Swedish Civil Contingencies Agency

GUIDANCE

Security measures for information systems

Guidance on security measures for information systems

Cover image: iStock
Printing: By Wind AB
Layout: Advant

Publication number: MSB2207 – Revised November 2023
Swedish edition: MSB2032 – Revised November 2023
ISBN: 978-91-7927-447-4

Guidance on security measures for information systems

This guidance supports the implementation of MSB's *föreskrifter och allmänna råd (MSBFS 2020:7) om säkerhetsåtgärder i informations system för statliga myndigheter*[1], but can be used by all organisations[2], including regions, municipalities or companies, to support their work with IT security. This guidance is primarily intended to support those who develop, manage and administer an organisation's IT environment, such as the CIO[3], IT managers, IT-security officers, IT-security architects and CISOs[4] in their role of coordinating the organisation's work with information security. The regulatory requirements for security measures correspond to what MSB recommends as the *minimum* that a government agency needs to do to achieve an acceptable level of security in its IT environment. Any additional security measures that are necessary are identified by the organisation through its systematic and risk-based information security work. Other regulations may also impose higher security requirements, such as the General Data Protection Regulation (GDPR)[5] or the Protective Security Act[6].

This guidance will be updated when necessary. Please send any suggested amendments, comments or observations to informationssakerhet@informationssakerhet.se

Reading guide

The guidance consists of several sections. Each section describes an area that is important to protect information systems.

Each section begins with a purpose that describes why the security measures are important. This is followed by a set of "shall" requirements, sometimes also "should" recommendations, and support for meeting the requirements and recommendations. Shall and should requirements/recommendations are taken from MSB's *Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter*[7], but sometimes expressed in a slightly more accessible way. Each shall requirement or should recommendation is followed by a reference to the corresponding requirement and recommendation in the regulations. The requirements imposed by the guidance are not

---

1. *MSB's regulations and general advice (MSBFS 2020:7) on security measures in information systems for government agencies.*
2. To further clarify this, the term organisation is used throughout the guidance.
3. Chief Information Officer.
4. Chief Information Security Officer.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
6. Säkerhetsskyddslagen (2018:585).
7. MSB's Regulations on security measures in information systems for government agencies

intended to have a different purpose or meaning from the regulatory requirements or recommendations. The guidance also uses the term "need to" where the regulations have no explicit requirements, but where MSB nevertheless wishes to emphasise the importance of taking a particular security measure.

In cases where MSB wishes to highlight a security measure, but has deemed that it is of less importance than a security measure that the organisation "needs to" take, the wording "appropriate" is used for the security measure.

As this guidance is intended for a broader target group than government agencies, with the exception of Chapter 5, "agency" has been replaced by "organisation" in the text. The term “agency” has been retained in Chapter 5 because these requirements are specially intended for agencies with specific civil preparedness responsibilities.[8] In addition, as a consequence of the broader target group of the guidance, the wording of the regulations regarding "the mission of the agency" has been replaced by "the activities of the organisation". No difference in scope is intended; rather, the terms are used here in an equivalent way.

The guidance covers all the areas for which an organisation needs to identify their requirements, pursuant to Section 3.1.2, but does not have specific sections for the security measures of business-continuity management during peacetime crisis or before/during a heightened state of alert, archiving and decommissioning.[9] For further support in implementing security measures, please refer to Appendix A. In Appendix A, we have collected references to other advice and support, both in general and regarding specific security measures.

Appendix B provides a list of the connections between the security measures in the guidance and what we consider to be the corresponding security measures in SS EN-ISO ISO 27002:2017 and SS EN-ISO ISO 27002:2022.

Rights

8. Förordning (2022:524) om statliga myndigheters beredskap (Ordinance on the preparedness of government agencies).

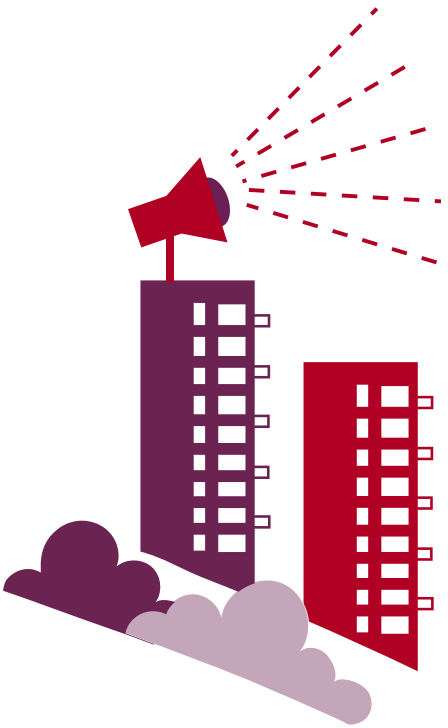
9. Support for business-continuity management and decommissioning is treated, e.g., in Chapter 4.14 Redundancy and recovery, and Chapter 4.13.6 Wiping and disposing of IT equipment. For requirements and support regarding archiving, please refer to the National Archives.

Content

Introduction

1. Introduction

Digitisation brings many benefits, but it also brings new risks by increasing the complexity of the IT environment and the need for continuous connection to the internet. This results in greater exposure of information and information systems to other organisations and their information systems. Insufficient IT security can mean that organisations cannot access their information, that information can be accessed by unauthorised parties or that information is corrupted or destroyed. IT security involves implementing security measures to protect information in information systems. Adequate security measures for information systems are a prerequisite for reaping the benefits of digitisation.



Information systems can take different forms. For example, they can be used to support office work (office IT), but also to interact with machines, vehicles and other equipment[10] (cyber-physical systems). This guidance does not distinguish between the different types of information systems, but can be used to support the implementation, administration, monitoring and evaluation of security measures for all information systems, regardless of their use. However, in the case of cyber-physical systems, additional considerations may need to be made.

Both an individual information system and information systems gathered in an IT environment need protection against different types of risks. Simple human errors and system errors account for most IT incidents reported to MSB, but the risk of intentional attacks and natural events needs to be managed. This guidance is premised on an all-risks perspective, i.e., all different types of risks must be considered.

10. For example, sensors that can collect data from the environment.

1.1 Explanation of terms

For the purposes of this guidance, the following terms have the following meanings:[11]

Term	Explanation
processing	A measure or combination of measures regarding information, whether or not performed by automated means, such as collection, recording, organisation, structuring, storage, processing or modification, retrieval, reading, use, disclosure by transmission, dissemination or otherwise making available, alignment or aggregation, restriction, erasure or destruction.
external actor[12]	Other organisation, hired personnel or equivalent that processes the organisation's information, such as a supplier.
information system	Applications, services or other components that process information. The concept also includes networks and infrastructure. Information systems include, for example, computer programs, apps, computers, printers, hard drives, mobile phones, WIFI and some parts of control systems.
information security	Preservation of confidentiality, integrity and availability of information.
information owner	Position responsible for ensuring that information is adequately protected.
IT environment	The sum total of information systems used to process information for which the organisation is responsible. The IT environment includes both internally managed and outsourced information systems.
IT security	IT-related technical security measures to maintain information security.
employees	Own and hired personnel.
Production environment	The part of the IT environment that the organisation uses to conduct its business.
redundant function	Two or more functions, identical or different, which independently fulfil the same purpose.
risk assessment	Approaches to identifying, analysing and evaluating risks.
administrator access	Access that includes privileged rights to modification of the basic and security-related functions of an information system.
system owner	Position responsible for implementing, administering, monitoring and evaluating the security measures of an information system.

11. The definitions are mainly based on MSB's regulations on security measures in information systems for government agencies (MSBFS 2020:7) and MSB's regulations on information security for government agencies (MSBFS 2020:6).

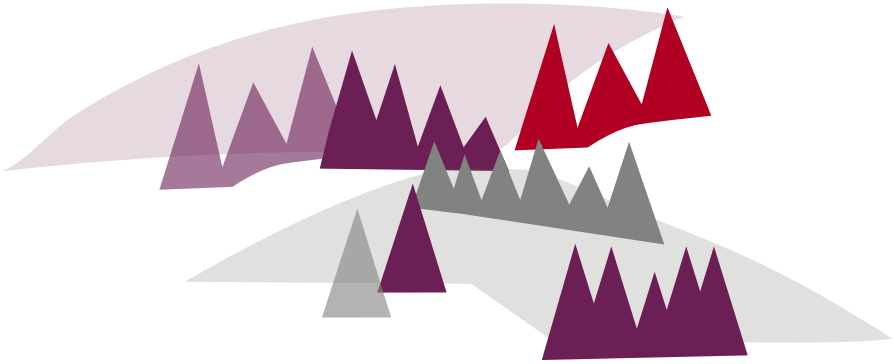
12. For government agencies, the term is defined in Section 3 of MSB's regulations on security measures in information systems (MSBFS 2020:7): External actor – Supplier not covered by these regulations, hired personnel or equivalent.

Term	Explanation
vulnerability	Deficient or absent security measures permitting one or more threats to be realised.
security function	A technical function that provides some element of security, such as access management systems, security logging, intrusion detection, intrusion protection or malware protection.
security logging	Automatic or manual recording of security-related events.
test environment	A part of the IT environment separate from the production environment and used to test information systems before deployment in the production environment.
outsource	To place part of the organisation's information, services or operations with an external actor, such as an IT operations provider.
training environment	A part of the IT environment separate from the production environment where users are given the opportunity to practice using the functions of an information system.
development environment	A part of the IT environment separate from the production environment, used to develop new and improve existing information systems before testing them in a part of the IT environment that is separate from the production environment.

1.2 Relation to general information security management

The security measures in this guidance are part of the security measures that an organisation needs to put in place to protect its information and information systems. The implementation of the guidance's security measures is part of the organisation's systematic and risk-based information security work.

MSB's methodological support for systematic and risk-based information-security work[13] is designed to support different types of organisations in different types of organisations in designing, improving and monitoring systematic and risk-based information security work, including responsibility, information classification, risk assessment, incident management and business continuity management. Further support for following up systematic information security work is provided in MSB's *Infosäkkollen* tool.



13. www.informationssakerhet.se/metodstodet/

Basic conditions

2. Basic conditions

2.1 Responsibility

2.1.1 Purpose

It needs to be made clear in the organisation who is responsible for ensuring that adequate security measures are implemented in an information system, and that there exist resources to adapt security measures as the needs of the organisation or conditions of the environment change.

2.1.2 Requirements

The organisation shall ensure that

1. each information system has a system owner14[14]
2. the system owner is responsible for implementing, adjusting, monitoring and evaluating security measures[15]
3. the system owner has the resources to implement and adjust adequate security measures in the information systems[16].

2.1.3 Responsibility to implement information security measures

Management has the overall responsibility to direct and focus information security work, and to ensure that adequate resources and mandates are in place. Otherwise, a typical division of responsibilities is as follows:

- The CISO is responsible for leading and coordinating information security work.
- The information owner is responsible for carrying out information classification and risk assessment for the information processed in his/her activity.
- The system owner is responsible for ensuring that the information system has the necessary technical security measures in place to protect the information it processes, and that there are approaches in place to evaluate and update security measures to ensure that the information system is adequately protected.

Management's governance and direction of the information security work shall make clear who the system owners are for the organisation's various information systems, and who has overall responsibility for the entirety of the respective parts of the IT environment, such as the development and test environment.

14. For each information system, the Authority must make clear which position is responsible for implementing, administering, monitoring and evaluating security measures (system owner). MSBFS 2020:7 Chapter 2, Section 1.

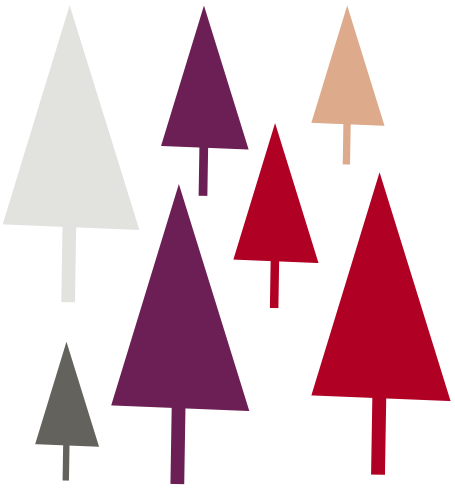
15. For each information system, the Authority must make clear which position is responsible for implementing, administering, monitoring and evaluating security measures (system owner). MSBFS 2020:7 Chapter 2, Section 1.

16. When designing the information security work, The Authority shall ensure that the necessary resources are allocated to the information security work, MSBFS 2020:6 Section 5 item 3.

2.1.4 Responsibilities of system owner

An organisation often has many different information systems. It is appropriate for a system owner to be responsible for several information systems of the same type. For example, one system owner may be given responsibility for the organisation's administrative systems (finance, personnel), another for property automation (electricity, cooling, lifts and similar), a third for the IT-environment network (routers, switches, DNS, DHCP and similar), a fourth for databases, a fifth for the web environment, etc. A system owner can also be given responsibility for all or part of an IT environment, such as a production environment, development environment, test environment or training environment. It is appropriate that the size of the organisation and the design of the IT environment determine how responsibilities are allocated.

The system owners in an organisation need to jointly and regularly, both among themselves and with the relevant information owner, discuss the need for future changes in their information systems, e.g., based on new risks, activity changes, new technologies or identified vulnerabilities.



2.1.5 Plan, do, check, act

System-owner responsibility means implementing, administering, monitoring and evaluating the adequacy of the security measures in place over time. Monitoring and evaluation should be done on a regular basis. If information-protection deficiencies are detected, the system owner needs to ensure that these are addressed, and inform the CISO and the relevant information owners. The need for additional security measures during peacetime crises, and before/during a state of heightened alert, also need to be considered.

In order to be able to assume responsibility, the system owner needs to know, among other things, the following:

- what information is processed in the information system and how it is classified
- who the information owner(s) are
- the hardware and software that make up the information system
- the dependencies on other internal and external information systems, and
- what security measures are in place.

The system owner also needs to ensure that procedures are in place to implement, administer, monitor and evaluate security measures in the information system, and ensure management if there are sufficient resources to enable the system owner to perform his/her task.

2.1.6 Resources, skills and knowledge

To support the ongoing work of system owners, additional resources may need to be allocated to technical administration and operations. The system owner also needs to appoint an information-system administration organisation, such as a technical administrator, to support the operational work. During budgeting and resource allocation, the system owner needs to take into account the need for personnel with the right skills.

This also includes being able to contribute resources to the incident organisation when incidents occur.

Some organisations shut down information systems at certain times when they do not have the resources to deal with potential incidents.

The system owner and his/her personnel need to understand the design of the information system, its purpose, limitations and how it is integrated with other systems. The need for skills can shift over the life cycle of the information system, from development and acquisition to deployment, updating, upgrading and decommissioning. The system owner needs to map and plan how the need for development, operation and administration skills vis-a-vis the information system shall be addressed.

Skills gaps can be addressed through training or by engaging external actors (consultants). External actors can be engaged to provide additional support with in-house operations, or to support with ordering expertise for acquisition and development. An organisation that relies on external resources for time-sensitive tasks needs to manage the risk that resources may not be available when the organisation needs them. Relying entirely on external resources for ordering expertise in acquisition and development can also pose risks, as the organisation may have difficulty understanding what is being acquired or developed and how it meets the organisation's needs. The organisation also needs to set requirements that reduce the risk of lock-in effects, i.e., difficulties in terminating a supplier relationship without risking unforeseen costs.

2.1.7 Dialogue with information owner

The system owner needs to have a dialogue with the relevant information owners in the different activities of the organisation in order to implement the security measures that provide the right level of protection for the information system. The need for security measures is identified on the basis of the information classifications and risk assessments carried out by the information owner, as well as the system owner's own risk assessments for the information system.

2.2 Threat intelligence

2.2.1 Objective

The organisation needs to collect threat intelligence to identify and manage threats to and vulnerabilities in the organisation's information systems.

2.2.2 Requirements

The organisation shall gather threat intelligence to[17]

1. identify potential threats to information systems
2. identify potential vulnerabilities in information systems
3. find support for how to handle threats and vulnerabilities in information systems.

2.2.3 Identify relevant sources

An organisation needs to follow developments in the field of information and cyber security in order to keep abreast of new threats, vulnerabilities and technological developments. The organisation needs to select relevant sources for its threat intelligence collection, such as

- the National Cyber Security Centre (the National Defence Radio Establishment, Armed Forces, MSB and the Security Service) regarding cyber attacks
- expert public authorities, such as
  - Authority for Privacy Protection (IMY) regarding personal data processing
  - MSB, including CERT-SE, regarding information and cyber security
  - The Security Service regarding protective security
  - Post and Telecom Authority (PTS) regarding electronic communications
  - The Defence Materiel Administration (FMV) for cyber-security certification of products and systems
- trade associations
- international actors in the field of cyber security, such as ENISA[18], NIST[19], CISA[20], CIS[21], OWASP[22].

What information is relevant depends on the information systems that the organisation uses in its activities. The system owner should take note of the relevant threat situations/indexes.

Regarding vulnerabilities, it is appropriate for the system owner to subscribe to newsletters and alerts from, inter alia:

- suppliers of the organisation's information systems and IT products
- CERT-SE – Sweden's national CSIRT (Computer Security Incident Response Team)[23] – at MSB.

Technological developments can be monitored by keeping the organisation up to date with the product changes planned by the organisation's suppliers.

Overall developments in new technologies also need to be monitored, for example through IT trade publications.

Threat intelligence facilitates the management of potential threats and vulnerabilities in information systems by helping the system owner identify actions that need to be implemented immediately (e.g., security updates) or need to be managed over a longer period of time (e.g., support for older versions being discontinued).

17. The Authority shall collect threat intelligence monitoring to facilitate identification and management of threats to and vulnerabilities in its information systems. MSBFS 2020:7 Chapter 2, Section 2

18. European Union Agency for Cyber Security.
19. National Institute of Standards and Technology (US).
20. Cyber Security and Infrastructure Security Agency.
21. Center for Internet Security.
22. Open Web Application Security Project.
23. www.cert.se.

2.3 Risk assessment

2.3.1 Purpose

Organisations need to identify, analyse and assess risks in order to take appropriate and proportional security measures for their information systems.

2.3.2 Requirements

The organisation shall

1. ensure consistent identification, analysis and evaluation of risks[24]
2. carry out a risk assessment of the production environment as a whole[25]
3. carry out risk assessment of information systems individually or collectively for information systems in the production environment with similar function, structure and use.[26]

The organisation should

1. ensure a risk assessment is also carried out for the organisation's[27]
   a. development environment
   b. test environment
   c. training environment.
2. give the system owner responsibility to ensure that the risk assessment is carried out for information systems for which the system owner is responsible.[28]

24. MSBFS 2020:6 Section 6, item 2 The Authority shall ensure that information security work is systematic and risk-based by identifying, analysing and assessing risks to its information (risk assessment).

25. MSBFS 2020:7 Chapter 2, Section 3 The Authority shall carry out a risk assessment for individual information systems and the Authority's production environment in its entirety.

26. MSBFS 2020:7 Chapter 2, Section 3 The Authority shall carry out a risk assessment for individual information systems and the Authority's production environment in its entirety.

27. General advice to MSBFS 2020:7 Chapter 2, Section 3 Risk assessments should also be carried out for the Authority's development, test and training environments.

28. General advice to MSBFS 2020:7 Chapter 2, Section 3 The Authority should consider giving the system owner of the information system concerned the task of ensuring that a risk assessment is carried out.

2.3.3 Assessing risks

The risk-assessment process provides a basis for deciding what security measures need to be put in place. Risk assessments raise risk awareness and increase knowledge of threats and vulnerabilities in the organisation's IT environment and the impact they can have on the organisation.

Simply, the risk assessment consists of answering four questions: "What can happen?", "Why can it happen?", "What are the impacts?" and "How likely is it to happen?". The basis for identifying threats and vulnerabilities in the risk assessment, and for assessing impact and likelihood, comes, inter alia, from external environmental monitoring. Impacts can include extra work, financial loss, missed opportunities, poorer health (in the worst case, death), financial costs of recovery and damage to confidence.

The objective of risk assessment is to describe all relevant threats and vulnerabilities that could lead to negative impacts on the functioning of information systems. It is important to devote resources and time to the risk-assessment process to ensure that as many relevant risks as possible are identified.

In a risk assessment for information systems and the IT environment, the system owner needs to consider, e.g., the following:

- the information – the need for protection of the information processed in the information system (assessed on the basis of the information owner's information classification and risk assessment)
- information systems – how and for what they are used
- equipment – clients, servers, mobile phones, printers, network components, USB sticks
- software – operating systems, drivers, firmware and applications
- physical conditions – access, server room, fire protection, electricity supply and cooling/heating

- approaches – rules and support for secure operation and administration
- resources – access to personnel with the right skills
- dependencies – on suppliers and services.

Information regarding threats, vulnerabilities and risks is often sensitive. It needs to be handled securely and be shared on a need-to-know basis.

2.3.4 Approach for identifying, analysing and evaluating risks

The organisation must have a defined approach for identifying, analysing and evaluating risks (risk assessment). In order for risk assessment to be conducted in a consistent manner, all system owners need to use the organisation's approach. The approach should indicate which positions are responsible for risk assessments, when and in what situations risk assessment shall be carried out, and what criteria and levels shall be used to assess impacts and likelihood.

Those carrying out the risk assessments need to document the results. The work includes providing the system owner with suggestions for risk-reduction measures. It is appropriate to use the results of the risk assessments both to develop the organisation's overall understanding of risk, and to see if the risk situation changes over time.

As a basis for a risk assessment, the system owner needs to have a dialogue with the information owner to learn about the risks that the information owner has identified and that are relevant to the system owner's risk assessment of the information system and IT environment.

For more information on risk-assessment procedures, see the methodology support for systematic information security work at Informationssakerhet.se/metodstodet.

2.3.5 Risk assessment of IT environment, production environment and individual information systems

Risk assessments need to be carried out for individual information systems and the production environment, both its components and as a whole. The organisation needs to have an approach to continuously identify and assess the technical risks associated with the organisation's IT environment and its constituent parts, so that the risks can be addressed through different types of security measures. In addition to the production environment, many organisations have other environments that should also be risk assessed.

This is commonly done for:

- environments for the development of information systems where developers can program and unit-test new or modified program code with the support of development software (development environment)
- environments for functional, system and user testing of information systems where testers can ensure that functions developed in the development environment meet the requirements, and that the information system will function as intended when commissioned (test environment)
- environments for training users where they can practice using the functions of an information system without risking the information and functions of the production environment (training environment).

When the organisation, in its activities, provides development, testing or training services to external parties, the part of the IT environment used for this is considered a production environment. This applies, e.g., to organisations providing development and testing services, but also to schools and universities' educational activities. The information systems developed or tested by external actors in such an environment do not process the organisation's information, and shall therefore not be considered part of the organisation's own

information processing.[29] The risks of allowing external actors to process their information[30] in this way in the organisation's production environment need to be assessed and managed.

Different risks can be identified for individual IT systems and the production environment in its entirety. Simply compiling the risks for each information system is not a sufficient basis for assessing risk in the production environment. When individual information systems are interconnected in an IT environment, risks can interact and change, even amplify. Thus, risks to the production, development, test, and training environments, as well as the IT environment in its entirety, need to be specifically assessed. The risks identified for the information systems included in each environment are one of several bases for that risk assessment.

The following are examples of conditions, threats and vulnerabilities that most organisations need to consider when assessing risk to the IT environment:

- Vulnerabilities in passwords can be exploited.
- Insufficient account and authorisation management.
- Weaknesses in the architecture of the IT environment, such as deficiencies in segregation, filtering and virtualisation.
- Lack of maintenance and updating procedures.
- Suppliers or other external parties with access to all or part of the organisation's internal IT environment.
- Need to change suppliers of hardware, software or service.
- Inadequate management of legacy information systems.
- Lack of equipment hardening leaving unnecessary services and protocols active.
- There is no verification or restriction of what software can be run or installed.
- Unsanctioned equipment can connect to the network.
- Private equipment, which the organisation can/may not administer, can connect to the organisation's internal IT environment.
- Lack of logging and knowledge regarding incident detection and management.
- Lack of ability to recover information from backups.
- Lack of physical security that may increase risk of fire, flooding or burglary.
- Lack of sufficient skills leading to dependencies on key personnel/external experts.
- Incorrect management of encryption keys, which can lead to information leakage.
- Lack of, or incorrect, documentation of information systems and dependencies.
- Lack of sufficient redundancy in essential information systems.
- Software lacks protection against simple user or administrator errors.
- The supplier of an outsourced service is subject to a denial-of-service attack.
- Network operator issues leave the internet inaccessible.
- Electricity or data/telecommunications cables are cut.
- Legal requirements are neglected.
- Lack of capacity in the VPN technology, complicating management of high loads, e.g., for remote working.

29. Such information systems are therefore not covered by the requirements of MSB's regulations on security measures in information systems (MSBFS 2020:7).

30. For example, software code, scripts or tests in the form of mapping the IT environment, attack methods, etc.

2.3.6 Risk assessment of training, test and development environments

In addition to the production environment, the organisation should risk-assess any development, test and training environments. Depending on the information and information systems present in these environments, in addition to the risks mentioned above, risks specific to these environments may need to be considered based on the information processed and the security measures in place.

2.3.7 Addressing risks

The findings of the risk assessment need to be documented in the form of a statement of identified risks, with an associated risk assessment. Work to address risks includes developing an action plan that provides an account of:

- who shall implement a security measure
- when it is to be introduced at the latest
- how its introduction and adequacy shall be checked.

Security measures that need to be implemented are developed in dialogue between system owners and information owners. The choice and design of security measures needs to be based on the information classification and risk assessment made by the information owner based on his/her activity, but also the risk assessments made by the system owner based on his/her knowledge of the IT environment as a whole. Dialogue also needs to be maintained with other support functions (e.g., legal) in order for the system owner to get an idea of the actual risks to be addressed.

2.4 Documentation of the IT environment

2.4.1 Purpose

The organisation needs to document its IT environment, its components, its information systems, its dependencies, and the hardware and software used in the IT environment in order to conduct secure operations and managment.

2.4.2 Requirements

The organisation shall, for all information systems, have up-to-date documentation regarding[31]

1. the hardware and software used in each information system
2. any dependencies on other internal information systems
3. any dependencies on information systems of external actors
4. if information that require enhanced security measures is processed in the information system
5. if the information system is particularly important for the organisation's ability to carry out its mission.

The organisation should

1. use technical tools to ensure that documentation of, e.g., information-system hardware, software and dependencies is up to date[32]
2. describe dependencies between information systems in a system map or equivalent[33]
3. use the result of classification of information to identify which information systems requiring enhanced security measures.[34]

31. MSBFS 2020:7 Chapter 2, Section 4 The Authority shall maintain up-to-date documentation on 1. the hardware and software used in each individual information system, 2. the dependencies between different internal information systems and the dependencies on information systems of external actors, 3. which information systems process information that needs enhanced protection, and 4. which information systems are central to the Authority's ability to carry out its mission.

32. General advice to MSBFS 2020:7 Chapter 2, Section 4 Technical support should be used to maintain up-to-date documentation.

33. General advice to MSBFS 2020:7 Chapter 2. Section 4 Dependencies should be made clear in a system map or equivalent.

34. General advice to MSBFS 2020:7 Chapter 2. Section 4 Information requiring enhanced protection should be identified with the support of information classification according to Section 6 MSBFS 2020:6.

2.4.3 Documenting the IT environment and its information systems

System-owner responsibility entails implementing, administering, monitoring and evaluating the adequacy of security measures over time. In order to do this, the system owner needs to ensure that there is sufficient documentation of the information systems or the part of the IT environment for which he/she is responsible.

This documentation needs to show what the IT environment looks like, including what products and services are used to conduct the mission.

It is also important to map dependencies between information systems in your own IT environment and dependencies on information systems of external actors, such as partners, service providers and subcontractors.

The organisation also needs to document other information required for operation and administration of the IT environment and information systems to be conducted safely.

It is therefore appropriate to document more than what is required by the regulations. In order to get the necessary overview of its IT environment, it is appropriate that the organisation document at least the following for each information system:

1. the purpose of the information system, including the activities in which it is used
2. what information is processed in the information system
3. the information owner(s) of the information in the information system
4. the information owner's classification of the information processed in the information system:
   a. if the information system processes personal data
   b. if the information system processes information covered by confidentiality
   c. if the information otherwise, after
   d. classification, requires enhanced protection as regards confidentiality, integrity or availability
5. the hardware and software that make up the information system
6. what dependencies, including integrations, exist with other internal information systems
7. what dependencies, including integrations, exist with information systems of external actors
8. who is authorised to access the information system and for what purpose
9. what security measures are in place
10. the information system's importance for the organisation to conduct its activities
11. the system owner's risk assessment for the information system
12. contact details for suppliers and public authorities to assist in the event of an incident.

When a system owner compiles the documentation for an information system, he/she needs to produce some parts, while other information is obtained from various sources.

Technical support for mapping IT environments can provide good support for documentation. It is also appropriate to obtain input from the CISO, the relevant information owners and the person who leads and coordinates the organisation's business-continuity management.

The system owner should, as part of the documentation, produce system maps describing the logical and physical location of informa-

tion systems in the IT environment. The system maps do not need to be complicated. The goal is to visually describe the IT environment to facilitate administration, troubleshooting and documentation. The system maps can also be produced using technical assistance.

If information processing is outsourced, this must be stated in the documentation. This applies regardless of whether it is a public authority that contracts with another authority, or whether an organisation contracts a supplier for, e.g., operation and administration of information systems.

It is appropriate that documentation that needs to be available for several different roles, e.g., operations personnel, CISOs and data protection officers, is stored in common inventories. As the inventory will contain detailed information regarding many information systems, the organisation will need to take appropriate security measures based on information classification and risk assessment. It is appropriate to pay particular attention to the increased risks caused by the aggregation of information. For example, it may be necessary to restrict access to different parts of the inventory.

2.4.4 Hardware, software and dependencies

Hardware can include desktop and laptop clients, servers, networking equipment (such as routers, switches, firewalls and access points), printers, storage networks, IP phones, mobile phones, tablets and IoT devices[35]. It is appropriate that, for each hardware unit, the inventory should at least specify

- type of hardware including model number
- identifiers, such as machine name, MAC address, network address and IP address
- the information system to which the hardware belongs.

It is appropriate that the inventory, for all types of software, including operating systems, drivers, firmware and applications installed on the hardware, at least state

- which version the software has
- when the software was installed
- when the software was last updated.

When documenting network traffic to and from other internal and external information systems, it is appropriate that the inventory at least specify

- between which network domains the network traffic passes
- between which information systems (internal and external) the network traffic passes
- information involved
- protocols, both for communication and encryption
- ports
- directions of traffic, including where it initiates and terminates.

2.4.5 Technical support for documentation

Documentation must be kept up to date to support the secure operation and administration of the organisation's IT environment. Software used in the various information systems of the IT environment changes during updates, installations or uninstallations, and hardware is sometimes moved between parts of the IT environment or different information systems. This means that updates may need to be made frequently. The process of documenting changes, especially in a more comprehensive IT environment, is greatly facilitated by the availability of technical support.

35. Internet of Things devices.

Those responsible for the operation and administration of the organisation's IT environment should use automated tools to actively identify and maintain a summary of

- the hardware (network and user equipment) connected to the IT environment
- the software (operating systems, drivers, firmware and applications) used in the IT environment
- network traffic (both internal and external) in the IT environment.

The summary can be used to check that no unauthorised hardware or software connects to the IT environment, and that all software has required licenses.

Use IT support to create system maps that visualise the logical and physical location of information systems in the IT environment, including data flows. System maps facilitate administration and troubleshooting of the IT environment.

Mobile devices, such as cell phones, are normally not directly connected to the network, but synchronise data via some type of service. A summary of these devices can be made via a Mobile Device Management (MDM) software.

2.4.6 Information requiring enhanced security measures

Information and information systems may need enhanced protection from one or more of the three information security perspectives: confidentiality, integrity and availability.

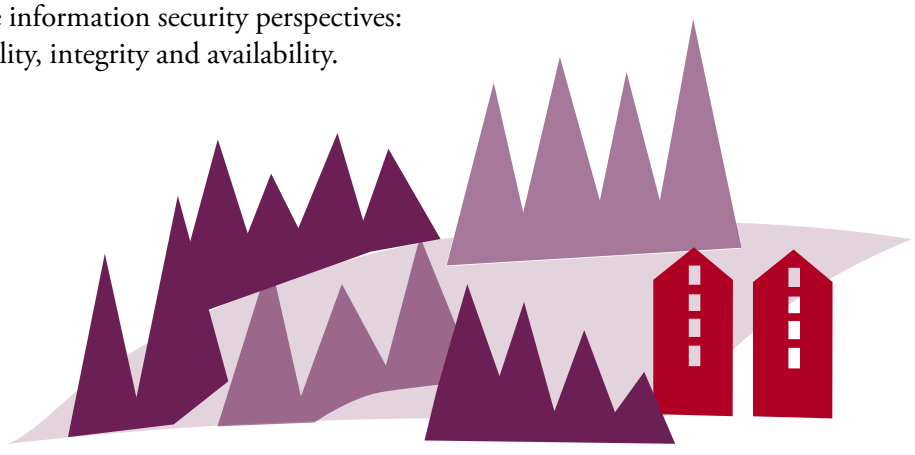
The need for enhanced protection is identified through the classification of information by the information owner. Assessment of an information system's protection needs is based on the information processed and how it has been classified. In addition to information classification, the results

of the risk assessment are also used when choosing security measures. All information systems must be protected by adequate security measures. If information requiring enhanced protection is processed, the security measures of the information system need to match the increased protection needs.

2.4.7 Information systems of particular importance to the organisation

The organisation needs to identify which information systems are particularly important for its ability to conduct activities. The basis for identifying such information systems can be drawn from business-continuity planning and information classification. In case of deviations, incidents, peacetime crises or a state of heightened alert, it is important that the organisation has prioritised which information systems need to function.

The prioritisation of information systems based on internal and external requirements needs to be determined by the organisation's management as part of its responsibility for the organisation's activities.



Development, acquisition and outsourcing

3. Development, acquisition and outsourcing

3.1 Identify security requirements

3.1.1 Purpose

Before developing or acquiring information systems or outsourcing information processing, the organisation needs to identify the requirements regarding security measures that are needed to provide adequate protection for information and information systems.

3.1.2 Requirements

The organisation shall[36]

1. when developing, acquiring or outsourcing information systems, identify security requirements relating to
   a. network segregation
   b. filtering of network traffic
   c. access, digital identities and authentication
   d. encryption
   e. security configuration
   f. security tests and review
   g. change management, upgrading and updating
   h. robust and accurate time
   i. backup
   j. security logging and related analysis
   k. network traffic monitoring
   l. monitoring of information systems including security functions
   m. protection against malware
   n. protection of IT equipment
   o. redundancy and recovery
   p. continuity during peacetime crises and before/during a state of heightened alert
   q. archiving
   r. disposal
2. document the security measures chosen to meet each requirement.[37]

The organisation should

1. combine organisational, administrative, physical and technical measures when choosing security measures[38]
2. group security measures decided upon into different levels of protection, which should correspond to the different impact levels used for information classification[39]
3. when acquiring information systems, consider products certified through third-party review using relevant established standards.[40]

36.MSBFS 2020:7 Chapter 3 Section 1 The Authority shall, when developing, acquiring or outsourcing information systems, identify security requirements relating to 1. network segregation, 2. filtering of network traffic, 3. access, digital identities and authentication, 4. encryption; 5. security configuration; 6. security testing and audits; 7. change management, upgrading and updating; 8. verifiable and accurate time; 9. backup; 10. security logging and associated analysis; 11. monitoring of network traffic, 12. monitoring of information systems including security functions; 13. protection against malware; 14. protection of equipment; 15. redundancy and recovery; 16. continuity during peacetime crises and before/during a state of heightened alert, 17. archiving, and 18. decommissioning. the security measures chosen to meet each requirement.

37. MSBFS 2020:7 Chapter 3, Section 1 The Authority shall document

38. General advice to MSBFS 2020:6 Section 6 When choosing appropriate and proportionate security measures, the Authority should combine organisational, administrative, physical and technical measures.

39. General advice to MSBFS 2020:6 Section 6 To facilitate information security work, the Authority should group security measures decided upon into protection levels, and link them to the information classification's impact levels.

40. General advice to MSBFS 2020:7 Chapter 3 Section 1 When acquiring information systems, the Authority should consider products that are certified by third-party verification with established standards.

3.1.3 Identify requirements for a secure IT environment

The process of identifying security requirements needs to be based on the needs of the organisation's activities, the results of the information classification and relevant risk analyses, and external requirements for information processing and its protection in, for example, regulations, standards and industry norms. Further, contracts and agreements may pose additional requirements for security measures.

Security requirements can be met by various security measures, and organisational, administrative, physical and technical measures should often be combined to achieve adequate protection. The distribution of responsibilities in the organisation determines which role poses/meets the requirements.

In many organisations, the information owner is responsible for developing information-processing requirements and for ensuring that organisational and administrative measures are in place to enable the activity to be safely and effectively conducted. It is then the responsibility of the system owner to implement appropriate technical security measures based on the information owner's requirements for the IT environment and information systems. The system owner is also responsible for putting in place the organisational and administrative security measures necessary to ensure that the information systems for which he/she is responsible can operate efficiently and securely. The system owner and the information owner in turn require the person responsible for the physical environment to implement adequate physical-security measures. The person responsible for the physical environment shall put in place the organisational and administrative security measures necessary to maintain physical protection.

The various security measures introduced in the IT environment must be able to protect against attacks as well as other undesirable events, such as human errors. This includes identifying requirements for security measures such as access management, encryption, backup, logging, monitoring, testing and auditing.

The different security measures also need to take into account that the different types of information in the organisation have different protection needs. The need for protection is shown by information classification and risk assessment. The person responsible for the IT environment should group the adopted technical security measures into different levels of protection corresponding to the need for protection of different types of information. By prioritising the use of security measures approved at a respective security level, the organisation can limit the number of products used to maintain a particular security function (e.g., malware protection). This facilitates secure administration by reducing the complexity of the IT environment, and available resources can be used more efficiently when fewer products are used.

3.1.4 Acquisition of information systems

An organisation must set the right security requirements when acquiring hardware and software for its IT environment. Security requirements shall be designed based on information classification and risk assessment, and shall address the needs of the organisation.

When acquiring information systems, the person responsible for the IT environment shall ensure that the organisation uses modern and up-to-date hardware and software with current security updates installed or available. Further, many products currently have built-in functions that transfer information regarding functionality and usage to the supplier. Ensure that the organisation information flows which, based on information classification and risk assessment, it deems inappropriate, without affecting the functions of information systems that the organisation needs.

Before acquiring information systems for use in maintaining a security function, it is necessary to check whether such functions are available, but inactivate, in existing hardware and software.

Such functions that exist need to be assessed regarding whether they are sufficient to achieve the desired level of protection, either alone or in conjunction with other security functions. When selecting interacting security functions, it may be appropriate to choose products using different technologies, e.g., different operating systems or programming languages. Thus, if a vulnerability is present in one product, the protection provided by other products may be unaffected. Acquisition needs to be made using a life-cycle perspective, ensuring that the supplier's plan for support, updates and upgrades of the information system matches the organisation's needs.

When acquiring information systems, the person responsible for the IT environment should consider products that are certified by third-party audit with the appropriate established standard. The purpose of the audit is to verify that the security requirements are satisfactorily met. An audit may have different purposes. It is important to check that the security requirements and configurations covered by the audit are relevant to the organisation, and that the results of the audit show that the information is adequately protected.

Resource allocation for the purchase of new information systems needs to be done on a long-term basis. In addition to the acquisition cost, there are costs for maintenance, management and decommissioning and replacement. The acquisition cost is often a small part of the total cost.

3.1.5 Development of information systems

An organisation must set requirements for both functionality and security when developing information systems for its IT environment.

Security requirements shall be designed based on information classification and risk assessment, and shall address the needs of the organisation.

Information-systems development here refers to the development and modification of software to meet an activity's need for both functionality and security. Development involves both coding and assembly of pre-coded modules to achieve what is requested.

Simply speaking, two main models of software development exist. The first, often called the *waterfall model*, produces all requirements at the beginning of the project, and then the programming work begins. The second, often referred to as *agile development*, produces the requirements and functions one at a time. This work needs to be done in close collaboration with the information owner. The information owner prioritises which part of the information system shall be required and programmed in the next step, based on the risk assessment.

Regardless of the model used, it is essential that the results of the development work are continuously documented and tested in order to detect security deficiencies. This also includes continuously assessing the existence of new or changing risks. It is essential that security requirements be addressed as early as possible in the development process, and the choice of model can influence this process. When security is monitored only at the end, before deployment, the cost of correcting deficiencies at this late stage may be much greater than if they had been dealt with in the initial phase. Security work needs to be conducted throughout the development process. This means, e.g., that developers need to be trained to create secure code and

deal with security requirements early on. The need for rapid modification in software sets new requirements for security work. Manually code-auditing each modification before deployment is in principle infeasible, as it would be very time-consuming and delay deployment. Many parts of the testing and security work in development may therefore need to be automated.

When developing software according to the *waterfall model*, there is a risk that security deficiencies (e.g., vulnerabilities and malfunctions) are identified late. Deficiencies may be more difficult to address at that time, if previously completed work on requirements and development needs to be redone or adjusted. Because this can be costly in terms of time and money, the developer and the information owners involved risk being forced to accept the deficiencies discovered or to try to resolve them by adding extra features that deviate from the original design of the information system. None of these options are appropriate. It is therefore important to implement a thorough risk analysis to identify potential problems before setting requirements.

When developing software according to the *agile method*, the requirements can be constantly clarified, and any deficiencies discovered can be tested and corrected. In contrast to the waterfall approach, the risk here is that the project is delivered in small parts, and the details of the requirements change constantly, which can make it difficult to see and risk-assess the whole.

This can be addressed in part by continuously identifying risks and addressing the greatest risks first. Here, too, a thorough risk analysis of both the whole and the parts is essential as a basis for setting requirements.

The following initial conditions need to be considered in the risk analysis for the requirements:

- legal requirements
- activity's needs for functionality in the information system
- the information owner's information classification and risk assessment for the information to be processed in the information system
- the choice of hardware and software to be included in the information system, including how long the hardware and software are updatable and provide sufficient functionality
- choice of security features to protect the information system
- functions of the information system and its location in the IT environment
- the development environment's tools for development and testing
- access to suitable test data in terms of quantity and content
- operation and administration regarding choice of programming language, skills, applications, services and other components
- archiving and decommissioning.

The risk analysis is best carried out in close cooperation between developers and those who will be responsible for operation and administration.[41]

3.1.6 Outsourcing

Outsourcing is when an organisation hires a supplier to carry out part of its own activities. An organisation can choose to outsource different degrees of its information processing. For example, this can involve IT development, IT support, or the operation of information systems. The motive for outsourcing may be, e.g., to cut costs[42], increase efficiency

41. To reduce the distance between developers (who want to see their code in production quickly) and operations (who want stable services without changes), the method of DevOps has come about.
Developers and operations are in close contact, and much of the installation and software updates are automated.

42. Outsourcing does not always cut costs. An organisation that outsources operations, instead of having its own operations unit, needs to spend more resources on requirements-setting and monitoring of suppliers regarding, e.g., meeting the organisation's information-protection requirements. When outsourcing IT development, costs are added to verify that security requirements are met over time by the party outsourced to. E.g., the organisation needs its own test environment to verify that the software is secure enough to be installed in the production environment.

or improve access to skills or hardware and software resources. Responsibility for the secure processing of the organisation's information and operations cannot be outsourced; only tasks can be outsourced. The organisation is responsible for its information regardless of where it is processed.

Before outsourcing information processing, it is important to check as a first step that any outsourcing meets the relevant legal requirements[43]. Such an analysis requires the organisation to specify

- what information is covered
- what information processing the supplier intends to carry out
- what suppliers might process the information, including any subcontractors
- where the information will be processed.

The next step is to check that it is appropriate, from the organisation's own perspective, to outsource information processing. In assessing this, the organisation needs to understand the challenges and risks of an external actor gaining access to and control over all, or part, of the information processed in the IT environment.

Many risks can be managed through clear and relevant requirements and monitoring. The organisation cannot assume that certain requirements are implicit, but must ensure that the contract is as comprehensive as possible. By setting functional requirements (what is to be achieved) rather than detailed requirements (how the requirement is to be achieved), the supplier can meet the organisation's needs even if it does not use exactly the same security measures as the organisation would have used. The security requirements for outsourced information processing need to be the same as if the organisation had processed the information itself. This means that the security requirements that the organisation imposes on its own information processing must also be imposed on the supplier. In addition, additional requirements may need to be placed on the supplier to compensate for the organisation's reduced control of the information.

In many cases, the organisation will need to compare its security requirements with the security measures offered in suppliers' standard deliveries and contracts. Getting larger suppliers to meet the organisation's requirements through supplements and adjustments to the requirements of the standard contract can require a lot of work by the organisation. In some cases, such changes cannot be brought about. It may also be difficult to check or ensure independent verification of the compliance of the supplier's information-processing with the organisation's requirements. If the organisation's requirements are not observed, or it is not possible to verify that security measures by the supplier are sufficient, the organisation needs to consider choosing another supplier or conducting the activity in-house.

Basic requirements for outsourcing

It is appropriate to set the following minimum requirements for the supplier's activities in the contract:

- The supplier shall comply with applicable regulatory requirements, such as those relating to data protection.
- There shall be established systematic and risk-based information security work.
- Risk analyses of the IT environment used to process the organisation's information shall be carried out in accordance with documented approaches.
- The supplier shall identify and manage the threat situation created by its own and its customers' activities.

43. For example, protective security, confidentiality and data protection.

- Security measures to protect information and information systems in terms of confidentiality, integrity and availability shall keep pace with technological developments and respond to changes in the threat situation.
- Security measures such as access and access control, encryption, logging, filtering, backup, monitoring and
- protection against malware must be in place.
- There shall be documented approaches for change management that include informing the organisation about upcoming changes.
- There shall be documented approaches for deviation and incident management. This includes when and how information shall be shared with the organisation, and how external incident reporting requirements shall be met.
- There must be documented procedures for business-continuity management, including crisis and contingency plans or equivalent. This shall include the supplier identifying which subcontractors it depends on to process the organisation's information during the contract period.
- There shall be physical protection that corresponds to the identified threat situation.
- Controls of the IT environment used to process the organisation's information shall be carried out.

At a minimum, it is appropriate that the contract set the following requirements for the relationship between the organisation and the supplier:

- The supplier shall provide documentation enabling the organisation to assess whether the design of the architecture, including the security architecture, used to deliver the contracted service meets the security requirements.
- The supplier shall provide documentation to enable the organisation to assess the conditions for the secure operation and administration of the information systems during the contract period.
- The supplier shall explain how it manages and informs about changes that may affect the organisation's information system.
- The supplier shall describe who accesses the organisation's information, where and how the information shall be processed and stored, and how it will be ensured that it is kept separate from the information of other customers.
- The supplier shall state in which countries the information processing will be conducted in such a way that the organisation can assess risks, suitability and the existence of legal obstacles.
- The supplier shall state which subcontractors are intended to be used at all stages. Subcontractors shall be approved by the organisation before they are granted access to information or other knowledge about the processing of information.
- It shall be clear what, how and when the supplier shall report to the organisation regarding deviations and incidents, risks identified, results of security controls and security measures taken to address deficiencies.
- The organisation, or a third party, shall be given the opportunity to test, audit and verify the security of the part of the supplier's IT environment used for the processing of information on a regular basis and as necessary.
- The organisation and the supplier shall agree regarding the activities to be carried out at the end of the contracts in order to promptly return, move or delete the organisation's information, including backups.

Compliance with the requirements needs to be checked before the contract is concluded. Monitoring and verification that protection is maintained over time also needs to be done throughout the contract period. If the requirements are not met, the organisation is at risk and needs to implement compensatory measures, change suppliers or terminate the outsourcing to process the information internally.

When outsourcing, there are additional costs for checking security-requirement compliance by the supplier over time. This may include checking approaches to prevent problems, testing updates in a test environment before deploying them in the production environment and ensuring that incident management works.

When outsourcing IT development

In addition to the above, if development takes place outside the organisation, suppliers may be required to carry out the development in a secure manner. This includes

- carrying out development work in a separate and protected IT environment
- protecting information, such as code, requirement/order documentation and communications such as code delivery and error correction.

In order to protect its production environment when deploying new or updated software, it is appropriate that the organisation have its own capability to test functionality and security before deployment. The organisation needs to ensure, regardless of any capability it possesses, that the tests performed and approved by the supplier are sufficient and verifiable by the organisation.

When outsourcing IT support

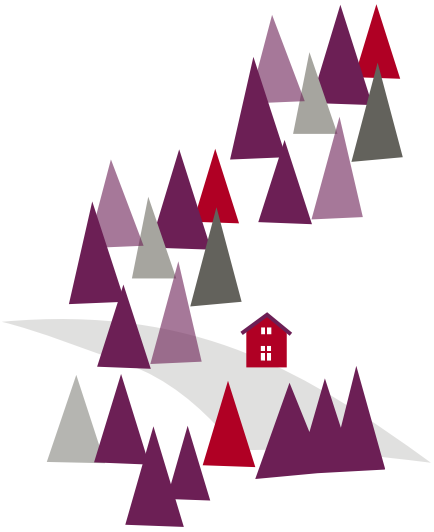
When outsourcing IT support, if information is processed in the organisation's IT environment, the supplier needs access to it. In practice, this often means that the supplier has access to all the information in the IT environment. The impacts of such access need to be risk-assessed before the organisation chooses to outsource.

External IT support to the internal IT environment often requires that the supplier be given the possibility of remote access. This can occur either to the entire IT environment, or to a limited part. Remote access rights may be granted to the supplier as a whole, or to specific employees of the supplier. The ability to perform support can be limited to a specific time, or to specific situations where the organisation approves access to the IT environment at any given time. If remote access is permitted, it needs to be designed according to the activity's needs and the risk assessment of the organisation.

Risk assessment also needs to be done if the supplier's employees perform their tasks on-site at the organisation and use the organisation's IT environment.

3.1.7 Documentation of security measures to meet requirements

By documenting which requirements are met by which security measures, it is easier to check that all requirements have been addressed and how. Many organisations choose to implement documentation at an overall level, and refer to detailed system information such as architecture descriptions. If the monitoring of the security measures in place reveals deficiencies, such documentation also supports the assessment of the risks that the deficiencies may pose. The documentation also facilitates the system owner's verification of the adequacy of security measures for secure operation and administration. When outsourcing, the organisation needs to assess which documentation they shall prepare themselves and which documentation the supplier shall be responsible for.



3.2 Controls

3.2.1 Purpose

In order to conduct secure operation and management, the organisation needs to verify that the chosen security measures are in place and provide adequate protection before deployment or any changes that may affect information-system security.

3.2.2 Requirements

The organisation shall, prior to deployment and before any change that may affect the security of the information systems,[44]

1. verify through security testing and review that the security measures chosen are sufficient to meet identified security requirements
2. verify the existence of the necessary documentation for operation and management
3. conduct risk assessment, and address security flaws identified through security testing and review, and in the verification of documentation.

The organisation should ensure that documentation for the operation and management of information systems includes[45]

1. architecture, components, configuration, data transfer and other relevant system information
2. the system owner
3. whether and to whom outsourcing take place.

44. MSBFS 2020:7 Chapter 3 Section 2 The Authority shall, prior to deployment and before any change that may affect the security of information systems, 1. Ensure through security testing and auditing that the chosen security measures are sufficient to meet identified security requirements, and 2. verify that the necessary documentation for operation and administration is in place. Where inadequacies are identified, The Authority shall risk-assess and address these inadequacies prior to deployment or any change that may affect the security of the information systems.

45. General advice to MSBFS 2020:7 Chapter 3 Section 2 Documentation required for operation and administration should include architecture, constituent components, configuration, data flows and other relevant system information. The documentation should also show the system owner and whether and to whom the information system is outsourced.

3.2.3 Design and carry out deployment controls

Even if the hardware and software developed has been thoroughly tested, vulnerabilities can be discovered afterwards. These can be caused by mistakes, faulty architecture, newly developed technology or administrative inadequacies. In serious cases, vulnerabilities may also have been deliberately introduced into the hardware or software by attackers, either during manufacture or in subsequent updates.

Therefore, before deploying new hardware or new/changed software, controls are needed to detect any shortcomings that may affect IT-environment security. Such measures can be carried out in various ways, e.g., by security testing, auditing or verification of documentation. This can be done, e.g., by testing updates in a test environment before installing them in the production environment, and by always ensuring that newly purchased hardware and software is updated to the latest version before installation in the IT environment.

It is appropriate for the organisation to have defined approaches for the implementation and combination of the different types of checks, as they can be resource intensive. The approach also needs to consider security needs by ensuring that high-security needs for information and information systems and high risk levels also mean more extensive checks of security measures.

During development, tests, audits and verification of documentation is carried out in the first place by the developing organization. In conjunction with development work, a test plan needs to be developed that describes the need for testing during development so that errors and inadequacies are detected and can be corrected before deployment. It is appropriate for the test plan to describe which tests are to be performed and when and how the tests are to be performed, including unit testing, system testing, integration testing, stress testing, acceptance testing, pilot testing and security testing such as client-, server- and

network-configuration testing and intrusion testing. Tests that may affect the IT environment need to be performed by people with specific skills and experience. External support may occasionally need to be engaged to carry out the tests.

In addition to testing, the organisation also needs to conduct audits at least at the end of the development process. Such audits need to be done before new hardware or new/modified software is installed in the IT environment.

A security audit means that the organisation verifies that the security requirements are met, both in terms of the level of protection and the chosen technology. This may involve verifying the security of developed code or that security measures have been properly implemented by auditing configurations and test results, for example. Audits are often performed manually, but the availability of automated audit support has increased in recent years. The audit is completed by verifying that the necessary documentation is in place for operation and administration as well as users to process information and information systems in a secure manner.

It is appropriate that deployment audits are carried out by personnel outside the development organisation. It is advantageous to assemble a group of personnel with different skills relevant for the audit, such as representatives from operations and administration, information and IT security, legal, information owners and system owners. It is appropriate for the organisation to assess the need to engage an external party with specific competence for the audit, particularly in the case of major and more sensitive development work, or when the organisation itself lacks the necessary competence.

Before the information system is approved and transferred to the production environment, selected security measures, including security functions, shall be activated, and inadequacies detected during testing, auditing and documentation verification shall be corrected. If there are inadequacies that cannot be remedied, these need to be risk-assessed.

See **Section 4.6** for further information regarding how security tests and audits can be conducted.

3.3 Development, test and training environments

3.3.1 Purpose

To protect the organisation's production environment from incidents that may occur in the organisation's development, test and training environments, the organisation needs to separate the production environment from these environments.

3.3.2 Requirements

The organisation shall

1. conduct development and testing that may affect security in an IT environment separate from the production environment[46]
2. identify and manage the need for a training environment separate from the production environment.[47]

3.3.3 Development and test environments

An organisation shall use separate environments for development and testing so that information processing in the organisation's production environment is not affected by problems related to development and testing. Lack of security in development and test environments can be used by an attacker to gain access to the organisation's production environment and the information managed there.

Environments can have various sizes and designs. Depending on its needs, an organisation can, e.g., use virtual development and test environments, or build these on an individual client. For an IT environment to be considered separate from the production environment, there must be no data flows or other integrations between them, except those required to move tested and proven hardware and software from the

test environment to the production environment. The organisation also needs to identify appropriate and secure ways to move completed code from the development environment to the test environment. The architecture needs to support the design of the environments through clear segregation. It is appropriate that each separate IT environment has a designated system owner responsible for implementing, administrating, monitoring and evaluating security measures. The system owner approves the information and information systems that the IT environment may contain.

Organisations that develop and modify hardware and software themselves must have a separate environment for development work, and a test environment to conduct tests, without affecting the security of the production environment. It is appropriate for organisations not conducting development work to have a test environment, in which they can check the security of acquired hardware and software before it is put into operation. Organisations outsourcing operation of their IT environment shall ensure in their requirements and compliance checks that the supplier keeps the organisation's production environment separate from the supplier's development and test environments.

About the development environment

The development environment shall be kept separate from the production environment, as development work often requires certain security features to be turned off to facilitate or even enable development. However,

46. MSBFS 2020:7 Chapter 3 Section 3 The Authority's work on development and testing that may affect the information security of the production environment shall take place in a part of the IT environment that is separate from the production environment.

47. MSBFS 2020:7 Chapter 3. Section 4 The Authority shall identify and manage the need for a training environment that is separate from the production environment.

information and information systems in the development environment need to be protected against, e.g., unauthorised access and unauthorised modification. This applies, e.g., to information such as source code and passwords to the development environment, to externally retrieved libraries used in the development work and the information systems used in development.

When developing information systems, it is important to have distinct approaches that describe how tested and approved program components/code shall be packaged. This is in order to have control over which versions of software code are under development, testing or approved for deployment.

About the test environment

Before deployment of newly developed or modified hardware/software in the production environment, security tests shall be carried out to verify that the security measures are sufficient to meet the security requirements, and that the hardware and software do not have any unwanted functionality. The tests shall be performed in an environment (test environment) separate from the production environment to prevent any security deficiencies in the hardware or software from affecting the production environment and the activity information processed there. Conducting tests in the production environment can cause serious disruptions. However, it may be necessary to verify that the information system is correctly set up in the production environment. This is not to be considered testing but, when done without affecting security, as a part of secure operation and administration.

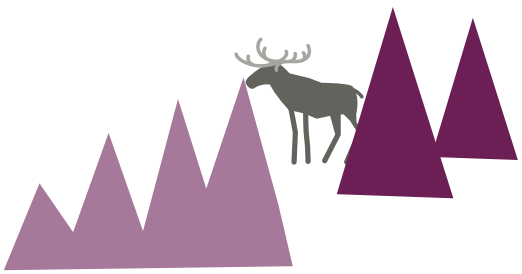
Testing can have different purposes, and this will determine how and in which environment it should be conducted. For example, in a development environment, tests can be done to ensure that developed or modified code has the intended functionality (unit testing).

The test environment is intended to be used for system testing and integration testing, for example. To create positive conditions for integration testing, the test environment needs to mimic the production environment as much as possible, or must simulate those parts of the production environment with which the hardware and software being tested will interact in the production environment. Security tests aimed at detecting vulnerabilities and verifying that implemented security measures are in place also need to be done in a test environment that is as similar as possible to the production environment.

The more similar they are, the more easily it is ensured that all vulnerabilities are detected.

System, integration and security testing requires the organisation to have access to an array of information systems in the test environment that can simulate the data flows of the production environment. This enables fully testing the functionality without using information from activities or risking the operation and security of the production environment.

Some organisations use two identically-defined environments for each information system, with identical hardware and software: one for production and one for testing. When the information system in the isolated test environment is tested, and the system owner has approved it for deployment, the addressing is redirected, so that the test environment of the information system becomes its production environment, and the former production environment becomes the new test environment.

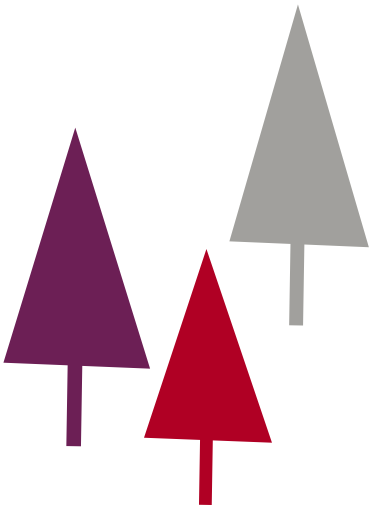


3.3.4 Training environments

In order to train employees on how an information system works, there should be a training environment where mistakes can be made without affecting operations in the production environment. When an organization assesses the need for such a training environment to be kept separate from the production environment, at least the following risks should be considered:

- unauthorised access to information in the production environment, e.g., personal data
- unauthorised modification of information used in the production environment
- information systems used in the production environment being linked to information systems in the training environment, e.g., to demonstrate the whole workflow.

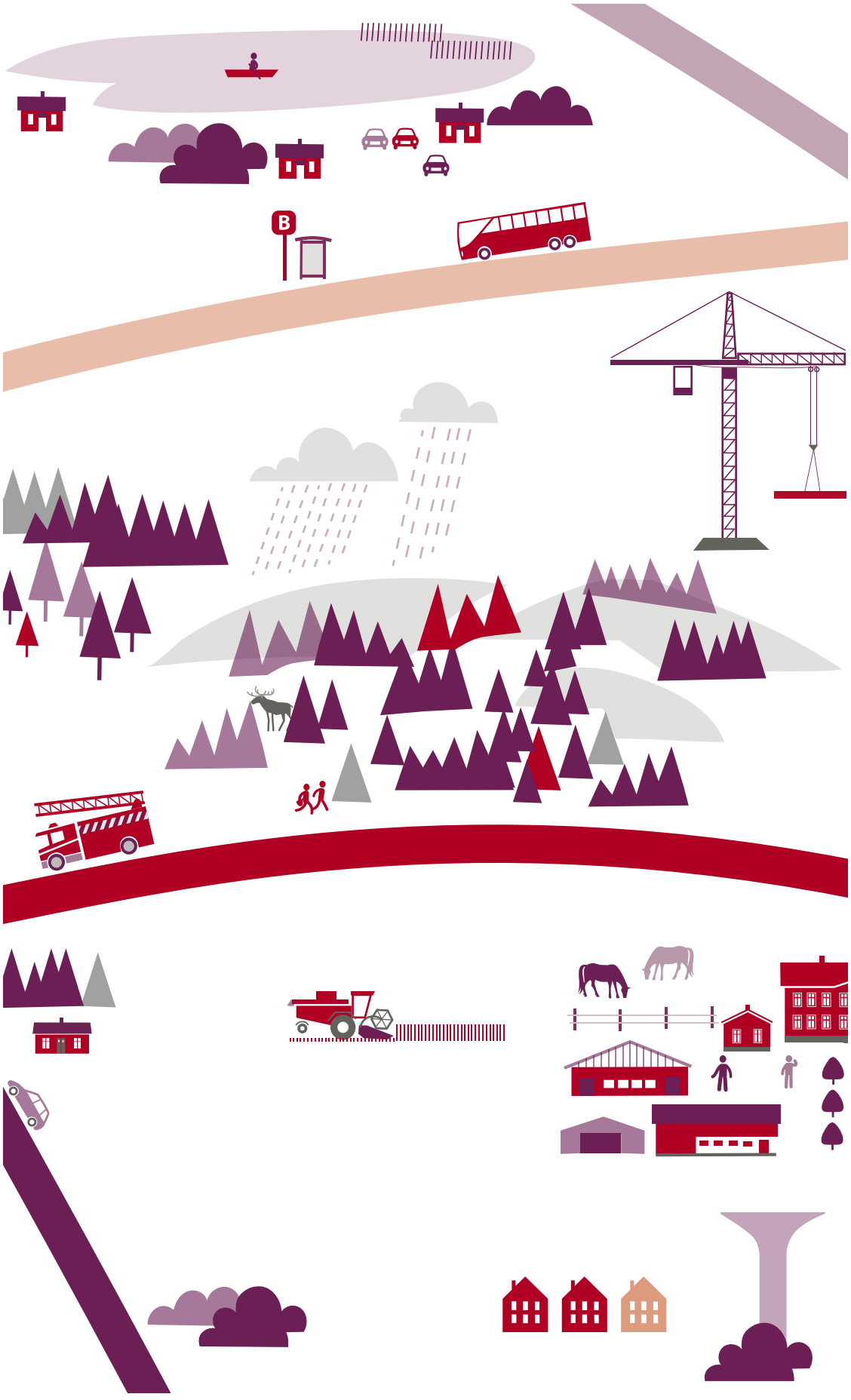
In order for the training environment to be seen as separate from the production environment, there must be no data flows or other integrations between the two environments. However, in order to make the training as realistic as possible, it is appropriate that the information systems in the training environment be as similar as possible to the information systems in the production environment in the areas in which the employees are to be trained. It may also be appropriate, as in the test environment, to be able to simulate the data flows needed to achieve a realistic training environment.



The information used in information-systems training should primarily consist of test data. If the organisation needs to use activity information, i.e., information from the production environment, in the training environment, it is important to verify that no legal regulations or operational requirements prevent such processing, such as the General Data Protection Regulation.

The system owner needs to authorise the processing of such information, and needs to ensure that the information system in the training environment is protected in a manner equivalent to the information system in the production environment. Employees undergoing training need to be informed about the information used in the training, in particular when activity information (production data) is used, and the processing rules that apply.

The training environment referred to here is intended to be used only for internal training of personnel in the information systems used in the activity. Organisations that carry out activities in the form of teaching do not use a separate training environment, but rather their production environment, for this purpose. This is because teaching is the activity that the organisation conducts. For this type of organisation, including, e.g., colleges and universities, it is appropriate to divide their production environment so that teaching takes place in an environment separate from the part of the production environment used for administrative tasks such as finance, grading, case management and study guidance. Depending on the focus of the teaching and its components, it may also be necessary to further segregate the teaching part of the production environment, e.g., if information systems are provided that can be used for code development, intrusion testing or similar. Lack of security in the training environment can be used by an attacker to gain access to the organisation's production environment and the information processed there.


B

Operation and administration

4. Operation and administration

4.1 Netwok segregation and filtering

4.1.1 Objective

To prevent the spread and impact of incidents, the organisation needs to segregate its IT environment and filter traffic so that only necessary data traffic is allowed.

4.1.2 Requirements

The organisation shall

1. place information systems with different functions in separate network domains in their production environment[48]
2. filter network traffic so that only necessary data traffic between different network domains .is allowed[49]

The organisation should place the following functions in separate network domains:[50]

1. clients for users
2. clients for system administration
3. servers
4. central system-security functions in the form of access-control systems, security logging, filtering, etc.
5. central support functions in the form of printers, scanners and the like
6. wireless networks
7. guest network
8. externally accessible services
9. information systems linked to information systems of external actors
10. industrial information and control systems (ICS-systems)
11. systems containing vulnerabilities that can not be eliminated.

48. MSBFS 2020:7 Chapter 4, Section 1 The Authority shall prevent the spread of incidents and reduce the impact of attacks by placing information systems with different functions in separate network domains in its production environment.

49. MSBFS 2020:7 Chapter 4, Section 2 The Authority shall filter network traffic so that only necessary data flows occur between different network domains.

50. General guidance to MSBFS 2020:7 Chapter 4 Section 1 The following functions in the production environment should be placed in separate network domains: 1. Clients for users. 2. Clients for administration. 3. Servers. 4. Essential system-security functions in the form of access-control systems, security logging, filtering, etc. 5. Essential support functions in the form of printers, scanners, etc. 6. Wireless networks. 7. Guest network. 8. Externally accessible services. 9. Information systems linked to the information systems of external actors. 10. Industrial information and control systems. 11. Systems containing unmanageable vulnerabilities.

4.1.3 Need for network segregation

The network is an important part of the organisation's IT environment. The organisation's network often extends far beyond the physical office premises when services are outsourced, wireless networks[51] are used, partner networks are interconnected, or services are made available to employees at home/on the road. It is no longer possible to speak of a physical delimitation of the network.

Networks must be protected against internal and external threats, as well as deliberate and accidental threats. The organisation needs to assume that all information systems in the IT environment contain known and unknown[52] vulnerabilities. These may be due to deficiencies in the design, implementation or configuration of hardware and software. To counter the impacts of deficiencies, the organisation needs to ensure that any incidents do not spread in the network, and that the impacts are limited to a small part of the IT environment. One way to do this is to segregate domains within the network.

51. Wireless networks include not only WIFI based on the 802.11 standard, but also wireless networks for, e.g., IoT devices (such as Zigbee, LoRaWAN, Z-wave), Bluetooth, mobile phone networks (GSM, 3G, 4G and 5G), etc.

52. Unknown vulnerabilities are vulnerabilities that have not yet been discovered by anyone, such as a vendor, hacker group, security researcher or public authority.

The network domains in turn need to be protected by various security measures. These include network traffic filtering, access, encryption, security configuration, backup, logging, monitoring, malware protection and redundancy. The design of the security measures, and the level of protection they need to provide, depends on the protection needs, use and purpose of each network domain.

A risk assessment shows whether certain network domains may need to be physically separated from the rest of the IT environment. A physically separated network domain has no connection to other network domains and no data traffic to or from the network domain via a network connection.

4.1.4 Segregation

Segregation of network domains is facilitated if the organisation (most appropriately the system owner of the network) has previously described the design of the network at an overall level. The design can be illustrated using a domain model. The different domains in such a model may differ, e.g., in terms of use, protection needs and the possibility of external communication.

The domains are separated from each other by filtering the network traffic between them, e.g., by means of firewalls. A domain can consist of one or more network domains. Network traffic between domains, even in the same domain, needs to be separated by filtering.

Below, the design of a network domain model is illustrated for an organisation that, in addition to its production environment, also has IT environments for development, testing and training. The production environment here consists of network domains for

- user system
- activity system
- system administration
- essential system-security functions
- externally exposed systems.

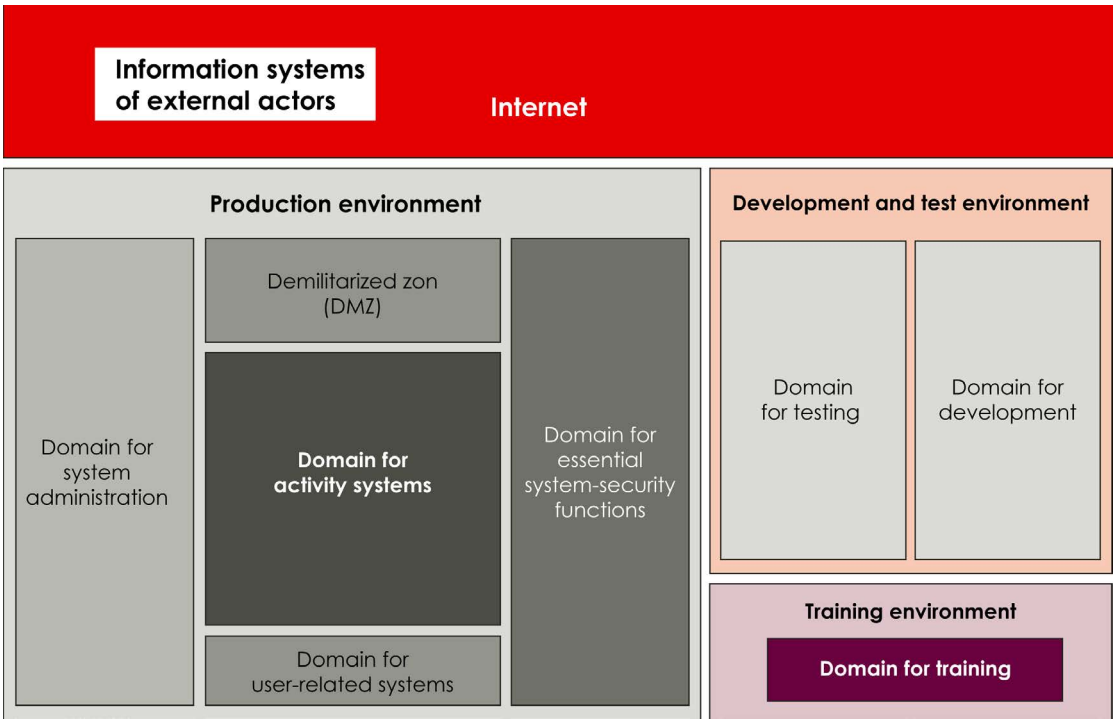


Figure 1. Examples of an organisation's surroundings and overall classification of IT environments and domains.

The different network domains have different uses, protection needs and external communication. Below are examples of domains and the information systems they contain.

- **Production environment**
  - **User-systems domain:** user clients and user applications.
  - **Activity-systems domain:** servers, databases, directory services and network equipment.
  - **System-administrator domain:** services and clients used for system-administrator operations.
  - **Domain for essential system-security functions:** access control system and security log.
  - **Externally exposed domain (aka DMZ):** services exposed to the Internet, e.g., public web servers, VPN concentrator and email gateway.
- **Development and test environment**[53]
  - **Domain for development.**
  - **Domain for testing.**
- **Training environment**
  - **Domain for training.** Information systems used, for example, to train users or system administrators when a new information system is implemented.

The information systems in each domain are grouped into different network domains.

The above domain model is just one example of how the IT environment can be schematically divided, and an organisation needs to design the network of its IT environment according to its needs. It may be necessary, e.g., to further segregate the development, testing and training environments.

53. The development and test environment does not need to be a two-domain environment. The organisation can also choose to have a separate development environment and a separate test environment, which in turn are divided into different domains.

The design of the network is influenced by the complexity of the organisation's IT environment. The complexity may involve, for example, that all or part of the information processing is outsourced, that other organisations have direct access to parts of the IT environment or that the public has access to various e-services. Building security into the network at multiple levels is one way to deal with such challenges.

4.1.5 Network segregation

A network domain can consist of one or more domains. The system owner of the network needs to ensure that segregation reflects the need for separation of:

- information with different levels of sensitivity
- information with different availability requirements
- information with different communication requirements
- information systems with different levels of exposure
- information systems with different functions
- information systems used by specific roles.

Segregation can be done with the support of logical measures, such as VLAN (Virtual Local Area Network). Segregation can also be done using physical separation, where one network has no physical interconnections with another network.

As in the DMZs, communication between domains is regulated by filtering traffic based on a strict need regarding the data traffic required. The system owners of the various information systems need to analyse what data traffic is required for the information system to meet the needs of the activity and what data traffic pose risks. The system owner of the network can then place the information system in the appropriate network domain corresponding to the needs. Some organisations place all their information systems in their own domains in order to filter completely based on the needs of each information system. To support the operation and administration of the different network domains, tools such as SDN (Software Defined Networking) can be used to describe the different parts of the network.

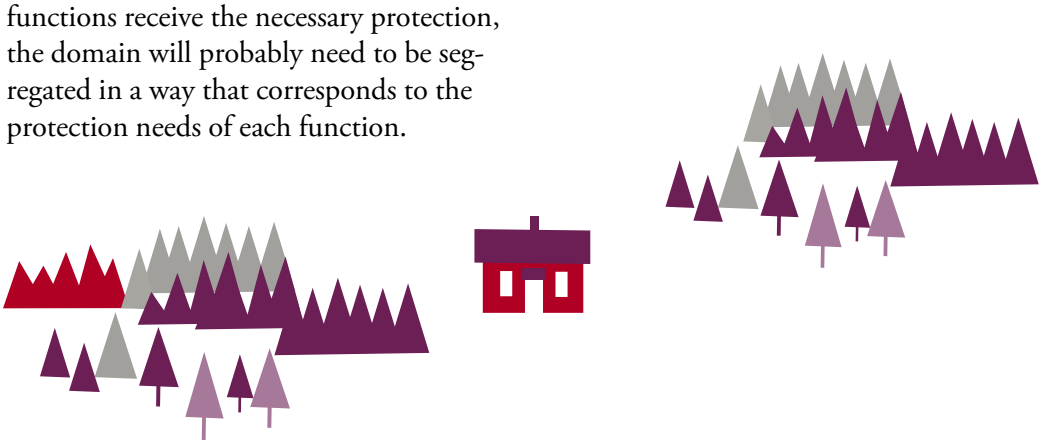
Some functions in the production environment should always be placed in separate network domains. The following list of such functions may need to be expanded depending on the needs of the organisation, risk assessment and technical conditions.

- clients for users
- clients for administration
- servers
- essential system-security functions
- essential support functions
- wireless networks
- guest network
- externally accessible services
- information systems linked to the information systems of external actors
- industrial information and control systems
- systems containing unmanageable vulnerabilities.

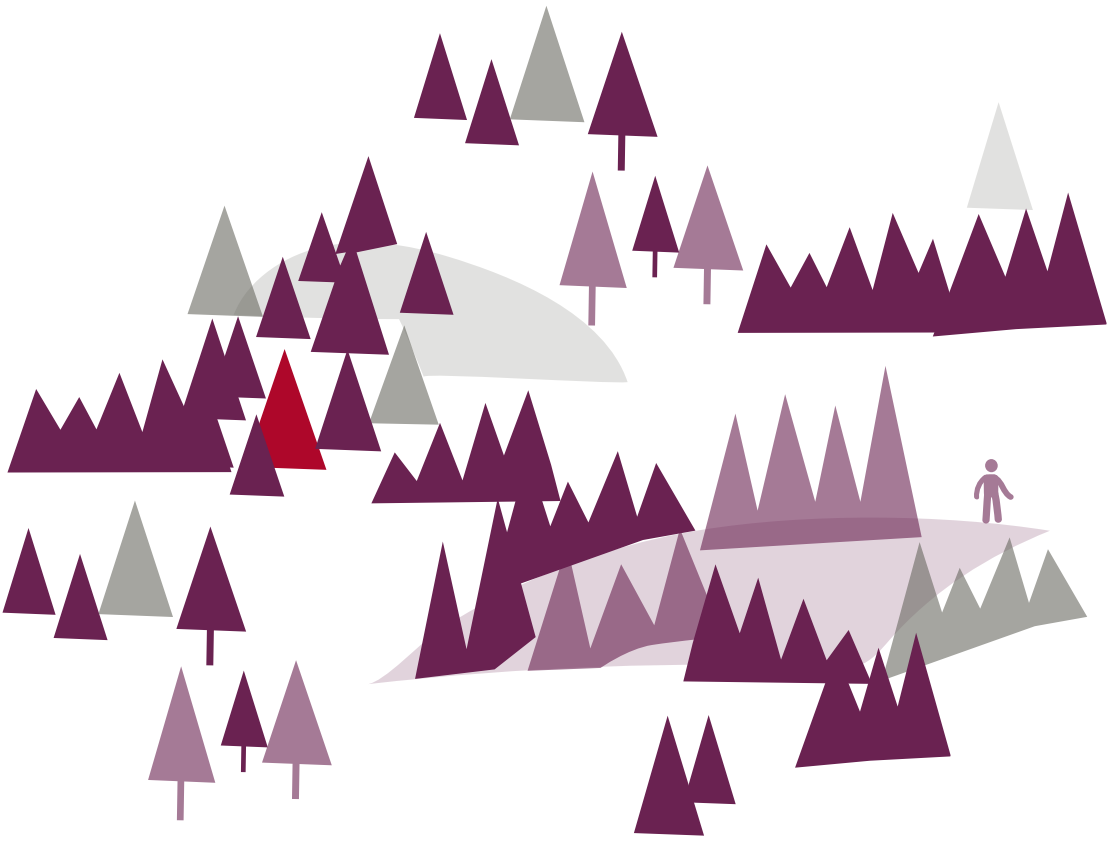
There are various reasons why the above functions should be placed in different network domains.

- **Clients for users:** The organisation's employees usually need access to the internet simultaneous to accessing the internal environment. In order to protect other parts of the organisation's IT environment from possible incidents caused by user-client exposure to the internet, these should be placed in one or more dedicated network domains. It is appropriate not to place too many user clients in the same network domain.

- **Clients for administration:** System administrators need high levels of access to perform their tasks, and can thus affect IT environment security. Unauthorised access to the IT environment via clients for system administration can have significant negative impacts. The system owner therefore needs to ensure that such clients are placed in one or more network domains where they are never given access to the Internet or other external networks.
- **Servers:** The servers handle one of the organisation's main assets, its information. To sufficiently protect both the information and the information systems, these should be placed in one or more separate network domains. For example, it is appropriate to place servers that, after information classification and risk assessment, have been assessed as requiring enhanced protection, e.g., in terms of availability, monitoring, confidentiality or redundancy, in a dedicated network domain that can provide that extra level of protection.
- **Essential system-security functions** in the form of access-control systems, security logging, filtering and so on. Essential system-security functions serve a crucial role in enabling an organisation to process information in a way that meets the needs of the activity for confidentiality, integrity and availability. They should therefore be placed in a special domain with high security requirements. In order to ensure that the various system-security functions receive the necessary protection, the domain will probably need to be segregated in a way that corresponds to the protection needs of each function.
- **Essential support functions** in the form of printers, scanners and the like. These information systems exist to facilitate users, which means they need to be easily accessible and simple to use. The benefit to users is thus sometimes prioritised over security, and this can be compensated for by placing such systems in a separate network domain, separated from the organisation's other information systems.
- **Wireless networks.** The use of wireless networks makes it more likely that outsiders can access the organisation's information, as the network signal can often be received by non-employees, both within and beyond the organisation's premises. Placing them in a dedicated network domain simplifies the control and administrative work of ensuring that all wireless networks are managed securely.
- **Guest network.** Guest networks offer the organisation's visitors internet access. This service for visitors must not simultaneously permit access the organisation's internal IT environment. Guest networks should therefore be placed in a dedicated network domain. If the organisation allows employees to connect personal equipment to the organisation's network (e.g., private mobile phones), this equipment must only be able to connect to the guest network, as it needs to be completely separated from other internal networks, and may not have any access to the rest of the IT environment.



- **Externally accessible services.** Services that are exposed to the internet, such as public web servers, VPN concentrators and email gateways, are visible to other actors on the internet and thus often vulnerable to attack attempts. The aim is in most cases to gain access to the organisation's internal IT environment.
- Externally accessible services should be placed in one or more network domains that can receive an extra layer of protection in the form of security measures that detect and manage the impacts of an attack.
- **Information systems linked to information systems of external actors.** In order that IT incidents which occur at an external actor do not impact one's own organisation, information systems that are interconnected with information systems of an external actor need to be placed in one or more separate network domains.
- **Industrial information and control systems.** This type of information system is particularly vulnerable, as it often lacks the ability to take advantage of the security measures used by office IT systems. This vulnerability therefore needs to be compensated for by other types of measures, which is simplified when they are located in network domains separated from the rest of the IT environment.
- **Systems containing unmanageable vulnerabilities.** Some information systems, due to age, design, use or other reason, cannot be protected by efficient and proportionate security measures. To prevent residual vulnerabilities from affecting other information systems in the IT environment, or from being exploited by attackers to access the organisation's IT environment, these need to be placed in one or more separate network domains.



4.1.6 Data traffic filtering

Filtering of data traffic is preferably done through what is commonly known as a firewall. The filtering function may also be implemented in other information systems or other types of network equipment, such as proxy services or data diodes.

Firewalls can be hardware- or software-based. The design of firewalls also differs according to their purpose, e.g., network firewalls and application firewalls. Many operating systems include a client/server firewall[54] which aims to protect the information system from attack by filtering by port, type of application and user accounts with access to initiate traffic.

The network firewall filters incoming and outgoing network traffic based on, for example, protocol, port number and IP address, and in some cases also content. Next-generation firewalls can filter information flows from the data warehouse up to the application layer in the OSI model.

Consider using proxy services to control certain types of data flows, such as web traffic, so that the organisation's clients cannot be identified when communicating on the internet. Proxy services can be used to terminate traffic, preventing external data flows from entering the information systems of the internal network domains. The internal systems instead retrieve the information in the proxy service. The proxy service may also restrict the websites to which data may flow, and provide some monitoring functionality. Internally, proxy servers can be used to regulate data flows between different internal domains.

Data diodes are used to prevent two-way communication. Such a hardware component allows communication only in one direction, making it impossible to transmit information in the opposite direction.

54. Also called Host-based firewall.

Rules for filtering

The organisation needs to regularly review the rules the traffic-filtering equipment follows to verify that filtering only allows the traffic needed by the network domain's information systems. If data traffic is only permitted for a limited time, the aperture allowing the data traffic should be automatically disabled when the time period ends.

Data flows to physically separated network domains[55] shall be controlled by, for example, moving information with external hard disks, USB sticks or CDs. Thus, this type of physical data flow also needs to be regulated. Organisations receiving information from external parties on, e.g., CDs, DVDs and USB sticks, also need rules to check and approve the content of such physical data streams before they are transferred to the physically separated network domain. It is appropriate that the check be carried out in a separate IT environment.

Filtering between domains

An organisation diving its network into different domains needs to ensure that the filtering rules applying to each domain support the purpose of the domain. The direction in which network traffic is permitted to travel, including where it may be initiated or terminated, has a major impact on the organisation's ability to protect the information systems in the different domains. For example, the organisation needs to ensure that network traffic from the internet is terminated in the domain of externally exposed systems, and does not go directly to an information system in an internal domain. Network traffic from information systems interconnected with information systems of an external actor should also be terminated in the domain of externally exposed systems, if possible, and then retrieved from there by the organisation's own corresponding information system.

55. In some cases, this can be called "air gapping", i.e., there is only air between the networks and no coupling (cabling, wireless transfer etc.) between the isolated network and other networks.

Further segregation (sub- or micro-segregation) of those domains connected to numerous other domain is also particularly important, especially when these domains are not interconnected. Otherwise, one domain risks becoming a bridge between the others.

The domain model has been complemented in Figure 2 with additional domains and arrows to illustrate the appropriate direction of data traffic.

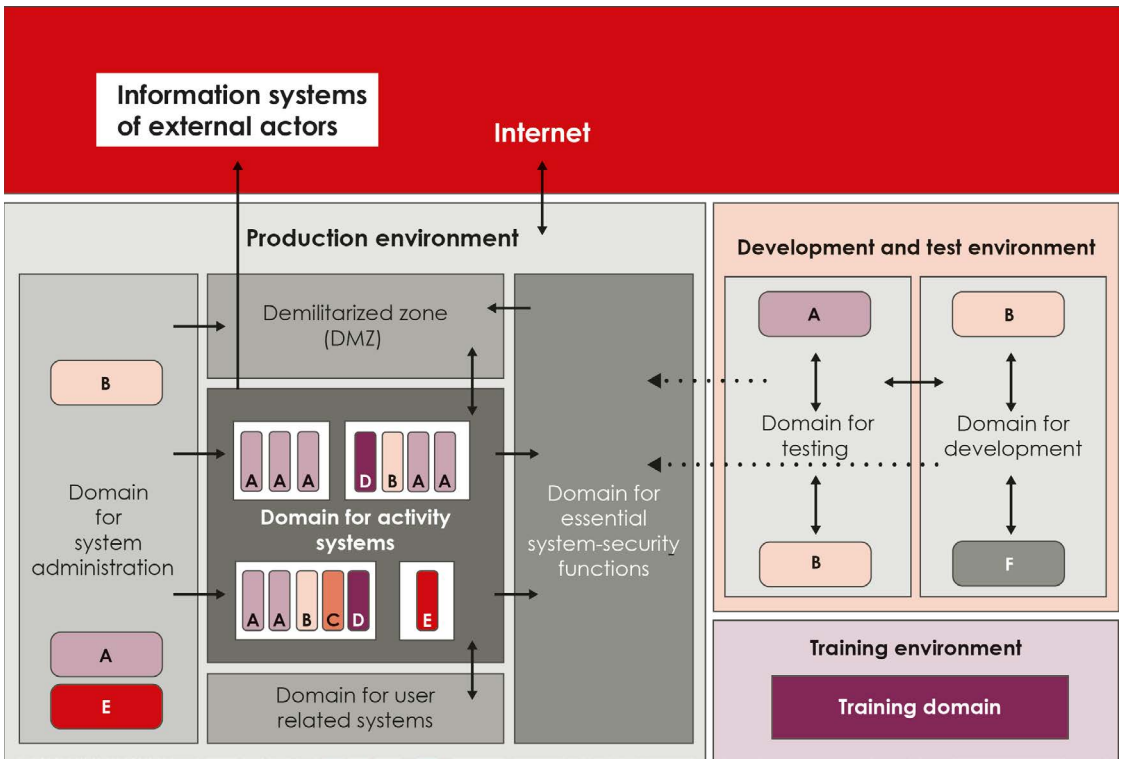


Figure 2. Examples of an organisation's domains and communication paths internally and with the surroundings. A–F symbolise information systems with different functions and/or processing information with different protection needs.

4.2 Access management and digital identities

4.2.1 Purpose

In order to control which users and information systems are allowed to access the IT environment, the organisation needs to assign them digital identities. To ensure that each digital identity only has the necessary access to the information and information systems in the IT environment, the organisation needs to manage access rights of the digital identities.

4.2.2 Requirements

The organisation shall

1. ensure that only permitted users and information systems have access to the IT environment[56]
2. design access management to ensure that each digital identity does not have more access
3. to information and information systems than necessary[57]
4. ensure that digital identities granting system administrator access rights are used only for system administration[58]
5. ensure that system administrator access rights are assigned restrictively.[59]

The organisation should

1. use access management to ensure that[60]
   a. digital identities in the production environment are unique
   b. digital identities and access rights are approved before they are linked to a user or an information system
   c. assigned access rights are time-limited and verified once a year
   d. the need to use different directories for digital identities and access rights is identified and managed
   e. digital identities used to access the development and test environment should be different from the digital identities used to access the production environment.
2. ensure that a digital identity can only be used by one individual[61]
3. manage digital identities and access rights that provide access to externally accessible information systems in directories separate from the directories of the production environment[62]
4. manage digital identities and access rights that provide access to the development, test and training environment in directories separate from the directories of the production environment[63]
5. ensure that a digital identity with system administrator access rights is only granted access to a limited part of the production environment.[64]

56. MSBFS 2020:7 Chapter 4, Section 3 The Authority shall ensure that only permitted users and information systems have access to the IT environment and ..

57. MSBFS 2020:7 Chapter 4 Section 3 The Authority shall ... design its access management so that each digital identity has no more access to information and information systems than necessary.

58. MSBFS 2020:7 Chapter 4. Section 4 Digital identities that provide system administrator authorisation shall only be used for system administration and ..

59. MSBFS 2020:7 Chapter 4. Section 4 Digital identities that provide system administrator authority shall... be assigned restrictively.

60. General advice to MSBFS 2020:7 Chapter 4, Section 3 Access management should ensure that 1. digital identities in the production environment are unique, 2. digital identities and access are approved before being associated with a user or an information system; 3. assigned access are time-limited and checked once a year; 4. the need to use different directories for digital identities and access is identified and managed; and 5. different digital identities are used when accessing the development and test environment and the production environment.

61. General advice to MSBFS 2020:7 Chapter 4 Section 3 A digital identity should only be used by one individual.

62. General advice to MSBFS 2020:7 Chapter 4 Section 3 Digital identities and access that provide access to externally accessible information systems and the development, test and training environment should be managed in different directories separate from the directories for the production environment.

63. General advice to MSBFS 2020:7 Chapter 4 Section 3 Digital identities and access that provide access to externally accessible information systems and the development, test and training environment should be managed in different directories separate from the directories for the production environment.

64. General advice to MSBFS 2020:7 Chapter 4. Section 4 A digital identity with system administrator access should only be granted access to a limited part of the production environment.

4.2.3 Digital identities

A digital identity identifies a person or a specific information system in the form of a username or system identifier. It is common to use the term "account" instead of digital identity, i.e., the person or information system is given an "account" in the IT environment that is unique to that person/information system. A digital identity should only be used by one person. All organisations often have at least three different types of accounts: user accounts, system administrator accounts and system accounts (for information systems). A digital identity to be used for system administration shall be assigned restrictively.

When an organisation assigns a digital identity to a specific person, in most cases the organisation needs to verify the identity of the person before they are assigned a digital identity and assigned an account in the IT environment. This can be done in different ways depending on the level of assurance required that this is the correct person. The level of assurance in the digital identities of individuals depends on how the identification is done. Compare showing a passport (applied for and collected at a police station) at an identity check, with a driving licence (applied for at the Swedish Transport Administration and collected by registered mail) and a homemade ID badge (unclear manufacturing and issuing process). In this example, a passport would provide most assurance, followed by a driving licence and then the homemade ID badge. If the person is to have access to the IT environment, the organisation needs to ensure identity, for example through a physical visit where the person has to show a valid and verifiable ID.

To achieve the intended assurance in digital identities, both internally and when communicating with external stakeholders, the organisation needs to ensure that digital identities are securely managed in terms of assignment, activation and deactivation. In addition, the organisation needs to ensure that passwords are protected, and that there is a capability to detect and manage incidents related to digital identities. It is appropriate to use technical support for the management of digital identities.

4.2.4 Access management

The organisation must be able to manage the access of the digital identities in a way that ensures that the right permission is associated with the right digital identity. Access can be designed in different ways. For example, access may grant the right to read, search, write, delete and create information and execute code in an information system, but access may also be limited to one or more of these rights.

To facilitate the process of linking the right access to each digital identity, the organisation needs to map and define the different user groups, both of personnel and information systems, that exist in the organisation. Examples of such user groups are:

- all in-house personnel
- hired personnel
- personnel groups adapted to the activity, based on their tasks, such as finance, research
- individually adapted competences, e.g., when greater skills to perform certain tasks is needed
- personnel with system administrator access
- digital identities for information systems and services
- digital identities for development and test environments
- temporary digital identities.

Access administration

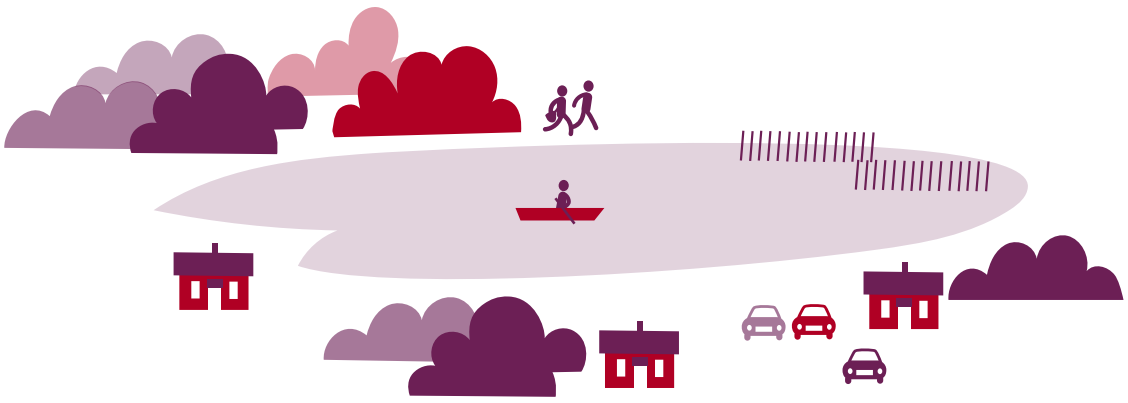
A digital identity needs to be administered over its entire lifecycle, and it is important to have control over digital identities for both users and information systems, including services. Access assigned to a digital identity often need to be changed over time. For

example, the user with the digital identity may change tasks or terminate employment. It is appropriate that all access is time-limited. This requires active permission management, including reminders that a time limit is set to expire. Reminders need to work such that the digital identities that must retain access are extended without disruption. The organisation needs the ability to order, approve and change the access of a digital identity or a group of digital identities in an accurate, fast and traceable way through its access management. Access needs to be assigned by a decision of the responsible party, who is often the information owner of the information systems concerned. Ensure that decisions regarding changes to access can be linked to a responsible person, and show when the decision was made. The organisation needs to assign access that provide access to highly sensitive information in a restrictive manner.

The organisation's approach to access management needs to include rules to immediately deactivate digital identities after the end of an employment (permanent or temporary) or assignment. It is far better to deactivate digital identities not in use than to delete them. This enables one to check who had the digital identity, if necessary, e.g., in the case of access audits or log checks. Rules to support regular checking and revising of access distribution are also needed. Checks also need to be made when personnel are hired, change positions, go on leave or quit. Assess the possibility of activating the digital identities used by suppliers to access the IT environment for the period of time needed for the supplier to perform the task given to them by the organisation and, if possible, automatically deactivating the digital identity after a given time limit. During revisions, it is of particular importance to review all digital identities for information systems including services, both internal and external, such as cloud services. Digital identities that cannot be linked to an activity need, or which lack an information owner who can demonstrate the need, are to be deactivated. It is also important to revise the system administrator access.

Roll separation

When assigning access to users, the organisation needs to ensure that the same person does not have the task (and access) to both perform a measure and audit it. For example, the person responsible for analysis of logs shall not have the authority to modify or delete the logs. Similar divisions (role separation) have long been standard in business administration, e.g., separating the role with access to the receipts and payments account (treasurer) from the role verifying the correctness of bank statements (auditor), and the person who submits receipts from the person authorising the expenditure (certifying officer). If there are too few employees to implement the necessary role separation, ensure the same person has different accounts for different tasks, and compensate with extra accounts. This is particularly necessary for tasks requiring high levels of access.



Management of high-level access

Where use of an information system requires a user have access to configure functions that may affect security, this needs to be risk-assessed and compensatory security measures put in place, such as additional monitoring and log analysis.

From an attacker's point of view, gaining control of digital identities with system administrator access is the best option, as in many cases it provides extensive access to the IT environment. The allocation of system administrator access shall therefore be made restrictively, and such access shall only be used for system administration. To reduce the impacts of mistakes, e.g., in IT environment configuration, one system administrator permission should not apply to the whole IT environment, but only a part. This also reduces the impacts of an attack. Use different digital identities for different functions, e.g., system administration of clients, servers, networks and various security functions.

To facilitate installation and operation, software often comes with high-level access pre-set. Exactly what access is needed for the software to work may be poorly documented by the supplier. This may cause many organisations to retain the pre-set high-level access. To ensure that the organisation has only enabled the access that meet the needs of the activity, the organisation needs to require the supplier to provide documentation of the access needed for different functions.

Well-performed access management reduces the risk that an external or internal attacker accesses the IT environment using, e.g., digital identities that should have been disabled or which have excessive access. Once an attacker has gained access to an information system, the next step is often to gain access to additional parts of the IT environment. This is done either by taking over more digital identities of users or information systems, or by attempting to elevate the access of the digital identity that the attacker has acquired.

4.2.5 Access to directory services and other tools

A directory service here refers to an information system (database) that collects and manages digital identities and access, a so-called Identity and Access Management (IAM) system. For most organisations, effective management of digital identities and access requires the use of directory services. To facilitate access audits and more easily ensure role separation, it is appropriate to avoid local management of identities for individual information systems. A directory service collects and facilitates updating all digital identities and their access. A directory service (e.g., Microsoft Active Directory) typically contains digital identifiers for users, system administrators and information systems (e.g., clients, servers and networks) including services.

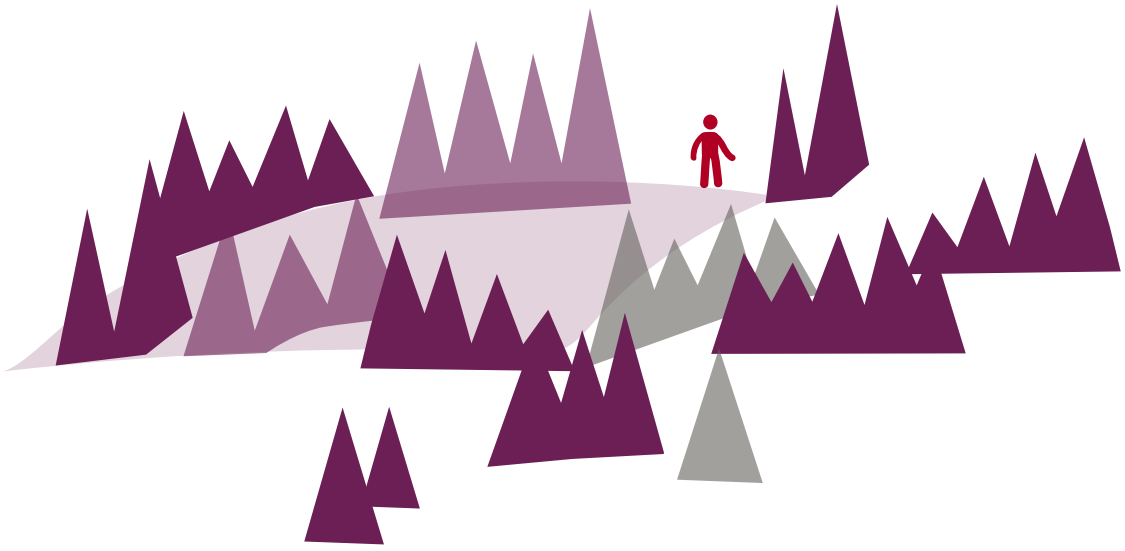
All changes to the directory service must be traceable. Use directory services that can not only manage digital identities at the individual level, but also support organisational change. As a basis for updating the digital identities and access, it is appropriate to have a reliable data source, e.g., the organisation's HR system. Having separate directory services provides increased security, so that an account used by an unauthorised person cannot provide excessive access to the IT environment. It is important to have a mode of operation ensuring directory services administrators manage the risks involved in the inter-reliance of the different directory services. Ensure that new information systems can use the existing directory service before procurement.

If an unauthorised person gains access to a digital identity with system administrator privileges in a directory, it can be used to gain access to the other digital identities in the directory. If only one directory is used, this means that the attacker can access the entire IT environment. Managing different digital identities in different directories reduces this risk. When creating directories, for example, the organisation's segregation can be used as a basis. As a minimum, the organisation should manage digital identities and access that provide access to externally accessible information systems in directories separate from the production environment directories.

In the IT environment, there may be a need to set up local or temporary digital identities in, e.g., databases and operating systems. These digital identities can also be used by attackers to gain access to valuable information, and grant access to other critical systems, and they therefore need to be protected accordingly.

4.2.6 Access management regarding development and test environments

Organisations should not allow employees to use the same digital identity and passwords in the development and test environments as in the production environment. This is because the IT environments for development and test often have less protection than the production environment. If the same digital identity is used in both these environments and the production environment, there is a risk that information about the digital identity and its passwords is more easily accessible during an attack on the more vulnerable development and test environments. One example is when a digital identity and its passwords used in development and test environments are written and stored unprotected in source code and software that can be accessed by unauthorised persons.



4.3 Authentication

4.3.1 Purpose

In order to protect the organisation's information systems against unauthorised access, the organisation needs to have internal rules to protect its passwords and in some cases use multi-factor authentication.

4.3.2 Requirements

The organisation shall

1. use multi-factor authentication for [65]
   a. access to the production environment via external network by in-house and hired personnel
   b. system administrator access to information systems
   c. access to information systems processing information in need of enhanced protection
2. have internal rules for handling passwords with requirements for [66]
   a. length and complexity
   b. expiration
   c. distribution
   d. protection of passwords.

The organisation should use technical systems to support compliance with rules regarding length, complexity and expiration.[67]

4.3.3 Authentication

In an IT environment, the organisation needs to be able to verify the identity of a person or an information system using a particular digital identity. This is done through authentication.[68] Authentication is used, e.g., when a user logs into an IT environment or information system, or when an information system must verify its identity vis-a-vis another information system. Common passwords for authentication include passwords, passphrases and PINs (i.e., something you know), fingerprints (something you are) and microchip cards (something you have). The traditional way to authenticate a given digital identity is for the user to provide their username and password, which is then checked against the organisation's register of digital identities, passwords and access. Using passwords alone for authentication is often not secure enough. This is especially true if the length or complexity of the passwords is insufficient, if they are easy to guess or if they lack sufficient protection during distribution or storage. The techniques used by attackers to find weak passwords are also improving.

Deficiencies in user password creation, distribution, storage and management permits attackers to, e.g.,

- guess passwords
- learn passwords by finding them when distributed/stored in plaintext
- forcing encrypted passwords using computing power
- trick the user into entering their password (e.g., phishing).

65. MSBFS 2020:7 Chapter 4. Section 5 Multi-factor authentication shall be used for 1. access by in-house and hired personnel to the production environment via an external network; 2. system administrator access to information systems; and 3. access to information systems processing information deemed to require enhanced protection.

66. MSBFS 2020:7 Chapter 4. Section 6 The Authority shall have internal rules for managing passwords with requirements on 1. length and complexity, 2. expiration, 3. how to distribute, and 4. how to protect the passwords.

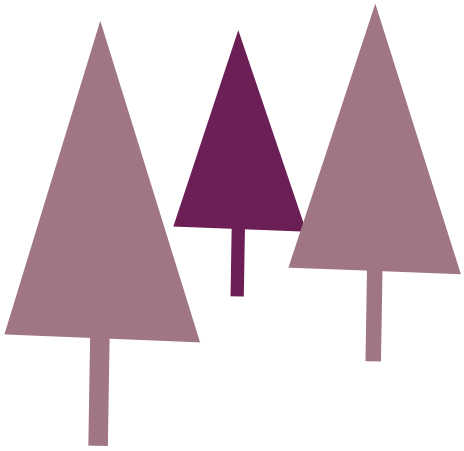
67. General advice to MSBFS 2020:7 Chapter 4 Section 6 Technical systems should be used to support compliance with the rules on length, complexity and expiration.

68. In eSAM's guidance Legal guidance for the introduction of e-legitimisation and e-signatures (release 1.1, June 2018) states that "authentication" and "e-identification" are the same thing

If the same password is used for several different digital identities, unauthorised access to the password has more serious impacts for the organisation because more information systems are affected, requiring more extensive incident management.

The need for secure means of authentication in different digital environments is increasing. One example is to be able to identify oneself in a digital environment outside the organisation in one's professional role. The development of dedicated authentication technologies for businesses is ongoing at both national and EU level.[69] The possibility of identifying oneself as a private individual has existed for some time.

At present, organisations that exchange information often use different federated authentication solutions. When using federated authentication solutions, an additional dimension needs to be protected, namely the management and communication of certificates sent between the information system performing the authentication and the information system requiring the certificate to grant access.



69. For more on the development of digital office passwords, see https://www.digg.se/digitala-tjanster/e-legitimering.

4.3.4 Multi-factor authentication

Due to the security issues associated with using username and password alone as authentication method, many organisations are moving to multi-factor authentication. This means authentication based on several different types of passwords (something you know, something you are and something you have). For example, logging in with two passwords (both known) is thus not multi-factor authentication. Multi-factor authentication can also be called 'strong' authentication.

Some examples of multi-factor authentication with two different factors (two-factor authentication):

- A card with a microchip together with the user's PIN (something you **have** combined with something you **know**).
- A card with a microchip together with a fingerprint (something you **have** combined with something you **are**).
- A PIN for a password box that generates a one-time code (something you **know** combined with something you **have**).

Multi-factor authentication reduces the risk of unauthorised authentication, as it is not enough for an attacker to gain access to only one authentication credential. For example, the attacker must obtain both the microchip card (by stealing or finding it) and the associated PIN (via hacking or by tricking the user into providing it) in order to use the digital identity's access.

The security of a multi-factor authentication technology requires that administrative procedures and technical security features are properly implemented. For example, administrative procedures need to ensure that:

- the assignment of passwords (e.g., password, passphrase or PIN) is done correctly
- users change assigned passwords before use
- credential tools (such as authenticators or microchip cards) are correctly assigned to the right user

In addition, there needs to be procedures in place to deal with the loss of an authentication tool, such as an authenticator. The technology needs to be installed and administer so that multi-factor authentication requirements cannot be circumvented.[70]

Some information systems do not allow the use of multi-factor authentication solutions in direct contact with the system. Such systems shall not be used for information in need of enhanced protection or for system administration.

4.3.5 Multi-factor authentication requirements

An organisation can choose the situations in which multi-factor authentication needs to be used based on information classification and risk assessment. In the three cases below, the organisation must always use multi-factor authentication.

Access by in-house and hired personnel to the production environment via an external network

Personnel working remotely often need to access the organisation's production environment. To protect the production environment against attacks, it is not enough to require only a username and password when logging in via an external network. Multi-factor authentication can be set up in different ways, but it is required whether personnel log in via the organisation's own clients or their own equipment. It does not count as multi-factor authentication when personnel log on to a client using only username and password, even if the client is connected with a certificate via a VPN tunnel to the production environment.[71] This is because the certificates areonly used to identify equipment, not people.

It is appropriate to only allow login via clients provided by the organisation and configured to meet the organisation's security requirements. An organisation that nevertheless allows personnel to log into the production environment via their own equipment needs to manage the risks involved, such as not being able to check whether the private equipment has sufficient security measures and not being able to address any deficiencies. One way to protect the production environment during access via an external network is to provide access only to a virtual copy of the production environment's information system, known as a Virtual Desktop Infrastructure (VDI).

Organisations may need to allow non-personnel access to certain parts of the production environment. This includes, e.g., external websites or equivalent to which the public has access.[72] Some organisations offer various services for non-personnel, which also means that the selected target group is given access to certain parts of the production environment. Based on information classification and risk assessment, the organisation then needs to assess which authentication methods and other security measures, such as network segregation and filtering, are needed to address identified risks. Services involving access to information requiring enhanced protection shall always be protected by multi-factor authentication.

System administrator access to information systems

In order to perform system administrator tasks, in most cases a high level of authorisation is required, i.e., the digital identity used by the system administrator is given permission to perform a number of measures that users don't have rights to perform. E.g., changing configurations, changing logging systems, changing access and reconfiguring firewalls. As such measures can have a significant impact on the security of information systems and the IT environment as a whole, digital identities with system administrator access shall be protected by multi-factor authentication.

70. If an information system accepts password-only access in parallel with multi-factor authentication, then, from an attacker's perspective, there is no multi-factor authentication: security is ultimately based on passwords. For example, if a web service requires citizens to log in with eID, while the administration interface of the service is protected only by username and password, the system is not considered to be protected by multi-factor authentication.

71. Since the certificate only authenticates the client, in this case the user is only identified by one credential – username and password.

72. Where in-house or hired personnel use external websites or equivalent, they are treated as members of the public.

Access to information requiring enhanced protection

Some information systems handle information requiring enhanced protection for reasons of confidentiality, integrity or availability. Which information requires such protection is established by the organisations information classification.[73] Examples of information that is often deemed to require enhanced protection vis-a-vis confidentiality are information that could be covered by confidentiality under the Public Access to Information and Secrecy Act (2009:400) or defined in the General Data Protection Regulation[74] as special categories of personal data, so-called "sensitive personal data".

4.3.6 Passwords management

Authentication passwords need to be of the required length and complexity to provide the intended protection. In addition, they need to be managed securely. This involves ensuring that passwords are assigned to the right users and information systems, that their transfer is protected and that they are stored securely. It needs to be clear to all concerned how this is to be achieved. The organisation shall therefore have internal rules that set requirements for the passwords length and complexity, when to replace them and how to deploy and protect them. All requirements need to be designed based on the organisation's risk assessment.

The following needs to be considered:

- Passwords used with usernames alone need to be long and preferably in the form of a passphrase, while a shorter PIN is often sufficient to unlock a microchip card or a disposable authenticator.
- Distribution of new passwords (e.g., passwords) needs to be done in a way that ensures that the right user gets access to the passwords. Secure distribution can be facilitated when the organisation uses multi-factor authentication.
- Passwords, at least in the production environment, need to be protected by not being sent or stored unencrypted.

4.3.7 Technical systems for managing passwords

Management of passwords and access is facilitated by the use of centralised system support. Identity and Access Management (IAM) systems, which manage usernames, passwords and access in a unified way, allow the people in the organisation who are involved in access management to easily add, remove or change both digital identities and access. With IAM, the organisation can easily get an overview of all users' access. An IAM system can also be used to ensure compliance with the organisation's password requirements in terms of length, complexity and expiration. It can also be used to ensure that passwords are unique and not reused.

If the organisation allows users to create and store their passwords and codes with the support of password managers, the organisation needs to require and audit this information system in the same way as other information systems requiring enhanced protection. Password managers that manage users' passwords on the internet are not suitable for use, as it may be difficult (or impossible) to guarantee that passwords are managed securely by the provider.

73. Requirements for classifying information in different levels in terms of confidentiality, integrity and availability are set out in MSB's regulations on information security for government agencies (MSBFS 2020:6), section 6, item 1.

74. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

4.3.8 Common approaches

A common approach for an attacker to obtain passwords is to send out an email inviting them to go to a web page resembling to a webmail login or other organisation service. If a user is tricked into entering their passwords on such a website, these are captured by the attacker.

The attacker then uses the passwords to gain access to the organisation's IT environment. The risk of this type of attack is reduced when the organisation uses multi-factor authentication during IT environment log-in. However, the organisation needs to be aware of the risk of the so-called 'man in the middle attack'[75] as it can also be used against some multi-factor authentication solutions, e.g., when using authenticators that generate one-time passwords.

Multi-factor authentication based on a one-time code sent by SMS over mobile operator networks is vulnerable, as SMS can be manipulated by an attacker. When using authentication via SMS services, the risk must also be considered of poor mobile coverage or insufficient security of delivery, which can cause problems when the organisation's users need a one-time code to log in.

75. In a 'man in the middle attack,' an attacker, by actively interfacing with a communication between two parties, simultaneously simulates the identity of each party to the other, and can thereby intercept or alter transmitted information.

4.4 Encryption

4.4.1 Purpose

To protect the organisation's information from unauthorised access and modification, both when information is being transferred and when being stored, the organisation needs to use encryption to meet its needs.

4.4.2 Requirements

The organisation shall

1. identify and manage the need for encryption to protect information against[76]
   a. unauthorised access during transmission and storage
   b. unauthorised modification during transmission and storage
2. have internal rules for encryption with requirements for[77]
   a. handling of encryption keys
   b. approval and management of encryption technologies
   c. choice of encryption algorithms, encryption protocols and key lengths
3. use Domain Name System Security Extensions (DNSSEC) for domain names registered in the Domain Name System (DNS).[78]

The organisation should[79]

1. use encryption to protect
   a. security logs against unauthorised access and modification
   b. passwords against unauthorised access and modification
   c. information requiring enhanced protection against unauthorised access and modification when transferred to information systems outside the organisation's control
2. introduce the possibility to verify the organisation as sender or recipient of e-mails
3. identify the need to encrypt emails on the transport layer.

In addition, **government agencies should** introduce the possibility of encrypting e-mails on the transport layer when transmitting to and from other government agencies.

4.4.3 Protection against unauthorised access and modification

Encryption is an important security measure to protect information when it is stored or transmitted. By using encryption correctly, the organisation can protect its information against unauthorised access (confidentiality) or unauthorised modification (integrity).

Encryption also enables verification that information sent by a sender is the same as that received by the recipient (content authenticity). It is also possible to verify that the message comes from the ostensible sender (authenticity of origin).

76. MSBFS 2020:7 Chapter 4. Section 7 The Authority shall identify and manage the need for encryption to protect information against unauthorised access and unauthorised modification during transmission and storage.

77. MSBFS 2020:7 Chapter 4. Section 9 The Authority shall have internal rules for encryption with requirements for (1) the handling of encryption keys, (2) the approval and management of encryption solutions, and (3) the selection of encryption algorithms, encryption protocols and key lengths.

78. MSBFS 2020:7 Chapter 4. Section 8 The Authority shall use Domain Name System Security Extensions (DNSSEC) for all domain names registered by the authority in the Domain Name System (DNS).

79. General advice to MSBFS 2020:7 Chapter 4. section 7 Encryption should be used to protect (1) security logs against unauthorised access and alteration, (2) passwords against unauthorised access and modification, and (3) information in need of enhanced protection against unauthorised access and modification when transferred to information systems outside the control of the Authority. The Authority should identify the need to encrypt e-mails at the transport layer in accordance with the OSI model (Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, ISO/IEC 7498-1) or equivalent. The Authority should also introduce the possibility of using such encryption for transmission of e-mails to and from other government agencies. The Authority should introduce the possibility to verify the Authority as sender and recipient of e-mails.

There are two main types of encryption, symmetric and asymmetric. Symmetric encryption uses the same encryption key for both encryption and decryption, assuming that the sender and receiver have identical keys. The protection provided by symmetric encryption requires that no one else has access to the keys, which makes the handover of the key to the other party a critical element. When using asymmetric encryption, a key pair is used instead. What is *encrypted* with one key in the key pair can only *be decrypted* with the other key in the key pair and vice versa. Each user of asymmetric encryption has its own key pair. One key needs to be protected against unauthorised access (private key) while the other key (public key) is available to anyone wishing to communicate with the user in encrypted form.

Hash functions are a common application of asymmetric encryption, with a specific application. Hash functions do not use keys but only an encryption algorithm to perform a calculation on selected information, thereby creating a hash sum (digital fingerprint) unique to the information. The hash sum cannot (by design) be decrypted (one-way encryption).

- *Symmetric encryption* is faster and less resource-intensive than asymmetric encryption, so it is often used to encrypt particularly large amounts of information to achieve confidentiality.
- *Asymmetric encryption* is mainly used to achieve integrity but can also ensure confidentiality. It is more technically advanced and requires more computing power than symmetric encryption, which often makes it slower. Asymmetric encryption is used, inter alia, to securely pass a symmetric key to the other party and to create digital signatures in public key infrastructure (PKI) technologies. By using digital signatures, a sender with a private key can *sign* a message[80], and the recipient verifies that the message really comes from the sender by *verifying* the signature of the message with the sender's public key.
- *Hash functions:* Hash functions are mainly used to detect unauthorised modification of information. If the hash sum that the sender calculates for a message's information, and attaches to the message, does not match the hash sum that the recipient calculates from the same message, the information has changed. Hash functions (one-way encryption) are part of the digital signing of messages. This is to ensure that the content has not been altered (the hash function) and to verify the sender (through asymmetric encryption).

Encryption may be needed both when information is transmitted and when it is stored. Information is transmitted both to other actors and within the organisation's own networks. When transmitting information to information systems outside the organisation's control, the organisation must always consider the need for encryption. In cases where information is transmitted that, per the information classification, requires enhanced protection, the organisation should always use encryption. There may also be reason to use encryption when transmitting internally between different network domains, especially if the information requires enhanced protection.

80. In most cases, the entire message is not signed, but only the hash sum of the message, which the sender has generated using a hash function.

When storing information, there are two main ways to encrypt. Either the information is encrypted before it is stored, or the information is encrypted when it reaches the storage layer (hard disk encryption). The procedure to be used depends on the needs of the organisation. For example, it is appropriate that logs and passwords be encrypted directly when collected and transferred to the storage area in an encrypted form. Hard disk encryption is often used on clients to protect the information when the client is off. Security logs should always be protected against unauthorised access and modification through encryption. The same applies to authentication data such as passwords, passphrases, PINs, fingerprints and passwords stored on microchip cards.

There are many different ways to meet an organisation's encryption needs. Encryption technologies are often included in other products and services where encryption may be needed, such as web browsers or email systems. The organisation can also acquire encryption functionality through stand-alone products, in the form of both hardware and software. The choice of encryption technology also needs to take into account whether it is a matter of protecting stored information or information transferred between information systems. The strength of the encryption needs to correspond to the need for protection both in terms of level and time period. Configuration of encryption technology in terms of algorithm, protocol, key lengths, and encryption key management must therefore be guided by the need for protection.

4.4.4 Internal rules for encryption

Encryption is an important security measure, but it must be properly implemented and managed to provide the intended protection for the organisation's information. If encryption keys are mishandled, or if incorrect configurations of encryption products are made, the organisation can experience major problems. Deficiencies in the protection of encryption keys can lead to unauthorised access to protected information. A lack of procedures for updating the organisation's encryption keys can result in sensitive information being inaccessible to the organisation. Incorrect or non-existent configuration of encryption products may have the impact that the organisation's image of the protection does not correspond to the protection in place. Encryption technologies offered in commercial products are often easy to launch, but the supplier's pre-settings may not suit the organisation's needs.

Employees who configure and administer encryption technologies must have the right training and skills for the job. There must also be internal rules regarding how encryption keys are handled, how encryption technologies are approved and managed, and how encryption algorithms, protocols and key lengths are selected. There needs to be documentation for each encryption technology describing the chosen configuration.

The internal rules for encryption should be developed by an IT-security specialist in conjunction with the person who leads and coordinates the information security work and the person responsible for IT operations in the organisation.

Encryption key management

For encryption to provide the intended protection, the organisation needs to manage encryption keys in a secure manner. Key management includes all the necessary steps to create, protect, control and finally deactivate or destroy the encryption key.[81] This applies both to keys used in symmetric encryption and to the private key in an asymmetric key pair. Through internal rules, the organisation can ensure that keys are handled securely. This includes managing the following risks:

- Encryption keys are made accessible to unauthorized individuals or information systems. Some common examples include when encryption keys are added to the codebase (often for convenience), when they are sent openly by email, or when they are unprotected on the file server.
- Encryption keys are destroyed or lost, making encrypted information unreadable. This can happen, e.g., when storage media containing keys or passwords to the keys are destroyed or lost.
- Encryption keys created are too weak, making it relatively easy for unauthorised people to create an identical key. Weaknesses can be caused, e.g., by using poor random numbers when creating the keys, or by the organisation not requiring that keys be long enough or that a secure algorithm be used.

The internal rules for cryptographic keys need to cover their entire life cycle. The rules also need to include how to handle key incidents, such as lost or stolen encryption keys.

The rules need to ensure that encryption keys are given at least the same, and preferably a higher, level of protection as the information they are supposed to protect through encryption. Regardless of how the encryption keys are created and stored, the protection of the key needs to be maintained throughout the lifetime of the key[82], given that the need to protect the information it protects remains. When the key is no longer to be used, it also needs to be securely destroyed.

Encryption keys can be created in several ways. For example, symmetric and asymmetric keys are created with different algorithms. Many commercial encryption products include the ability to create your own encryption keys. The internal rules need to clarify how strong the encryption keys need to be to meet the needs of the organisation. Different applications may have different needs. Some providers offer encryption as a service.

In most cases, this means that the provider also has access to the key, and is therefore able to decrypt the information. The organisation needs to assess whether such a technology is appropriate and, if so, manage any risks this may entail.

Encryption keys can be stored in various ways, such as in a file system, smart cards, USB memories, trusted platform module chips (TPM chips) or in hardware security modules (HSM). Storing encryption keys in software is common in many encryption technologies. The possibilities to protect cryptographic keys are here limited to the conditions of the software and the security measures implemented in the information system. An HSM stores the key information securely and protects it from direct access. Instead of letting the encryption technology have access to the encryption key, the information to be encrypted is sent to the HSM and encrypted there. HSMs generally provide higher protection than software solutions. It is therefore appropriate to use HSM for encryption keys that have a high-level protection requirement, or which are used for a long period. The technology to be chosen for key storage must be decided after the risk assessment. Whatever the technology, encryption keys must be protected against unauthorised access or modification.

81. The entire process, from the creation of an encryption key to its destruction, is called the key management life cycle.

82. An encryption key can have different lifetimes, from seconds to years. It is appropriate to consider whether the protection is for long-term keys or session keys, as the impacts in case of loss are often different.

Approval and management of encryption technology

As with other hardware and software, vulnerabilities and deficiencies are also found in encryption technology. It is essential not to use weak encryption algorithms or protocols, and that sufficient key length is selected. It is also important to consider whether encryption keys can be recovered or backed up. The risks of recovery and backup need to be weighed against the risks of losing an encryption key and thus the possibility of using the information.

It is important that the organisation have internal rules for both approval and administration of encryption technologies before they are implemented in the IT environment. The approval needs to apply to both the encryption technologies that may be used in the organisation's IT environment, and what encryption needs each technology can meet. In addition, there needs to be internal rules requiring that each implementation of encryption technology be tested and approved before use. Testing needs to be carried out by personnel with the necessary competence, and approval is made by the system owner as part of the approval for operation.

The organisation's internal rules for encryption need to specify the encryption algorithms, protocols and key lengths to be used to meet the different encryption needs of the organisation. This creates the conditions for effective management of encryption protection, allowing the organisation to deal with algorithms that are not strong enough and detect vulnerabilities in the protocol as well as the need to increase key lengths.

The management of encryption technologies requires the organisation to conduct external environmental monitoring to identify early on any future needs to replace algorithms, detect vulnerabilities in protocols and prepare for extended key lengths. The internal rules also need to include requirements for documentation regarding which information systems use which encryption technologies.

The documentation helps the organisation to deal with vulnerabilities detected during the monitoring process.

There are suppliers who claim their proprietary encryption technologies are better or faster than well-established technologies on the market. This is often not the case. The strength of the established technologies is that they are based on publicly available algorithms and protocols that are continuously scrutinised and tested for weaknesses. The actual level of protection provided by an encryption technology depends on the competence of the manufacturer

and the supplier's ability to protect the product against manipulation during delivery. All this needs to be taken into account when choosing an encryption technology.

To reduce the risk of vulnerabilities in commercial hardware and software used for encryption technology, it is appropriate to have the technology audited in whole or in part by a certification body or another trustworthy third party.

Encryption algorithms, protocols and key lengths

Different encryption technologies use different protocols, and these protocols are based on an encryption algorithm. In order to assess whether a particular encryption technology is suitable for a particular purpose, it is important to know

- which protocols can be used
- which algorithms the protocols are based on
- the length of the encryption keys that can be created.

In addition, the organisation needs to be able to monitor the environment to continuously assess whether selected protocols contain vulnerabilities that need to be addressed, whether selected algorithms have become too weak to be used, and what key lengths are required to provide a secure encryption technology. The assessment made by the organisation will form the basis for the internal encryption rules that are developed.

4.4.5 DNS servers

All internet traffic depends on the ability to make accurate and reliable DNS[83] lookups. The Domain Name System (DNS) translates the text-form web address (hostname) into computer-readable IP addresses in numeric form, and vice versa. However, DNS is vulnerable to a variety of different attacks that can manipulate responses to DNS queries. Such attacks can redirect you to the wrong web server (host) without your knowledge. Domain Name System Security Extensions (DNSSEC) is an extension to the DNS system that aims to increase DNS security with cryptographic signatures. DNSSEC ensures that the DNS response comes from the right source and that the data has not been manipulated during transmission. This can prevent misuse where the DNS system is tricked with false information.

Most DNS products on the market now include support for DNSSEC. Similarly, DNS service providers commonly provide DNSSEC. DNSSEC is also often a prerequisite for web service and email authentication methods to work as intended. In addition to supporting DNSSEC, the DNS service managing external queries to the organisation's domain name should also be selected for robustness.

An organisation often has several domain names. Some are aimed at external users or external information systems, while others have an internal purpose only.

If the organisation has an externally accessible information system, such as a web service, web page or e-mail server, it needs to be registered in DNS so external users and information systems can find it. The organisation shall activate DNSSEC in the name servers of all domain names registered by the organisation in DNS. The name lookup service (resolver) used by the organisation for looking up external name lookups also needs to support and be able to validate DNSSEC.

Internal information systems are accessible via the organisation's internal network. To keep track of information systems and IP addresses on the internal network, the equivalent functionality provided by DNS on the internet is often needed.

However, the organisation needs to ensure that the internal information systems are not externally accessible and not registered in the DNS. If such registration is made, which enables lookup of the information systems and makes them externally visible, DNSSEC is required.

4.4.6 Security logs

The organisation should use encryption to protect its security logs. When designing the encryption protection for the security logs, it is important to consider where the logs are created, where they are stored and how they are transmitted from one place to the other.

83. Domain Name System.

Encryption protection must be used in conjunction with other security measures to protect the security logs, e.g., network segregation, access controls, monitoring and physical access protection.

To prevent unauthorised access and modification, security logs need to be encrypted as soon as possible after they are created and as close to their source as possible. By using hash numbers and signature functionality, unauthorised changes to the content of the security logs can be detected.

Technologies to verify integrity can also be created using blockchain technology.

Encryption protection needs to be maintained during transmission and storage. Deficient protection of security logs can have the impact that the organisation cannot trust their content, which makes the organisation's security work more difficult. It can be difficult, e.g., to detect and investigate suspected unauthorised access, technical errors or other security deficiencies.

Because the organisation needs to analyse security logs as part of its security work, the encryption protection needs to be designed to allow this while maintaining protection. This is facilitated in most cases by the collection of security logs in a dedicated information system (central security log).

4.4.7 Passwords

The organisation should use encryption to protect passwords. This applies both to the password database itself and to the individual passwords used to identify a user or information system. In order to protect passwords with encryption in the password database, they need to be stored there both "salted "[84] and hashed. Unauthorised access to unencrypted passwords can have significant impacts for an organisation.

When a user or an information system authenticates, e.g., via a web-page login box or other interface, encryption protection needs to be present both in the interface and in the transmission to the password database. The encryption protection aims to protect the passwords from unauthorised access. In most cases, it is not appropriate to send passwords in clear text from input to verification.

4.4.8 Information requiring enhanced protection

The information that the organisation has identified in its information classification[85] as requiring enhanced protection should be protected against unauthorised access and modification when transferred to information systems outside the organisation's control. This applies regardless of whether the need for enhanced protection relates to confidentiality, integrity or availability, or combinations thereof.

Information systems outside the control of the organisation are defined here as all information systems that are not physically located on the organisation's own premises[86] or in other areas at the disposal of the organisation, such as during co-location. If an organisation has multiple premises in different physical locations, or uses a service provider with premises in a different physical location, the need for encryption to protect the information must be identified and managed. This can be done, e.g., by setting up a virtual private network (VPN) between the different premises. The need for encryption must also be identified and managed when the organisation allows employees to connect to the organisation's IT environment while working remotely.

84. Salting involves adding a random extension to passwords, making them longer and harder for an attacker to crack.

85. For more information on information classification, see the methodological support ”utforma klassningsmodel” at www.informationssäkerhet.se.

86. For example, the organisation’s laptops used by personnel when working remotely.

When an organisation, e.g., has a website that handles passwords, the need for encryption must be identified and addressed. Encryption should be used, as such information is generally considered to require enhanced protection. Most web-service applications have built-in support for encryption, including support for various authentication methods, to allow visitors to verify they are visiting the right website. For example, it is appropriate to use HTTPS on all web services as the default for application level. Transport Layer Security (TLS) is often used as the encryption protocol at the transport layer.

A prerequisite for TLS to work as intended is, on the server side, a digital certificate. The digital certificate needs to contain server-side information about the owner of the web service corresponding to the Fully Qualified Domain Name (FQDN), i.e., the format "www.statligmyndighet.se". The client, web browser or other information system, checks the trustworthiness of a web service by comparing the name of the certificate holder with the address of the web service. If name and address do not match, the web service does not have a valid certificate and may be unreliable. To reduce the risk of imitating the address of the organisation's web service by replacing domain name information in DNS, the organisation needs to enable DNSSEC.

An organisation must always assess the need for encryption to protect information from unauthorised access and modification during both transmission and storage.

4.4.9 E-mail

An organisation should introduce the possibility for e-mail recipients to verify the organisation as the sender. This reduces the risk of the organisation, and those with whom it communicates, being "spoofed" via email, i.e., someone falsely representing themselves as the organisation in messages. Depending on what is being communicated, and on how well the fake email is designed, the impacts can be tangible for the organisation and the recipients trusting the e-mail's content. Those sending false e-mails in this way are becoming increasingly adept at mimicking other people's ways of communicating.

To avoid as far as possible that personnel are fooled by fake messages, either internal or external, the organisation needs to implement technical protection for e-mail. E.g., ensure that e-mail accounts not intended for external communication can only receive e-mails from the organisation itself. The organisation needs to use authentication methods[87] to allow recipients to validate emails sent from or to the organisation. The method chosen needs to be configured so that the protection cannot be bypassed.

For authentication methods to also enable the organisation itself to identify false messages, it is appropriate to contact the organisations with which there is extensive communication, and invite them to activate the corresponding technical protection.

87. For example, DNS-based Authentication of Name Entities (DANE), Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC). DANE, SPF, DKIM and DMARC all rely on the recipient looking up information associated with a domain name in DNS, which is an additional reason for an organisation to enable DNSSEC.

E-mail is a flexible way to communicate and can be used for many different types of information. An organisation thus needs to identify the need to protect email against unauthorised access. If all or part of e-mail services are outsourced, the protection of e-mail communication to the e-mail service, and from the e-mail service to the organisation, must be examined.

The protection of information sent by email can be simplified in one of the following ways:

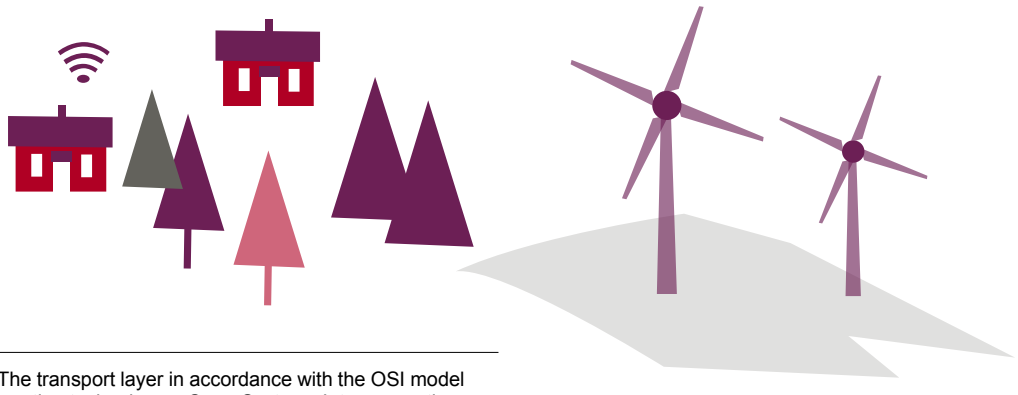
- protection of transport between email servers
- protection of information in individual e-mails.

In the first case, Transport Layer Security (TLS), or a VPN solution, is often used between the servers. However, full protection of e-mail communications against unauthorised access using TLS or VPN, transport-layer encryption[88], requires the recipient as well as the sender of the e-mail to have that functionality in place.[89] The organisation should therefore identify the other organisations with which such protected communications need to take place, then mutually decide on the most appropriate technology.[90] Government agencies should introduce the possibility of encrypting e-mails at the transport layer when communicating with other government agencies.

If the organisation determines that the information in individual e-mails, based on the information classification and risk assessment, needs to be protected at message-level during transmission and storage, one of the following technologies is usually used:

- encryption technology based on Pretty Good Privacy (PGP) or Gnu Privacy Guard (GPG)
- encryption technology based on Secure/ Multipurpose Internet Mail Extensions (S/MIME)

The above technologies are based on recipient/sender agreement regarding technology, employees having access to the technology and keys being exchanged correctly and securely. If this has not been done, the information in the message can be protected by not sending the message directly to the recipient, but by storing it on an authorised server, with only a notification going to the recipient, who can log on to the server (e.g., via a web browser) and access the information there.



88. The transport layer in accordance with the OSI model (Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, ISO/IEC 7498-1) or equivalent.

89. If only the receiving organisation uses TLS, the traffic is still at risk of being unencrypted, unless the receiving organisation requires the sender to use TLS, so-called enforced TLS. In the latter case, instead of being sent unencrypted, the email will not be sent at all.

90. Regardless of the technology used, it is important that certificate usage be well planned.

4.5 Security configuration

4.5.1 Purpose

To protect its IT environment from unauthorised access, organisations need to replace pre-set passwords and configure information systems by allowing only necessary system functions.

4.5.2 Requirements

The organisation shall, in order to protect information systems against unauthorised access,[91]

1. replace pre-set passwords
2. turn off, remove or block unnecessary system functions
3. otherwise customize configurations to achieve the intended security.

4.5.3 Configuring security

Information systems that are improperly configured, not updated or which use default settings can provide an entry point for attackers. All information systems in the organisation's IT environment therefore need to be configured for security, e.g., mobile phones, network devices, servers, clients, printers, e-mail, cloud services and security features. This applies especially to information systems linked to external networks, such as e-mail, web pages, web services and DNS servers.

Before installing applications, services or other information-system components processing information, the default settings must be reviewed, and the information system must be configured so that only the functions the organisation needs are activated. Other functions must be turned off, removed or blocked. The system functions that need to be activated must in turn be configured so that the intended security level is achieved. In addition, the organisation must replace default passwords. Configuration is best performed by IT technicians based on the needs of the activity and knowledge of the information system, risks, best practices and the IT environment in which the information system will be used.

4.5.4 Replace passwords

An organisation must replace all pre-set passwords in information systems before they are commissioned. Such pre-set passwords, such as default/factory passwords, are found in applications, operating systems, firewalls and networking equipment, for example. The pre-set passwords can be associated with several different types of digital identities (accounts) for users, information systems and system administrators.

New passwords must be selected according to the internal rules for managing authentication regulations, so that the needs for length and complexity are met.

4.5.5 Customize system configurations

Most information systems come with a standard configuration designed by either the manufacturer or the retailer.

This is usually designed to simplify installation and use, and to allow backward compatibility with older versions – not to provide good security. Upon delivery, products are often not updated to the latest version, and more services and protocols are activated than the organisation needs for the intended functionality of the information system. Unless such deficiencies are addressed prior to deployment and network connectivity[92],

91. MSBFS 2020:7 Chapter 4 Section 10 To protect information systems against unauthorised access, the Authority shall: 1. Replace pre-set passwords; 2. disable, remove or block system functions that are not needed; and 3. otherwise customize configurations to achieve the intended security.

92. If configuration requires network connectivity, it is important to ensure that the information system does not contain any information, and that only the network ports and services required for configuration are open.

the risk of attackers gaining access to the organisation's IT environment increases. To ensure that the organization has turned off, removed or blocked system functions that are not needed, and otherwise adjusted configurations to achieve the intended security, it is appropriate to take the following steps:

- *Update and upgrade*
  It is appropriate to begin preparations for the deployment of new information systems by updating all software and, if necessary, upgrading hardware and software to the latest version, to ensure that all available security updates are implemented. Older protocols and outdated, pre-installed software may contain vulnerabilities.
- *Disconnect network cables*
  Minimize the number of possible attack points by disabling and physically disconnecting network cables from unused network ports and network adapters.
- *Shut off unnecessary functionality*
  Hardware and software often have more functions – such as network protocols and network applications – than the organisation needs. These features are generally enabled upon delivery. Configure information systems with only the minimum functionality necessary for the organisation's operations. If there are functions, such as network protocols and network applications, that the organisation does not need, they should be removed immediately. If this is not possible, they should be shut off. Those functions that cannot be shut off need to be blocked, sometimes using other security measures such as firewall rules[93]. The functions in use need to be updated to remove vulnerabilities, and monitored for unmanaged vulnerabilities used by unauthorised persons.
- *Remove unnecessary high-level access*
  To facilitate installation and deployment, many software products are delivered with high-level access pre-set. It is important to know what access is needed for the information system to work as the organisation needs. If there is insufficient documentation regarding the required access, the organisation needs to require the provider to obtain such information. Otherwise, the organisation may have to spend a lot of time testing what access is necessary. It is not appropriate to keep the default high-level access, as they may make it easier for attackers.
- *Customize configuration*
  After shutting off unnecessary functionality, the organisation needs to adapt the configuration for the functionality the organisation needs, so that it both meets the needs of the activity and achieves the intended security. This involves, for example, choosing the most secure protocols, only allowing traffic to be initiated in one direction, using encryption, using certificates, restricting physical and logical access, and configuring logging and monitoring. Examine whether the security features already built into the products meet the organisation's requirements and, if so, modify them to reduce complexity. Do not turn off code protection that makes it difficult for software to run outside of allocated CPU and internal memory space.
- *Using existing security measures in the IT environment*
  In addition to the configuration of the information system itself, it is appropriate to increase security by siting the information system in the right place in the IT environment. This involves, e.g., choosing the right network domains, and using firewall protection to minimise attack opportunities.

93. Examples of firewall rules include not allowing connections to/from other information systems and allowing remote logins only from specifically designated information systems or network domains.

In order to streamline this process, it is appropriate to develop templates for secure configurations that can be reused on all similar information systems in the IT environment. These may consist, e.g., of Group Policy Objects (GPO)[94], start-up scripts and configuration files installed in information systems. The security configuration is used when installing new information systems. It is appropriate that information systems in operation are automatically updated with new security configurations when available. However, in the case of information systems that, e.g., are highly sensitive to disruptions or with unusual configurations, performing updates manually after tests have been carried out with satisfactory results may be more appropriate. The choice between automatic or manual updates of different information systems is based on the risk assessment.

Administration

The organisation's security configurations need to be reliably administered. Having a unified security configuration, which is documented and changes to which are tracked, makes it easier to keep security configurations continuously up to date. It is appropriate to use tools that make it easier to control which security configurations are installed in the IT environment. Such tools provide, among other things, support for automatically and regularly checking that the latest security configurations are in place in the IT environment. It is appropriate to use tools that provide notification when a device's security configuration does not match the current security configuration.

Review and update security configurations periodically to ensure they are up to date regarding vulnerabilities and attack methods. The configuration needs to be reviewed periodically or as needed, e.g., when

- software/hardware is upgraded or updated
- other security updates are installed
- new vulnerabilities are discovered
- the activity requires a new mode of operation
- new information systems are introduced.

Also ensure that new security configurations are installed in the information systems as soon as possible, in accordance with the organisation's change management. Determining and deploying security configurations is a complex task, as it can sometimes involve evaluating thousands of potential settings. Developing and administering a secure configuration therefore requires technical expertise for the configuration of components, which means that some organisations need to bring in external specialists to configure these information systems in the IT environment.

The security configurations that are used need to be protected against unauthorised access and modification, at least at the same level as the protection of the information processed in the information system. An attacker with access to the security configuration can discover exploitable vulnerabilities or change the existing security configuration to facilitate future attacks. Automatically and regularly check that the security configurations have not been changed without authorisation.

94. Group Policy Object (GPO), a means, in Windows environments, to communicate a number of configuration settings from the directory service to clients and servers.

4.6 Security testing and review

4.6.1 Purpose

To identify and manage vulnerabilities in individual information systems and the IT environment as a whole, the organisation needs to verify that information systems are up to date, and that the security measures and configurations which have been chosen are in place and adequate.

4.6.2 Requirements

The organisation shall[95]

1. ensure that security tests and reviews identify existing vulnerabilities
2. have internal rules regarding how to verify that
   a. information systems are up to date
   b. security measures which have been chosen are correctly implemented
   c. implemented security configurations are sufficient.

The organisation should combine automated security tests and manual reviews when verifying the security of information systems.[96]

4.6.3 Security checks of information systems and the IT environment

The organisation must regularly test and audit its ability to protect its information systems. The objective is to find errors and vulnerabilities that can be corrected.

Security testing and auditing can be done in different ways, with different purposes and scope.

The main purpose is to detect deficiencies in the protection of confidentiality, integrity and availability. Security testing and security audits are complementary.

The organisation shall have internal rules regarding the implementation of checks. Since security testing and audits take time and resources, it is appropriate to develop and implement a standardised approach to security testing and audits that are always carried out. The standardised security tests and audits need to be adapted to the object of the test/audit as well as its protective value as based on information classification and risk assessment.

Most organisations perform security tests and audits of individual information systems, but checking the entire IT environment as well as individual components may also be needed. To ensure adequate protection in the processing of particularly sensitive information by information systems, even the quality of the software may need to be checked, for example through code testing and auditing. Many of the checks that need to be done require specific skills.

4.6.4 Security tests

The purpose of security testing is to find technical vulnerabilities, and it is mainly carried out through vulnerability scans and intrusion tests (pen tests).

Vulnerability scanning

Vulnerability scans are performed using automated tools that, e.g., check for deficiencies in the information system based on a predefined list of vulnerabilities. Vulnerability scans can detect, e.g., missing patches, insecure protocols and expired certificates. A scanning tool can be adjusted to scan certain information systems or parts of the IT environment. The scanning tool can also be granted different levels of access. With high-level access

95. MSBFS 2020:7 Chapter 4 Section 11 The Authority shall ensure that security tests and audits enable the identification of vulnerabilities. The Authority shall have internal rules on how to check that 1. the information systems are up to date, 2. selected security measures are properly implemented; and 3. implemented security configurations are adequate.

96. General advice to MSBFS 2020:7 Chapter 4, Section 11.

(e.g., higher than system-administrator level), the scanning tool can enter the information system and detect vulnerabilities such as weak passwords, configuration problems, unauthorised installed software and malware. Access that only allow scans from outside the information system show how accessible the information system is to an attacker.

The organisation needs to conduct regular vulnerability scans. The period between scans should be determined on the basis of the information classification and the risk assessment. Vulnerability scanning always needs to be done before new or changed information systems are commissioned. Be aware that some scanning tools store results in cloud services, where it can be difficult to assess who has access to the vulnerability data.

Intrusion tests

Intrusion testing aims to identify vulnerabilities and ways an attacker might gain access to the organisation's information systems or IT environment. Conducting an intrusion test requires a high level of technical expertise and experience, as the test aims to identify vulnerabilities and entry points that are not necessarily known beforehand. The intrusion tester needs to be able to realistically act as an attacker without exposing the organisation's information systems or IT environment to unacceptable risks, such as disruptions. It is appropriate that tests be implemented in a test environment that is configured identically to the production environment, but which does not contain any activity information.

An intrusion test is an advanced security control and, for efficient use, the organisation should prepare by first checking with a vulnerability scan that the IT environment is configured for security. Intrusion tests generally do not need to be performed as often as vulnerability scans. Nor is it always necessary to conduct intrusion tests of all information systems. It is appropriate that priority be given to information systems accessible from external networks.

Before the organisation decides to carry out intrusion testing, a risk assessment needs to be carried out, taking into account the views of affected system owners and activities. The risk assessment may result in certain parts of the IT environment being excluded from the intrusion test, e.g., because the impacts of their being potentially affected are too great. In such cases, it is appropriate to perform a tabletop exercise instead, where the exempted information systems are security-audited based on the described configurations, integrations and other relevant documentation.

If resources permit, it is appropriate for the organisation to also use the intrusion tests to check whether monitoring systems detect an ongoing "attack". This will enable development of monitoring functionality as necessary, thus improving the ability to detect incidents. It is also appropriate to practice the organisation's incident management during the intrusion test.

Accounts used for security testing (both vulnerability scans and intrusion tests) need to be monitored to verify that they are only used as intended and disabled after the security test. The tools used for security testing need to be regularly updated to ensure that they themselves do not contain vulnerabilities, and that they detect the latest vulnerabilities.

4.6.5 Audits

Security auditing involves a manual audit of documentation in order to find errors and deficiencies. This could include reviewing code, configurations, architecture and firewall rules. It also includes checking that the documentation describing the IT environment and information systems is sufficient to allow operation and administration to be conducted safely.

Security audits should be carried out prior to deployment and when changes are made to the information system or IT environment that may affect security.

4.7 Change management, updating and upgrading

4.7.1 Purpose

To implement changes to information systems without affecting IT-environment security, the organisation needs structured and traceable change management.

4.7.2 Requirements

The organisation shall[97]

1. ensure that changes to information systems are implemented in a structured and traceable manner
2. have internal rules for change management, with requirements for
   a. a. criteria for hardware/software approval before installation or use
   b. how to identify and manage risks of incidents and deviations related to changes in the production environment
   c. how to update software, without unnecessary delay, to the latest version
   d. how hardware/software that is no longer updated or supported by the supplier shall be replaced/ upgraded without unnecessary delay
   e. how risks are to be managed when updates/upgrades according to c) & d) cannot be carried out.

The organisation should[98]

1. promptly implement security updates
2. consider the need to automate security updates
3. clarify in internal rules how risks of incidents and deviations related to changes in the
4. development, test and training environments are identified and managed
5. conduct tests and develop a recovery plan before a change in the information system is implemented in order to avoid disruption related to the change.[99]

4.7.3 Change management

An organisation's IT environment often needs to be changed; in many organisations this even occurs frequently. This may be because, e.g., new information systems are commissioned, hardware/software is updated/ upgraded or bug fixes. To ensure that changes are implemented in a structured and traceable way, the organisation shall have internal change management rules[100]. The rules shall include criteria regarding what needs to be done before the IT environment is changed, e.g., by installing or using hardware and software. The criteria can be formulated as requirements for the following:

- Approved result when testing the change in the test environment.
- Identification and management of risks of incidents and deviations occurring in connection with changes to the production environment, including the impact on activities and other information systems.

97. MSBFS 2020:7 Chapter 4 Section 12 The Authority shall ensure that changes to information systems are implemented in a structured and traceable manner. The Authority shall have internal change management rules requiring 1. the criteria to be used to identify and manage risks of incidents and deviations related to changes in the production environment; 3. how to update software to the latest version without undue delay; 4. how to ensure replacement or upgrade of hardware and software no longer supported or maintained by the supplier without undue delay; and 5. how to manage risks when updating or upgrading according to items 3 & 4 cannot be performed.

98. General advice to MSBFS 2020:7 Chapter 4 Section 12 Security updates should be introduced promptly, and the need to automate updates should be considered. The internal rules should clarify how risks of incidents and deviations related to changes in the development, testing and training environment are identified and managed.

99. General advice to MSBFS 2020:7 Chapter 4 Section 12 To avoid disruption in the event of change, the Authority should conduct tests and develop a recovery plan before the change is implemented.

100. A more detailed description of change management is described in, e.g., the Informational text Technology Infrastructure Library (ITIL) Change Management.

- Identifying the appropriate time to implement the change so as to minimise the impact on activities and other information systems.
- Documentation for operations and administration updated based on the change.
- Recovery plan prepared and approved in latest version, in the event the update/ upgrade fails wholly or in part.
- How the decision to implement the change is made.

The rules shall require that software be updated to the latest version without undue delay. The organisation needs an approach to ensure comprehensive monitoring of security updates and other necessary updates, and that the updates are incorporated into the information system.

The latest version includes not only updates with new features etc., but also the latest security updates sent out by the vendor. It shall also be required that hardware and software no longer updated or supported by the supplier shall be replaced or upgraded without undue delay. If no suitable IT products are available, or if a risk assessment has shown that updating or upgrading cannot be carried out without undue delay because the impact on an activity or other information system is deemed too great, the rules shall clarify how the risks arising in that respect are to be managed. This may include the introduction of compensatory security measures, such as additional network segregation. The internal rules of the organisation should also clarify how risks of incidents and deviations related to changes in the development, testing and training environment are identified and managed.

It is appropriate that the internal change-management rules also address situations where change management needs to take place during an ongoing incident. Such change work often occurs under time constraints, where risk assessment, planning and implementation of changes need to be done quickly. It is appropriate to conduct exercises involving both the change organisation and the incident organisation.

Change management approach

The organisation's change management is best coordinated by a specifically designated role in the IT department. Change management needs to include the following steps:

1. Identifying the type of change needed, such as deploying a new information system, upgrades or bug fixes.
2. In collaboration with information and system owners, planning for implementation of the change, e.g., timing, scope and resources, and how those affected by the change will be informed
3. Ensuring that the necessary documentation exists, e.g., risk assessment, recovery plan and updated operation and administration documentation.
4. Identifying and manage any impact on the security measures in place during the implementation of the change.
5. Deciding on and implementing the change.
6. Monitoring that the change has the intended effect, including not introducing new vulnerabilities.
7. Regularly evaluating change management to improve internal rules and modes of operation.

To increase the efficiency of change management, certain types of frequently recurring changes can be managed in specific fast tracks, where items 2–5 can be done in a simplified form. This can be done, e.g., by reusing risk assessments and delegating management of routine, low-risk changes to designated personnel. It may also be necessary to use fast tracks for particularly time-sensitive updates, such as security updates. Decide on pre-approvals for security updates and frequent low-risk changes, so that the organisation's resources are primarily used to manage more extensive, complex and risky changes. The internal rules need to clarify the

respective situations in which fast tracks may or must be used. Certain tools can also automatically introduce approved changes to the organisation's IT environment.

The use of such tools makes it easier for the organisation to, e.g., implement timely security updates.

4.7.4 Update

Update refers to the installation of the supplier's latest version of software which is already in the information system.

It is important to update to the latest version without delay, as in most cases newer versions contain fewer vulnerabilities and often more and better security features than older versions. This applies to all software, including operating systems, firmware, drivers and applications. An update may include new features, which means that the security configuration may need to be revised to meet the needs of the organisation.

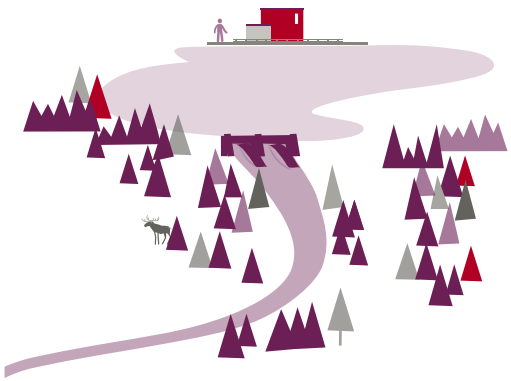
Security updates are a special type of update. In order for an IT environment to be as secure as possible, the organisation needs to have the latest security update installed on every single information system at all times. Such installations should also be carried out promptly. Within only a few hours of a supplier's release of a security update, the known vulnerability may be exploited on a larger scale, and attacks may be carried out against organisations that have not yet updated security. The organisation should therefore consider the need to automate security updates. In some cases, the vulnerability is exploited before the supplier can produce a security update, a so-called zero-day vulnerability. It is therefore important to have multi-layered security measures and an approach to quickly implement additional security measures when the extent and nature of the vulnerability becomes known. It may be necessary to completely shut down vulnerable information systems pending updates.

4.7.5 Upgrade

Hardware and software become less secure over time. This may be because new vulnerabilities have been discovered that cannot be managed with the older technology on which the information system is built, or because the supplier no longer provides updates or support.

It is important to upgrade hardware and software without undue delay where updates are no longer provided by the supplier. The organisation can also choose to completely replace the legacy hardware and software with a new technology.

Organisations may have difficulty finding the resources to upgrade information systems by replacing older hardware and software. Begin the process of upgrading information systems by developing a plan for how new hardware and software will be acquired and managed over its lifetime, and how and when it will be replaced. To provide a basis for the plan, dependencies on other information systems, and how they are affected by an upgrade, need to be analysed. Failure to plan for timely hardware/software upgrades brings the risk of possessing outdated information systems in which an attacker can exploit known vulnerabilities.



4.8 Robust and accurate time

4.8.1 Purpose

To enable comparison of logs between different information systems, and to use functions that increase security when communicating with third parties, the organisation[101] needs to use the official Swedish standard time provided by
a robust time service.

4.8.2 Requirements

The organisation shall use robust and accurate time traceable to the Swedish application of Coordinated Universal Time UTC (SP) in its production environment.[102]

The organisation should[103]

1. use the Swedish Distributed Time Service at www.ntp.se
2. identify and manage the need to use robust and accurate time traceable to the Swedish application of Coordinated Universal Time UTC (SP) in the development, test and training environment.

4.8.3 Robust and accurate time

Accurate time here means time that is traceable to Coordinated Universal Time (UTC). UTC is based on the International Atomic Time and is used for precise time indications worldwide. The Swedish equivalent, the official Swedish standard time, is called UTC (SP). The Post and Telecom Authority offers a robust time service[104] which is freely available and traceable to the official Swedish standard time UTC (SP).

Robust and accurate time is a prerequisite for investigating various events in the IT environment. When logs from different information systems need to be compared to detect errors (system logs) or security incidents (security logs), it is considerably easier if the information systems use the same time. It becomes difficult or sometimes impossible to know the order in which different events occurred, if different times are used. Some means of communicating with other organisations also require the use of accurate time.[105] This creates the need for different organisations to use the same time and preferably the same time service.

The organisation's IT department shall therefore ensure that the organisation uses a robust and accurate time traceable to the Swedish application of Coordinated Universal Time UTC(SP) in its production environment.[106] The organisation should also identify the need to use such time in its development, test and training environments.

It is often appropriate for the organisation to install a central time server in its own IT environment, which continuously retrieves time from the time service. The organisation needs to identify and manage the impacts should the central time server be unable to contact the selected time service, as well as reviewing the need for backup time services.

Some information systems in the organisation's production environment may lack the ability to retrieve time from the organisation's central time server, e.g., due to age or geographical location. In these cases, it is better to use any time source than no time source at all. One option is for the organisation to permit information systems to synchronise with pre-selected standby time services.[107]

101. Since the main purpose of the guidance is to facilitate the application of regulatory requirements on security measures in information systems for Swedish authorities, reference is made to official Swedish standard time. Other organisations in the international context may have cause to use a different national standard time.

102. MSBFS 2020:7 Chapter 4 Section 13 The Authority shall use robust and accurate time traceable to the Swedish application of Coordinated Universal Time UTC(SP) in its production environment.

103. General advice to MSBFS 2020:7 Chapter 4 Section 13 The Authority should use the Swedish Distributed Time Service at www.ntp.se. The need to use robust and accurate time traceable to the Swedish application of Coordinated Universal Time UTC (SP) in the development, test and training environment should be identified and management.

104. Network Time Protocol (NTP.) For more information on the PTS NTP service, see www.ntp.se which describes the service.

105. This applies, for example, to the use of TLS connections103, DNSSEC103, SAML103 and Kerberos.

106. If external services are used, the organisation needs to require the use of UTC (SP), including in cloud services.

107. E.g., the Global Navigation Satellite System (GNSS).

4.9 Backup

4.9.1 Purpose

To restore information destroyed or altered by accident or without permission, organisations need to back up their information and protect their backups.

4.9.2 Requirements

The organisation shall

1. regularly back up their information, in order to be able to restore information that is lost or corrupted[108]
2. keep backups separate from the production environment and protect them from damage, unauthorised access or unauthorised modification.[109]

The organisation should[110]

1. once per day, back up information needed for the organisation's ability to conduct its mission.
2. once per year, or during major changes to the production environment, verify its ability to restore information from backups within an acceptable time frame.
3. manage software, configurations and information separately when assessing the scope and interval of backups
4. identify and manage the need for backup, and the ability to restore information, in the development, test and training environments.

108.MSBFS 2020:7 Chapter 4 Section 14 In order to be able to recover information that has been lost or corrupted, the Authority shall regularly back up its information.

109.MSBFS 2020:7 Chapter 4 Section 15 Backups must be kept separate from the production environment and protected against damage, unauthorised access or unauthorised modification.

110. General advice to MSBFS 2020:7 Chapter 4 Section 14 The authority should 1. back up information needed for the authority's ability to carry out its mission once per day, and 2. once per year, or during major changes to the production environment, verify the ability to restore information from backups within a period of time acceptable to the Authority. When assessing the scope and interval of the backup, software, configuration and information should be handled separately. The need for backups, and the capacity for recovery of information in the development, test and training environments, should be identified and addressed.

4.9.3 Backup

Lost or corrupted information needs to be recoverable. Backing up information creates a copy of the information in an information system at a specific point in time. The organisation needs to regularly back up all relevant information, i.e.,

- activity information
- configurations
- software.

The IT department needs to implement backups based on the needs of the activity, both in terms of access to its information and functionality of the IT environment.

Necessary backup intervals depend on which information and IT functionality the activity can accept the loss of. For certain time-sensitive activities, backups may need to be made more frequently than once per minute.

However, the organisation should back up information needed to conduct its activities at least once per day. How often backups are needed can determine which backup technology can be used.

The scope of backup also needs to be based on the needs of the activity. An organisation must be able to restore information that has been lost or corrupted. Information not in danger of being lost or corrupted, either because it can be easily recovered by means other than backup, or because it is of such low value to the organization that it can lose the information without any impacts, need not be backed up.

The need to restore functionality in the IT environment may require access to backups of configurations and software. Backups of configurations and software need to ensure that the latest version is available.

In development, test and training environments, the organisation needs to determine the scope and interval of backup and recovery based on the activity needs of the environment.

Two examples of incidents that require backups for recovery:

- Ransomware encrypts part or all of the information system, making the information inaccessible.
- The file system becomes corrupt, and the information becomes inaccessible.

As some incidents can be difficult to detect, it is appropriate to save not only the last backup made, but also backups of several historical versions. The information system can then be restored even if the most recent backup includes errors or malware. It is also appropriate to use technologies that prevent the backup from being accidentally overwritten.[111]

It is appropriate to include in a given information system's operation and administration documentation how the backup shall be conducted by describing the following:

- what information must be backed up
- how often backups must be performed, and how changes made after backups shall be handled
- how quickly recovery needs to be possible
- the manner in which recovery is to be carried out
- how long backups will be stored
- how backups will be protected.

4.9.4 Information recovery

Backup failures can result in readback taking a long time, or in some cases even being impossible. For backups made, the organisation must verify the following:

- they contain the correct information
- the information is in the correct format
- the information can be recovered within a period defined by the activity.

Recovery can be made in different ways. Sometimes all or part of the activity information needs to be restored, sometimes the configuration and software of the information system also needs to be restored.

In some cases, the information system needs to be completely rebuilt from scratch, including the installation of new hardware.

Once per year, or during major changes to the production environment, the organisation should verify its ability to restore information from backups within an acceptable period, in accordance with the information system's recovery procedure. However, it is appropriate to perform such verification more frequently for activity information and functionality in the IT environment that is essential for the organisation's ability to conduct its activities.

4.9.5 Backup storage

Backups can be stored digitally on internal or external hard drives, data tapes and sometimes CDs or DVDs. The organisation shall keep at least one backup separate from the production environment, and protect all backups against damage, unauthorised access or unauthorised modification. The information on the backups needs to be protected during both transfer and storage.

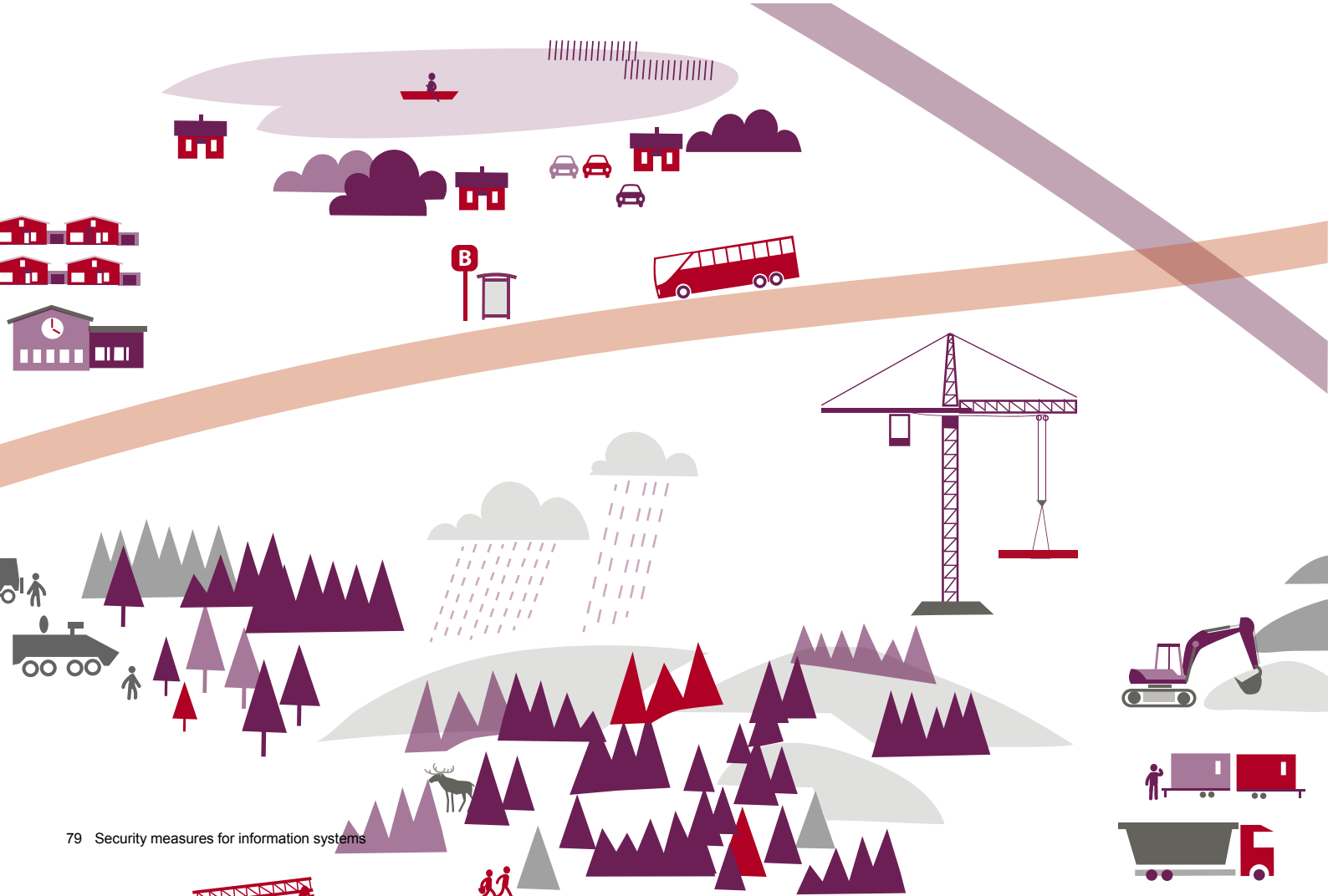
111. Write Once Read Many (WORM).

It is appropriate to apply the 3-2-1 rule when backing up:

- Create three (3) backups of the information: one primary and two extras.
- Keep the information on two (2) different storage media to protect against different types of threats.
- Keep one (1) backup physically separate from the production environment at a different geographical location.

The backups need to be protected at the same level as the information backed up. For the storage of different copies of the backups, it is appropriate to place one close to the production environment, to facilitate quick recovery, and one in a geographically remote location to protect the backup from environmental events (e.g., fire or flood) affecting the production environment. It is also appropriate to keep different versions of backups separate from each other. If multiple backups are stored in the same location, the level of protection needs to accommodate the aggregate amount of information backed up.

Backups stored on hard drives and accessible via the network are vulnerable to malware, such as encrypted viruses. If backup copies are stored on such a hard disk, it is appropriate to store another copy in a logically separate way, i.e., an off-line copy. Data tapes are normally removed from drives or libraries and stored separately from the enclosed data storage facility, usually in a safe. The tape drive or library must also be protected at the same level as the information it copies.



4.10 Implement security logging

4.10.1 Purpose

The organisation needs to log security-related events in order to detect and manage incidents and deviations that may affect the security of information systems.

4.10.2 Requirements

The organisation shall

1. ensure traceability in information systems by logging the following security-related events:[112]
   a. unauthorised access or attempted unauthorised access to the IT environment or individual information systems
   b. changes to configurations or security functions that require privileged rights
   c. changes to user or information-system access rights
   d. access to information that require enhanced protection
2. analyse security log content to detect and manage incidents and deviations; and the security logs shall[113]
   a. enable investigation of intrusions, technical failures and security deficiencies
   b. be designed to enable comparability between different logs
   c. be accessible for log analysis during the defined time period of log-storage.
3. document[114]
   a. how to use the security logs
   b. where logging data is retrieved from
   c. where the security logs are stored
   d. how they are protected
   e. how long they should be stored.

The organisation should[115]

1. ensure that a security log contains information regarding
   a. who or what has acted
   b. what has happened
   c. at what time
2. create comparability by using the organisation's time service for all security logs
3. collect security logs in a dedicated information system.

4.10.3 Security logging

Logging records various events in an information system. Security logging records events that have been identified in advance as important from a security perspective, so-called security-relevant events. Security logs are important to detect and manage incidents and deviations in information systems. The organisation should ensure that security logs contain the logging information necessary for the organisation to understand the course of events. In principle, all information systems must compile their log data in a standardised format and retrieve log data times from the organisation's time service in order to compare security logs from different information systems, and thus understand the course of events.

112. MSBFS 2020:7 Chapter 4 Section 16 The Authority shall, in order to ensure traceability in information systems, log the following security-related events: 1. Unauthorised access and attempted unauthorised access to the IT environment or individual information systems. 2. Changes to configurations or security features that require privileged rights. 3. Changes to user or information system access. 4. Access to information deemed to require enhanced protection.

113. MSBFS 2020:7 Chapter 4 Section 17 The Authority shall analyse the content of the security logs in order to detect and manage incidents and deviations. The security logs shall: 1. allow investigation of intrusions, technical failures and security deficiencies; 2. be designed in a way that allows comparability between different logs; and 3. be available for analysis for a defined retention period.

114. MSBFS 2020:7 Chapter 4 Section 17 The Authority shall document how security logs are to be used and where logging data are retrieved and stored, how they are protected and how long they are to be retained.

115. General advice to MSBFS 2020:7 Chapter 4 Section 17 A security log should contain data about who or what acted, what happened and at what time. For the sake of comparability, the Authority should use the Authority's time service for all security logs. Security logs should be collected in a dedicated information system.

The organisation shall always record in a security log

- unauthorised access or attempted unauthorised access to the IT environment or individual information systems
- changes to configurations or security features that require privileged rights
- changes to user or information system access
- access to information deemed to require enhanced protection.

Security logging design

The following initial conditions need to be used for the design of security logs:

- what information systems process information requiring enhanced protection (confidentiality, integrity, availability)
- what information systems the organisation needs to carry out its activities
- what digital identities have system administrator access
- what digital identities have access to information requiring enhanced protection
- what digital identities have extended access to perform certain tasks
- what traffic-filtering equipment information passes through.

Other data needing to be security-logged depends on the organisation's need for additional IT-environment traceability. For each information system, the organisation needs to analyse what additional security-relevant events need to be collected, and what log analyses need to be performed, to understand a course of events.

Security logs need to be created in almost all information systems. What distinguishes different information systems is what needs to be security logged, and how long it needs to be stored.

Even if the organisation itself has a limited ability to analyse security logs, it is important to collect all the log data needed to understand a course of events. If an incident occurs, the organisation can then provide the security logs to law enforcement agencies or to external support to help manage the incident.

Security logs often contain sensitive information about individual employees. Therefore, the organisation's interest in collecting logs containing personal data must always be balanced against the need to protect privacy. The logs also may only be used in a predetermined way. The General Data Protection Regulation states that data may only be processed if this is both necessary and proportionate with regard to the privacy of the individual. Security logging can also protect the privacy of the individual by contributing to traceability of who interacts with personal data. Security logging can also protect individual privacy by providing traceability of who interacts with personal data, and is thus often an important element of GDPR compliance.

The design of the security log shall be documented. The documentation must show the following:

- the purpose of security log collection, i.e., what needs to be detected
- how security logs will be used, i.e., when and how they will be analysed
- what information security logs contain
- where logging data are retrieved from, i.e., from which information systems
- where security logs are stored, i.e., both temporary and permanent storage
- how they are protected, i.e., against damage, unauthorised access or unauthorised alteration during transmission or storage
- how long they shall be retained and used for analysis.

In documenting how the security logs will be used and how long they shall be retained, the organisation needs to describe the purpose of the personal data processing.

In order to ensure the traceability of information systems, the organisation shall regularly verify that the right security-relevant events are collected, such as who or what has acted and what happened[116], including at what time. The analysis of the content shall enable detection and management of incidents and deviations.

Protect security logs

Security logs need to be protected against unauthorised access or modification.

- An attacker with access to an information system often tries to erase his tracks. This can often only be done by changing the security logs.
- The logs often contain personal data, which need to be protected according to the requirements of the General Data Protection Regulation.
- For the logs to be useful in the analysis work, it must be ensured that they have not been changed.
- Logs may also contain other critical information, such as sensitive activity information or information about system configurations and vulnerabilities.

The organisation needs to ensure sufficient access control to prevent unauthorised access to log content. It is appropriate to log access, modification and deletion of logs. Encryption technologies need to be used to detect unauthorised changes to the logs.[117]

Log data created in an information system can either be transferred to an information system used for security log storage, or stored in the information system where they are created. To make it easier to protect and analyse security logs, the organisation should collect them in a dedicated information system, such as a logging system with central storage.[118]

Enabling security logging on all information systems can generate large quantities of information. Regardless of where security logs are stored, the organisation needs to ensure sufficient storage space to avoid the risk that new log data are no longer entered, or that older data to be saved are overwritten.

4.10.4 Analysis of security logs

Deficiencies in either collection or analysis of security log data may prevent incidents and deviations from being detected or investigated. This may, e.g., permit attackers to enter the organisation's IT environment undetected.

Such deficiencies can also prevent the course of events from being understood, even if an organisation discovers that someone has gained unauthorised access to its information systems.

Security log analysis is required to detect and understand events deviating from the normal and permitted use of the organisation's information systems. To investigate intrusion, technical errors and security deficiencies, organisations need to be able to recreate a sequence of events, often involving multiple information systems. It is important to have ensured the comparability of log data retrieved from different information systems. If the organisation discovers deficiencies in the content or design of the security logs during analysis of an incident or deviation, these deficiencies need to be addressed, e.g., by collecting additional log data, reviewing the format of the logs or performing security logging in more information systems.

116. For example, events that involve someone reading, searching, writing, deleting or creating information.

117. See also section 4.4.6 Security logs.

118. Log Management System (LMS).

Log analysis needs to be carried out in a structured way. The organisation's approach to security-log analysis therefore needs to clarify

- who is allowed to handle and/or perform analysis of security logs, e.g., log data from an information system may need to be manually retrieved by the technical system administrator, while analysis of security logs is performed by a designated log analyst
- when analysis shall be carried out for each information system, e.g., on a regular basis, through spot checks or on an ad hoc basis
- how analysis of security logs shall be carried out, e.g., automatically, manually or both, and with what technical support
- what action to take and whom to contact when an incident/deviation is detected
- what event summaries and statistics shall be produced to provide information regarding deviations and incidents and to improve the security logging process.

Suspected security deficiencies need be investigated promptly in order to confirm or dismiss them. This can involve, e.g., suspected incidents where personnel failed to comply with internal rules regarding personal data processing in a particular information system, or an attacker seeking access to the IT environment.

Analysis of security logs usually requires support from automated tools, as it often involves large quantities of log data that need to be compared. The appropriate tool depends on the purpose of the analysis. Any analysis tool needs to be continuously adapted and calibrated to detect intrusions, technical errors and security deficiencies in the organisation's security logs.

4.11 Monitoring

4.11.1 Purpose

Organisations need to monitor security-related events in their information systems to detect and manage intrusions and incidents that may affect security.

4.11.2 Requirements

The organisation shall identify and manage the need for

1. intrusion detection[119]
2. intrusion protection[120]
3. real-time monitoring of information systems.[121]

The organisation should assess the need for intrusion detection and protection for[122]

1. individual information systems
2. the organisation's production environment as a whole
3. the organisation's development, test and training environments.

4.11.3 Intrusion detection and intrusion protection

Intrusion detection aims to detect attempted and successful intrusions. The intrusion detection system can be complemented by intrusion protection that also allows permits acting on discovered intrusion attempts, e.g., by directly blocking the attack. Intrusions that can be assumed criminal are to be reported to the police.

An intrusion-detection system can monitor both network traffic and activities in individual information systems. Monitoring is particularly important in the production environment, but depending on how the development, test and training environments are used, it may be necessary there as well. Which information systems need monitoring depends on their location, the information being processed and its importance to the organisation's ability to conduct its activities. Monitoring is particularly important in information systems linked to external networks, such as e-mail, web pages, web services and DNS servers.

It is appropriate to monitor

- network traffic
- security features
- configurations
- information systems processing information requiring enhanced protection
- information systems deemed to require monitoring for other reasons.

Configure the intrusion-detection system to examine both incoming and outgoing network traffic (both internet traffic and system-to-system communication with another organization), as well as network traffic in particularly vulnerable network domains, for known vulnerabilities and attack methods. Intrusion detection shall also encompass traffic to and from particularly sensitive information systems, such as information systems processing information requiring enhanced protection, and security functions such as directory services, security logs and backup.

The implementation of intrusion-detection systems and other monitoring requires time, as the tool needs to be adapted to a level where events that may indicate an intrusion are noticed while others are ignored.

If an attack is detected, the organisation needs to manage it in accordance with its incident-management procedures. Most com-

119. MSBFS 2020:7 Chapter 4 Section 18 The Authority shall identify and manage the need for intrusion detection and protection.

120. MSBFS 2020:7 Chapter 4 Section 18 The Authority shall identify and manage the need for intrusion detection and protection.

121. MSBFS 2020:7 Chapter 4 Section 19 The Authority shall identify and manage the need for real-time monitoring of information systems.

122. General advice to MSBFS 2020:7 Chapter 4 Section 18 The need for intrusion detection and protection should be assessed for individual information systems and for the Authority's production environment as a whole. The need should also be assessed for the Agency's development, test and training environments.

monly, the attacker is blocked. In some cases, where there is no risk of further damage, it may be appropriate to permit the intrusion to continue under close supervision to obtain further evidence of how the intrusion was carried out with a view to preventing future intrusions. Intrusion-detection systems used in the network's external protection and those used to protect internal networks need to be different to fulfil their respective internal and external purposes. Having different internal and external intrusion-detection systems also helps to reduce the risk of both systems being affected by an attack.

IT personnel working with intrusion detection need to understand intrusion methods and malware management. It is also appropriate that they have experience in handling and investigating incidents.

4.11.4 Real-time monitoring

The organisation shall identify and manage the need for real-time monitoring. Real-time monitoring allows organisations to monitor the status of information-system functionality in real time. Tools used for real-time monitoring can be configured to provide alerts upon incidents and deviations, such as when pre-set thresholds are exceeded. It is appropriate to use real-time monitoring to detect

- if unauthorised equipment is connected to the IT environment
- execution or attempted execution of unauthorised software
- if unauthorized commands are executed on command interfaces
- software bugs
- storage-space problems
- abnormal use of system resources
- unauthorised use of system administrator access
- unauthorised access or attempted unauthorised access
- abnormal network traffic, e.g., regarding time
- unauthorized network traffic between network domains.
- detection of malware.

Real-time monitoring is often initially resource intensive. Real-time monitoring does not always require 24-hour personnel presence. An organisation may choose to have its own personnel on-site during the day, while alerts received at other times are handled by on-call staff. Provided that the organisation considers that all alerts received outside normal working hours can be handled, with sufficient security, by intrusion protection that blocks attacks, and then dealt with the following working day, this process is also feasible. The need for and design of surveillance needs to be based on the needs of the activity and the current threat environment.

4.12 Protection against malware

4.12.1 Purpose

To prevent the installation, spread and execution of viruses, worms, Trojans, spyware, ransomware, etc., in its IT environment, an organisation needs to protect itself against malware.

4.12.2 Requirements

The organisation shall

1. use software that protects against malware.

For information systems where such software does not exist, other measures shall be taken.[123]

4.12.3 Malware

Malware is a constant threat to the IT environment. In addition to causing damage, such code is often designed to evade, disable or attack security features.

Malware can spread quickly, change as necessary and can enter via e-mail, websites and removable storage media, among other means. The malicious code can result in different types of damage, e.g., allowing an attacker to

- enter the IT environment and map the best method of attack, e.g., to take over the entire IT environment
- access information, including destroying or changing information
- use the organisation's information systems to mine cryptocurrencies or send spam
- encrypt the organisation's information to engage in extortion.

Malware is commonly introduced in the IT environment by tricking users into clicking on links or opening email attachments containing macros. The organisation can also obtain malware through information-sharing with other organisations. Risk assessment of exposure to malware therefore needs to take into account the different entry points and propagation possibilities in the IT environment.

How malware spreads, its impacts and which information systems are most vulnerable constantly changes. Therefore, external environmental monitoring vis-a-vis malware development and the information systems it attacks is important.

4.12.4 Anti-virus software

An organisation must have protection against known malware and known methods of spreading code. But preparedness to deal with newly developed malware is also required. There are two ways to protect against malware using software (antivirus software[124]): blacklisting and whitelisting.

Blacklisting is a common feature of antivirus software, but to be effective it is important that the software supplier provide timely updates as soon as new malware is detected. Until such updates have taken place, the organisation is vulnerable to the new malicious code.

Protection is improved by introducing whitelisting functions. However, whitelisting requires a structured approach. This is to ensure that software needed for the organisation's activities is allowed, while malware is excluded. To avoid burdening users unnecessarily when whitelisting is implemented, it is appropriate to use the learning-mode of the function for a transitional period.

123.MSBFS 2020:7 Chapter 4, Section 20 The Authority shall use software that protects against malware. For information systems where such software is not available, other measures shall be taken to provide equivalent protection.

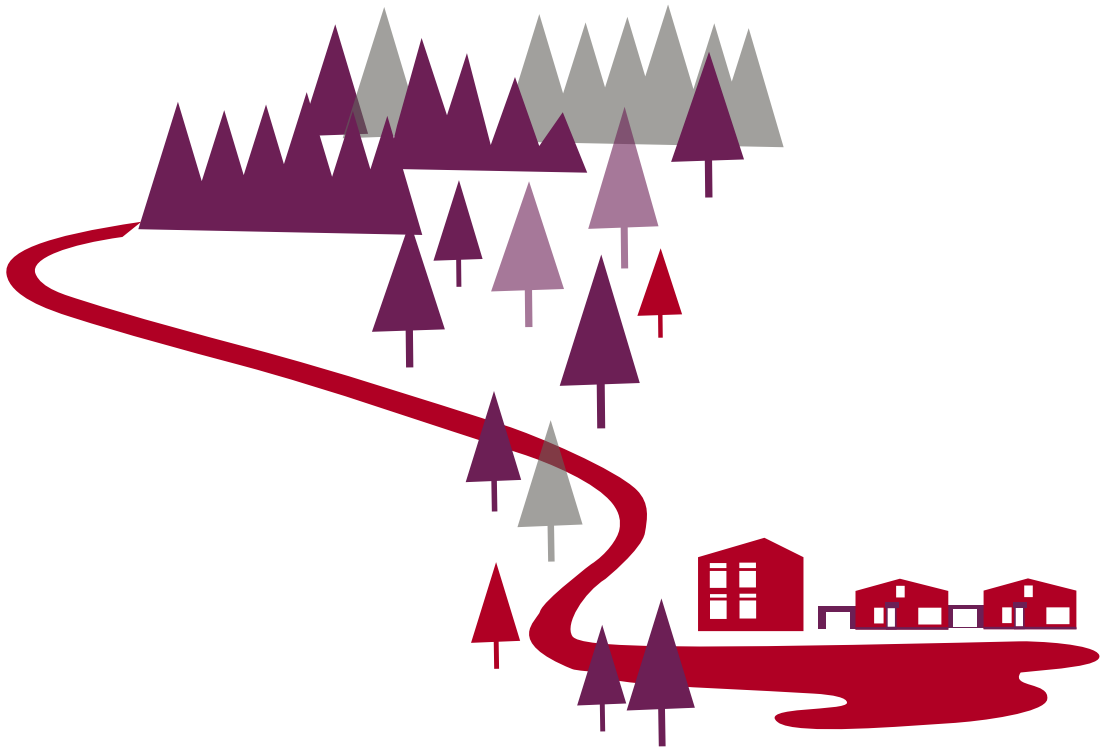
124.Anti-virus software is used both colloquially and, here, as a description of software that protects against all types of malware.

For more comprehensive protection, organisations need to combine blacklisting and whitelisting.

Anti-virus software needs to be available on both clients and servers, especially those processing information from external networks. It is appropriate to use a dedicated information system to manage installation, updates and alerts from anti-virus software in a unified way. The organisation needs an approach that clarifies how malware alerts are handled based on the severity of the code, i.e., its risk of dissemination and damage. In some cases, it is important to act quickly and decisively to stop the attack.

4.12.5 If anti-virus software does not exist

For some types of information systems, the supplier does not provide anti-virus software. This may be because the design of the technology is considered to preclude malicious attacks, or because information system functionality cannot be maintained if anti-virus software is running. The latter is often highlighted in the context of industrial information and control systems. Since it cannot be excluded that such information systems are nevertheless affected by malware in some form, the organisation shall take compensatory measures. In risk assessment of these information systems, the organisation needs to address the increased risk posed by the absence of anti-virus protection. This affects the design of security measures such as network segregation, filtering, access, security configuration, monitoring and protection of equipment. It is appropriate, e.g., to place such information systems in one or more dedicated network domains with extensive monitoring and strict access management.



4.13 Protection of equipment

4.13.1 Purpose

To prevent damage and unauthorised access to IT equipment, the organisation needs to ensure adequate physical protection.

4.13.2 Requirements

The organisation shall protect the equipment of information systems against damage and unauthorised access by[125]

1. placing central servers and network equipment in dedicated
2. enclosed data storage facilities.
3. restricting access to enclosed data storage facilities
4. identifying and managing the need for monitoring and alerts in specific
5. enclosed data storage facilities.
6. registering access to dedicated
7. enclosed data storage facilities at individual level, and saving the documentation for a defined time period for storage of the documentation.
8. having internal rules regarding protection of mobile equipment.

4.13.3 Physical protection

Protection against unauthorised access to and interference with the functionality of information systems cannot be achieved by organisational, administrative and technical security measures alone; physical protection is also needed. Physical protection is constructed through security measures such as

- external security, e.g., fencing, concrete barriers and crash barriers, flower beds, lighting and patrols
- security perimeters that prevent unauthorized
- access to the organisation's building or office, e.g., locked doors and windows, manned reception, badge requirements, access-control systems and camera surveillance
- alarm system in case of unauthorised access[126]
- fire protection, including alarms and evacuation routes
- sectoral division of the internal environment, e.g., visitor domains, domains for ordinary activities, domains for handling sensitive information and dedicated enclosed data storage facilities.
- protected storage, e.g., strongboxes, fireproof cabinets[127], lockable spaces[128] and archive spaces.

Measures need to be chosen and designed according to the needs of the organisation. The design and administration of physical protection is led and coordinated by the organisation's security organisation. A common approach is for the CISO to contribute by communicating the protection needs regarding information and information systems, so that the property owner can implement security measures. If the premises are leased, the organisation needs to regulate the security measures in a contract and engage in dialogue with the property owner or his representative regarding the physical protection.

125.MSBFS 2020:7 Chapter 4 Section 21 The Authority shall protect the equipment making up information systems against damage and unauthorised access by 1. placing central servers and central network equipment in dedicated enclosed data storage facilities, 2. assigning access to dedicated enclosed data storage facilities restrictively, 3. identifying and managing the need for monitoring and alarms in dedicated enclosed data storage facilities, 4. recording access to dedicated enclosed data storage facilities at individual level and retaining the documentation for a defined retention period, and 5. having internal rules regarding how mobile equipment is to be protected.

126.The Swedish Anti-Theft Association's (SSF) standard SSF 130 describes four alarm classes based on protection needs.

127.When storing backups, it is important to use cabinets that are fire rated according to the SS-EN 1047-1 standard and suitable for such use, such as S60 DIS or S120 DIS.

128.Storage should be burglar-proof, e.g., pursuant to the requirements of SSF 3492.

4.13.4 Equipment siting and protection

Dedicated enclosed data storage facilities can include computer halls, computer rooms, cross-connection rooms, cabinets, etc., that are adapted for a single piece of sensitive IT equipment, a large amount of IT equipment, or where the organisation places central servers and central network equipment.

The placement of an enclosed data storage facility in a building, and how it is protected, needs to be considered to protect IT equipment placed there from damage or unauthorised access. When designing dedicated enclosed data storage facilities, the organisation needs at least to identify and manage risks of

- fire and flooding, inside and outside the dedicated enclosed data storage facility, and in the surrounding area
- disruptions in electricity, district cooling and ventilation
- vandalism or burglary.

The organisation shall ensure that IT equipment processing information that is essential for conducting the organisation's activities is adequately protected against damage and unauthorised access. Servers, databases, routers, switches, etc., processing such information shall therefore be located in dedicated enclosed data storage facilities.

The organisation must always assign access permission to these areas restrictively, record access at individual level and retain the documentation for a defined retention period. The organisation must identify and manage the need for monitoring and alarms in its dedicated enclosed data storage facilities and, based on information classification and risk assessment, also needs to identify and manage the need for

- reinforced walls, doors, windows and locks
- surveillance
- internal zoning and locked cabinets
- redundancy in electricity, communications and climate-conservation measures such as ventilation and temperature control
- fire and flood protection.

When designing dedicated enclosed data storage facilities and their protection, the security organisation including the CISO needs to collaborate with IT operations and property managers.

4.13.5 Mobile equipment

Mobile devices, such as portable clients, mobile phones and USB sticks, need protection mainly against unauthorised access to information or loss of information through theft or loss of the device[129]. The protection needs to take into account that the equipment can often be used to manage the organisation's information beyond the organisation's own premises.

The organisation shall have internal rules regarding how to protect mobile equipment. The rules need to accommodate both technical and administrative security measures. It is appropriate to require at least such technical security measures as

- encrypted storage
- security configuration, e.g., limiting the ability to boot a computer from a USB stick
- multi-factor authentication
- the ability to delete information remotely
- screen lock and screen protector
- receipt for mobile equipment
- anti-theft marking[130] and any GPS tracking[131].

129. See also Guidance for more secure management of mobile devices, MSB405 (June 2012).

130. The purpose of anti-theft marking is to make it more difficult to resell stolen equipment, since the marking makes the origin impossible to remove. The equipment is thus less desirable to steal.

131. A decision to implement GPS tracking needs to be preceded by a risk assessment and reconciliation with the organisation's data protection officer.

The security of mobile equipment also depends on how users handle equipment beyond the organisation's premises. It is therefore appropriate to regulate at least

- the situations and environments where mobile devices may be (e.g., travel or hotel rooms)
- the situations in which the mobile equipment may be used
- which USB sticks and similar devices may be connected to the organisation's information system
- how to charge mobile equipment securely (e.g., data blockers)
- how mobile equipment may be stored
- how users shall act to reduce the risk of unauthorised viewing or overhearing of information.

The internal rules need to be designed based on the organisation's information classification and risk assessment, and adapted to the way the organisation conducts its activity. Rules may be needed, e.g., regarding the extent to which mobile devices can be taken on trips abroad. Such rules may need to look differently depending on the country in question. Some countries may have legal regulations granting law enforcement agencies the authority to seize equipment, require information to be copied, and require the provision of codes or keys to access encrypted information. One way to deal with such regulations is to provide special travel kits that carry only necessary information.

4.13.6 Deleting and disposal of IT equipment

The information contained on IT equipment needs to be deleting before the equipment is returned for repairs, reused or disposed of to prevent unauthorised access to the organisation's information. The information can be wiped in different ways. Which approach is most appropriate depends on the type of IT equipment, whether the IT equipment is to be reused, the classification of information processed in the IT equipment and the outcome of the risk assessment. It is important to identify all IT equipment where information can be found. This can include, e.g., printers with hard drives that retain printouts, phones with call lists and more advanced screens that handle calendar appointments.

If the equipment is to be reused within the organisation, all previous information usually needs to be deleted using a data erasure program. The data erasure programs overwrite the original information with meaningless information before the equipment is reused. For some IT equipment, such as solid-state hard drives[132], data erasure programs are not sufficient to completely delete information. Organisations always need to consider whether IT equipment storing information requiring enhanced protection in terms of confidentiality must be disposed of rather than reused.

To ensure that information in IT equipment to be discarded cannot be reconstituted, the organisation may, e.g., use incineration, demagnetisation or grinding of the IT components containing information. It may be appropriate to use a supplier specialised in destruction. Destruction services can often be offered on-site at the organisation's premises, or the organisation's representative may accompany the organisation to the destruction facility to verify secure destruction.

Ensure in contracts that the organisation can also erase information processed in equipment belonging to a supplier (e.g., through loan, rental or lease), as well as requiring, as necessary, that equipment be disposed of securely upon return.

132.Storage media that do not require an electrical power supply to keep information intact.

4.14 Redundancy and recovery

4.14.1 Purpose

In order to be able to carry out its **mission without** unacceptable disruption during incidents and deviations, the organisation needs to ensure sufficient redundancy and the ability to recover information systems in the IT environment.

4.14.2 Requirements

The organisation shall, in order to ensure the availability of information and information systems in the event of incidents and deviations,[133]

1. have internal rules for the recovery of the production environment as a whole and for individual information systems
2. practise recovering information systems essential to the organisation's ability to conduct its mission
3. placing central servers and network equipment providing redundancy in different dedicated enclosed data storage facilities.

The organisation should practice recovery regularly, based on identified needs for availability.[134]

133.MSBFS 2020:7 Chapter 4 Section 22 In order to ensure the availability of information and information systems in the event of incidents and deviations, the Authority shall: 1. have internal rules for the recovery of the production environment in its entirety and for individual information systems; 2. practice recovering information systems essential to the Authority's ability to carry out its mission; and 3. situate central servers and equipment providing redundancy in different dedicated enclosed data storage facilities.

134.General advice to MSBFS 2020:7 Chapter 4 Section 22 Recovery exercises should be carried out regularly and based on identified needs for availability.

4.14.3 Recovery

If activity information, configurations or software are lost or corrupted, through mistake or malice, the organisation needs to be able to recover them. Normally, information processed in digital form is restored from a backup. Information systems processing backups often support the readback of everything from individual files to entire information systems. Even IT equipment can be damaged, which may require all or part of the IT environment to be recovered. This presupposes the availability of replacement equipment[135] and documentation regarding information system configuration.

It is appropriate that the organisation's internal rules for restoring the entire production environment include instructions prioritising different information systems based on function and dependency. It is also appropriate that the internal rules describe, for each information system, what skills are needed for recovery and how quickly recovery needs to occur, how recovery must be practised and where information on recovery can be found in operation and administration documentation.

Practice recovery

Recovering individual files is usually not complicated, but recovering an entire information system from scratch can be more difficult. That's why it's important to practice. After an incident, such as a ransomware attack or IT failure, all information, and sometimes even the configuration of the information system, may need to be recovered from scratch. The operational organisation shall practice recovering information systems essential to the organisation's ability to conduct activities. Such exercises should take place on a regular basis and should be based on the organisation's needs for the availability of its information and information systems. A suitable interval for practice can be between three months and one year.

135.To ensure access to replacement equipment, organisations need to identify and manage their dependencies on external suppliers to secure their digital supply chains.

Exercises need to be designed to correspond as far as possible to a realistic scenario without compromising the security of the production environment. In some cases, all or part of the exercise may consist of a tabletop exercise. It is advantageous if the organisation's test environment is designed and approved to practice full or partial recovery of information systems.

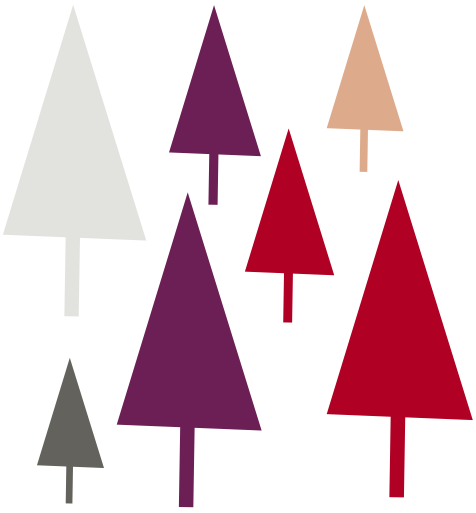
4.14.4 Redundancy

The purpose of redundancy is to maintain availability despite failure of an information system, or a function within an information system. This is achieved by ensuring availability of two or more, identical or different, information systems or functions that independently deliver the same result.

The organisation shall situate central servers and network equipment providing redundancy in different dedicated enclosed data storage facilities. Further, based on information classification and risk assessment, the organisation needs to identify and manage additional needs for redundancy of all or parts of the original functionality. To meet various availability needs, redundancy can be achieved in different ways, e.g.:

- divide personnel possessing the same skills into different groups so that, if one group is unable to work due to illness, the second group can take over
- mirror (copy) information so that the same information exists on multiple hard drives to reduce the risk of information loss from damaged IT equipment, e.g., hard drive crashes[136]
- use different software that performs the same function, or the same software on different information systems, to make the function available even if one software or information system suffers an incident, e.g., malware
- install a duplicate information system ready to assume functionality immediately upon disruption of the primary information system
- provide dedicated enclosed data storage facilities with dual power supplies that are, in turn, connected to different distribution boards to reduce the impact of power supply disruptions
- use two separate network connections to reduce the risk of data-communication failures during a network outage
- establish a business continuity site enabling operation of the organisation's information systems when the regular site cannot be used.

Different measures often need to be combined to create sufficient redundancy for the organisation's IT environment. It is appropriate to test redundancy regularly and as necessary, e.g., after a change in the IT environment.



136.Redundant Array of Independent Disks, RAID. A set of technologies enabling use of multiple hard drives to reduce the risk of data loss if one hard drive fails. The simplest form is to mirror (copy) the information on one hard disk to the other (called RAID 1). A more advanced form is to use three (or more) hard disks, where the information is spread over all the hard disks (except the last one) and where a checksum is written to the last hard disk (RAID 5). If one disk fails, the information can be recreated from the other three disks

For agencies with specific responsibility for emergency preparedness

5. For agencies with specific responsibility for emergency preparedness

5.1 Increased security requirements

5.1.1 Purpose

Pursuant to Section 18 of the Ordinance (2022:524) on the preparedness of government agencies, agencies with specific responsibility for emergency preparedness shall, given their mission, have a level of security beyond the requirements for security measures in Chapters 2–4.

5.1.2 Requirements

The Authority shall protect the equipment of the information system against damage and unauthorised access by

1. using multi-factor authentication for information systems essential to the Authority's ability to carry out its mission[137]
2. using real-time monitoring for information systems essential to the Authority's ability to carry out its mission[138]
3. quarterly verify the recovery capability of these information systems[139]
4. quarterly review the functioning of information systems used for information sharing during peacetime crises.[140]

The Authority should, to support information sharing in peacetime crises, us[141]

1. Swedish Government Secure Intranet (SGSI)
2. Radiokommunikation för effektiv ledning (RAKEL).

137. MSBFS 2020:7 Chapter 5, Section 1 Agencies withspecific responsibility for emergency preparedness pursuant to Section 10 of the Ordinance (2015:1052) on emergency preparedness and measures by security authorities during a heightened state of alert shall, in addition to what is set out in Chapters 2–4 of these Regulations, 1. use multifactor authentication and real-time monitoring for information systems essential to the Agency's ability to carry out its mission, and 2. verify the ability to recover these systems on a quarterly basis.
Note – "Agencies with specific responsibility for emergency preparedness" corresponds to "preparedness agencies " in the Ordinance (2022:524) on the preparedness of government agencies.

138. MSBFS 2020:7 Chapter 5, Section 1 Agencies withspecific responsibility for emergency preparedness in accordance with Section 10 of the Ordinance (2015:1052) on emergency preparedness and measures by security authorities during a heightened state of alert shall, in addition to what is set out in Chapters 2–4 of these Regulations, 1. use multi-factor authentication and real-time monitoring for information systems essential to the Agency's ability to carry out its mission; and 2. quarterly verification of the ability to recover these systems.
Note – "Agencies with specific responsibility for emergency preparedness" corresponds to "preparedness agencies " in the Ordinance (2022:524) on the preparedness of government agencies.

139. MSBFS 2020:7 Chapter 5, Section 1 Agencies with specific responsibility for emergency preparedness pursuant to Section 10 of the Ordinance (2015:1052) on emergency preparedness and measures by security authorities during a heightened state of alert shall, in addition to what is set out in Chapters 2–4 of these Regulations, 1. use multifactor authentication and real-time monitoring for information systems essential to the Agency's ability to carry out its mission, and 2. verify the ability to recover these systems on a quarterly basis.
Note – "Agencies with specific responsibility for emergency preparedness" corresponds to "preparedness agencies " in the Ordinance (2022:524) on the preparedness of government agencies.

140. MSBFS 2020:7 Chapter 5, Section 2 The Agency shall, on a quarterly basis, check the functioning of information systems to be used for information sharing during peacetime crisis situations.
Note – "Agencies with specific responsibility for emergency preparedness" corresponds to "preparedness agencies " in the Ordinance (2022:524) on the preparedness of government agencies.

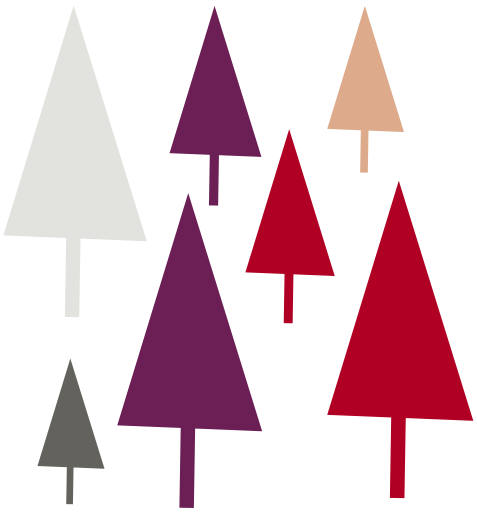
141. General advice to MSBFS 2020:7 Chapter 5, Section 2 The Authority should use the Swedish Government Secure Intranet (SGSI) and Radio Communications for Effective Management (RAKEL) to support information sharing during peacetime crisis situations. *Note – "Agencies with specific responsibility for emergency preparedness" corresponds to "preparedness agencies " in the Ordinance (2022:524) on the preparedness of government agencies.*

5.1.3 Increased requirements for security measures

Agencies with special responsibility for emergency preparedness must be able to withstand threats and risks, prevent vulnerabilities, manage peacetime crises and carry out their mission in the event of a state of heightened alert.[142] They must also, given their mission, implemented additional security measures. This involves the use of multi-factor authentication and real-time monitoring for information systems essential to the authority's ability to carry out its mission. Authorities must also verify the ability to recover these systems at least quarterly.

In the case of information systems used for information sharing in peacetime crises, functionality also needs to be checked at least quarterly. Examples of information systems used for information sharing in peacetime crises include information systems that enable

- internal communication necessary to carry out its mission
- communication necessary for cooperation with other authorities/organisations
- dissemination of information to the public.



It is appropriate to check the functionality of the above-mentioned information systems by, e.g.,

- verifying that information systems work properly
- ensuring that the right people have access to the information system
- verifying that the right skills are in place to operate and administer the information systems
- training personnel in the use of information systems
- verifying that information systems are correctly configured
- practising the recovery of information systems, and checking that the need for redundant functions can be met, for example by conducting tabletop exercises for management of power supply failures or network outages
- checking that information systems are up to date
- checking that documentation is sufficient for safe operation and administration.

Checks are ideally planned and implemented in collaboration between the system owner, the authority's emergency response organisation and the IT operations organisation. Checks of information system functions necessary for communication with other authorities/organisations are preferably planned and carried out together with the authorities/organisations concerned.

142.Section 20 of the Ordinance (2022:524) on the preparedness of government agencies. *Note – "Agencies with specific responsibility for emergency preparedness" corresponds to "preparedness agencies " in the Ordinance (2022:524) on the preparedness of government agencies.*

5.1.4 About SGSI and RAKEL

To increase access to communication services in peacetime crises, MSB currently provides two services:

- **SGSI** (Swedish Government Secure Intranet)[143] is an intranet, separate from the internet, for secure and encrypted communication between users within Sweden and Europe. The network is designed to meet high standards of availability and reliability. Using SGSI, connected organisations can access other connected services, send protected email and have protected videoconferences. Joining the SGSI poses requirements for an organisation's information security work.
- **Rakel** (Radio Communications for Efficient Management)[144] is a digital radio communication system for ensured and secure communication between personnel in organisations engaged in critical infrastructure. It is used by the police, emergency and rescue services, medical services and the armed forces, among others, but also by numerous other authorities, energy companies, public-transport authorities and organisations, e.g., handling hazardous substances. All county councils, municipalities and regions across Sweden are connected to Rakel. It is built to withstand severe weather conditions and prolonged power supply disruptions. Rakel works when other systems are down, e.g., in the event of overload or other disruptions to mobile phone and network communications.

These services can be used to spread information when normal communication channels do not work.

143.Additional information about SGSI at MSB's website https://www.msb.se/sv/verktyg--tjanster/sgsi/om-sgsi/ Note – "Agencies with specific responsibility for emergency preparedness" corresponds to "preparedness agencies" in the Ordinance (2022:524) on the preparedness of government agencies.

144.More information on MSB's website https://www.msb.se/sv/verktyg--tjanster/rakel/.

Appendices

Appendix A – References for further support and in-depth information

Standards and guidelines

In addition to the support in selecting and designing security measures provided by the SS-EN ISO/IEC 27001 and 27002[145] standards, additional standards and guidance can be used, some examples of which are provided below.

Standards

- **ISO/IEC 27000 series –** international standard for information security.
  - **SS-ISO/IEC 27004** Information technology – Security techniques – Information security management – measurement
  - **SS-ISO/IEC 27005** Information technology – Security techniques – Information security risk management
- **ISO/IEC 20000 series –** international standard for IT service management
- **Information Technology Infrastructure Library** (ITIL)
- **IEC 62443 series –** International Standard for Automation and Control Systems Cybersecurity (ICS/SCADA).
- **NIST SP 800-53 –** American standard providing guidance and a catalogue of information and cyber security features https://www.nist.gov/privacy-framework/nist-sp-800-53

Guidelines

- **MSB's methodological support for systematic information security work** https://www.informationssakerhet.se/metodstodet/
- **MSB, Guidance for increased security in industrial information and control systems** https://rib.msb.se/dok.aspx-?Tab=2&dokid=29984
- **MSB, Basic security in cyber-physical systems: Guidance** https://rib.msb.se/bib/Search/Document?id=29983
- **Swedish Security Service, Guidance on Security Protection – Information Security** https://sakerhetspolisen.se/download/18.3752daf918b4971127 12b/1698133722307/Informationssäkerhet_anpassad.pdf
- **Armed Forces Handbook** hsäk/ infosäk https://www.forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/handbocker/handbok-sak-infosak-andring-2.pdf

145.SS-EN ISO/IEC 27001:2017 & 2022 Information technology – Security techniques – Information security management systems – Requirements, and SS-EN ISO/IEC 27002:2017 & 2022 Information technology – Security techniques – Code of practice for information security controls.

- **CIS CSC Top-20 Security controls –** guidance with twenty basic information and IT security controls from the Center for Internet Security (formerly the SANS Institute). https://www.cisecurity.org/controls
- **OWASP SAAM Software Assurance Maturity Model (SAMM).** https://owaspsamm.org/model/
- **NSM Grunnprinsipper for IKT-sikkerhet 2.0 – vägledning för it-säkerhet.** https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/
- **BSI IT-Grundschutz –** German counterpart to MSB's methodological support for systematic information security work (available in English) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
- **ANSSI Recommendations to secure administration of IT Systems –** French guidance for system administration (available in English).
- **NCSC-UK Cyber Assessment Framework –** English-language guidance for the implementation of security measures in critical infrastructure.
- **MITRE ATT&CK –** support for the design of threat models regarding adversarial threats to IT environments.
- **NIST Cyber Security Framework** https://www.nist.gov/cyberframework

In-depth support for each chapter

The following is a list of in-depth references related to the different areas of the guidance. The organisation needs to make its own assessment regarding whether and how extensively the in-depth references are to be used in its own work. This list is not exhaustive. Other documents may be more relevant to the organisation's activities.

Chapter	References
Chapter 2	
2.1 Responsibility	MSB, *The role of management in information security, 2021* https://www.informationssakerhet.se/siteassets/metodstod-for-lis/ledningens-roll-inom-informa-tionssakerhet---ett-stod-for-dig-med-en-ledande-funktion.pdf MSB's methodological support for systematic information security work, *Design – Organisation* https://www.informationssakerhet.se/metodstodet/utforma/#organisation-anchor Finnish Transport and Communications Agency TRAFICOM, *Cybersecurity and Board Responsibility*, 2020 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_SWEdigi_auk280120.pdf ACSC, *Information security manual- guidelines for cybersecurity roles*, 2022 https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-roles

Chapter	References
2.2 External environmental monitoring	MSB's methodological support for systematic information security work, *Analyse – External environmental analysis* https://www.informationssakerhet.se/metodstodet/analysera/#omvärldsanalys ENISA, ENISA *Cybersecurity threat landscape methodology*, 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology See also regularly updated sources, e.g., the CERT-SE *weekly newsletter* or CISA *Alerts* https://www.cert.se/nyckelord/Veckobrev/ https://www.cisa.gov/uscert/ncas/alerts
2.3 Risk assessment	MSB's methodological support for systematic information security work, *Design – About the need for risk assessment* https://www.informationssakerhet.se/metodstodet/utforma/#om-behovet-av-risk-be-d%C3%B6mning Collaborating agencies in the National Cyber Security Centre, *Cyber Security in Sweden – Threats, Methods, Deficiencies and Dependencies*, 2022 https://www.ncsc.se/siteassets/publikationer/ncsc-rappor-1-cybersakerhet-i-sverige-2022-hot-metoder-brister-och-beroenden.pdf National institute of standards and technology, NIST SP 800-30 – *Guide for conducting risk assessment*. See in particular chapter 3. SS-ISO 31000:2018 *Risk management – Guidelines* SS-ISO/IEC 27005:2018 *Information technology – Security techniques – Information security risk management*
2.4 Documentation of the IT environment	MSB's methodological support for systematic information security work, *Governance documents* https://www.informationssakerhet.se/metodstodet/utforma/#styrdokument-anchor NSM, *Grunnprinsipper for IKT-sikkerhet 2.0 – Kartlegg styringsstrukturer, leveranser og understøttende systemer* https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/identifisere-og-kartlegge/kartlegg-styringsstrukturer-leveranser-og-understottende-systemer/ ASCS, Information security Manual – *Guidelines for security documentation*, 2022 https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-security-documentation
Chapter 3	
3.1 Requirements	MSB, *Procurement of information security: A guide*, 2018 https://www.msb.se/RibData/Filer/pdf/28742.pdf SS-ISO/IEC 27036-1:2014 Information technology – Security techniques – Information security for supplier relationships ENISA's *Indispensable baseline security requirements for the procurement of secure ICT products and services*, 2017 https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services CSEC - Swedish Certification Body for IT Security https://www.fmv.se/verksamhet/ovrig-verksamhet/csec/
3.2 Checks	Swedish Security Service, *Guidance on protective security - information security*, 2020. Sections 7.7, on measures to be taken prior to deployment, and 7.6, on functionality testing and security audits https://sakerhetspolisen.se/download/18.310a187117da376c6601d43/1636446528314/Vagled-ning-Informationssakerhet_2020.pdf
3.3 Development, test and training environments	NCSC-UK, *Secure development and deployment guideline* https://www.ncsc.gov.uk/collection/developers-collection/principles/secure-your-development-environment NCSC-UK, *Secure design and development* https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=secure%20design%20and%20development&sort=date%2Bdesc

Chapter	References
Chapter 4	
4.1 Network segregation and filtering (Network Domains)	Collaborating agencies in the National Cyber Security Centre, *Cyber Security in Sweden - Recommended Security Measures (*2020) Chapter 8. Network segmentation and filtering traffic between networks See the Swedish Security Service's *Guidance on Protective Security – Information Security*, 2020. Section 7.4 regarding Architecture NSA, *Segment networks and deploy application-aware defenses* https://media.defense.gov/2019/Sep/09/2002180325/-1/-1/0/Segment%20Networks%20and%20Deploy%20Application%20Aware%20Defenses%20-%20Copy.pdf MSB and Defense Research Agency on *Remote Access Technologies for Industrial Information and Control Systems*, 2019 https://www.msb.se/contentassets/6840a9f762184a869b39954f670c8e77/ncs3---fjar-ranslutning.pdf
4.2 Access and digital identities	Swedish Security Service, *Guidance on protective security – information security*, 2020. Section 7.4.5 on identity and access management NIST 800-63 Digital Identity Guidelines, section 5.1.1.2 “Memorized Secret Verifiers” NCSC-UK, *Introduction to identity and access management* https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management ANSSI, *Recommendations to secure administration of IT systems*, 2015, Section 7. Identification, authentication and administration privileges https://www.ssi.gouv.fr/guide/secure-admin-is/ NSA, *Defend privileges and accounts*, 2019 https://media.defense.gov/2019/Sep/09/2002180330/-1/-1/0/Defend%20Privileges%20and%20Accounts%20-%20Copy.pdf
4.3 Authentication	ENISA, *Authentication methods* https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods NSCS-UK regarding the need for a policy on authentication solutions https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/enterprise-authentication-policy
4.4 Encryption	More detailed descriptions of DNSSEC services are described in the *Recommendations for the implementation of DNSSEC in municipalities and similar activities,* published 2014 by the Swedish Internet Foundation at https://internetstiftelsen.se/domaner/doman-namnsbranschen/teknik/dnssec/ (retrieved 25/08/2020). A publicly available tool to check domain and DNS server configuration and status is ZoneMaster (formerly DNSCheck), provided by the Internet Foundation, at https://zonemaster.iis.se/. Periodically check that the registered domains are correctly set up for DNSSEC, e.g., by using ZoneMaster from the Internet Foundation, https://zonemaster.iis.se/ NSM, *NSM cryptographic recommendations* https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/nsm-cryptographic-recommendations/ Informationssäkerhet.se om kryptolösningar https://www.informationssakerhet.se/kryptolosningar/
4.5 Security configuration	Collaborating agencies in the National Cyber Security Centre, Cyber Security in Sweden – Recommended Security Measures, 2020. See sections 4, 6 and 7 See also MITRE ATT&CK's examples of security configurations https://attack.mitre.org/mitigations/M0942/

Chapter	References
4.6 Security tests and audits	MSB's methodological support for systematic information security work, *Monitor and improve* https://www.informationssakerhet.se/metodstodet/folja-upp-och-forbattra/#m%C3%A5luppfyllelse-av-informationss%C3%A4kerhetsm%C3%A5l-och-strategisk-inriktning ENISA, *Proactive detection – good practices gap analysis recommendations*, 2020. Chapter 2 Good practices and gap analysis https://www.enisa.europa.eu/publications/proactive-detection-good-practices-gap-analysis-recommendations Also see NSCS-UK information on *Vulnerability scanning and Penetration testing* https://www.ncsc.gov.uk/guidance/vulnerability-scanning-tools-and-services https://www.ncsc.gov.uk/guidance/penetration-testing
4.7 Change management, upgrading and updating	Swedish Security Service, *Guidance on protective security – information security*, 2020. Section 8.3-4 on Change Management and Updating ITIL, *Change management* https://www.itsm-docs.com/blogs/news/itil-change-management-process NCSC-UK, *Keeping devices and software up to date* https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date
4.8 Accurate and traceable time	PTS, *Accurate traceable time and rate* https://pts.se/sv/bransch/internet/Om-robust-kommunikation/robusthetshojande-atgarder/korrekt-och-sparbar-tid-och-takt/ Netnod, *Swedish distributed time service* https://www.netnod.se/swedish-distributed-time-service
4.9 Backup	Collaborating agencies in the National Cyber Security Centre, Cyber Security in Sweden - Recommended Security Measures, 2020. Ch. 3 Make backups and test if the information can be read back. NSM, *Grunnprinsipper for IKT-sikkerhet 2.0 – Etabler evne til gjenoppretting av data* https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-opprettholde/etabler-evne-til-gjenoppretting-av-data/ ACSC, *Backups* https://www.cyber.gov.au/backups
4.10 Security logging	NCSC-UK, *Logging and protective monitoring* https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/logging-and-protective-monitoring TRAFICOM, *How to collect and use log data* https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-samlar-du-och-anvander-loggdata
4.11 Surveillance	MSB's methodological support for systematic information security work, *Monitor and improve - surveil and measure* https://www.informationssakerhet.se/metodstodet/folja-upp-och-forbattra/#%C3%B6verva- ka-och-m%C3%A4ta ENISA, *Proactive detection – measures and information sources*, 2020 https://www.enisa.europa.eu/publications/proactive-detection-measures-and-information-sources Informationssakerhet.se, Skyddspaket ICS/SCADA https://www.informationssakerhet.se/stod--vagledning/saker-it-infrastruktur/skyddspaket-icss-cada/
4.12 Protection against malware	ENISA, *Malware* https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware NCSC-UK *mitigating malware and ransomware* https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Chapter	References
4.13 Protection of equipment	MSB, *Guidance for Physical Information Security in Enclosed data storage facilities*, 2013 (pub.no: MSB629) https://www.msb.se/sv/publikationer/vagledning-for-fysisk-informationssakerhet-i-it-utrymmen/ The Armed Forces handbook *Hsäk Physical Security*, published in 2015, includes a description of how IT equipment can be protected https://www.forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/handbocker/handbok-sakerhetstjanst-fysisk-sakerhet.pdf Swedish Security Service, *Guidance on protective security - information security*, 2020. Section 8.6 on Decommissioning
4.14 Redundancy and recovery	NSM, *Håndbok i kartleggning og vurdering av avhengigheter* https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/handbok-i-kartlegging-og-vurdering-av-avhengigheter/prosess-og-metode/steg-2-vurdering-av-avhengigheter/vurdering-av-beskyttelse-og-resiliens/ FSPOS, *IT Business Continuity Framework - Description of content and application*, 2020 https://www.fspos.se/siteassets/fspos/rapporter/2020/regelverk-kontinuitet-it-verksamhet.pdf MSB's methodological support for systematic information security work, *Design - Business continuity management for information assets* https://www.informationssakerhet.se/metodstodet/utforma/#kontinuitetshantering-f%C3%B6r-informationstillg%C3%A5ngar-anchor FOI on the National Centre for Security in Control Systems for Critical Infrastructure (NCS3) https://www.foi.se/forskning/informationssakerhet/ncs3.html
Chapter 5	
5.1 Increased security requirements	The Swedish Security Service's *Guidance on Protective Security – Information Security, 2020 security measures required for increased security requirements* MSB, *Secure communications* https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/sakra-kommunikationer/

Appendix B – Connecting chapters of the guidance, regulatory requirements and sections of SS-EN ISO/IEC 27002

Chapter of the guidance	Regulatory requirements MSBFS 2020:7	Sections of SS-EN ISO/IEC 27002:2017	Sections of SS-EN ISO/IEC 27002:2022
2 .1 Responsibility	Ch. 2 Section 1	6.1.1 Information security roles and responsibilities 8.1.2 Ownership of assets 18.2.3 Technical compliance audits	5.2 Information security roles and responsibilities 5.10 Acceptable use of information and other associated assets 5.9 Inventory of information and other associated assets
2.2 External environmental monitoring	Ch. 2 Section 2	6.1.4 Contact with special interest groups 12.6.1 Management of technical vulnerabilities	5.5 Contact with authorities 5.6 Contact with special interest groups 5.7 Threat intelligence 8.8 Management of technical vulnerabilities
2.3 Risk assessment	Ch. 2 Section 3	6.1.1 Information security roles and responsibilities	5.7 Threat intelligence 5.13 Labelling of information 5.2 Information security roles and responsibilities 8.8 Management of technical vulnerabilities
2.4 Documentation of the IT environment	Ch. 2 Section 4	8.1.1 Inventory of assets 8.2.1 Classification of information	5.9 Inventory of information and other associated assets 5.12 Classification of information 5.13 Labelling of information 5.37 Documented operating procedures 8.8 Management of technical vulnerabilities

Chapter of the guidance	Regulatory requirements MSBFS 2020:7	Sections of SS-EN ISO/IEC 27002:2017	Sections of SS-EN ISO/IEC 27002:2022
3.1 Requirements	Ch. 3 Section 1	14.1.1 Analysis and specification of information security requirements	5.8 Information security in project management 5.19 Information security in supplier relationships 5.20 Addressing information security within supplier agreements 5.21 Managing information security in the ICT supply chain 5.22 Monitoring, review and change management of supplier services 5.23 Information security for use of cloud services 5.31 Legal, statutory, regulatory and contractual requirements 8.26 Application security requirements 8.28 Secure coding 8.30 Outsourced development
3.2 Checks	Ch. 3 Section 2	12.1.1 Documented operating procedures 12.6.1 Management of technical vulnerabilities 13.1.2 Security of network services 14.2.3 Technical audits of applications after changes to production environment 14.2.8 Security audits 15.1.1 Information security rules for supplier relationships 15.1.2 Security management in supplier agreements 15.1.3 Supply chain for information and communication technologies 18.2.3 Technical compliance audits	5.22 Monitoring, review and change management of supplier services 5.19 Information security in supplier relationships 5.20 Addressing information security within supplier agreements 5.21 Managing information security in the ICT supply chain 5.36 Compliance with policies, rules and standards for information security 5.37 Documented operating procedures 8.8 Management of technical vulnerabilities 8.21 Security of network services 8.32 Change management 8.29 Security testing in development and acceptance 8.33 Test information
3.3 Development, test and training environments	Ch. 3 Sections 3 & 4	12.1.4 Separation of development, test and operational environments 14.2.6 Secure development environment 14.2.7 Outsourced development	8.25 Secure development life cycle 8.27 Secure system architecture and engineering principles 8.28 Secure coding 8.30 Outsourced development 8.31 Separation of development, test and production environments
4.1 Network segregation and filtering	Chapter 4 Sections 1 & 2	13.1.3 Separation of networks 13.1.1 Network security measures	6.7 Remote working 8.20 Network security 8.22 Segregation of networks 8.23 Web filtering 8.31 Separation of development, test and production environments 5.14 Information transfer

Chapter of the guidance	Regulatory requirements MSBFS 2020:7	Sections of SS-EN ISO/IEC 27002:2017	Sections of SS-EN ISO/IEC 27002:2022
4.2 Access and digital identities	Chapter 4 Sections 3 & 4	6.1.2 Division of tasks 9.1.1 Access control rules 9.2.1 Registration and deregistration of users 9.2.2 Allocation of user access 9.2.5 User access rights audits 9.2.6 Removal or adjustment of access rights 9.4.1 Restricting access to information 9.2.3 Management of privileged access rights 9.4.4 Use of privileged utility programs	5.3 Segregation of duties 5.15 Access control 5.16 Identity management 5.18 Access rights 8.2 Privileged access rights 8.3 Information access restriction 8.4 Access to source code 8.18 Use of privileged utility programs
4.3 Authentication	Chapter 4 Sections 5 & 6	9.4.2 Secure login procedures 9.2.4 Management of users' confidential authentication information 9.3.1 Use of confidential authentication information 9.4.3 Password management system	5.17Authentication information 8.5 Secure authentication
4.4 Encryption	Chapter 4 Sections 7 & 9	10.1.1 Rules for the use of cryptographic security measures 10.1.2 Key management	8.24 Use of cryptography
4.5 Security configuration	Ch. 4 Section 10	12.1.1 Documented operating procedures 12.2.1 Security measures against malware 12.5.1 Installing software on operating systems 12.6.1 Management of technical vulnerabilities 12.6.2 Restrictions on installing software	5.37 Documented operating procedures 8.7 Protection against malware 8.8 Management of technical vulnerabilities 8.9 Configuration management 8.19 Installation of software on operational systems
4.6 Security testing and audits	Ch. 4 Section 11	12.6.1 Management of technical vulnerabilities 14.2.8 Security audits 16.1.3 Reporting of information security weaknesses	5.27 Learning from information security incidents 5.35 Independent review of information security 5.36 Compliance with policies, rules and standards for information security 6.8 Information security event reporting 8.8 Management of technical vulnerabilities 8.29 Security testing in development and acceptance 8.33 Test information 8.34 Protection of information systems during audit testing

Chapter of the guidance	Regulatory requirements MSBFS 2020:7	Sections of SS-EN ISO/IEC 27002:2017	Sections of SS-EN ISO/IEC 27002:2022
4.7 Change management, upgrading and updating	Ch. 4 Section 12	12.1.2 Change management 12.6.1 Management of technical vulnerabilities 14.2.4 Restrictions on changes to software packages	8.8 Management of technical vulnerabilities 8.32 Change management 8.19 Installation of software on operational systems
4.8 Accurate and traceable time	Ch. 4 Section 13	12.4.4 Synchronization of time	8.17 Clock synchronization
4.9 Backup	Chapter 4 Sections 14 & 15	12.3.1 Backups of information	5.33 Protection of records 8.13 Information backup
4.10 Security logging	Chapter 4 Sections 16 & 17	12.4.1 Logging of events 12.4.3 Administrator and operator logs 12.4.2 Protection of log information 16.1.1 Responsibilities and procedures (Information Security Incident Management and Improvements)	5.24 Information security incident management planning and preparation 5.28 Collection of evidence 8.15 Logging
4.11 Monitoring	Chapter 4 Sections 18 & 19	16.1.1 Responsibilities and procedures (Information Security Incident Management and Improvements) 16.1.5 Information security incident management	5.24 Information security incident management planning and preparation 5.26 5.28 Collection of evidence 8.12 Data leakage prevention 8.15 Logging 8.16 Monitoring activities
4.12 Protection against malware	Ch. 4 Section 20	12.2.1 Security measures against malware	8.7 Protection against malware
4.13 Protection of equipment	Ch. 4 Section 21	6.2.1 Rules for mobile devices 11.1.1 Physical security perimeters 11.1.2 Physical access restrictions 11.1.3 Securing offices, rooms and facilities 11.1.4 Protection against external and environmental threats 11.1.5 Working in secure areas 11.2.1 Siting and protection of equipment 11.2.6 Security of equipment and assets beyond the organisation's premises 11.2.7 Secure disposal or re-use of equipment	5.11 Return of assets 7.1 Physical security perimeters 7.2 Physical entry 7.3 Security offices, rooms and facilities 7.4 Physical security monitoring 7.5 Protecting against physical and environmental threats 7.6 Working in secure areas 7.8 Equipment siting and protection 7.9 Security of assets off-premises 7.10 Storage media 7.11 Supporting utilities 7.13 Equipment maintenance 7.14 Secure disposal or re-use of equipment 8.1 User endpoint devices 8.10 Information deletion

Chapter of the guidance	Regulatory requirements MSBFS 2020:7	Sections of SS-EN ISO/IEC 27002:2017	Sections of SS-EN ISO/IEC 27002:2022
4.14 Redundancy and recovery	Ch. 4 Section 22	17.2.1 Availability of information processing resources	5.29 Information security during disruption 8.14 Redundancy of information processing facilities 5.30 ICT readiness for business continuity
5.1 Increased security requirements	Chapter 5 Sections 1 & 2	See references for sections 4.3, 4.6, 4.11 and 4.14	5.31 Legal, statutory, regulatory and contractual requirements

Swedish Civil
Contingencies
Agency

651 81 Karlstad Telephone 0771-240 240 **www.msb.se/en/**
Publication no. MSB2207 – Revised November 2023 ISBN 978-91-7927-447-4