, the internet is a familiar operating environment for users

Advantages

- On the internet it is possible to build highly protected services with strong information security. On the internet are used numerous standards and technical solutions on which the service can be securely built.

- Internet communications works well, even though the root name servers or other key components of some networks are not in good working order.

Disadvantages

- The internet in structurally open, so particular attention must be paid to protecting telecommunications and possibly to instructing end-users.

- Malware (viruses, worms, advertising programs etc.) can cause undesirable events such as blocking the operation of services.

- The international dimension can prove to be challenging for the service. In offering services abroad, attention should be paid to possible restrictions imposed on the operation of the service by local laws.

- The wilful action of users, such as the exploitation of possible information security weaknesses, may have an adverse effect on the operation of the service and on its users.

- Internet services are vulnerable to phishing. Phishing relates not only to the banks' internet services, it is also to be found in various organisations, e-mail services and virtual worlds.

2.4.2
The mobile network and other data transfer paths supported by mobile devices

The mobile network has developed from a conveyor of speech and text into a respectable channel for the delivery of other electronic services, too. There are many users of mobile devices, and consumers are accustomed to using the network. A number of terminal devices support several other data transfer methods, such as Bluetooth[1], infrared and WLAN[2], using which it is possible to develop very local services.

Advantages

- Current networks are reasonably well insulated and protected.
- Terminal devices are developing rapidly and they can already access many different distribution channels and networks that allow the use of various information security solutions.
- Short-range networks enable the creation of very local networks.

Disadvantages

- With the rapid development of the field, information security functions used in a service can quickly become obsolete.
- Malware can cause undesirable events on users' terminal devices and the service provider's servers.
- The information security of Bluetooth and infrared connections, particularly on spontaneous networks, is limited. For example, arranging secure log-ins on a spontaneous network can be difficult.
- All terminal devices do not support the more advanced WLAN connection encryption methods. There are also configurations in use that have not yet been standardised.
- As devices become more complex and the number of interfaces grows, compatibility may be a problem. For information security this means maintaining several different versions of the service, which requires the allocation of sufficient resources. On the other hand, open interfaces will increase the amount of malware familiar from the internet world.

1. A short-range (10 m) wireless data transmission technology.
2. Wireless Local Area Network.

2.4.3
Digital television network

The data stream in the digital television network consists for the present mainly of the transmission of sound and pictures using the DVB standard over a closed network from sender to recipient. Today, in addition to sound and pictures, data services can also be delivered. Moreover, cable television companies offer interactive additional services, whose data transmission is based on interactive data transmission technology under the IP standard.

Advantages

- The transmission network operator and distributor control a unidirectional programme stream packaged by the TV company, as a result of which the information security threats to transmissions (TV programmes) are under control.

- In interactive services the open MHP standard supports encryption technologies and public key methods.

Disadvantages

- Standards subject to strong development slow down the creation of services and the establishment of related protection methods.

- In terms of information security, interactive services are the subarea most vulnerable to risk. Threats as far as the data transmission channel is concerned are similar to those associated with internet information security threats.

- Data transmitted between the consumer and the service in connection with interactive services moves via the internet service provider to servers, so the information security threats are often distributed over a wider area.

Digital television in Finland is based on DVB standards. Terrestrial networks use the DVB-T standard, cable networks use DVB-C and satellite broadcasts are based on the DVB-S standard. Mobile terminal devices can utilise the DVB-H standard, which is based on DVB-T. The above standards differ from each other chiefly in the modulation techniques optimised for the different transfer paths. Terminal devices differ correspondingly.

Notes


MasterCard

3
Planning the service

This chapter focuses on key measures that promote information security at the planning stage, including describing the service's business and operating process, identifying internal and external connections, making an information security and risk survey, and deciding and documenting information security requirements and settings. One outcome of the planning stage is the setting for the service of adequate information security requirements that will be enforced at the implementation stage.

The planning of the electronic service is the most important stage in terms of the information security of the service. The decisions made at this stage will influence significantly whether the service will be reliable from the user's perspective. In addition, planning stage decisions have an impact on the maintenance and development of information security. Experience has shown that at the planning stage of services sufficient attention is not yet being paid to information security, and that service planning does not necessarily involve those individuals who are responsible for and have expertise in information security.

Planning stage task list

1. Include information security, and information security resourcing, as part of the different stages of planning.
2. Describe the business and operating processes connected with the service.
3. Describe the service's internal connections and its connections with different systems.
4. Identify the devices with which the service will or can be used.
5. Survey the information security risks and the present situation (risk analysis).
6. Describe the service's information security requirements, which will be implemented at the development stage.

At the planning stage, the following questions should be asked:

What kind of functions will be included in the electronic service and its use? Will customers have to pay to use the service? Will use of the service require the identification of users?

How are the different stages of the service linked to each other? How will the service as a whole be produced?

What kind of functions will be included in the service configuration? What information systems will be used to produce the service?

Are the information security requirements in line with the commercial objectives?

What kind of information will be collected in the service? Is all the information to be collected necessary, and is it legal to collect it? How will the information be processed, transferred and stored?

In planning the service, will the organisation's information security expertise be utilised in the best possible way?

Is the planning team aware of the information security risks? How are they to be managed?

3.1
Specification of processes

Effective information security is part of an organisation's operating processes. Information security should also be part of the electronic service's service process. For this reason, a thorough knowledge of operating processes and models forms the basis of information security planning, and the specification of information security should be done in conjunction with the surveying and description of business and operating processes. This is often difficult when the service is only at the planning stage. Making such a survey is important, however, because with process surveying and recognised control points[3] it is easier to consider the risks associated with using the service and to plan the information security solutions required for the implementation of the service.

One way of specifying processes is to prepare use-case scenarios. By the term use-case scenarios is meant examples, based on reality, of using the service in different ways and the actions connected with these. Ordinarily, use-case scenarios include preliminary descriptions of the service functions developed during user-interface planning.

The specification of processes takes place through modelling, which results in descriptions of business and operating processes. Operating processes can be divided into processes connected with use and the company's internal processes connected with producing and maintaining the service. Process descriptions must take into account both the organisation's internal functions as well as external actors connected with processes, for example subcontractors and their service-related functions. In addition, process descriptions should outline measures to ensure the information security of each process at different stages. Such measures include, for example, identifying users, encrypting information, back-up copying of systems and regular monitoring of log files. All the controls by which effective information security is ensured will not necessarily be identified at the early stages of service planning. These control descriptions will be supplemented later, for example through information obtained from risk analyses.

3 By control point is meant a point in the process, for example the interface between two systems, where the integrity and confidentiality of information can be checked.

The specification and modelling of processes:

- Go through in detail all possible events and ways of use during the production and use of the service.
- Identify and describe the cash and data streams connected with the service.
- Assign the parties, systems and functions connected with the service.
- Systematically specify and document service processes and related issues.
- Survey and describe service risk points and process controls as far as this is possible at the planning stage.

Process descriptions help guide discussion during risk mapping and when planning control measures. When processes are being described, it is good to involve an information security expert, who will help draw attention to issues essential to information security.

3.2
Identifying and documenting the service's internal and external connections

At the planning stage, the ways by which the service will be delivered to the customer should be identified. Distribution channels and their advantages and disadvantages were considered at the creation stage. After the selection of the distribution channels, the next step is to plan how the service will be used through the distribution channels and what kind of internal and external system connections will be needed to implement the service.

Distribution channels selected at the planning stage are examined more deeply so that data transfer between the various connections needed for implementing the service can be studied at the protocol level. Information security threats connected with the transfer of data can be controlled with various data transfer protocols. This means, among other things, always using when necessary encrypted data transfer protocols that secure the delivery of data in the service's internal and external connections. It is essential to understand that different data transfer methods offer different possibilities for encrypting traffic, reliably identifying the origin and destination of traffic, and managing traffic capacity.

There are hundreds of different protocols and data transfer methods associated with electronic services.

Electronic service planning should take into account consumers' and the service's requirements for the reliability of data transfer. If an analysis of the service's internal and external connections is not carried out, then it is possible that the system will be implemented using insecure protocols, even though the service and the data being transferred would require better protection. The use of such protocols is common because they are easy to use and they have been utilised for a long time in various systems and services. Possibly only later is it noticed that the implementation does not fulfil the data's protection needs, at which time changing the service is difficult and expensive.

3.2.1
Interfaces and interdependencies between systems

Many systems and services are dependent on other systems that will either produce or transmit data relating to the new service under development. Identifying and reviewing these systems is useful, particularly for ensuring the usability of the service and the reliability of data.

When high demands are set for the usability of a new service, and if this service is dependent on other systems, the usability of the other systems and the actions taken ensure this usability must be at least on the same level as the information security requirements of the service being implemented.

If the new service receives data from other systems or transmits data to other systems, data transfer between systems must be protected appropriately. Particularly in situations where data accuracy and confidentiality is especially important for the service, data transfer must be protected, for example, with encryption and origin of data checked using various certificates.

Examples of information protection:

In services implemented with web services technology, sender authenticity and data confidentiality can be ensured by using an implementation according to the Web Services Security (WAS security) specification. At a minimum, identification based on passwords must be used, in which case traffic encryption to secure the passwords and other transferred information is also recommended. Encryption is most practical to implement by selecting for use encryption protocols and implementations such SSH, SFTP, HTTPS or SNMP Version 3.

3.3
Ways of accessing the service

Connections between the service and its users, and the implementation of these connections, are naturally influenced by the way the service is accessed, such as the hardware or application by which customers or other users connect to and use the service. The choice of access method also influences the number of potential users of the new service. For example, nearly every operating system has a browser, but a separate client program may have to be delivered in some way to new users of the service.

• Client program. By using a separate client program, many information security problems, such as securing the connection and identifying users, can be removed. However, traffic protection and user identification methods, for example, have to be specifically built for each client program in turn, which means that the level of information security of the implementation may vary significantly. Moreover, customers cannot access the service immediately; they must first expend some effort installing the program and possibly adjusting its settings. Accessing the service may not be possible if customers lack operating system level rights to install applications on the devices they use.

• Browser. Browser-based services are accessible from nearly all terminal devices that connect to the internet. Use of the service is therefore not tied to a certain location or item of equipment. In relation to the information security of browser-accessible services, particular attention should be paid to telecommunications between the browser and the application server as well as activity between the browser and the rest of the system, such as data saved by the browser. The planning of a browser-based service should examine how the service functions on different browsers. All browsers do not, for example, display web pages in the same way.

• Terminal device. On mobile devices it is possible to access electronic services by, for example, text message, a

separate client application or with a browser via an internet connection. From the service provider's perspective, the challenges associated with mobile devices are the large number of software versions, poor program maintenance (virus protection, updating of system components and back-up copying) and the open interfaces of new operating systems, which increase information security threats, for example. Service providers can prepare for the challenges posed by terminal devices by improving the reliability of their own service so that it supports various terminal devices and their functional characteristics.

3.4
User identification

As the number of electronic services grows, the importance of security and the reliable authentication of identity in electronic services and communication grows. User identification is based on things that the user knows (for example, a password), the user possesses (for example, a mobile phone, mobile certificate or smart card) or on something that is specific to the user (for example, a fingerprint). The reliability of user identification depends on the identification method used.

The necessity of identifying users should be evaluated with respect to the service process as well as the confidentiality of the information used. Commonly the reliable identification of users requires registration as a user of the service (user ID and password) and possibly a personal, organisation or mobile digital certificate. Strong identification of users is not always necessary. Strong identification would be required in services where confidential information is processed, such as sensitive information under the Personal Data Act or an organisation's secret data, or when a user can do things that are financially or legally significant. On services where strong identification is not used, it is recommended that users be advised not to transmit confidential information via the service in question.

Methods used in strong user identification include:

- User ID and password together with a changing or one-time password.
- User ID and password together with a telephone call.
- Certificate chip card or mobile certificate together with a PIN code.
- Biometric identification.
- Certificate chip card together with biometric identification.

3.4.1
Electronic signature

An electronic signature is used for the same purposes as a handwritten signature, i.e. to certify the identity of the signature's author in connection with some other information or declaration of intent. Advanced electronic signatures can be used to certify the integrity and origin of information transferred electronically. Methods used to make an electronic signature can be used, for example, to encrypt confidential information.

As its name suggests, an electronic signature is a signature in an electronic form, for example a name written at the end of an e-mail. A digital signature is an electronic signature that has been produced using some encryption method. Under the Act on Electronic Signatures, a signature based on a qualified certificate is always legally valid. However, electronic signatures based on other methods can also be completely valid, so service providers can choose the signature method to be used in their service. A court of law will ultimately assess their validity. Qualified certificates are granted in Finland by the Population Register Centre.

An electronic signature made with a qualified certificate is executed using the public key method (Public Key Infrastructure, PKI). For example, an e-mail program formulates from a message a digital signature encrypted with the signatory's private key. In simple terms, the message recipient, i.e. a party who trusts in the certificate, opens the signature using the sender's public key. The program carries out the identification and comparison. If the sent and received information match, then the signature is genuine.

Notes

3.5
Electronic payment

Electronic payment methods should be considered at the planning stage, so that the most secure and most flexible payment method for the operation of the service can be selected. Electronic payment methods can be divided based on their nature into electronic bank transfer, credit transfer and electronic money as well as mobile payment. In respect of information security measures connected with electronic payment, the service provider must tell the user of the service about the risks associated with payment, and about the operations for whose information security the service provider is or is not responsible.

3.5.1
Internet bank - Electronic bank transfer

Electronic bank transfer is an online payment service offered by banks. Bank payment services answer the real-time requirement set by e-commerce, because in an online payment purchases are debited from the customer's bank account in connection with the purchase. Online payment can be said to be secure due to the SSL encryption[4] and strong identification used by Finnish banks, but there are also certain information security threats connected with online payment.

Information security threats connected with electronic bank transfer:

Threat	Protection
Disclosing user ID and password	Typically online banks use a changing password, so disclosing a password does not result in any direct danger. The probability of a risk being realised is reduced if the user acts in accordance with instructions issued by the banks. The browser cache should be emptied after the service is used and information security updates should be installed regularly.
Phishing	In phishing, an attempt is made to mislead users into revealing one or more of their changing identity numbers or other important identification data, which are then misused, for example, to withdraw money from the customer's account. The training of users plays a significant role in preventing phishing[5].
Misuse of an account due to data trespass, for example	Installation of information security updates on service-related servers and users' terminal devices immediately after publication (banks' internal process).

4 Secure Sockets Layer. Telecommunications encryption protocol.
5 By the term phishing is meant an attempt to fraudulently acquire information, for example passwords and usernames, from the owner of the information by using false or erroneous e-mail messages or websites.

3.5.2
Credit card – Credit transfer

Credit card payment is currently the internationally most important electronic payment method and, for the time being, the only one that enables goods purchased in different foreign currencies to be paid for electronically.

Information security threats connected with credit transfer:

Threat	Protection
Losing the credit card	No information other than that appearing on the credit card is needed for the card to be misused. If the credit card company is informed of the disappearance of the card in good time, the responsibility for misuse is transferred away from the credit card holder. The credit card companies have drawn up various information security maintenance guidelines and standards (PCI-DSS[6]), with which providers of network services must comply. Restrictions are imposed, for example, on the saving of information on credit cards, such that all information must not be saved (even encrypted).
Disclosing credit card information	In electronic payments paid with a credit card, attention must be paid to ensuring that traffic between the internet browser and the web server is encrypted (SSL or TSL[7]), whereby only the recipient is able to decrypt the data. The service provider must ensure that prohibited or unnecessary credit card information is not saved, for example, in an application database or in application and telecommunications logs.
Authentication of buyer fails	In electronic payment transactions the parties are identified with digital certificates. The certificates are issued by, among others, the credit card companies. When a certificate is used in a purchase, the seller can be reasonably certain that the cardholder has an agreement with the card issuer. Similarly, the cardholder can be confident that the seller has made an agreement with the card company about the acceptance of payment cards.
Changing information	Telecommunications is encrypted and the sender signs the information sent with a digital signature. This procedure detects if the information sent has been changed during its transmission.

6 Payment Card Industry Data Security Standard
7Transport Layer Security. Telecommunications encryption protocol.

3.5.3
Electronic money – micropayment

By micropayment and electronic money is meant the payment of small amounts over a network. Typical features of electronic money are electronic wallet software, real-time checking and user anonymity. Electronic money can be bought from a service provider and it is saved in the user's electronic wallet. A recipient of electronic money certifies the payment transaction and at the same time cancels the virtual coins in the user's wallet. When the recipient of the money has certified the authenticity of the money, the product is delivered to the customer. After this a third party (the service provider) transfers real money to the seller's account.

ECash and PayPal services are examples of electronic money services. Electronic money also encompasses smartcards on which electronic money is saved. A standard system for this has not been available. Different countries and market areas each have their own ways of implementing micropayment. Complex and multiple overlapping payment systems usually increase information security vulnerabilities and make the implementation of services more difficult.

Information security threats connected with electronic money:

Threat	Protection
Forging, copying and re-using the money	The threat can be reduced by continuous development of software. Every electronic money unit (virtual coin) is furnished with a digital identifier, the purpose of which is to ensure that the coin cannot be forged or re-used. The service developer should, in the planning stage, weigh up the information security features and opportunities for misuse of different implementations and choose the most suitable payment method.
Misuse of electronic money due to data trespass, for example	The service provider's software and information security programs must be kept up to date.
Losing the money	The software used in payment must give appropriate protection, for example with password and data encryption.

3.5.4
Mobile payment

Mobile payment solutions can also be used in the billing of electronic services. The solutions generally in use are text message payment and payment based on telephone calls. Billing can tale place via different channels. Telecom operators can bill for use of the electronic service in connection with the telephone bill or with a separate bill. Banks and credit institutions have, on the other hand, drawn up various billing practices in connection with credit card billing. Such operating practices are agreed separately with the service provider and the operator responsible for billing.

Information security threats connected with mobile payment:

Threat	Protection
The dependence in terms of billing on the telecom operator or bank	The threat can be reduced by offering various payment options. Billing agreements can be made with a number of operators.
Delays in settlement of payments	The idea is to minimise the number of intermediaries who process billing information.
Unauthorised use of means of payment (telephone)	The user should look after, for example, the telephone as a means of payment with same care as any other means of payment. The telephone should be protected with a password and a balance limit set, if this is considered necessary. The service provider should offer the said protection options and inform users about them.
Losing the money	The software used in payment must give appropriate protection, for example with password and data encryption.

3.6
Making a survey of information security and risks

In connection with electronic service planning it is good to conduct a survey of information security risks. The survey should take into account the information security risks from the implementation and use standpoint and from the perspective of the service provider's organisation. The aim of information security and risk surveys is to identify significant information security threats connected with the electronic service as well as the service provider's current capabilities for providing a secure service. In connection with electronic service planning, insufficient emphasis is generally placed on the organisation's own information security principles. The service provider should be aware, however, that information security must be on an appropriate level throughout the entire organisation to ensure that the electronic service itself is secure.

The surveying of information security risks utilises the descriptions made earlier of service implementation processes, internal and external connections, the information to be used in the service, and the ways that the service will be used. One objective of surveying the information security risks is also to classify the risks and to set them in order of importance. It is not necessary to protect against all of the risks in the best possible way, because this is not always appropriate or financially sensible. The surveys are used to identify the risks that are significant for the electronic service and to find means of protecting against them.

3.6.1
Surveying the risks of a new service

The objective of surveying the information security risks is to gain an overall picture of the risks relating to the provision of the electronic service.

A risk survey gives a picture of:

- Threats and risks
- The consequences of risks
- The current level of information security
- The significance of risks and their order of importance
- The measures necessary to manage the risks

Different tools exist for the surveying of information security risks, such as tables forming the basis of risk maps, series of questions for the surveying of risks, and various lists of known vulnerabilities and information security holes, whose potential threat to the electronic service must be assessed. The surveying of the new electronic service's information security risks is achieved through various group meetings and interviews. These are utilised to survey the information security threats connected with the electronic service. The meetings will help identify the risk and control points of business processes, the information security threats of service interfaces, and the threats arising from the organisation's resources. Ordinarily, the group meetings are attended by individuals responsible for the organisation's business operations and by technical experts. In addition, a lawyer and external consultants, for example, may participate in the group. The outcome is a list of the risks directed at the service as well as the identifiable control shortcomings. The risk survey results can also lead to changes in service and business processes or in the technical implementation of the future system. It is also possible to test the electronic service's information security risks and the standard of the technical implementation using various technical testing approaches, such as vulnerability testing. This is, however, not possible until the implementation stage of the service, when there is something concrete to test.

The leader of the risk survey group meeting may stimulate discussion by presenting various questions, such as:

- What takes place technically at the particular stage of the process?
- What happens if a certain message does not reach its recipient?
- Is the accuracy and integrity of information checked at a certain stage of the service, and using which protocol is the information transferred?
- How will a service user act in a certain situation?
- How can a service user unintentionally do some thing wrong?
- Have you thought of the possibility where...? What would happen if...?

3.6.2
Surveying an organisation's general risks

The objective of organisation-level risk surveys is to obtain a general impression of the operational risks of the organisation that arise, among other things, from information systems, the nature of the information held in them, and the people who use them. Ordinarily, some international information security standard or framework is used as benchmark for risk surveys. Examples of these are the ISO 17799 and ISO 27001 standards and the COBIT[8] and ITIL[9] frameworks, according to which information security management processes can be developed or audited. Generally, however, they are not used to uncover the risks and control shortcomings connected with the specific service in question. The results are more general in nature and relate to the whole, or part, of the organisation. For the new service to be secure, and also to remain so, organisation-level issues such as change management, user rights management and continuity planning must be in good shape. Information security standards and frameworks are discussed in the appendix to this guide.

An organisation's information security surveys should cover:

- An evaluation of current information security practices.
- The quality level of processes centrally connected with information security and their application in practice.
- A survey of the current state of network and system security.
- An evaluation of the security of network applications to be used in the electronic service.
- An evaluation of the management's and employees' information security expertise.
- An evaluation of the level of information security training.

The scope of the information security surveys is influenced chiefly by the level of precision desired in terms of results. Small-scale surveys will reveal the general information security risks and the level of the means used to protect against them. The information security survey findings are typically compiled into a memorandum which identifies the most important risk areas as well as the measures currently being used to protect against the risks. If necessary, corresponding information security surveys should also be conducted in subcontractors' organisations.

3.7
Specification of an electronic service's information security requirements and solutions, and protection from threats

Only after the process descriptions and the information security risk surveys are completed can the planning and specification of the electronic service's information security requirements begin. Their purpose is to remove the threats noted in the surveys or to minimise their probability and their effects.

The service's information security requirements are specified in practice on the basis of process descriptions of the operation of the electronic service, the information content to be used in the service, and interviews conducted with key individuals connected with the service. The specification adjusts the results of the risk analysis, while the requirements set for information security are updated after the specification of the service's functionalities. The information security requirements should be approved at the same time as the other requirements, before the information security solutions are specified. The information security requirements must accord with the organisation's information security policy and prevailing information security guidelines.

Based on the information security requirements, a review is made of solutions suitable for implementing the electronic service's information security. A secure service is obtained by specifying, in respect of the use of the service, appropriate information settings for the telecommunications network, the hardware to be used, and applications. In addition, the service must manage users' identities as well as their actions within the service. Information security experts can carry out a risk analysis and an information security audit of the future service on the basis of documentation, when the necessary documents are ready. This is also an advisable way to supplement the risk surveys and to ensure that the new service

8 Control Objectives for Information and related Technology. A framework for the organisation and management of IT functions.
9 IT Infrastructure Library. A set of best practices for the provision of IT functions.

has adequate information security before starting the construction of the service.

3.7.1
Protection of information to be used in the service

Service information is usually stored in a centralised database or in various files maintained but the service provider. In some cases, information can also be stored on the user's own terminal device. In such situations, the service provider can influence the protection of information only by communicating the possible risks and by guiding users to protect their own terminal devices appropriately. If separate client software is used to access the service, the service provider also has the option of influencing the protection of information on the customer's equipment. The means of protection presented below are aimed as a rule at protecting the information managed by the service provider.

Means of protecting information:

- By restricting access rights, information is made available only to those individuals who are entitled to process the information. Generally it is justified to use various roles, such as service users, content providers and service maintainers as well as maintainers of the databases and operating systems that act as the platform for the service.
- From a network technology perspective, the information can be protected by separating the service's different parts and information from each other. Users should have access rights only to the front servers that act as various channels into the service. Hardware maintenance should ideally be done from its own separate maintenance network.
- Firewalls can be used, for example, to prevent access via the internet to a device where the actual information needed in the service is kept. Firewalls are recommended for isolating the service from public networks and from the networks of service providers and partners.
- Data encryption is often justified during both data transfer and data storage. In this way the confidentiality and integrity of information is secured.

3.7.2
Specification of server and application information security settings

Irrespective of the selected distribution channel, the provision of services requires various kinds of servers, such as channel servers, application servers and database servers, which need an operating system in order to work. A number of services also have other network technology components, such as routers and firewalls. Documented information security requirements must be prepared for all operating systems and hardware connected with providing the service. In terms of externally purchased functions necessary to provide the service, information security requirements should be reviewed in detail and the requirements recorded in the service contract. Externally acquired equipment and services should be evaluated and audited regularly. The right to audit should also be stated in the contract.

Systems' information security requirements, which are often also called hardening guidelines, should take at least the following issues into account:

- The specification of the system services required in the electronic service and which will be installed on a server, and the removal of unnecessary services from use.
- Password requirements (minimum length, expiry time, history, complexity and minimum validity period).
∑ File rights, in the Unix system for example: SUID and SGID as well as minimising of the number of world-writable files.
- Log settings (What is written to the log? Where is the log written and where is it transferred to? How long will the log be kept? Who has access to the logs?) Special attention should be paid to how maintenance personnel are prevented from changing log data. In practice, a separate log server is always required for this.
- System maintenance IDs (individual), which are personal. Group IDs should not be used.
- The making of system and information security updates and the management of the rights necessary for these.
- Windows operating system register rights and changes.

Assistance in specifying systems' information security settings is available from the internet, for example from the Center for Internet Security website, from companies expert in auditing information systems, and possibly also from the information security experts in one's own organisation.

3.7.3
Information security of hardware to be used

In respect of information security, the choice of hardware platform is influenced by the information security requirements that have been set for the operation of the service. In terms of the hardware, the following issues should be considered:

- What kind of hardware configuration will be acquired? Complex hardware platforms can be susceptible to outages and other faults. Technology that has proved itself to be good in practice will most probably guarantee the trouble-free operation of the service.

- From where will the equipment be acquired? Equipment can be purchased outright, it can be leased, or it can be purchased as a service from an equipment manufacturer, for example. The various options should be evaluated on the basis of the requirements set for the service. With respect to equipment that is leased or purchased as a service, it is worth ensuring that the supplier will adhere to the information security operating practices outlined in a service level agreement and, if necessary, that an information security audit of the supplier can be performed.

- Where will the equipment be kept? The physical storage of the equipment requires, in terms of information security, that the premises be adequately protected, for example from water damage. If the equipment is purchased as a service from a supplier, a separate service level agreement (SLA) should be agreed on the storage and monitoring of the equipment.

- How have the physical components been certified? For example, a number of network cards can be used to implement the same network connection or several physical disks used to implement one logical disk.

3.7.4
Network-level protection

The technical means of protecting the service depend on the selected distribution channels. The encryption of all data transferred in all distribution channels is one of the best and most reliable protection options. Particularly in terms of mobile devices, the use of encryption can be restricted by the technology and capacity of the equipment. Encryption is easiest to arrange by using known encryption protocols and implementations (such as SSH and HTTPS).

Network-level protection can also be improved by isolating parts of the service from each other and establishing the actual service as separate entity. This requires the service to be ring-fenced from other services and the network using firewalls and Virtual LAN (VLAN) networks. System components management, monitoring and data checking are worth separating into their own network and the provision of the service itself into another network. In this way, most hardware components will have many network interfaces. Such components must route traffic between different networks (excluding the equipment intended for routing).

3.7.5
Management of users connected to the service

The users of the electronic service comprise the customers and the service organisation personnel who maintain the service. Management of the user rights of all users is one of the most important issues in terms of the service's information security. Various applications have been created for the management of information system user rights and user identities, and these applications can be utilised in managing the users of companies' internal services.

User management applications also have their place in electronic services offered to consumers. A suitable management system should be selected according to the service requirements by comparing the technology features of different solutions. There are certain technical features that a good identity management system should have:

- The system should support different authentication methods, such as certificates, smartcards and biometric

identification. For passwords and other authentication methods it should be possible to set restrictions that fulfil the organisation's and users' requirements.

- The system should be able to read authentication and authorisation data from different directories, such as databanks or text files, and be able if necessary to fetch authorisation data from external systems. It should be possible for the authentication and authorisation data in the directories to be normalised and presented as one, and for them to be managed centrally. In the system it should also be able to decentralise the management of rights.

- The system must allow the implementation of various access restrictions. For example, to some documents or systems it may be necessary to permit access to users identified, for example, with a separate electronic identifier or to permit access to some resources only at a certain time of day or from certain IP addresses or certain terminal devices, the identification of which can be based, perhaps, on an A-subscriber identifier[10] or an IMEI code.

- The system must cope with errors, it must operate efficiently as the number of visitors grows, using load balancing for example, and allow encryption of data transferred between all system components.

- Users should be offered the possibility of managing their own information. Independent management of information reduces the service provider's information management measures and gives users better opportunities to check and maintain the accuracy of their own information.

- Legislative statutes governing the protection of privacy and information security must be taken into account in the system to be acquired. This is particularly important with respect to software acquired from abroad.

3.7.6
Checking user input data

One of the most common information security weaknesses of electronic services is inadequate checking of texts written into the electronic service by users (i.e. user input data). Users can mistakenly or intentionally feed into the system "invalid parameters", for example in the fields of a web form. If the system does not check what the user puts in, and removes invalid characters, the user may succeed in changing data contained in the system that the user is not authorised to change, and at worst may succeed in cracking the system itself.

At the planning stage, a review should be made of the methods available for communication between the user and the system, and what data can be fed into the system via these methods. In terms of input data, the service provider should specify the characters required to access the service. For example, in the name field, that no characters other than letters are required and that the number of characters is restricted.

A still better way is to specify the permitted characters and to remove all others, instead of trying to list all the non-permitted characters and block them.

In general, the following characters are unsafe in terms of information security and they should be removed from users' input data:

- | (pipe)
- & (ampersand)
- ; (semicolon)
- $ (dollar sign)
- % (percent sign)
- @ (at sign)
- ' (apostrophe)
- " (quotation marks)
- \' (backslash escape character)
- \" (backslash quote escape character)
- <> (chevron brackets)
- () (brackets)
- + (plus sign)
- CR (Carriage return, ASCII 0x0d)
- LF (Line feed, ASCII 0x0a)
- , (comma)
- \ (backslash)

10 DTMF signal at the beginning of calls that discloses the subscriber identity.

3.7.7
Log settings

In connection with system planning, the following issues should also be considered: what log files should the system compile, where should these files be saved, what information should be included in the log data, and what should be done with the log data.

Logs are compiled on very different levels in electronic services. Often an application keeps a log of the use of application, the actions executed, and log-ins. The operating system, database, web server, firewalls and other system components keep their own logs.

Logs can and should be compiled for operational purposes.

- Application or network traffic raw data is often needed to solve problems. It is not necessarily worth collecting these data continuously, because the volume of data is often large.

- Operating system and database logs are necessary, for example, to monitor the actions executed by applications and maintenance staff, and to investigate cases of possible misuse.

- Log files from firewalls and intrusion prevention systems can be used to monitor external threats such as gate and vulnerability scanning.

- Reconciliation, and similar, logs are necessary to ensure the accuracy of various system events.

When specifying log settings, the service provider should also consider, in addition to various use cases, the protection of log files, because only those people whose job it is to monitor the systems should be allowed to access log files. In general, the use of a centralised log server is recommended. Log files should not collect unnecessary data, because they complicate the interpretation of the logs and waste space in the file system. Legislation places its own restrictions and obligations on the content and processing of log files, for example in terms of identifiers and other identification data as well as personal data of a sensitive nature. These restrictions and obligations to protect data must be recognised and taken into account in planning the service.

3.7.8
Protecting against information security threats

The information security threats connected with the electronic service are surveyed at the creation stage. Protecting against these threats requires more concrete measures both at the service planning stage and the construction stage. Protection is based particularly on identifying the various risks and control shortcomings.
Protection against malware, which cause events in the service without the owners' consent, is achieved by adding in connection with the service a mechanism, such as virus protection, e-mail filtering or an intrusion prevention system, that removes malware detected in telecommunications. Service users should be told about the kinds of events that malware can cause in the service, so that users are able to act in the proper way in these situations.

Many different methods are employed to acquire information through phishing. The service provider and the user must be aware of various situations, such as e-mail messages that urge users to log in to a service that looks like the real service but in reality has been forged, or obtaining information by social means, for example by promising services in return for the disclosure of information. Phishing can be prevented by personalising the electronic service so that users know that they are in the right service. Users can be given the opportunity, for example, to easily add to the home page of the service a background picture, or similar feature, of their choice. User training and information is of particular importance, however.

Data eavesdropping can be protected against by encrypting the transfer of data. The selection of encryption methods is influenced by the changing of encryption keys, the suitable encryption components and the terminal devices used.

Service penetration and information misuse can be protected against by suitably restricting service access rights for each user, and through the secure configuration and maintenance of systems. In addition, the information used in the service should be saved and backed

up so that the service can be restored in situations where an intruder has, for example, destroyed or changed system functions or information. Clear agreements between the different actors involved also pay a role in reducing the misuse of information.

Protecting against denial-of-service attacks is a challenging task. Preventive protection measures include close observation of the environment as well as monitoring discussion of vulnerabilities to ensure that information security holes in the electronic service can be closed as quickly as possible after detection. Intrusion detection systems are a means of protection that monitors service traffic and saves service events for later examination. As well as monitoring traffic, the service provider can build a backup system, which can help reduce the disruption caused to customers from a denial-of-service attack. Otherwise, protecting against denial-of-service attacks generally requires cooperation with operators. However, the risk can also be reduced by the system settings, for example in routers and at the kernel level of operating systems, as well as by removing unnecessary system services.

3.8
Estimation of information security costs

Information security costs can be roughly estimated on the basis of information accumulated earlier at the creation and planning stages. Information security requirements together with development and testing plans serve as a basis for cost estimates. The more precisely the organisation can specify the information security needs, the more precisely information security costs can be estimated. A cost-benefit analysis of information security measures can be performed if a "price ticket" can be determined for the realisation of risks based on the probability and impact of risks. The cost of protection measures should be lower than the cost caused by the realisation of risks, unless there is some compulsory basis for the protection measures, such as the requirements of legislation.

The financial objective of information security activity is to reduce the losses arising to operations from the realisation of risks. For many services, information security also has a significant impact on the use and popularity of the service and thereby on cashflow arising from the service.

Information security expenses can be roughly divided into variable and fixed costs, and risk provisions:

- Variable expenses are development investments (consultancy work, investments in information security solutions).

- Fixed expenses are the costs of information security activity of a permanent nature (salaries of own personnel, licence costs, operating expenses and service agreement expenses).

- Separate risk provisions are needed for the repairing of damage caused by information security risks that may be realised, because it may be that it is not possible, or there is no desire, to provide for all risks.

An adequate budget should be allocated for the implementation of the electronic service's information security. This budget must take into account not only the protection of the actual service but also future costs such as training and value network coordination. It is also worth providing in the budget for small overruns of the cost estimate and other additional expenditure that arises during the project. Costs and workloads can be quantified for example by comparing the project with the costs of other, similar projects or by requesting non-binding cost estimates of various information security solutions from suppliers. As a rule the implementation of information security is cheaper and easier the earlier that issues are considered and planned.

Information security costs mainly consist of the following components:

- Information security solutions of a technical nature, comprising for example virus protection, firewalls, encryptions and back-up systems.

- External consulting, which may comprise, among other things, current state reviews, auditing, certifications, various installations and specifications as well as

training relating to the use of the service platform and the application.

- The organisation's own work input consists of document preparation, monitoring and supervising the different service process actors, training one's own organisation and users, and participating in training. One's own organisation's human resources are often a bottleneck in electronic service development projects. At the budgeting stage it is also worth taking into account the costs arising from the work of one's own organisation, which is needed, for example, in service planning and content production as well as in project coordination.

When the information security costs are clear, they can be compared with the achievable benefits in order to assess the profitability of the project. Assessing the profitability of information security requirements acts as an important justification for whether a requirement should be fulfilled or not.

There must be sufficient justifications for investments made in information security. Examining information security measures with the aid of a cost-benefit analysis gives the service provider a picture of how profitable it is to protect the service with strong methods. Information security administration standards and frameworks help in estimating information security costs and in linking the objectives of the electronic service with business objectives.

The benefits sought through the electronic service can in many cases also be qualitative. Benefits of this type are, for example, improving the organisation's image, better flow of information within the company and to partners, better customer service, and providing more up-to-date information. On the other hand, the realisation of information security risks can inflict significant harm on the organisation's reputation and weaken customers' trust in the electronic service. Loss of image also has a financial impact.

4
Service construction and development

The earlier stages have specified the service content, distribution channels, information security requirements and other issues important for the construction of the service. This chapter presents how to monitor the advance of the construction process and supervise the attainment of the information security level specified at the planning stage. A key role is played by testing, which is divided into functional testing and information security testing. The chapter also discusses in particular practices relating to auditing the implementation of information security requirements.

Agreeing a comprehensive operating model and operating practices among the different actors as well as testing the service at different stages of construction are among the most important issues at the construction stage.

Construction stage task list from an information security standpoint:

1. Monitoring the fulfilment of information security requirements.

2. Documenting the system to be constructed and its components.

3. Testing service functionality and information security.

4. Approving, documenting and testing the addition of new features (intraproject change management).

At the construction stage the following questions should be asked:

Are the parties complying with the agreements?

Are the agreed information security requirements being delivered?

Is service construction proceeding according to plan?

Is sufficient documentation about the system being produced?

Is information security being tested often enough at the different stages of construction?

Have the people responsible for the electronic service appropriately approved any changes made?

4.1
Construction process

The electronic service must be constructed using a clear process model that adheres to general project management principles. This can be the application provider's own process or some other suitable model. The most important thing is that all parties are aware of the stages of the construction process and that they adhere to them appropriately. The service provider must also ensure that the process follows information security principles, for example in relation to programming. Such principles include appropriate commenting on code as well as code reviewing principles.

It is recommended that the service provider takes at least the following issues into account during service construction:

- The programming tools to be used in construction, together with an assessment of their use in possible further development, and whether other suppliers, too, have experts for the tools in question. Programming tools and languages in general use will facilitate the finding of expert personnel for future development projects. In terms of information security, programming languages have their own typical weaknesses.

- Close attention must be paid to the selection of the hardware platform, because a platform that is unsuitable for providing the service or is otherwise unstable may jeopardise the functionality of the electronic service in future.

- The personnel who will construct the service should be selected carefully. Expert programming personnel will observe the principles of information security in the construction and installation of the application and will work in accordance with rules and instructions.

4.2
Service components and documentation

As the construction work proceeds, the various system components must be documented together with the settings of the system components required for the provision of the service. If the organisation has a hardware and software register, the different components should also be recorded in this register.

The software and hardware register as well as the careful documentation of system components will be of significant benefit at the maintenance stage of the system. For system maintenance personnel, information about software components and their versions is essential for monitoring system updates, among other things. Similarly, information about the hardware used is important, because a number of information security holes are only associated with certain hardware platforms. When all the components and their versions are known, it is possible to concentrate on monitoring only the essential information security holes and updates.

4.3
Service testing at different stages of the development work

Testing of the electronic service can properly begin only at the construction stage, when the first concrete versions of the actual service are produced. At the creation and planning stages, the practicality of the idea from several different perspectives is tested and some certainty about the feasibility of the idea obtained, but proper testing of the adequacy of usability, information security and capacity cannot be done until the construction stage. It is essential that information security testing is carried out in conjunction with the other testing of the service. It is not sensible to measure performance and test functionality, for example, before the information security settings are in good order, because different information security settings can have a significant impact on the above-mentioned aspects that are generally tested.

The most important feature of the testing process is that it is as exhaustive and as comprehensive as possible. Examining the testing process from various standpoints will improve the operational reliability of the electronic service. Information security testing differs from functional testing, because with functional testing the aim is to check that the service is working in a specified way. The purpose of information security testing, on the other hand, is to check that the application is not working in a way that would jeopardise the information security of

the service. The same type of testing methods are used in both functional testing and information security testing.

4.3.1
Functional testing

- Usability testing, performed within a targeted group or with selected end-users, measures the functionality of the service's user-interfaces. Usability testing is used to obtain a picture of how easy it is to use the service. Moreover, usability testing helps in localising problem areas connected with using the service and which, for example, may require guidance or other information to be provided to the user. In terms of information security, usability testing can localise service process risk points, which information security measures can address.

- In load testing, the electronic service's functionality can be assessed in a normal situation, and bottlenecks that weaken service functionality as loading increases can be identified. Such testing is used to obtain a picture of the number of users a certain service level can be offered to.

- Interface testing is used to find errors resulting from wrong parameters or from other measures connected with the specification of connections. Interface testing is particularly important in mobile and internet channels. The impact of the environment on the operation of the service must be exhaustively tested, in order to ensure that the software interfaces are reliable.

- Reviewing the source code is a good way of ensuring the quality of programming work. The person performing the review should be someone other than the person who wrote the code. The reviewer, however, must have adequate knowledge of the software, the development tools used in it, and information security.

- Conformance testing relates particularly to digital television terminal devices, which must conform to a certain standard. Conformance testing is used to check that the services to be delivered via a digital television can be used on the terminal device.

4.3.2
Information security testing

Information security testing is used to survey errors made at the construction stage. Such testing should be performed in conjunction with other testing at the different stages of constructing the service. Information security testing is used to search for vulnerabilities that remain in the electronic service. These information security holes can be found in operating systems, hardware and servers, as well as in the databases used for storing data. Technical testing of information security should be performed at the different stages of system development and in different environments, in order to check the accuracy and permanence of information security settings through the entire process. Typically testing is done in development, testing, quality assurance and production environments (section 5.2).

Vulnerability and breach testing

Testing the information security of systems is recommended at the different stages of development, in development and test environments, and in the production environment after transfer into production. In vulnerability testing, the same methods and tools are used that hackers use when they attack information networks and systems. Vulnerability and breach testing is typically used to ensure that no simple programming and configuration errors have been made. This testing generally includes studying the services provided by the hardware, searching for known information security weaknesses in the services, testing authentication methods, and technology testing of other key aspects of information security. The results can be compared with the planning documentation, particularly the systems hardening instructions. An attempt is made to find known information security holes in the services using software and manual methods. An attempt is also made to exploit shortcomings perceived in breach testing and to crack into the system or otherwise misuse the service. In this way the real situation with respect to possible weaknesses is obtained with some certainty.

Vulnerability and breach testing provides valuable information to the system developers, who can still at the system development stage rectify perceived shortcom-

ings more easily. These tests can be performed by the organisation's own information security experts or by the experts from companies who offer information security services.

It is recommended that testing be performed from the network where the hardware to be tested is located, so that as true a picture as possible is obtained about the information security of this hardware. In addition, it is worth carrying out testing "from outside" the network components, such as firewalls, that protect the hardware, to obtain a picture of how effectively these components protect the hardware with which the service will be provided.

Auditing the settings of operating systems, application servers and databases

Vulnerability and breach testing provides a picture of what the system's information security looks like as seen from the network. All essential aspects in terms of information security cannot, however, be tested via the network. For this reason, the information security of the service must also be tested and analysed from the system to be used for providing the service. By this means the accuracy of the configuration of the system's information security settings can be elucidated by comparing them with the key information security settings documented at the planning stage. Adequate resources must be allocated for such procedures already in the project plan. As tools in the auditing of information security settings can be used, for example, the Windows operating system specification documents (domain policy) as well as software intended for the auditing of information systems, which many companies specialising in information security can provide.

Code auditing

Source code should be reviewed throughout the entire programming process. A practice that has proved to be effective is the nomination of programmer pairs. Daily reviewing of code takes a lot of time, and provision should be made for this in the project plan. It is also possible to audit code for the most common programming errors, buffer overflows and the examination of user inputs by using software tools, which are listed on the Open Web Application Security Project (OWASP) website, among others. With critical applications it can be justifiable to obtain external help with code auditing.

Source code auditing should answer the following questions:

Does the application used in the service fulfil the requirements set for it?

Does the software contain excess functionality?

Does the work comply with good programming practice and issued guidelines?

Is the source code accompanied with a sufficient number of comments. Are comments removed from compiled code?

Does the code have known information security weaknesses, for example functions vulnerable to buffer overflow?

Can compiled code be easily restored to source code?

Would the source code help an attacker find weak points in the service?

Notes


5

5
Service introduction

Chapter five goes through the most critical issues connected with the introduction of the service. The chapter discusses the phasing of the introduction as well as questions of responsibility relating to the various parties involved. The chapter also outlines the instructions or guidance that should be offered to end-users in connection with the introduction in order to promote secure ways of using the service.

The introduction of the electronic service covers a very short period of time compared with the early stages. Nevertheless, the introduction includes many aspects that affect the use of the service in the future. A successful introduction gives service users an image of a secure and high quality service and service organisation.

An introduction task list from the standpoint of information security:

1. Ensure that all part of the service are appropriately tested and approved before the introduction of the service.

2. Clarify the various parties' responsibilities and actions in the introduction phase.

3. Consider and document a prepared backup plan in case introduction does not go according to plan.

4. Allocate adequate resources for any malfunctions that might arise during introduction.

5. Provide end-users with guidance on the secure use of the service.

6. Continue testing the service immediately after introduction, but avoid disrupting the usability of the service.

Questions connected with introduction:

Has the final version of the service been tested?

Does the final version fulfil the set information security requirements or the settings of systems tested in a quality assurance environment?

Have the various parties been informed of introduction-related issues?

What course of action will be followed if significant problems arise in the introduction?

Are personnel able to act correctly in different situations?

How have various courses of action in the case of malfunctions been agreed with external parties?

Has adequate capacity been allocated for the provision of the service? Have the back-up systems been tested?

How will service users be advised in the case of malfunctions?

How will information security be tested after the introduction stage?

5.1
Roles and responsibilities in connection with service introduction

The introduction of the service is a critical situation for both the service user and the service provider. The customer must access the service successfully and the service provider must ensure that the service works according to plan in the actual operating environment.

5.1.1
The service provider's responsibilities

The successful introduction of the electronic service requires time and often a lot of resources. Ordinarily, introduction planning is weighted towards the end of development work on the entire service concept, even though the launch of the service should be taken into account in marketing the service, for example. Before service introduction, the service provider should have a marketing plan, guidelines for the use of the service and possibly even a training programme. The information offered to customers should include the following:

- Information about the service provider and other information required by the Consumer Protection Act.

- Information about the service content and price as well as other contractual terms.

- Information about the data that the service provider stores about the customer, how this data is processed and protected (register description) and information about the data protection of the service.

- Key information security factors that depend on the service but are often connected with user identification, the input and storing of information, the handling of malfunctions as well as the user's rights and obligations.

- Information on how the service should not be used or how the service provider will act or will not act. This is significant, for example, in the prevention of cases of phishing, whereby the customer can, for example, be given information about how the service provider will communicate with customers only by letter post, but not by e-mail.

- Information about where the customer can receive further information about the service and problem situations.

A support or feedback channel for end-users must be ready before the service is launched. Due attention should be paid to service guidelines, and all the factors essential for the information security of the service should be explained in common language.

The service provider's responsibilities during introduction

- Communicating introduction-related issues, such as possible functional shortcomings.

- Allocating adequate resources for the time of introduction, to ensure that the service operates without malfunctions or outages visible to the user.

- Communicating secure ways of using the service and other matters important for customers, as presented in the list above.

- Communicating parties' service-related roles and responsibilities.

- Organising a feedback channel.

5.1.2
Responsibilities of other actors

A number of parties are involved in providing the service. In addition to the service provider and the user, the introduction stage and use of the service in future also involve the operator who conveys the service to the customer. The number of parties involved can create problems in the introduction of the service, because the customer does not necessarily have a full understanding of the relationship between the electronic service provider and the network service provider.

The service provider must clearly inform the user about the roles and responsibilities of the parties involved in the service.

The provider of the service to the customer is also responsible for the actions of subcontractors. The most significant issue between the service provider and subcontractors are clear and comprehensive agreements in which information security aspects and requirements are taken into account.

5.1.3
The customer's responsibilities

From the customer's perspective there are many information security risks connected with the introduction of the service. Bringing the service into operating condition may require customers to download a separate application onto their terminal device or to change the device's settings to be compatible with the service. Services that use standard components, and applications that belong to operating systems, are often easier to accept and take into use than services that require various client programs.

The customer's responsibilities are:

- Installing information security updates on the device used to access the service (the customer-owned and administered terminal device).

- Assimilating and complying with guidelines so the user can access the service appropriately. Requesting additional information, if necessary.

- Checking the accuracy of customer-related information used in the electronic service.

5.2
Testing information security after transfer to production

In connection with introduction, the service provider must ensure that the service is working in the planned way. Information security testing in a production environment can begin immediately after introduction, but at the same time any disruption to the usability of the service should be avoided. Careful planning and the specification of a suitable time for testing are therefore required. Practical experience shows that information security settings stated as being according to requirements in a testing or quality assurance environment may no longer necessarily be according to requirements after introduction. There are at least two probable reasons for this:

1. The transfer to production process is such that the system component settings change (for example the operating system acting as a platform is re-installed without the information security settings being configured according to requirements).

2. Settings are intentionally changed, for example by an outsourcing partner involved in producing the service (for example a supplier's desire to ensure the functional characteristics and capacity of the service).

The same methods used during the construction stage can also be used in information security testing. Particular attention should be paid, however, to ensuring that the operation of the system in production is not jeopardised by the testing.

The ideal situation with respect to introduction is one in which introduction can be performed first for a small number of users, so that errors that remain undetected during testing can be rectified before the launch of the service to the general public. Piloting can be used to test introduction-related measures before the publication of the actual service. An open pilot for all users is problematic, because it requires the content and use of the service to be so interesting that the user is ready to try out an incomplete and deficient service. Here, the risk is also that users obtain a poor impression of the service due to possible problems. Where the service is particularly large, piloting can be a very effective form of testing, but it requires well organised feedback channels as well as efficient error localisation and rectification routines. In the pilot stage it is easy to lose customers' trust by failing to acknowledge feedback or by the adjusting service in an uncertain way. Moreover, at the beginning of a pilot there is good reason to test the service's information security using one's own organisation or external experts.

6

6
Service production and maintenance stage

Chapter six discusses the correction of errors and vulnerabilities that appear at the production and maintenance stage of the service as well as ensuring the operation and maintenance of the service and the provision of back-up systems. In addition, the chapter goes through the role of information security during the transfer of the service's development stages into production as well as the measurement of the service's information security.

Developing and monitoring the electronic service's information security does not end with the publication of the service; it also continues during the operational stage of the service. Safeguarding service usability is essential during the service's operational and production stage. In practice, this means regular measurement of the service's information security, an effective process for handling vulnerabilities and errors, and clear operating procedures in the event of malfunctions.

Maintenance and production stage task list from an information security standpoint:

1. Prepare a model for service development and maintenance.
2. Create a process for handling vulnerabilities and errors.
3. Make regular back-up copies of the data contained in the service as well as other essential information, such as system settings files.
4. Ensure the continuity and trouble-free operation of the service.
5. Measure the level of information security.

Questions to be asked at the maintenance and production stage:

What procedures have been established to check that the service development stages comply with the original information security requirements?

How does the service provider control that the service in production is kept up to date in respect of prepared documents?

Is there a copy of the information stored in the service? Does this copy work correctly? Has it been tested? Is there sufficient checked and documented information to allow the service to be reconstructed quickly enough?

How does the service provider receive information about malfunctions or telecommunications problems arising in the service? What is the procedure in the event of malfunctions and who is informed about them?

Does the customer know the kind of channels and means of communication the service provider uses and does not use?

What is the procedure for dealing with complaints made by consumers?

6.1
Correction of errors and vulnerabilities, and handling of information security breaches

Malfunctions and change requirements in the electronic service may be linked to information security holes and vulnerabilities perceived in the service or to changes in the operating environment, such as the distribution channel standard, detected new viruses and change requirements arising from them.

Errors may result from actions performed at the various stages of the service process. Malfunctions may arise as a consequence of human error, incorrect production processes or similar management problems. A malfunction may also arise in a situation in which a user tries to crack into the system. A handling process for malfunctions and information security breaches means a set of software and hardware repair functions that includes measures to detect and rectify errors as well as other required actions, such as possible cancellation of contracts or reporting of offences.

The electronic service development organisation must investigate any malfunction and decide whether external assistance may be needed. The original cause of the malfunction must always be identified and the necessary measures instigated to correct the problem.

Stages of the error-correction development and change process:

1. Detecting the error.
2. Forwarding a report of the error, for example to a helpdesk or information security organisation.
3. Evaluating the error and allocating the correction of the error to a suitable party.
4. Specifying the necessary change.
5. Performing the change.
6. Testing the change.
7. Approving the change.
8. Transferring to production.

The impact of the error and its correction must be extensively evaluated, because changing program code, for example, can have an impact on other parts of the application or on other information systems connected to it.

Typical service production malfunctions:

- Growth in user numbers can lead to a situation in which server and software capacity is insufficient to serve all users, resulting in the interruption or slowing of the service.
- Careless action by users can cause a malfunction that interrupts the service of the individuals in question or at worst even the service of other users.
- The malfunction of application or database servers can result in the immediate cessation of the service, if no back-up system exists.
- Malware can cause malfunctions in which the use of the service is slowed or interrupted. Malware can also change or destroy the information contained in the service.

The spread and effects of malware can be reduced through correct working procedures. These include:

- Management of the electronic service must be carried out with identity codes used only for this purpose. E-mail or web links must not be used with management rights, nor other applications that are not expressly connected with the management of the hardware in question. The management network and hardware should be separated from the rest of the network.
- Servers intended for providing the electronic service should not provide other services or use these for other functions.
- User rights to extensive distribution lists should be minimised in the maintenance of electronic service's e-mail distribution lists. Extensive distribution lists accelerate the spread of e-mail worms, for example.

6.2
Safeguarding the usability the service, and back-up arrangements

The availability of information used in the service as well as system continuity are improved by making regular back-up copies. Back-up copies guarantee the availability

of information. This is essential for the service provider, as it ensures that the service can be accessed by customers as promised. Measures to safeguard the usability of the service include:

- Preparing service level agreements with system and equipment suppliers allows the measures that suppliers are obliged to carry out in the case of disruptions to be specified. Sanctions imposed for failing to achieve the agreed service level must be sufficient to ensure that the supplier actually complies with the agreement. Furthermore, the fulfilment of service level agreements must be monitored regularly. In terms of such agreements, restrictions set by possible force majeure conditions must be recognised and taken into account.

- Service usability can be influenced on the architecture level significantly at the planning stage, but at the maintenance stage the work mainly involves the appropriate service and maintenance of selected components.

- Service continuity can be safeguarded by regularly backing up application files and data stored in the service. Service continuity, moreover, can be safeguarded by acquiring production capacity large enough to cope with possible disruption. A well planned system is easily expandable and fault tolerant. Maintaining back-up systems is expensive, however, so the costs of such measures and the benefit arising from them must be carefully assessed. Good back-up practice includes a description of the backed up information, the back-up method and the storage and testing of the back-up copies.

- Specify the data to be backed up. In terms of file servers this means the specification of those files that fall within the sphere of the back-up procedure, and in terms of database servers the agreement to adopt either a simple file back-up method or the use of more advanced database agents. Often it is justifiable to replicate the whole database.

- Rotation of back-up copying and storage. Back-up robots typically adopt a recycling of back-up tapes based either on calendar time or on file versions. The back-up procedure can vary but back-up of changing data is typically performed daily and back-up of complete data once a week.

- Testing back-ups. The functionality of back-ups must be tested for each back-up tape to ensure that the data has been saved on the tape. Particularly in relation to databases, the service provider must ensure that each database can be restored to operating condition from the back-up tape.

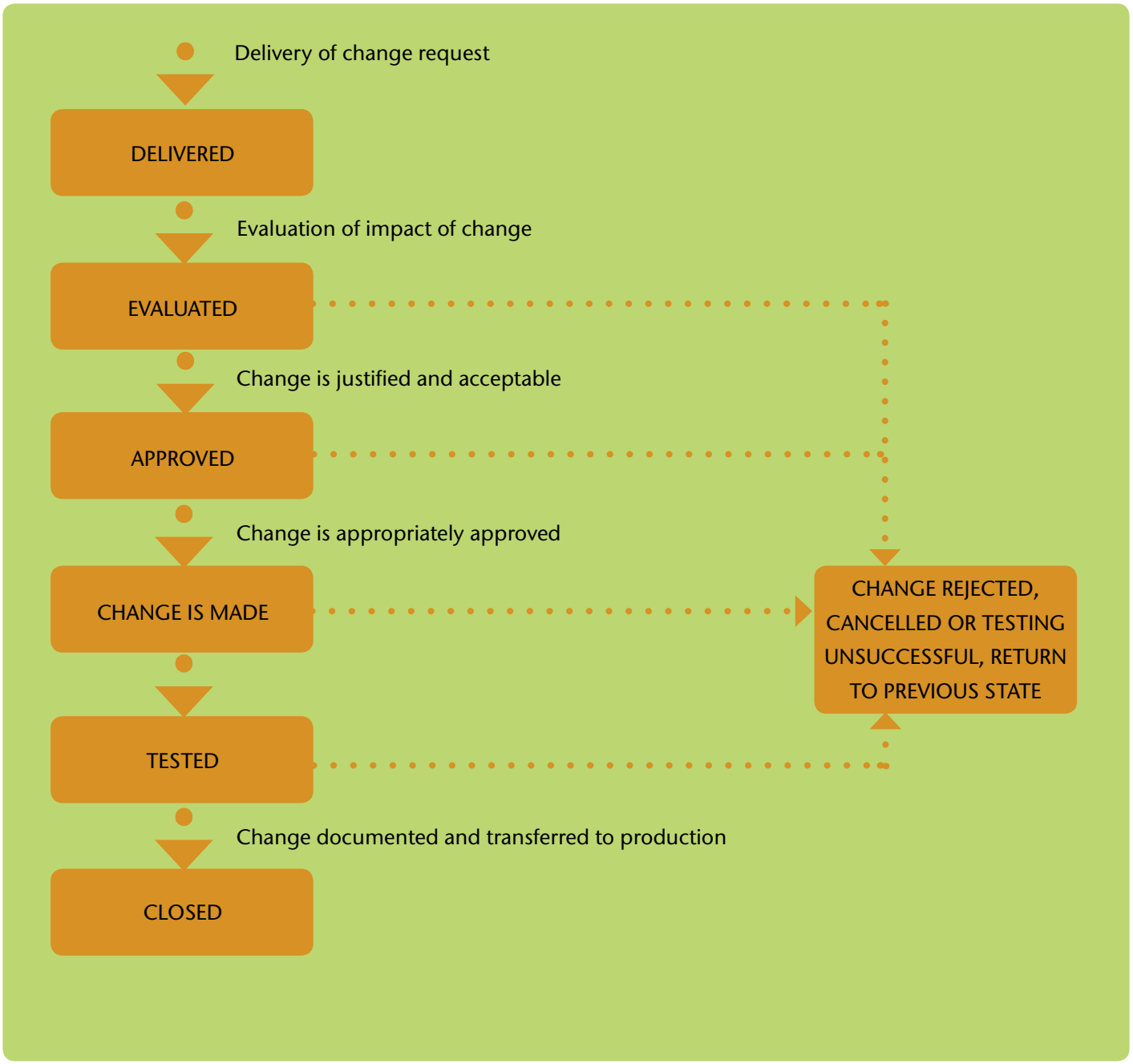
6.3
Transferring the service development stages into production

The life cycle of the electronic service's various development stages goes through three phases. Firstly, a new version of the service is planned in a development environment. Next, a suitably developed version of the service is transferred to a test environment, where a check is made that the version in question works correctly and is ready for the final phase, the production environment.

Without a clearly defined change management procedure, good and secure information systems quickly become unreliable. It is for this reason that change management must be clearly defined and that it should also extend to application services purchased from external parties.

Changes made to the service must fulfil the information security requirements specified in the planning stage. The basic idea of the change management process is that all system changes take place in a controlled way and are tested and appropriately approved and documented. In change management, user rights play a vital role; no change should be implemented, tested and approved by the same person (the separation of tasks is discussed earlier in this guide).

A simplified version of the course of change management is outlined below:



6.4
Measuring the service's information security

Monitoring the electronic service and the systematic measuring of information helps in managing the service as well as information security mechanisms. As far as measurement is concerned, collecting the correct data requires the measurement of information security to be planned at the planning stage of the electronic service.

The purpose of information security measurement is to produce information that will help in operational management, particularly in planning and prioritising protection measures, and in making investment decisions. An indicative list of information security measurement methods for electronic services is given below. These methods are suitable for use by most companies, either as they are or slightly adapted:

- Risk analyses at regular intervals provide a picture of how the level of information security has developed from the previous evaluation.

- Information security testing can be performed at regular intervals, thereby revealing the current state of the system and whether the necessary information security updates have been made in good time.

- By monitoring the performance of systems used in providing the service, it is possible to detect if a system is not working in the customary way. Divergent performance can be a sign of a virus epidemic, for example.

- The number of successful and unsuccessful events in users' log-ins and log-outs can be measured. As a result of measuring, user identification methods can be made more effective.

- System alerts act as an indicator of system functionality. The number of malfunctions, erroneous events or information breaches that affect the service reveal how well or poorly the service has been planned and help to prioritise information security development projects.

- Monitoring the audit trail of service events is useful, particularly where monetary transactions or other valuable property is concerned. Recording events is particularly helpful in interpreting cases of misuse. Moreover, a large volume of event chains can be analysed to detect possible anomalies and misuse.

- The results of interest group information security surveys, complaints and customer feedback will help in developing the service.

- On the system level, the number of risky job combinations or particularly broad user rights for system maintenance can be evaluated.

- The number of detected information security holes within a certain period.

- The number of repaired information security holes within a certain period.


Off

7
Closing the service

This chapter discusses the closure of the service. The closure of the service is not often included in the life cycle stages of the service. However, the destruction or preservation of information accumulated in the service when the service is closed is significant in terms of information security. The service may also be discontinued as a consequence of it merging with another service, so this is also discussed in the chapter.

Information security matters connected with the closure of the electronic service must be resolved before the service's life cycle ends. The closure of the service may come as an unpleasant surprise to users if the service provider does not inform them of the various closure measures in good time, so that users can take appropriate steps to protect important data contained in the service. Moreover, before the service is closed, the service provider must resolve the challenges posed by storage and destruction of data contained in the service.

Service closure task list from the standpoint of information security:

1. Ensure that information stored in the service is handled appropriately after the end of the service.

2. Inform the various parties involved that the service will be closed.

3. Draw up operating practices that explain how information should be appropriately preserved or destroyed.

Questions relating to service closure:

- Should information be preserved e.g. for the authorities?

- Who owns the information and log data contained in the service?

- Will the information be preserved after the closure of the service?

- How will the information be accessed? Who will handle the information?

7.1
Destroying data

The service provider should plan an operating model for the closure of the service. Procedures for the destruction of stored data must be written down and made available to all the parties involved. At the service closure stage, the requirements of various official bodies regarding the destruction of data stored in the service must be examined. It is important that data is destroyed appropriately. Destroying data is not always simple. Data can be recovered from deleted or partially destroyed storage media. To ensure complete destruction of data, it is worth turning to experts, who will advise on the most suitable method. The following methods can be used to destroy confidential data:

- Overwriting, which means that new data is saved randomly, or in a way specified in advance, on top of the existing data. In this way, all the existing data on a hard disk, including the operating system, is destroyed and recovery of the data is therefore impossible. There are a number of easy-to-use and reasonably priced applications available for doing this. Formatting does not work like overwriting, because it does not prevent the option of recovering the data.

- Physical destruction of data stored in electronic form, for example by chopping the hard disk used for storage into small pieces, so that it is impossible to use it again.

7.2
Preserving data

In the event of the closure of the electronic service, the service provider must find out whether the data used in the service needs to be preserved. Possible reasons for preserving the data are as follows:

- Legislation may require the preservation of data, for example with respect to bookkeeping, financial statements or billing.

- Service delivery contracts and their terms and conditions must also be fulfilled after the closure of the service.

- Actions relating to service billing must be verifiable also after the closure of the service, insofar as this is necessary.

- Data stored in the service should be handed over to the customer, stored by the service provider or appropriately destroyed.

7.3
Merger with another service

One reason for closing the service may be the merger of the service with another, similar service. In terms of information security, the following issues should be assessed in the merger of services:

- Information security must be in good order when data is transferred from one system to the other.

- User rights must work in the new system without changes. In other words, users must be able to access the information in the same way as in the earlier service.

- Information contained in the service must be incorporated within the sphere of the new service's backup procedures so that the integrity of the information is maintained. This requires the databases and protection methods used in the service to be compatible with the new service, or the conversion of the data to make them suitable for use in the new service.

- The information security level of the service must not decline, or at least customers should be informed of any decline in the level of security in a way that they understand.

In such cases the service provider should assess the information security requirements of the new service created after the merger and should follow this guide's stages for service planning and construction, just as if a new service were being constructed.

Notes

8 Source list

Publisher of the LUOTI project http://www.mintc.fi/paattyneetohjelmat

Chapter 2. Creation

Matkaviestinverkkojen tulevaisuus, Liikenne- ja viestintäministeriö, (The Future of Mobile Networks, Ministry of Transport and Communications), Helsinki 2005 http://www.mintc.fi/oliver/upl569-Julkaisuja%2040_2005.pdf
Mobiilipalvelumarkkinat Suomessa 2005, Liikenne- ja viestintäministeriö, (The Mobile Services Market in Finland 2005, Ministry of Transport and Communications), Helsinki 2005 http://www.mintc.fi/oliver/upl964-Julkaisuja%2022_2006.pdf
OECD Organisation for Economic Co-operation and Development
http://www.oecd.org/topic/0,2686,en_2649_37441_1_1_1_1_37441,00.html
The Finnish Banker' Association (Pankkiyhdistys) http://www.pankkiyhdistys.fi/
The Finnish Financial Supervision Authority (Rahoitustarkastus) http://www.rahoitustarkastus.fi/

Standards and frameworks

ISACA http://www.isaca.org/
COBIT 4.0 http://www.icasa.org/cobit
COBIT 4.0 Reviewed by Rob Singh-Latulipe, CISA, CISM, CISSP – Information Systems Control Journal 1/2006
ISO International Organization for Standardization http://www.iso.org/
ISO 17799: Then, Now and in the Future, Scott H. Sweren, CISM, CISSP, PMP – Information Systems Control Journal 1/2006
ISO – Iso in Brief http://www.iso.org/iso/en/prods-services/otherpubs/pdf/isoinbrief_2005-en.pdf
ISF Information Security Forum http://www.securityforum.org/html/frameset.htm
ISF - The Standard of Good Practice for Information Security, v 4.1 1/2005
http://www.isfsecuritystandard.com/index_ie.htm
National Institute of Standards and Technology http://www.nist.gov/
Tietoturvalliseen tietoyhteiskuntaan, Kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle (Towards An Information Security Society, National Information Security Advisory Board's report to the Government) 14.12.2004 http://www.mintc.fi/oliver/upl163-tietoturvastrategia%2014.pdf
PCI-DSS standard http://www.luottokunta.fi/fi/pci/

Legislation and decrees

Finnish Law (FINLEX) http://www.finlex.fi/fi/
Act on the Protection of Privacy in Electronic Communications http://www.finlex.fi/fi/laki/ajantasa/2004/20040516
Personal Data Act http://www.finlex.fi/fi/laki/ajantasa/1999/19990523
Act on the Provision of Information Society Services http://www.finlex.fi/fi/laki/ajantasa/2002/20020458
Act on Electronic Signatures http://www.finlex.fi/fi/laki/ajantasa/2003/20030014
Act on Electronic Services and Communication in the Public Sector http://www.finlex.fi/fi/laki/ajantasa/2003/20030013
Communications Market Act http://www.finlex.fi/fi/laki/ajantasa/2003/20030393
Act on the Openness of Government Activities http://www.finlex.fi/fi/laki/ajantasa/1999/19990621
Consumer Protection Act http://www.finlex.fi/fi/laki/ajantasa/1978/19780038
Pending Government bills (FINLEX): http://www.finlex.fi/fi/esitykset/he/

Chapter 3. Planning

Buyer's guide for an Access and Identity Management Infrastructure, An Oracle White Paper, April 2005
http://www.oracle.com/technology/products/id_mgmt/coreid_acc/pdf/wp_oracle_identity-management-buyers-guide_060205.pdf
Cert http://www.ficora.fi/suomi/tietoturva/cert.htm
Ficom http://www.ficom.fi/
Helppokäyttöisten digi-tv –palvelujen suunnitteluopas, ArviD julkaisuja (Design Guide for Easy-to-use Digital TV Services, ArviD publications) 7/2005, http://www.kuluttajavirasto.fi/user/loadFile.asp?id=6183

Internetin tietoturvaongelmat kotikäyttäjän näkökulmasta, Liikenne- ja viestintäministeriö (Internet Information Security Problems from the Home User's Perspective, Ministry of Transport and Communications) Helsinki 2005
http://www.mintc.fi/oliver/upl964-Julkaisuja%2088_2005.pdf
IT Infrastructure Library, Office of Government Commerce http://www.itil.co.uk/
Katso-tunnus, Kansaneläkelaitos ja verohallinnon sähköinen organisaatiotunnus (Katso, an identity system for organisations maintained by the Social Insurance Institution of Finland and the Finnish Tax Administration)
https://yritys.tunnistus.fi/h/help/fi/index.html
Käyttäjän opas hallinnon verkkopalveluihin (A Citizens' Guide to Online Public Services) http://www.asiointiopas.fi/
Mobiililähimaksaminen – nykykäyttö ja tulevaisuus, Liikenne- ja viestintäministeriö (Mobile Local Payment – Current Practice and the Future, Ministry of Transport and Communications) 2003
http://www.mintc.fi/www/sivut/dokumentit/julkaisu/julkaisusarja/2003/a222003.pdf
Mastercard http://www.mastercard.com/us/merchant/security/index.html
Opas palvelunrakentajille kansalaisvarmennetta hyödyntävien palvelujen rakentamiseen, Väestörekisterikeskus (Service Constructors' Guide for Services Utilising the Citizen Certificate, Population Register Centre) 2005
http://www.fineid.fi/vrk/fineid/files.nsf/files/D9FF496723B005F9C225707B0038B147/$file/Opas+palvelunrakentajille+092005.pdf
Pankkien Tupas-varmennepalvelu palveluntarjoajille, Suomen pankkiyhdistys (Banks' TUPAS Certification Service for Service Providers, The Finnish Bankers' Association) 2005 http://www.pankkiyhdistys.fi/sisalto/upload/pdf/tupasV21.pdf
Pang Leslie Ph.D. – A Manager's Guide to Identity Management and Federated Identity, Information Systems Control Journal 4/2005
PayPal, http://www.paypal.com/cgi-bin/webscr?cmd=_merchant-outside
SANS Institute http://www.sans.org/resources/
Sähköisen kaupan palvelukeskus (eCommerce Service Centre) http://www.e-finland.org/center/etusivu/?
The Administrator Accounts Security Planning Guide, Microsoft 2005
http://www.microsoft.com/technet/security/guidance/serversecurity/administratoraccounts/default.mspx
Tietosuojalautakunta (The Finnish Data Protection Board) http://www.tietosuoja.fi/
Tietoturvaopas.fi (Information Security Guide) http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/index.html
VAHTI tietoturvaohjeet ja määräykset (Government Information Security Management Board's information security guidelines and regulations) http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp
Visa http://corporate.visa.com/pd/security/main.jsp
Population Register Centre (Väestörekisterikeskus) http://www.vaestorekisterikeskus.fi/

Chapter 4. Construction stage

Best Practices for Enterprise Network Security 2005, Vernier Networks
http://www.verniernetworks.com/products-and-solutions/white_papers.html
Center for Internet Security http://www.cisecurity.org/bench.html
Disaster Recovery Plan Testing: Cycle the Plan, Plan the Cycle, SANS Infosec
http://www.sans.org/reading_room/whitepapers/recovery/563.php
Open Web Application Security Project http://www.owasp.org/index.php/Main_Page
Penetration Testing: The Third Party Hacker, SANS Infosec
http://www.sans.org/reading_room/whitepapers/testing/264.php?portal=3799a0e7446ad95746ef35d6d4ce92f6
Total Access Protection for Your Network, Checpoint http://www.checkpoint.com/

Chapter 5 and 6. Introduction and maintenance

ITIL Problem Management White Paper, Chorus Systems,
http://www.chorussystems.com/downloads/PM-Key_Leveraging_ITIL_Implementation_Out_of_Network.pdf
Consumer Agency (Kuluttajavirasto) http://www.kuluttajavirasto.fi/
Richard A. Bassett, Rita Mack, Jason Foster and Andrew Swiatlon – Security and Ownership of Personal Eletronic Devices – Information Control Journal 6/2005
The British Starndards Institute http://www.bsi-global.com/index.xalter
The Disaster Recovery Institute International http://www.drii.org/

Appendix - Information security standards

Information security standards guiding the activities of organisations:

ISO standards are key information security standards covering information security as a whole, with an emphasis on information security management.

The ISO 27000 series of standards are specifically reserved for information security matters. The standards provide specifications for companies' information security management measures and requirements for information security management systems.
http://www.iso.org/

British Standards (BS) act as a basis for many ISO information security standards. Currently, BS7799 is the only information security management standard for organisations that can be certified.
http://www.bsi-global.com/

The Information Security Forum (ISF) is an international body with nearly 300 member organisations around the world. ISF has published the Standard of Good Practice for Information Security, which is freely available. The standard includes a business-oriented approach to the development of a company's or organisation's information security.

Compared with the ISO standard, the ISF information security standard deals more with technical implementation.
http://www.securityforum.org/

Technical information security standards

The ISO 15400 series of standards focuses on the specification and evaluation of criteria for the security features of information technology products and systems. The ISO 15408 series is also known by the name Common Criteria.
http://www.iso.org/

There are numerous technical standards referring to information security. Standards relating to a particular aspect can be requested from the manufacturers or suppliers of the selected distribution channel, technology, systems and applications.

Frameworks guiding the activities of organisations:

COBIT (Control Objectives for Information and related Technology) is a set of best practices (framework), created by the Information Systems Audit and Control Association (ISACA). Organisations can utilise COBIT in specifying the business objectives and requirements of information management. The framework provides advice to management on how to combine business and IT objectives as well as on how to measure the achievement of these objectives.

The framework specifies processes and related controls for IT operations, and it can be used as a tool in specifying control points for business processes, for example.

COBIT is not directly a model for information security implementation, but the framework provides information on the solving of significant information security questions.
http://www.isaca.org/

The Information Technology Infrastructure Library (ITIL) is a set of best practices created by the Office of Government Commerce. The library has eight parts, one of which lays down principles for information security management.
http://www.itil.co.uk/

The OECD guidelines present nine information security principles, whose purpose is to answer the current challenges of the information society. The OECD guidelines specify information security principles in which the building, maintenance and development of information security are viewed as processes. Compliance with these guidelines is not compulsory but is recommended, because the principles presented are useful in terms of information security.
OECD Organisation for Economic Co-operation and Developmen
http://www.oecd.org/topic/0,2686,en_2649_37441_1_1_1_1_37441,00.html

Abbreviations and terminology

"A" identifier	DTMF signal at the beginning of calls that discloses the subscriber identity.
BETA	Beta testing means the release of an unfinished service for trial use before the actual release date.
BT	Bluetooth. A short-range (10 m) wireless telecommunication technology.
CA	Certification Authority.
CERT	Computer Emergency Response Team. CERT-FI is a Finnish national CERT team (part of Vlestintävirasto, the Finnish Communications Regulatory Authority) whose task is the preven tion, detection and solution of information security breaches as well as the dissemination of security threats.
COBIT	The Control Objectives for Information and related Technology (COBIT) is a set of best practices that an organisation can use to define the business objectives of information management.
Cracking	Penetration of a secured system. Cracking, or data trespass, is a criminal offence under the Penal Code.
Denial-of-service attack	Attack intended to adversely affect the operation of a service or to block it completely.
DNS	Domain Name System. Internet name system, which converts domain names into IP addresses.
DRM	Digital Rights Management. A method for controlling the distribution of electronic content.
Electronic certificate	An electronic certificate is used to prove that the holder is a certain person, organisation or system.
Encryption	The changing of information into a form that makes it unreadable by an unauthorised party.
FTP	File Transfer Protocol.
HST	Electronic Identification of a Person (in Finnish Henkilön Sähköinen Tunnistaminen) A Finnish chip-based identity certificate.
HTTP	Hypertext Transfer Protocol. File transfer protocol used by browsers; https is encrypted with the SSL protocol.
ID	Identity.
IDS	Intrusion-Detection System.
IMEI	International Mobile Equipment Identity.
IP	Internet Protocol. IP is responsible for the addressing of mobile devices and for packet routing in a network. IPv4 and IPv6 are different versions of IP.
IPSec	IP security. A collection of IP security protocols.
ISACA	Information System Audit and Control Association.
ISIM	IMS (IP Multimedia Subsystem) Subscriber Identity Module.
ISO	International Organisation for Standardisation.
ITIL	IT Infrastructure Library.
Katso	An identity management, authorisation and authentication platform for organisations, main tained by the Social Insurance Institution of Finland and the Finnish Tax Administration. The Katso system is replacing the TYVI system.
LUOTI programme	A development programme of the Finnish Ministry of Transport and Communications for 2005-2006. The programme's objective is to promote the information security of new electronic services.
Malware	Software that intentionally causes events in hardware or information systems without the owner's consent.
MHP	Multimedia Home Platform. An open application programming interface for interactive applications of digital television.
MPLS	Multiprotocol Label Switching.

ODBC	Open Database Connectivity. Interface for databases.
PCI-DSS	Payment Card Industry Data Security Standard. International data security standard for the payment card industry.
Phishing	By the term phishing is meant an attempt to fraudulently acquire information, for example passwords and usernames, from the owner of the information by using false or erroneous e-mail messages or websites.
PIN	Personal Identification Number (GSM).
PKI	Public Key Infrastructure.
Remote Login	Unix function, which allows a user to log in to a remote system.
Return channel	Technical solution by which the viewer can send information to a service provider and search applications or other content. Currently this is typically implemented in Finland with a modem connection. In the future, the return channel will be a broadband internet link as terminal devices that support it come on to the market.
Root name server	Internet top-level DNS server.
S/MIME	Secure Multi-Purpose Internet Mail Extensions. Protocol for protecting e-mail.
SATU	Electronic identifier in HST (In Finnish Sähköinen henkilöllisyyden tunnus).
Secure Shell	Protocol for securing remote connections and data transfer (SSH).
SMS	Short Message Service. Text message system for mobile phones.
SNMP	Simple Network Management Protocol. Communications protocol used in network management.
SSL	Secure Sockets Layer. Communications encryption protocol.
TCP	Transmission Control Protocol. TCP is responsible for creating a data transfer link between two terminal devices, packet structuring and retransmission of lost packets.
TCP/IP	Transmission Control Protocol/Internet Protocol. Combination of network protocols used in internet communications.
TELNET	Internet protocol for remote connections.
TLS	Transport Layer Security. See also SSL.
TMSI	Temporary Mobile Subscriber Identity. A temporary subscriber identifier used for identity protection during the transfer of subscriber information.
Trojan Horse	A malicious program that is disguised as or embedded within legitimate software.
TUPAS	TUPAS a joint electronic identification service of Finnish banks.
TYVI	TYVI is an electronic identifier for organisations in the electronic transfer of information between companies and official bodies. The parties involved in transmitting information to officials are as follows: a company, an authorised accounting office, an operator and an official body e.g. the Finnish Tax Administration.
USIM	User Services Identity Module (UMTS). “SIM card” in UMTS.
Value network	A term used to describe a complex field of business in a more versatile way than a traditional value chain. In contrast with a value chain, a value network can have a number of actors belonging to the same sector.
VPN	Virtual Private Network. A solution that allows an organisation’s intranet to be extended securely over an unsecured public network such as the internet.
WEB Services	The publishing of services on the internet in a manner independent of the technology.
WLAN	Wireless Local Area Network.
X.25	Protocol for communication services that use packet switched networks.

www.luoti.fi

www.mintc.fi/paattyneethankkeet