NORWEGIAN
NATIONAL SECURITY
AUTHORITY

NSM ICT
Security Principles

version 2.1

About the Norwegian National Security Authority (NSM)

NSM is a Norwegian directorate for national preventive security. Among the various tasks of NSM is the publication of security advice.

NSM ICT Security Principles and compliance with legal frameworks

The security principles are relevant for all types of organisations. By following these recommendations, organisations will achieve a good foundation for security in their ICT-systems, but the recommendations must be assessed and adapted for each organisation. *Note that various legal frameworks may have requirements that differ from these recommendations*. One example is the national "Security Act" ("Sikkerhetsloven"), which has more and stricter requirements than recommended in this document.

Other resources from NSM

Go to nsm.no/ict-sp for additional information in English on the security principles, including a spreadsheet containing the security measures. Other information in English can be found at nsm.no/en.

Most important changes from version 2.0 to version 2.1

- Links and references have been updated.
- Change in the definition list: "whitelisting" has been updated to "allowlisting".
- Principle 3.1: Added clarification of "known" vulnerability and threats.
- Measure 2.3.2: Added clarification on execution/installation.
- Measure 2.4.1: Added clarification of network ports.

Version history

Version	Date	Description
1.0	28 August 2017	Version 1.0 completed (in Norwegian only)
1.1	01 November 2018	Version 1.1 completed (in Norwegian only)
2.0	15 April 2020	Version 2.0 completed (in Norwegian only)
2.1	31 May 2024	Version 2.1 completed

About this English edition

The content is equivalent to the Norwegian version 2.1, with the exception that two illustrations are not included/translated. Also, links to resources in Norwegian are included in the English edition to indicate that these security principles are supported by other national resources. Linked resources in Norwegian are clearly marked as such.

CONTENTS

I. Introduction

NSM ICT Security Principles are a set of principles and measures designed to protect information systems against unauthorised access, damage and misuse. They are relevant to all organisations.

Digitalisation creates new opportunities but can also increase risk

Society is constantly changing. Many organisations are adopting new technologies and digitalising all or some of their processes. Change is happening ever more quickly, and ICT portfolios now comprise both new and old systems which are based on different technologies yet have to work together. More and more organisations are also using cloud services often run by different providers.

Increased use of digital services can simplify operations, improve mobility, increase productivity and ensure more automated security for an organisation. However, digitalisation can also lead to increased complexity, more assets being exposed on public, unsecured networks and long digital value chains which are difficult to monitor.

Many organisations do not know where to begin

How can organisations ensure that their knowledge is up to date and their technology relevant when information systems are developing this rapidly with a seemingly infinite number of potential solutions? What are the most critical areas that should be addressed, and where should the organisation even begin? How do we ensure that we start in the right place with the most basic steps and adopt fundamental principles to secure, maintain, monitor and improve our ICT systems?

The amount of information about how an organisation should make their information systems secure can be overwhelming. Organisations also need to observe various legislation, industry standards and internal and external delivery requirements. All this information can quickly turn into a jungle of opposing options and criteria which distract decision-makers from making the right decisions.

NSM ICT Security Principles will aid the digitalisation process

NSM ICT Security Principles are a set of recommendations on how organisations can make their information systems more secure. Which recommendations are relevant will vary from organisation to organisation. Most of the measures will be relevant to large organisations, while smaller organisations to a greater degree will have to prioritise. The principles can provide a starting point for industry standards and help supplement ICT recommendations in sectoral regulations. They can be adopted by organisations and provide guidance when procuring ICT services.

NSM ICT Security Principles are intended to be dynamic and current and will be updated when needed. We would like to thank everyone who has contributed to the development of this document.

Who is the target group?

Which organisations are the principles relevant for?
NSM ICT Security Principles have been developed in partnership with organisations in charge of critical civic functions and/or critical infrastructure. Although these organisations constitute the main target group, the principles are relevant to all public and private organisations. The principles are relevant for organisations managing their own information systems and for organisations outsourcing one or more ICT services to a third party.

What roles in the organisation are the principles aimed at?
In most organisations the business and IT management level will often serve as a link between executive management level and implementation/operation level. The business and IT management are the main target group within the organisation for NSM ICT Security Principles. They include system owners, security managers, business units and process owners. Below is an explanation of the different levels and how the principles can be used to improve the security information flow.

The **executive management** focuses on organisational risk. They determine what the business priorities are, communicate the organisation's risk tolerances and allocate funds from the budget to business and IT level. It is crucial that the executive management take ownership of and get involved in the security processes at the organisation. The different categories and principles can be used to govern this process.

Guidelines for information security and budget allocations are determined at **business and IT management level** in line with the executive management's priorities. Business and process owners are best familiar with the organisation's deliverables and should support in determining criteria and guidelines. Each of the security principles includes measures describing **what** an organisation should do to protect its information systems and assets.

The business and IT management must also communicate the latest risk status to the executive management and explain why the measures are necessary. The principles will help in this regard because they explain **why** each principle is important.

The security measures are established and maintained at **implementation and operations level** in line with the management's guidelines and choices. This group can use the measures described in the principles to determine what can and should be implemented. Status and changes for deployment should be reported to the management.

What are NSM ICT Security Principles?

NSM ICT Security Principles are a collection of principles and measures designed to protect information systems against unauthorised access, damage and misuse. The collection is based on NSMs experience and feedback from various organisations in the public and private sectors. By implementing the recommended measures, organisations will have a robust defence against cyberthreats.

The principles focus on technological and organisational measures. Measures concerning physical security and the human perspective are generally not covered. The measures apply to both unintentional and intentional acts, although the main focus is on intentional acts.

The principles are not a replacement for a robust security management system. Key factors for succeeding with their implementation are management involvement, adequate ICT security expertise and established management and reporting lines.

Selection of security measures is decided by the organisation's risk management process. If an organisation fails to implement a recommended security measure, it may face an increased risk which it needs to mitigate. That risk must then be assessed against the organisation's risk tolerances as well as legislation, industry standards and contracts. If the risk is found to be unacceptable, the organisation must consider compensatory measures.

The security principles are grouped into four categories

1. Identify – acquire and maintain an understanding of the organisation, including its management structures, management priorities, deliverables, ICT systems and users. This will ensure efficient implementation of the principles of the three other categories. The aim is to understand the organisation's deliverables and services, determine which technological resources need to be protected, and identify roles and users at the organisation. This will allow the organisation to focus and prioritise the security measures in line with business needs and risk management strategy. The category also focuses on establishing processes to maintain this knowledge over time.

2. Protect and maintain – ensure appropriate protection of the ICT system and maintain security state over time and during changes. This category contains principles on establishing a secure state for the ICT system in order to withstand or limit damage from a cyberattack. This includes how the ICT system is planned, procured, built, configured and maintained.

3. Detect – detect and remove known vulnerabilities and threats, and establish security monitoring. The principles in this category focus on detecting and removing known vulnerabilities and threats by performing vulnerability assessments and monitoring the ICT system. The category also addresses how to detect irregularities in the desired, secure state by analysing data from the security monitoring.

4. Respond and recover – respond to security incidents effectively. The aim of these principles is to establish activities to respond to incidents. This means preparing for, assessing, controlling and responding to incidents, returning to a desired state, and improving security based on the experiences gained from the incident response.

Structure of the principles

Every principle is a continuous activity which must be assessed for the entire duration of the information system's life time, from planning and deployment to disposal. Each principle has the following structure:

- The principle (heading) – a recommended principle that the organisation ought to adopt.

- Aim of the principle – describes what is achieved by implementing the principle.
- Why is this important? – describes why the principle is important and potential consequences of not implementing it.
- Recommended measures – describes security measures the organisation should take in order to comply with the principle.
- Supplementary information – describes information which is "nice to know" about the principle along with links where one can find additional information.

Other relevant advice and recommendations

There are several other relevant governance frameworks, action frameworks and technical guidelines which can be used in conjunction with the security principles.

Examples of relevant governance frameworks and guidelines:

- NSM's security governance guidance – related to the Security Act
- The Norwegian Digitalisation Agency (Digdir) - Internal security revision guidance
- ISO/IEC 27001 – International standard describing management systems for information security.
- ITIL – Information Technology Infrastructure Library – framework for quality-assuring deliverables, operations and support in the IT sector.

Examples of frameworks with security measures:

- ISO/IEC 27002
- CIS Critical Security Controls (CIS Controls)
- UK NCSC – Cyber Essentials and Cyber Assessment Framework
- NIST Cyber Security Framework (NIST CSF)
- NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations
- Australian Government Information Security Manual (ISM).

Definitions

Readers should be familiar with the following terms used in the NSM ICT security principles:

- **Device** – Could be a client, a server, a sensor (e.g. an IoT device) or network equipment. Devices can be physical objects or virtual objects. Subcategories of devices mentioned in this text include:

  - **Managed device** – Device controlled and operated by the organisation. In the case of clients, the user should not be able to alter the security configuration.
  - **Unmanaged device** – Device not controlled by the organisation. These can be personal devices (Bring Your Own Device – BYOD), IoT devices, devices distributed by the organisation or devices for visitors. Unmanaged devices should only be able to access a limited part of the organisation's infrastructure.
  - **Mobile device** – Any portable device (primarily clients) used either on or outside the organisation's premises.
  - **Client** – A computer used by an end user, e.g. a PC, Mac, mobile phone, tablet or virtual client (Virtual Desktop).
  - **Server** – A computer running applications or infrastructure services, typically from a data room or data centre. A server can be either physical or virtual. Most modern physical servers run a "hypervisor" – a platform for virtual servers and/or containers.
  - **Virtual device** – A virtual, non-physical device. This includes: virtual servers, virtual clients (desktops) and virtual network components (e.g. virtual switches).

- **Allow list/allowlisting** – A principle where one specifies which actions are permitted. Actions which are not explicitly permitted are automatically blocked. It is typically easier and less time-consuming to list which actions are permitted rather than which actions are not. The latter is known as a **deny list/denylisting.**
- **IaaS/PaaS/SaaS** – Terms describing different models for the organisation's own or outsourced virtualisation services. The most common models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).
- **ICT system** – Hardware, software and associated infrastructure.
- **Information system** – An ICT system, the data and services it provides, its use, and human interaction with the ICT system to support business processes.
- **Security incident** – An anomaly where there is a potential for loss of confidentiality, integrity and/or access to information or ICT services. A security incident can occur as a result of a cyberattack, technical failure or human error.
- **Secure state** – The desired security level adopted by the organisation. Category 2 – Protect and maintain describes a possible structure for a secure state.
- **Vulnerabilities** – A vulnerability in an ICT system as described in these principles can be anything that can be exploited by an attacker. It can be either organisational or technical. Examples include failure to segment a network, insufficient control over which software users are able to run, inadequate access control and failure to perform security updates on devices. The sum of all the vulnerabilities is often described as the potential "attack surface". Human and physical vulnerabilities must also be addressed but are generally not covered by these ICT security principles.

Outsourcing and cloud services

Public and private organisations see the use of ICT as an increasingly important part of their operations and as a way of achieving their strategies. At the same time, we see an increase of costs, use of resources and dependency on ICT deliverables. As a result, there is growing focus on how ICT can be improved and ICT services rendered more efficiently. For many, the conclusion is to outsource all or parts of their service portfolio to one or more providers. Outsourcing in this context means that the organisation decides to procure services from an external provider instead of providing them in-house. One example of outsourcing is cloud-based services. Adequate security measures are crucial, irrespective of the operator of the service. NSM ICT Security Principles are just as relevant for outsourced ICT services as they are for in-house ICT services. The difference is whether one is specifying security requirements to an internal or an external service provider.

Before making a strategic decision on outsourcing, the organisation should consider whether it is capable of managing all phases of an outsourcing process. To ensure ICT security when outsourcing, we recommend:

1) Obtain an overview and understanding of the entire service life cycle
2) Ensuring adequate procurement skills
3) Conducting adequate risk assessments in order to make the right decisions
4) Defining adequate and correct requirements for the ICT service and for the provider
5) Making the right decisions at the right level

Anything that is not possible to resolve before outsourcing can be impossible to rectify once a contract is signed.

See principle 2.1 – “Include security during procurement and development processes” and read NSM’s reports (see www.nsm.no/sky, in Norwegian) on outsourcing for more information about outsourcing and cloud services.

1. Identify

1.1. Identify management structures, deliverables and supporting systems

Aim of the principle: The organisation identifies structures and processes for security and risk management which are vital for securing the ICT systems. The organisation should identify deliverables, information systems and supporting functions. These should be compared to the established risk tolerances in order to establish and adjust security measures.

Why is this important?

A lack of management structures and processes for risk assessment can lead to insufficient status information which will reduce the management's ability to prioritise and manage the organisation's security activities.

The organisation's information systems should support the activities and deliverables so that the agreed quality is achieved. The organisation must identify, prioritise and protect its most important deliverables. Insufficient oversight may lead to some lesser important parts being well protected while vital parts are left exposed and vulnerable to attack. The availability, integrity and confidentiality of information systems and data must all be addressed by the organisation.

Recommended security measures: Identify management structures, deliverables and supporting systems

ID	Description
1.1.1	**Identify the organisation's strategy and priorities**, as well as regulations, industry standards and contracts which may have an impact on information system security.
1.1.2	**Identify the organisation's structures and processes for security management.** This would normally include **a)** management policies, **b)** management structure with well-defined responsibilities, **c)** processes for risk management (see 1.1.3), **d)** established risk tolerances (see 1.1.4), **e)** ensure sufficient resources and specialist skills to support the management. **f)** Establish structures and processes for security management if such do not exist. Ensure that they are tailored for the organisation and becomes an integrated part of the governance of the organisation. For further information see "Supplementary information".
1.1.3	**Identify the organisation's processes for ICT risk management.** This would normally include **a)** asset valuation, **b)** threat assessment, **c)** identifying existing security measures, **d)** risk identification, **e)** risk assessment, **f)** risk reporting, **g)** risk management, **h)** establishing or adjusting security measures to reduce risk, **i)** verifying that the security measures are working as intended.

	j) Establish processes for risk management if such do not exist. Ensure that the processes are tailored for the organisation and become an integrated part of the governance and security management of the organisation. See "Supplementary information" for further information.
1.1.4	**Identify the organisation's tolerances for ICT risk.** The management must determine the organisation's acceptable risk tolerances, included defining unacceptable risk. This must be communicated across the organisation. It is normal for organisations to determine risk tolerances based on consequences in the event of a loss of confidentiality, integrity and availability of information and information systems. See 4.1.1, 4.1.2 and "Supplementary information" for further information.
1.1.5	**Identify the organisation's deliverables, information systems and supporting ICT functions**. Identify **a)** ICT systems, data and services, including ownership, **b)** critical business roles and **c)** internal and external ICT dependencies. **d)** Group items a-c according to the organisation's risk tolerances (1.1.4) and use the results to establish a secure ICT architecture, see principle 2.2 – Establish a secure ICT architecture.
1.1.6	**Identify information processing and data flow.** Map the flow of information between work processes, users, devices and services and use the results to establish a secure ICT architecture, see principle 2.2 – Establish a secure ICT architecture.

Supplementary information

Tailor the security management to the organisation
Processes for security and risk management must be tailored to suit the organisation. Bigger organisations with a large workforce often have a comprehensive management structure with a number of defined processes at different levels, as well as a large number of people dedicated to this work. Smaller organisations will often have a simpler management structure and less extensive processes.

Choose the right method for risk assessment
There are a number of different methods for identifying and assessing risk. It is important that the organisation chooses a method that makes risk assessments manageable and allows one to identify, discuss and manage the most significant risks. Examples of different methods/frameworks include ISO/IEC 27005 [8], NIST SP 800-30 [9] and Octave Allegro [10].

Identify critical deliverables, information systems and functions
Identifying deliverables and services will help to identify and assess important value chains, information and dependencies. One can use this to protect and maintain the ICT system, e.g. in connection with security architecture, network segmentation, access control, secure configuration, logging and security monitoring.

Choose the right measures based on the risks identified
Risk assessments often result in a set of security measures that must be adjusted or established. It is important to identify existing security measures and assess their effectiveness against the assets they

are meant to protect. It is also important to see the different types of security measures in context when adjusting or establishing a security measure. The various standards and frameworks categorise security measures in different ways. NSM's ICT security principles largely focus on organisational and technological measures.

There are numerous examples of security measures being introduced to protect less important assets at an organisation. Failure to take a holistic approach when choosing which measures to implement means important assets are omitted or forgotten. In a worst-case scenario, the security measures can be counterproductive.

"The security measures have been correctly implemented, but have the right measures been implemented in the right place?"

Links

[1] (Norwegian) NSM: Veileder i sikkerhetsstyring: https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-sikkerhetsstyring/om-denne-veilederen/
[2] (Norwegian) NSM: Samleside for sky, tjenesteutsetting og sikkerhet: www.nsm.no/sky
[3] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[4] (Norwegian) Digitaliseringsdirektoratet: Internkontroll i praksis - Informasjonssikkerhet: https://www.digdir.no/informasjonssikkerhet/internkontroll-i-praksis-informasjonssikkerhet/2601
[5] (Norwegian) DSB: Risikostyring i digitale verdikjeder: https://www.dsb.no/rapporter-og-evalueringer/risikostyring-i-digitale-verdikjeder/
[6] NCSC UK: Cyber Assessment Framework – Managing security risk: https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-a-managing-security-risk
[7] ISO/IEC 27001- Information security management systems: https://www.iso.org/isoiec-27001-information-security.html
[8] ISO/IEC 27005 – Information security, cybersecurity and privacy protection: https://www.iso.org/standard/80585.html
[9] US NIST: SP 800-30 – Guide for Conducting Risk Assessments: https://www.nist.gov/privacy-framework/nist-sp-800-30
[10] CMU: Octave Allegro – Operationally Critical Threat, Asset, and Vulnerability Evaluation methodology: https://www.cert.org/resilience/products-services/octave/index.cfm

1.2. Identify devices and software

Aim of the principle: The organisation identifies devices and software on the organisation´s network and keeps a record of managed (and unmanaged) devices and associated configurations.

Why is this important?

It is important to register devices and software in order to obtain an overview of what exists in the organisation's network. The device register should identify organisation-controlled devices, legitimate devices with limited privileges (e.g. IoT devices) and unknown devices (e.g. employees' personal devices or malicious devices). Similarly, the software register should include all software used at the organisation, including those installed by the IT department as well as unauthorised software. It is important that the organisation creates an inventory of devices, software and associated vulnerabilities before an attacker gets a chance to do so.

Recommended measures: Identify devices and software

ID	Description
1.2.1	**Establish a process to identify devices and software in use at the organisation.** One should ideally use automated and centralised tools to detect and monitor devices and software and to determine which software is running on which devices. The inventory should also include ownership, older unsupported products (should be explicitly identified) as well as devices and software not connected to the organisation's network (e.g. USB devices). More details in 1.2.3 (devices) and 1.2.4 (software).
1.2.2	**Establish organisational guidelines for approved devices and software. a)** For example, the organisation should decide *i)* which types of devices and software the employees need, *ii)* which devices and software are not required for work purposes but still permitted, *iii)* which devices and software are unwanted, and *iv)* how to enforce it. **b)** Develop and maintain a list of devices and software approved for use at the organisation (including version number if appropriate). Assess needs against recommended measures in principle 2.1-2.3. **c)** Communicate the guidelines to staff. Describe security targets and permitted use of devices and software.
1.2.3	**Identify devices in use at the organisation** in accordance with the process described in 1.2.1. **a)** Identify information such as network addresses, hardware addresses, device names, department affiliation and whether the devices are managed by the organisation. Every device with an IP address on the network should be included on the list, including stationary and portable computers, servers, network equipment (routers, switches, firewalls etc.), printers, storage networks, IP phones, IoT devices etc. **b)** Create a list of all mobile devices and storage media in use outside the organisation's network which contain organisation data. **c)** Create a plan for managing devices not approved for use at the organisation (see 1.2.2). For access control, see 2.4.1.b. **d)** The organisation should also maintain a list of virtual devices (whether they are running at the organisation's premises or in a provider's cloud). Such devices are often temporary (e.g. stateless virtual desktops), so one can simplify this by keeping in the inventory only the templates that the virtual devices are based on. Keeping a list of virtual devices running in a provider's cloud is strictly only necessary when buying IaaS. The process described above can be simplified by being consistent in allowlisting all devices (and/or wired and wireless network connections) on the organisation's network. See also principle 2.4 – Protect the organisation's networks.
1.2.4	**Identify the software in use at the organisation** in accordance with the process described in 1.2.1. **a)** Identify firmware, operating system and applications (name, version number, manufacturer, installation date, whether it is still supported) installed on servers, clients and network equipment

	etc. **b)** Create a plan for how to approve software for use at the organisation (see 1.2.2). The process described above can be simplified by being consistent in allowlisting all applications (especially clients) (alternatively the use of app stores). Systematic use of application allowlists (or app stores) can make it easier to maintain an inventory of software in use. This is particularly relevant for end user clients.

Supplementary information

Attackers are continuously in search of new and unprotected systems, and vulnerable versions of software. They are also looking for devices (especially mobile devices) connecting to an organisation network and not having the necessary security updates and security configuration. Even devices not visible from the internet can be exploited by an attacker who has already gained internal access and is looking for vulnerable targets. As new technologies emerge, unmanaged devices are becoming increasingly common at organisations where staff are permitted to use their personal mobile devices. Many organisations have little or no control over the security status of these devices and very limited opportunity to conduct security monitoring. These devices can be, or have already been, compromised and used to attack internal resources.

Poorly managed or unmanaged devices are more likely to execute unwanted software or malware. A threat actor usually wants to acquire as many access rights and privileges in an ICT system as they can in order to access information and resources. One way of doing this is by hacking a vulnerable device and using it to start gathering information from the compromised system and from other devices and systems the device communicates with. Compromised devices can be used to move around the entire network as well as connected networks. One compromised device quickly ends up as many compromised devices. Organisations not fully in control of what software is running on devices in their network will be unaware if their systems are running vulnerable or harmful software.

In practice it can be difficult for an organisation to stay in full control of its entire ICT infrastructure. When choosing between security and the need to fulfil deliverables, an organisation will often be forced to accept devices with lower than desirable security levels. The key thing here is that organisations must be conscious of the strategies they choose and assess their functional needs against the risk profile. In some cases, the organisation will not be in control of a given type of equipment, e.g. when using external providers or by permitting use of unmanaged devices. The organisation must be conscious of the security threats this poses and consider compensatory measures such as reinforcing its detection capabilities, network segregation and reducing exposure of valuable information and ICT systems.

Links

[1] NCSC UK: Cyber Assessment Framework – A3. Asset management: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/a-3-asset-management
[2] CIS: CSC 1 – Inventory and Control of Enterprise Assets: https://www.cisecurity.org/controls/cis-controls-list/
[3] CIS: CSC 2 – Inventory and Control of Software Assets: https://www.cisecurity.org/controls/cis-controls-list/

1.3. Identify users and access requirements

Aim of the principle: The organisation knows which user groups, users and access requirements exist within the organisation and has defined responsibilities for ICT security.

Why is this important?

Once attackers have gained access to an information system, their first goal is often to increase their access rights. This can be done by taking control of various accounts and attempting to escalate their privileges. Many users may have access rights to systems and services they do not require, and have more privileges than they need in order to do their job. If users have more access rights than what they need, only one compromised user is needed for the entire system to become compromised. Access to the different parts of an information system should therefore be separated to reduce the damage caused by a compromised system or by a disloyal employee. The organisation must therefore stay in control of all its users, the accounts they have access to and what access rights are granted to each account.

Recommended measures: Identify users and access requirements

ID	Description
	This principle should be read in conjunction with principle 2.6 – Control identities and access rights
1.3.1	**Identify the users of the information systems, including**: **a)** user identity, **b)** work location(s), **c)** required access to ICT systems, services/applications, **d)** particular privilege requirements, see 1.3.2. See also principles 2.2 – Establish a secure ICT architecture and 2.6 – Control identities and access rights.
1.3.2	**Identify and define the different user categories** and define and grant access levels according to user needs. Examples of user categories could be: • Ordinary users only requiring office support. • Users with a particular need for extended privileges, e.g. developers. • Users running the organisation's systems. • Suppliers and consultants. • System users, e.g. system processes such as backup operations and similar running in the background.
1.3.3	**Identify roles and responsibilities linked especially to ICT security. a)** This concerns responsibilities internally at the organisation, e.g. security manager, IT manager, applications manager, platform manager etc. **b)** Clarify who should be notified in the event of an incident. See 4.1.1 and 4.1.3. **c)** Identify roles and duties maintained by external providers and partners.

Supplementary information

Intentional and unintentional security breaches

Unauthorised access to information or services can be obtained through both intentional and unintentional actions. This may, among other things, inflict financial losses on the organisation.

An *intentional action* could be an employee (often described as an "insider") exploiting their privileges to make a gain for themselves or others. An intentional action could also be carried out by an external attacker who e.g. manages to take control of a user account.

An *unintentional action* could be when an employee accidentally or negligently changes the security settings e.g. deletes information or opens an email containing malware.

Links

[1] (Norwegian) NSM: Temarapport – innsiderisiko
https://nsm.no/getfile.php/133153-1591706148/NSM/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf
[2] UK NSCS: Cyber Assessment Framework – B2.Identity and access control:
https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-b-protecting-against-cyber-attack
[3] CIS: CSC 14 – Controlled Access Based on the Need to Know:
https://www.cisecurity.org/controls/cis-controls-list

2. Protect and maintain

2.1. Include security during procurement and development processes

Aim of the principle: Security is an integral part of the processes for procurement and development, and the organisation minimises the risk of new ICT products and services introducing vulnerabilities to configurations and architecture.

Why is this important?

ICT security is important when procuring new ICT products and services, not just when procuring security products such as firewalls. Systems may become more vulnerable and less secure if an organisation purchases ICT products and services with poor security features or with security features which do not integrate well with the organisation's other security architecture and existing ICT products.

Vulnerabilities may go undetected if the organisation does not have adequate processes for development, testing, verification and deployment. It is also usually more cost-effective to include security in the beginning of a project than to add security later as an afterthought.

Recommended measures: Include security during procurement and development processes

ID	Description
	Procurement of ICT products
2.1.1	**Include security in the organisation's procurement process.** Determine ICT security specifications when procuring *any* type of ICT product or service, see principle 2.2 – Establish a secure ICT architecture. Include life cycle security from procurement to disposal.
2.1.2	**Procure modern and up-to-date hardware and software** to ensure that the latest security functions are built in. Ensure that the organisation **a)** only uses ICT products supported by and receiving security updates from the provider, **b)** only acquire ICT products which contain recent security functions and protocols, and **c)** phase out older ICT products. **d)** Where appropriate, one should ask the provider (who knows the ICT product best) to *i)* disclose any risks and vulnerabilities associated with the product, and *ii)* specify how the ICT product can be security-hardened and protected.
2.1.3	**Prefer ICT products which have been certified and evaluated by a trusted third party.** Common Criteria is one example of a certification regime. Common Criteria is an international standard for evaluating the security properties of ICT products and systems.
2.1.4	**Reduce the risk of targeted manipulation of ICT products in the supply chain. a)** Organisations should assess the risk of being exposed to such targeted attacks. **b)** Ask national

	resellers/importers to practise *discretion* and not divulge too much *customer information*, e.g. names of customers, how the product is used, where the product is being used. **c)** Protect the integrity of *physical products* (in consultation with national resellers/importers) at the earliest possible stage in the supplier chain. Products should be checked at every national stage of the chain (including by the customer before deployment) for broken seals and stored so that only a limited number of personnel have physical access. **d)** *Software products* should only be downloaded from the provider's official website (only via https). The organisation should keep all installation software in file folders that only those responsible for software installation have write access to. **e)** When performing maintenance on ICT products, physical provider access should be regulated and monitored.
	Development and testing of in-house software
2.1.5	**Use a secure software development method** in order to reduce vulnerabilities in the software. This includes: **a)** Adequate *planning*, including the organisation's needs, legal conditions, ICT security considerations and the need to train personnel. **b)** *Analysis* of user needs, including ICT security requirements. **c)** *Design* of the software according to requirements. **d)** *Development* of the software, including secure coding and testing (see 2.1.6 and 2.1.7). **e)** *Deployment* of the software. **f)** Secure *management* of the software, including *i)* planning for performing and distributing security updates, and *ii)* planning support for newer and more recent security functionality.
2.1.6	**Use separate environments for development, test and production** so that operational business processes are not affected by errors in development and testing. Also consider zone segmentation as described in measure 2.2.3. Use sensitive production data only in secure development and testing environments.
2.1.7	**Implement adequate testing throughout the development process.** This will allow one to correct any errors, vulnerabilities and omissions before deployment. **a)** The measure includes testing to verify that the security functions of the various affected ICT products are interacting seamlessly, cf. principle 2.2 – Establish a secure ICT architecture, as well as unit testing, integration testing, system testing, acceptance testing, pilot testing, Perform penetration tests (principle 3.4) and stress testing. **b)** Check that only permitted actions are allowed and perform spot checks to ensure that other actions are denied.
2.1.8	**Maintain the software code developed/used by the organisation**. **a)** Sustain a development process which includes methodical security assessments of the code. **b)** Be especially aware of code with particular security significance e.g. code for *i)* access control, *ii)* traffic encryption, *iii)* logging, *iv)* parsing user input, *v)* buffer overflow etc. See [4] and [11]. **c)** When using open-source code and commercial tool kits, the organisation should regularly check for new versions (ideally automatically). **d)** Security checks of the organisation's own code should also be automated where appropriate when using DevOps/DevSecOps. Particularly security-relevant code (cf. previous item) should be quality-assured.
	Outsourcing – including cloud services
2.1.9	**Maintain security responsibility during outsourcing**. This includes **a)** staying in control of the entire life cycle of the service(s) being outsourced, **b)** procurement expertise (e.g. management, administrative and IT architecture expertise) for the duration of the outsourcing, **c)** conducting adequate risk assessments which includes ICT throughout the entire life cycle, **d)** a requirement document for every stage of the outsourcing **e)** contracts on the outsourcing of ICT services, and amendments to such contracts, in accordance with the organisation's authority hierarchy. See also chapter – Outsourcing and cloud services and [1].

	It must be stressed that the organisation's *security obligations* do not end when one outsources. The organisation remains responsible regardless of who is performing the tasks.
2.1.10	**Review the service provider's security when outsourcing.** As a minimum, one should review if the provider: a) has a management system in place for information security along with any certifications in accordance with international standards, e.g. ISO/IEC 27001. b) provides details of the security architecture used to deliver the service. c) has development plans for future security functions for the service in response to technological advances and changes with threats over time. d) maintains a list of who is granted access to the organisation's information, where and how it will be processed and stored, and the extent of mechanisms to segregate it from other customers. e) has security functions that meet the organisation's needs. f) carries out security monitoring in order to detect security incidents that could impact the organisation. g) has procedures in place for managing incidents and for non-conformance and security reporting. h) has established incident management plans which works with the organisation's own plans. i) has procedures for approving subcontractors and their use of subcontractors. j) has specified which activities should be performed when terminating the contract, including returning/moving/deleting the organisation's information. Read more in NSM's reports on outsourcing, see [1].

Supplementary information

DevOps/DevSecOps are increasingly relevant terms in connection with *software development and software operations*, especially when it comes to services. In short, it involves making changes to code in a system in production relatively quickly without using traditional segmentation processes as described in 2.1.6. The word itself erases the traditional boundary between *Dev*elopment and *Op*eration*s*, including in an organisational perspective. If the organisation uses DevOps, one should take great care not to introduce vulnerabilities that could impact the business processes. As development and operations are becoming increasingly automated, the security procedures to identify software code with vulnerabilities should follow the same path. As a minimum, one should be more thorough when working on code with particular security implications.

Links

[1] (Norwegian) NSM: Samleside for Sky, tjenesteutsetting og sikkerhet: www.nsm.no/sky
[2] (Norwegian) NSM: Sikkerhetsfaglige anbefalinger ved tjenesteutsetting: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/introduksjon/
[3] (Norwegian) NSM: Nasjonal kontroll av IKT-tjenester: https://nsm.no/regelverk-og-hjelp/rapporter/nasjonal-kontroll-av-ikt-tjenester

[4] (Norwegian) Datatilsynet: Programvareutvikling med innebygd personvern: https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern
[5] (Norwegian) DFØ: Fagsider om offentlige anskaffelser: https://www.anskaffelser.no
[6] (Norwegian) Regjeringen: Veileder om ivaretakelse av sikkerhet i offentlige anskaffelser: https://www.regjeringen.no/no/dokumenter/veileder-om-ivaretakelse-av-sikkerhet-i-offentlige-anskaffelser/id2678434
[7] UK NCSC: Secure development and deployment guidance: https://www.ncsc.gov.uk/collection/developers-collection
[8] UK NCSC: Application development https://www.ncsc.gov.uk/collection/application-development
[9] CIS: CSC 16 - Application Software Security: https://www.cisecurity.org/controls/cis-controls-list
[10] Common Criteria: https://www.commoncriteriaportal.org/
[11] OWASP: Top Ten Web Application Security Risks https://owasp.org/www-project-top-ten

2.2. Establish a secure ICT architecture

Aim of the principle: The organisation has established a comprehensive security architecture which maintains the desired level of security using adequate and verifiable security functionality.

Why is this important?

An attacker will take the path of least resistance in order to gain entry and assume control of an information system. Poor planning prior to deployment, insufficient control during the deployment and inadequate maintenance after the deployment will leave many holes and potential points of entry for an attacker to exploit. An ICT system must be planned and built in a secure manner. Key elements are:

- An ICT system contains numerous security functions (see 2.2.1) and many different ICT products, often from different vendors. They must all work well and securely together, otherwise the organisation risks doubling up on work and making human errors during operation. This often creates additional vulnerabilities that an attacker can exploit. One classic error is to run a separate user database in an application instead of reusing the common user database shared by the entire ICT system. This could lead to any number of errors and forgotten accounts which can be misused by attackers.
- Operations and security configurations should be managed centrally and in the same way for every device of the same type. Otherwise, the organisation risks duplicating the workload, resulting in human errors and additional vulnerabilities.
- The ICT system should be divided into different sections depending on trust level. One should create such segmentation for networks and for logical components (e.g. in a domain

architecture). In the event of an attack or human error, failure to do so could have consequences for the entire organisation rather than just a limited part of it.

Recommended measures: Establish a secure ICT architecture

ID	Description
2.2.1	**Establish and maintain a comprehensive security architecture** to ensure a secure and defensible ICT system. The following *functionality in an ICT system* should be implemented, made secure and integrate together in a security perspective: a) Functionality for managing users and accounts b) Functionality for staying in control of devices (e.g. clients) c) Functionality for managing access to resources and services d) Functionality for controlling software execution and software installation (especially on clients) e) Operating systems f) Tools for operating and virtualising all or parts of the ICT architecture (on-prem and cloud) g) Network devices (switches, routers, access points) and firewalls h) Mechanisms for dealing with malware (antivirus) i) Cryptographic modules j) Digital certificates and public key infrastructure (PKI) k) Databases l) Tools for system monitoring m) Tools for managing security configurations n) Intrusion detection (IDS) and protection (IPS) systems o) Backup and restore p) Hardware and firmware All of the above-mentioned functions should be managed centrally and automatically as much as possible.
2.2.2	**Design the ICT system using ICT products which integrate well.** **a)** The products should be module-based (ability to activate only functionality that is useful to the organisation). **b)** Products should comply with industry standards with respect to security functions such as access control, logging, operation, code control, resource management and accessibility functions see 2.2.1. **c)** Products and security functionality (also from different vendors) should work well together from a security perspective. In particular, ICT products should reuse identities (of users and devices) taken from a shared database of the organisation's identities rather than implement their own product or application-specific identities.
2.2.3	**Segment the organisation's network in accordance with its risk profile**. Segment (divide) the network into zones with different needs for communication, exposure, function and roles. For example, one could consider creating separate zones for system administration, application servers, organisation-operated clients, industrial production (e.g. SCADA and industrial control systems), internet access, wireless networks, guest clients and externally available services (e.g. web servers). In data centres servers can be segmented into security groups such as a data plane (data going through the network), control plane (data going to network devices) and management plane (management data going to network devices). One could also consider creating a network architecture with even more granular zone segmentation, e.g. by department or by group of

	devices. Please note that one can create zones in many different ways: VLAN zones, virtualised networks, micro segmentation etc. Zones should be managed centrally, not locally on each switch. Use the chosen segmentation model to manage data flow, see principle 2.5 – Control data flow.
2.2.4	**Physically isolate the most critical subnets.** One should consider whether to physically isolate particularly sensitive subnets from the rest of the organisation's networks (air gap).
2.2.5	**Partition the domain architecture in accordance with the organisation's needs.** As a minimum, separate clients from the organisation's servers.
2.2.6	**Control access to services based on knowledge of users and devices.** One example is if a user logs in via an unmanaged device (the organisation trusts the user but does not control the device) and gains access to fewer services than if the user logs in via an organisation-managed device (the organisation knows both the user and the device).
2.2.7	**Establish a robust and resilient ICT architecture** which maintains access to critical functions and deliverables. **a)** Perform risk assessments for hardware failure, human operating error, cyberattack, internet access (incl. denial of service attacks), service provider availability, natural damage and geopolitical situation. **b)** Based on the risk assessments and level of criticality, one can make parts of the IT solution more robust. This could involve measures such as duplicating the internet connection, duplicating the data centre in an alternative location, duplicating domain controllers, partial outsourcing, robust (temporary) power supply, keeping critical spare parts etc.

Supplementary information

Links

[1] (Norwegian) NSM: Statens muligheter for IT-modernisering og digital transformasjon: https://nsm.no/hold-deg-oppdatert/meninger/statens-muligheter-for-it-modernisering-og-digital-transformasjon
[2] (Norwegian) NSM: Samleside for sky, tjenesteutsetting og sikkerhet: www.nsm.no/sky
[3] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[4] UK NCSC: Cyber security design principles: https://www.ncsc.gov.uk/collection/cyber-security-design-principles
[5] US GOV et. al.: Secure by design: https://www.cisa.gov/securebydesign
[6] UK NCSC: CAF B4 System Security: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/b-4-system-security
[7] ISO/IEC 27033-1 Network security – Part 1-6: https://www.iso.org/standard/63461.html

2.3. Maintain a secure configuration

Aim of the principle: The organisation configures hardware and software to meet its security needs. Procedures are in place for identifying, verifying, reporting and correcting security configurations on devices, software and services to prevent attackers from exploiting them.

Why is this important?

Most ICT products (software and hardware) are delivered with a standard configuration from the product developer. These standard configurations are normally made for easy installation and use, and not to provide a high level of security. *Open services and ports, standard accounts and passwords, older (and often vulnerable) protocols and pre-installed software can provide a number of opportunities for an attacker to gain unauthorised access. A system that has not been explicitly configured will most probably have vulnerabilities that an attacker can exploit.* Organisations must therefore harden their ICT products, e.g. by removing/disabling unnecessary functionality and replacing standard settings and passwords.

Recommended measures: Maintain a secure configuration

ID	Description
	Security configuration is important on both software, hardware devices and virtual devices.
2.3.1	**Establish centrally managed practices for security updates.** Install security updates as quickly as possible. **a)** Create a list of updates according to priority. The operating system and applications on employees' clients should be given priority. One should also update servers containing standard applications and operating systems, printer software and the devices running the organisation's network (switches, routers). **b)** Establish a procedure with clear lines of responsibility for *i)* how often updates should be carried out (one should be able to automate much of it), and *ii)* following up on any updates that cannot be performed or have to be postponed. **c)** Isolate servers and other equipment that are difficult to keep up to date, see 2.5.4. **d)** Organisations should automate and simplify the process of implementing new security updates.
2.3.2	**Configure clients so that only software known to the organisation is able to execute.** Keep in mind that software can execute even if not installed. **a)** On employees' clients one should explicitly allowlist all programmes that will be running on the device, ideally by having permitted source code signed by a trusted party who can also quality-assure the code against the operating system's application criteria. In practice, the code could be signed by the device provider's app store, alternatively also in the organisation's own app store. If required, the selection of applications in a supplier's app store could be restricted by allowlisting only required applications (e.g. with tools like Mobile Device Management – MDM). **b)** If an app store is not used, one should use application allowlisting. Use *file folder-based* allowlisting, as allowlisting individual applications is usually too time-consuming. **c)** If required, one can also refine the application allowlisting further by setting it to denylist any unwanted provider-signed programmes for defined user groups, e.g. one can explicitly block any built-in script engines (keep in mind that script engines such as powershell*.exe can provide an unnecessarily large attack surface if end users are permitted to execute them) one does not want end users to be able to run (only administrators). **d)** The software that accompanies some documents (e.g. macros) also provides a large attack surface. To reduce this attack surface, one should *i)* remove unwanted software from external documents and emails before they reach the users, e.g. in the firewall, *ii)* deactivate the option to run such software for users who do not need it, and *iii)* explicitly allowlist software in documents that the users actually need, e.g. by using digital signatures.
2.3.3	**Deactivate unnecessary functionality.** Consider deactivating built-in functions (in both operating systems and applications) on clients, servers and network equipment not needed by the

	organisation in order to reduce the attack surface. This could include *i)* older or unused protocols, *ii)* built-in support for personal cloud services, for example, *iii)* other built-in services that the organisation will not be using.
2.3.4	**Establish and maintain standard security configurations,** ideally one template for each type of device across the organisation. This applies to operating systems (client and server), firewalls, network equipment, applications and hardware. **a)** All management of security configurations should be centralised and standardised for each type of device. **b)** The configuration should be reviewed and updated regularly to eliminate the latest vulnerabilities and attack vectors. **c)** Changes to the configuration should follow the organisation's process for change management and be overseen by authorised staff. **d)** Security configurations must only be changed by authorised operating staff and not be able to be changed by end users on their clients.
2.3.5	**Verify that activated security configurations comply with the organisation's approved security configurations. a)** Regularly compare activated configurations on system components such as network equipment, firewalls, clients and servers with the approved/authorised configuration defined for each type of device across the organisation. **b)** Any unauthorised changes to the configuration should be investigated, reported and acted on. **c)** The approved/authorised configuration should be integrity-protected. Only IT and information security staff should have access to the configuration. **d)** Automate the verification process insofar as possible and run automated processes regularly, e.g. every night.
2.3.6	**Ensure that maintenance of all configurations, installations and operations are done securely. a)** Perform management operations in trusted channels. Consider *i)* installing trusted TLS certificates, ideally issued internally, in as many administrator interfaces as possible, see 2.7.1. and 2.7.2. And *ii)* avoid exposing administrator interfaces to the internet and to the servers/clients using the service. **b)** Use trusted and dedicated clients for management operations. **c)** Reduce interactive log-ins directly on servers and clients to a minimum when performing management operations. Interactive log-in increases the risk (attacks such as "pass the hash") and goes against the goal of automating and standardising configuration, and also against the goal of automated verification of the configuration.
2.3.7	**Change all standard passwords on ICT products before deployment**. This includes applications, operating systems, routers, firewalls, printers and access points. If the ICT products support it, one should use certificate-based authentication and reduce use of password-based authentication over the network.
2.3.8	**Do not deactivate exploit protection functions.** Newer operating systems come with activated exploit protection functions such as DEP, SEHOP and ASLR. They make it more difficult for an attacker to exploit vulnerabilities even when one has not updated the system. Create exceptions for older applications that do not work well with exploit protection so that one is not forced to deactivate the protection in its entirety. Then contact the application provider to remove the vulnerabilities.
2.3.9	**Synchronize time across devices and use trusted time sources.** Choose time sources that have a high degree of trust, and check that all device clocks use time of the desired quality.
2.3.10	**Reduce the risk posed by IoT devices**. **a)** Create a plan for deploying such devices to include security aspects with risk assessments, incl. an assessment of the cloud the devices connect to. **b)** Only purchase devices with built-in security functions, e.g. which *i)* provide security updates (2.3.1), *ii)* are able to change all standard passwords (2.3.7), *iii)* can be forced to only use networks the organisation has control over. **c)** Monitor traffic from the devices (see principle 3.2 – Establish security monitoring), **d)** isolate the devices in separate network zones (see principles 2.2 –

	Establish a secure ICT architecture and 2.5 – Control data flow) and **e)** consider their location with regard to unauthorised physical access to the devices. See [6] for more information.

Supplementary information

Hardening security configurations is an important aspect of information security. Failure to harden system components is often the reason why attackers are able to gain a foothold inside the organisation. *Operating systems on client computers and servers, databases, firewalls, cloud services, email clients and network equipment are all examples of ICT products that should be hardened.* These products should be installed and configured so that only the needed functions are activated. Unnecessary functionality should be removed or deactivated to reduce the attack surface, vulnerabilities and the work that goes into security updates.

ICT systems are constantly changing as new solutions are deployed. Examples include upgrades of devices and software, access to data and services based on new user needs, changes in the threat assessment, recently discovered vulnerabilities etc. Attackers will often exploit the weakening of the security configuration on network components that occurs over time. Attackers are looking for unchanged, vulnerable standard settings and logical holes in clients, servers, firewalls, routers and switches and will exploit them to circumvent or break through security barriers. It is therefore important to *update* and *verify* the configurations at regular intervals and to record, report and manage discrepancies in an effective manner.

Developing configuration templates with a high level of security functionality is a complex task. In order to make good decisions, one must consider, decide on and implement potentially thousands of settings in all parts of the ICT system. Creating a secure configuration requires technical expertise on the components being hardened. One should therefore rely on external assistance. The first step will often be to approach the supplier of the ICT product. The supplier can recommend best practice for more secure use of the product and maybe also provide a template of security settings for those needing more than just the default settings. The security authorities of some countries often also provide good recommendations on detailed hardening.

Links

[1] (Norwegian) NSM: Fem effektive tiltak mot dataangrep: nsm.no/5tiltak
[2] NSM: Security measures against ransomware and other malware attacks: nsm.no/ransomware
[3] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[4] UK NCSC: Configuration management: https://www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=configuration%20management
[5] CIS: CSC 4 – Secure Configuration of Enterprise Assets and Software: https://www.cisecurity.org/controls/cis-controls-list
[6] CIS: Controls Internet of Things Companion Guide: https://www.cisecurity.org/blog/new-release-cis-controls-internet-of-things-companion-guide/

[7] CIS: Benchmark:
https://www.cisecurity.org/cis-benchmarks/

2.4. Protect the organisation's networks

Aim of the principle: The organisation is in control of and protects its networks against internal and external threats.

Why is this important?

The organisation's own networks often extend beyond the office, which makes it difficult to determine their physical reach. An organisation may operate in multiple geographical locations, and services may have been outsourced to external providers.

The distinction between an organisation's internal and external networks is increasingly difficult to define. Staff often use mobile devices and need to be able to work from home and while they travel. Many organisations also use external services, which further complicates the situation.

Connecting the organisation's network to the internet or other networks outside the organisation's control exposes the systems to new attack surfaces.

Devices and data traffic can also be attacked from the inside: a compromised server or client (organisation-managed, hired or private device), a disloyal employee, a (compromised) provider with access to the network, insufficiently secure wireless networks or an absence of physical protection of ports/cables.

The organisation's networks should therefore be protected against both internal and external threats, and devices should not uncritically trust everything that is connected to the organisation's network. Access to the network should be made secure, and data flow on the network should be protected with encryption.

Recommended measures: Protect the organisation's networks

ID	Description
	Network security is important for both hardware-based devices and virtualised devices (e.g. cloud-based).
2.4.1	**Establish access control on as many network ports as possible.** Keep in mind that ports can be physical, wireless or virtual. **a)** Network traffic should only be permitted on organisation-approved ports (allowlisting principle). **b)** Only permit access from managed devices. **c)** Unmanaged devices should only be able to access a guest network or similar.
2.4.2	**Encrypt all wireless and wired connections. a)** Encrypt all wireless connections. Use up-to-date protocols such as WPA2/WPA3 in "enterprise mode". **b)** Encrypt all wired connections on the

	organisations own network, as a minimum those connections not physically controlled by the organisation.
2.4.3	**Identify physical access to switches and cables.** Organisations are often unaware of where their cables run and whether they can be physically accessed by unauthorised parties. If one has not authenticated and encrypted all connections, one should identify where the cabled networks are and determine whether unauthorised parties are able to physically access them (between buildings, between floors in buildings shared with other organisations, between different geographical locations, semi-public reception areas, etc.).
2.4.4	**Activate firewall on all clients and servers.** Firewalls are usually built into operating systems and can be used for traffic management and logging. Use firewalls to **a)** regulate incoming/outgoing traffic, **b)** log security-related events. One should integrate the log with the organisation's other solutions for security monitoring. **c)** Integrate client/server logging with centralised logging.

Supplementary information

Links

[1] NSM: Security measures against ransomware and other malware attacks: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/digital-utpressing/security-measures-against-ransomware-and-other-malware-attacks
[2] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[3] CIS: CSC 12 – Network Infrastructure Management: https://www.cisecurity.org/controls/cis-controls-list

2.5. Control data flow

Aim of the principle: The organisation is in control of the information flow between different parts of the system so that devices can communicate subject to defined rules. The organisation is also in control of the information flow in and out of the organisation.

Why is this important?

A cyberattack often begins with a takeover of a less important computer. An attacker will then normally want to move on to a different part of the network to increase their privileges. It is important to control data flow in the organisation's systems for a variety of reasons, including in order to:

- prevent compromise of a device or zone to spread further in the network. One can limit the damage if one maintains good control of the data flow.
- force data traffic to go through the organisation's security measures.
- isolate devices which are especially critical, vulnerable or exposed.

Recommended measures: Control data flow

ID	Description
	Controlled data flow is important irrespective of how physical or virtualised (e.g. cloud-based) the infrastructure is.
2.5.1	**Control data flow between network zones. a)** Use the segmentation in principle 2.2 – Establish a secure ICT architecture to filter legitimate (allowlisted) network traffic between zones and to the internet. The filtering can be based on criteria such as IP address, zone identifier, protocol, application, user etc. **b)** The rules (incl. changes) for the traffic between the zones should be documented and justified. **c)** Check regularly that the actual configuration of the data flow is in line with the desired data flow.
2.5.2	**Restrict access to internal services from external locations. a)** Allow only organisation-managed devices to access critical internal services. **b)** Access to internal services from unmanaged and personal devices should only be permitted following a criticality assessment of the service. For instance, one may need to be able to access email and time sheets. If so, one should consider measures to reduce risk, e.g. by offering less functionality, shorter search history, an additional layer of authentication etc.
2.5.3	**Block all direct traffic between clients.** Applications requiring peer-to-peer should instead use a server service. Alternatively, reduce direct traffic between clients to an absolute minimum based on what is needed for work purposes.
2.5.4	**Isolate vulnerable and low-trust equipment**, e.g.: **a)** Outdated applications and old servers with unsupported operating systems should be isolated (filtering criteria as described in 2.5.1.a and subject to strict access control) so that only one well secured server/proxy has direct access. **b)** Printers with poor security configuration and a lack of security updates.
2.5.5	**Control the data flow of especially exposed services. a)** Exposed services such as web and email with external content for users should be subject to strict controls. **b)** There should be no direct data flow between such exposed services and the organisation's most critical services.
2.5.6	**Protect particularly critical services with their own data flow. a)** Consider which services are particularly critical and should have their own rules for data flow. Backup services are one example. **b)** Consider validating critical services on the application layer, e.g. with an application firewall.
2.5.7	**Maintain control of data flow between the organisation and its partners / service providers.** An attack can hit the organisation via the systems of a partner or service provider. Traffic to and from these systems should be directed only to the relevant parts of the organisation's system.
2.5.8	**Direct all data flow (not just internal services) to and from managed mobile clients via the organisation's network** and not directly to the internet. Managed mobile clients should always (regardless of where they are) be subject to the security functions in the organisation's systems, in order to prevent and detect data leaks from compromised clients.

Supplementary information

How to control data flow. One way of controlling data flow is to use zone segmentation as described in principle 2.2 – Establish a secure ICT architecture. The *tools* used to control data flow could be switches, routers, firewalls (including host firewalls), domain partitions, proxies, DMZs and network-

based detection (IDS) and protection (IPS) systems. Organisations requiring a high level of security should consider using multiple tools to ensure defence in depth.

Dataflow much be efficient. Otherwise, the organisation risks that end users find their own and potential unsafe workarounds, e.g. memory sticks or private cloud storage.

2.6. Control identities and access rights

Aim of the principle: The organisation is in control of identities and accounts in its information systems and manages access to resources effectively and in accordance with guidelines.

Why is this important?

Attackers will often attempt to take control of a legitimate user in an information system. Their next goal is usually to increase their access rights and privilege levels to exploit the user account, go deeper into the system and access more resources.

Employees being granted more privileges than they need is a problem in many organisations. Often employees are permitted to write to and delete any file or file folder and even to execute all installed software, whether they need to or not. This is usually unnecessary but very useful for an attacker.

If all users have access to “everything”, it is possible for one compromised user to compromise the entire ICT system. Access to the different parts of an information system should therefore be separated to reduce the damage caused by an external attack or by a disloyal or careless employee. The organisation needs to stay in control of its users, i.e. the accounts and access rights associated with them, and the privileges assigned to the users.

Inadequate control of unused accounts is a recurring problem. There are numerous examples of accounts belonging to suppliers and past employees being misused by attackers or disloyal employees.

Recommended measures: Control identities and access rights

ID	Description
	Staying in control of identities and access rights is important regardless of how virtualised (e.g. cloud-based) the chosen infrastructure is. *These measures should be seen in the context of the measures in principle 1.3* – Identify users and access requirements.
2.6.1	**Create guidelines for access control. a)** The guidelines should cover as many of the organisation ’s resources as possible: users, clients, shared folders, server applications, servers, network devices, security devices and databases. **b)** The guidelines should follow the principle of least privilege: do not give end users, service accounts, developers or system managers any more privileges than

	necessary. Not everyone needs access to everything. And if someone does need access, it is often sufficient to give them read privileges. Not everyone needs to be able to write, delete and execute everything. **c)** It should be possible to trace every account to the responsible user (including non-personalised accounts without personal names). **d)** All accounts, access rights and privileges should be traced to a responsible role and the individual who approved it. **e)** Accounts, access rights and privileges should be revised regularly. This is especially critical for accounts, access rights and privileges for system management and special users. **f)** Reuse identities whenever one can across systems, sub-systems and applications (ideally with single sign-on). **g)** Remind users that it is their responsibility to keep passwords personal and secret and to never share them with anyone, including close colleagues or superiors. Users should also screen-lock their clients when leaving them.
2.6.2	**Establish a formal process for administration of accounts, access rights and privileges. a)** The process should cover **i)** *accounts* for users, devices and system processes, **ii)** *access rights* to systems and applications, **iii)** *privileges* in relation to operating systems (e.g. admin privileges) and the organisation's shared user database. **b)** The process should include the entire life cycle and cover creation, maintenance and deactivation. Deactivate rather than delete accounts and access rights in order that there is an audit trail in accordance with prevailing laws and regulations. **c)** The guidelines on access control (2.6.1) and the process for administering accounts, access rights and privileges (2.6.2.a) should be documented and communicated across the organisation.
2.6.3	**Use a centralised tool to manage accounts, access rights and privileges. a)** Ideally, one should manage accounts, access rights and privileges for as many of the organisation's resources as possible (cf. 2.6.2.a) using just a *single* tool for the entire organisation. **b)** Use the tool to keep track of all accounts, access rights and privileges. The tool should be able to perform as many of the tasks described in 2.6.1 as possible. **c)** When creating individual accounts (e.g. for contractors), one should set preliminary dates for deactivation. **d)** Deactivate or delete accounts that have not been used for a while (possibly with the exception of supplier maintenance accounts, for example). **e)** Use a centralised tool to check password quality against the organisation's security requirements. As a minimum, avoid using common words and names in Norwegian and English as well as years and seasons. See also [1].
2.6.4	**Minimise privileges for end users and special users. a)** Do not assign administrator privileges to end users. **b)** Manage special users (e.g. developers) who may exceptionally need extended system privileges, including administrative privileges. Each special user should have two separate accounts: one for ordinary office use such as email and internet searches, and one for tasks requiring elevated privileges. There should be adequate security barriers between these two accounts and, as an absolute minimum, they must not have the same password.
2.6.5	**Minimise privileges for management accounts. a)** Create different accounts for different management operations (even though it may be the same person carrying out the operations in practice), so that if one account is compromised, it will still not grant privileges to the entire system. I.e. different management accounts for backup, user administration, managing clients, managing servers etc. **b)** Limit the use of accounts with domain admin privileges to a minimum of the organisation's management operations. Accounts with domain admin privileges should never be used interactively on clients and servers (mitigates the consequences of "pass the hash" attacks). **c)** Avoid non-personalised accounts ("backup_john" is better than just "backup") to ensure accountability and make it easier to deactivate accounts when someone leaves the organisation. If it is difficult to avoid non-personalised accounts, one should ensure that the user first logs in with a personal user ID to ensure accountability.
2.6.6	**Manage access to devices. a)** Identify devices securely and uniquely e.g. with certificates. This is

	especially important on employees' clients. **b)** Adopt unambiguous rules on which network zones, resources and services the devices should have access to.
2.6.7	**Use multifactor authentication** such as smart cards, certificates or one-time passwords to authenticate users. **a)** As a minimum, use multifactor on user accounts that have access to critical data or systems and system management users. If multifactor authentication is not supported, the user accounts should be compelled to use strong passwords. **b)** Use biometrics (e.g. fingerprint recognition) on clients frequently used in public areas (users can be observed/filmed when entering passwords). Please note that there may be privacy concerns around biometrics, see [3].

Supplementary information

Links

[1] (Norwegian) NSM: Råd og anbefalinger om passord: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord
[2] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[3] (Norwegian) Datatilsynet: Biometri: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri
[4] UK GOV: Password Guidance: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf
[5] CIS: CSC 6 – Access Control Management: https://www.cisecurity.org/controls/cis-controls-list

2.7. Protect data at rest and in transit

Aim of the principle: The organisation protects data stored on various storage media and when it is being transmitted across information channels.

Why is this important?

Encryption is crucial to protecting ICT systems. An organisation manages information of varying value with varying needs for protection. The information is stored on and transferred using various media with varying degrees of trust in locations where the organisation has varying degrees of control.

If the organisation does not encrypt data, unauthorised parties will be able to read or manipulate it, i.e. the confidentiality and integrity of the information can be breached. One runs the same risk if the software or hardware used has been implemented or configured with unintended vulnerabilities or if encryption keys are poorly protected.

Recommended measures: Protect data at rest and in transit

ID	Description
	Data should be protected regardless of how virtualised (e.g. cloud-based) the infrastructure is.
2.7.1	**Establish crypto strategy in the organisation.** The strategy should include which cryptographic tools to use, how to manage certificates, how to ensure secure key generation, how to store keys/passwords, backup copying of keys, renewing of keys, and what to do if keys are compromised. Key management should distinguish between long-term keys and session keys, whereby long-term keys should be given additional protection.
2.7.2	**Activate encryption in services which offer such functionality** and ensure that only recommended algorithms and key lengths are used. See [1].
2.7.3	**Encrypt storage media which contain confidential data and which can easily be lost or compromised**, e.g. storage in mobile clients. Define how different types of data should be protected, e.g. by encrypting individual files, partitions or entire disc drives.
2.7.4	**Use encryption when transferring confidential information or when trust in the information channel is low.** For each channel decide what level of encryption to perform, e.g. in the application (TLS), on the network layer (Ipsec) or on the data link layer (MACsec).
2.7.5	**Define security levels for different types of information** with different needs for confidentiality protection. Define for both information stored on different media and for information being transferred in different information channels.

Supplementary information

Links

[1] NSM: Cryptographic Recommendations: https://nsm.no/getfile.php/133478-1591960609/NSM/Filer/Dokumenter/NSM%20cryptographic%20recommendations.pdf
[2] (Norwegian) Digitaliseringsdirektoratet: Referansekatalogen for IT-standardar, Grunnleggande datakommunikasjon: https://www.digdir.no/standarder/grunnleggande-datakommunikasjon/1488

2.8. Protect email clients and browsers

Aim of the principle: The organisation reduces an attacker's opportunity to manipulate user behaviour with respect to mail clients and browsers.

Why is this important?

Secure configuration is important to prevent attackers from exploiting the organisation's assets and resources. Functions and applications receiving and processing data from unknown external sources

are especially vulnerable. Emails and websites infected with malware are common entry points for attacks where content can be modified to trick the user. Email attachments and links are two of the most common ways of distributing computer viruses, worms and other types of malware. The attachments (e.g. spreadsheets and text documents) and links often exploit vulnerabilities in applications, or the file extension displayed in the email client (.jpg, .exe, .zip etc.) does not always correspond to the actual file format.

Recommended measures: Protect email clients and browsers

ID	Description
	It is recommended that this application-specific principle be implemented after *other measures, see information underneath this list.*
2.8.1	**Verify the sender address of incoming emails** (detect spoofing). Do so by using DMARC, DKIM, SPF and DNSSEC.
2.8.2	**Activate STARTTLS on the organisation's email server** to authenticate and ensure the confidentiality of all emails between the organisation and other organisations that have activated STARTTLS.
2.8.3	**Only use supported email clients, browsers and plugins**. Only use the latest version with the latest security functions and the latest security updates. Uninstall/deactivate browsers which were included with the operating system but are no longer supported.
2.8.4	**Only permit organisation-approved plugins.** For many organisations, necessary plugins will only be those that integrate email readers and browsers with e.g. CRM-systems and archiving systems. A plugin not needed for the organisation's activities can represent a vulnerability and should therefore not be permitted (i.e. use allowlisting of application plugins).

Note that the measures in the above list are supplementary measures for email and browsing. Other security measures linked to operating systems and networks remove more of the attack surface and should be given priority, e.g.: 2.1.2 (use modern hardware and software), 2.3.1 (security updates), 2.3.2 (managing client applications), 2.6.4.a (do not give administrative privileges to end users) and 2.5.1 (managed data flow).

Supplementary information

Take steps to protect email at multiple levels: where different network protocols are being used, where the organisation connects to the internet, on the email server, in the operating system and client applications, and the human recipient.

Browser technology has developed rapidly. Compared with its original function of loading and displaying text and pictures from the internet, it is now a universal front-end. Browsers handle a wide range of different file and media formats. They also provide a platform for running applications, be it on a local server (e.g. customer management or email management) or in an external cloud (SaaS). Browsers can cause a number of security problems due to incorrect use, incorrect configuration or incorrect programming. The number of options and functions means complex configuration parameters and therefore potential security issues.

Links

[1] (Norwegian) Norid: Sikrere norske domenenavn med DNSSEC: https://www.norid.no/no/om-domenenavn/veiledere/sikrere-norske-domenenavn-med-dnssec
[2] (Norwegian) Digitaliseringsdirektoratet: Referansekatalogen for IT-standardar, Grunnleggande datakommunikasjon: https://www.digdir.no/standarder/grunnleggande-datakommunikasjon/1488
[3] CIS: CSC 7 – Email and Web Browser Protections: https://www.cisecurity.org/controls/cis-controls-list

2.9. Establish capability to restore data

Aim of the principle: Establish a method for backing up and restoring critical data to prevent losses.

Why is this important?

The organisation should establish capacity for restoring lost or modified data and system configurations. Some cyberattacks cause critical configurations, software or information to be modified or made unavailable. This can affect organisation -critical processes. One example of such an attack is ransomware, where both information and the underlying system can be encrypted and therefore be made unavailable.

Recommended measures: Establish capability to restore data

ID	Description
2.9.1	**Plan for regular backups of *all* the organisation's data.** As a minimum, the plan should describe: **a)** Which data should be backed up. **b)** Frequency of backups of various data, based on value. **c)** Responsibility for backing up various data. **d)** Procedures for failed backups. **e)** How long to store backups. **f)** Logical and physical criteria for backup security. **g)** Criteria for how long it should take to restore the organisation's systems and data (see principle 4.1 – "Prepare the organisation for incident"). **h)** The roles responsible for approving the plan. More information on backup and recovery of data and systems in [1].
2.9.2	**Include backups of software** to ensure recovery. This includes (as a minimum) **a)** security configuration, cf. 2.3 – "Maintain a secure configuration", **b)** templates for virtual machines and master images of operating systems, and **c)** installation software.
2.9.3	**Test backups regularly** and verify that the backup is correct and restorable.
2.9.4	**Protect backups against intentional and unintentional deletion, manipulation and reading.** **a)** Backup copies should be kept separate from the organisation's production environment. See e.g. principle 2.1 – "Include security during procurement and development processes". **b)** Access rights to backup copies should be restricted to only employees and system processes involved in restoring data. **c)** Offline backups which are inaccessible through the organisation's networks should be created regularly. This is in order to prevent intentional/unintentional deletion and manipulation. **d)** Backups should be protected with encryption when being stored or moved over the network. This includes external security backups and cloud services.

Supplementary information

Links

[1] NSM: Security measures against ransomware and other malware attacks (Recommendation category 2: Establish good procedures for backup and recovery): www.nsm.no/ransomware
[2] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[3] UK NCSC: Backing up your data: https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data
[4] CIS: CSC 3 – Data Protection: https://www.cisecurity.org/controls/cis-controls-list
[5] ISO/IEC 27040 – Storage security: https://www.iso.org/standard/44404.html

2.10. Include security in the change management process

Aim of the principle: Maintain the organisation's secure state when making changes.

Why is this important?

Over time an organisation will make changes as a result of changing business processes, upgrades and replacements of ICT equipment, organisational growth or adjustments. Many organisations will also see changes to their IT operating model in the event of key ICT services being outsourced or insourced, major organisational changes such as acquisitions or mergers, or restore and renewal following a cyberattack.

Each change can affect the organisation's established secure state. It is essential that these changes are handled appropriately. One needs to understand the consequences of the changes, adjust and configure the ICT systems to adapt to the changes, and carry out sufficient testing to verify that the desired secure state is maintained.

Recommended measures: Include security in the change management process

ID	Description
2.10.1	**Include security in the organisation's change management process.** The process for change management should include: **a)** Considering change proposals to identify their effect on established security measures, e.g. the measures described in the security principles. **b)** Requirements for testing of changes before and after deployment, see principle 2.1 – "Include security during procurement and development processes". **c)** Informing and involving parties

	affected by the change. **d)** Documenting assessments, recommendations, decisions and reviews/tests relevant to the secure state.
2.10.2	**Involve necessary ICT security staff when making changes.** This could involve general and technical assessments and reviews, testing, approval/signatures or notification.
2.10.3	**Test affected security functions** both before and after deployment in order to maintain secure state.
2.10.4	**Integrate security into the organisation's urgent change processes.** Stipulate minimum requirements for staff involvement, security assessments, testing and documentation before and after deployment, see 2.10.1 – 2.10.3.

Supplementary information

There are many examples of changes to ICT systems creating vulnerabilities which are then exploited by persons with malicious intent. Openly announcing that the organisation is making major changes (e.g. a press release about a merger or announcement of a major ICT procurement) can in itself make the organisation a more attractive target for attackers.

When planning major changes to the ICT system, it is important to consider the security implications at an early stage. Security can become more expensive, more complex and less effective if security issues are addressed after a new ICT architecture has been decided.

Organisations should instigate a formal change process where security implications form an integral part of the planning. This also applies to changes that need to be made swiftly, what we describe as urgent changes. These changes are so important that they cannot be subject to a normal change process due to time constraints.

Links

[1] AXELOS: ITIL 4: the framework for the management of IT-enabled services: https://www.axelos.com/certifications/itil-service-management
[2] ISO 10007 – Quality management — Guidelines for configuration management: https://www.iso.org/standard/70400.html

3. Detect

3.1. Detect and remove known vulnerabilities and threats

Aim of the principle: The organisation detects and removes known vulnerabilities and known harmful code in its ICT systems.

Why is this important?

Harmful code is a dangerous cyberthreat and can be designed to affect systems, devices and data. Even the best products have faults and vulnerabilities that can be exploited by attackers. Malicious software can move swiftly and make its way in through e.g. end user equipment, email attachments, the organisations externally exposed services, websites, cloud services and removable media. The harmful code is often activated by tricking the user into performing an action (e.g. open, run, install). Modern malware can be developed to circumvent certain security barriers or to attack or deactivate these barriers. The organisation should be familiar with known vulnerabilities and publicly known threats (such as malware) and protect itself accordingly.

A "*known"* vulnerability is typically *a)* a software security update has been published but not applied, *b)* a common misconfiguration is applied or *c)* commonly/publicly known passwords are used. A "*known"* threat is typically malware that has been registered by most security products/services.

Recommended measures: Detect and remove known vulnerabilities and threats

ID	Description
3.1.1	**Conduct regular vulnerability assessments** in the information system using automated tools. The assessment should cover clients, servers and networks. **a)** Rank the findings according to priority and verify that any detected vulnerabilities are dealt with. **b)** Ensure that the tools used for vulnerability assessments are updated regularly with information about all relevant security vulnerabilities.
3.1.2	**Subscribe to vulnerability intelligence services** to keep up to date with new and expected vulnerabilities. Use this information as input for vulnerability assessment tools.
3.1.3	**Use automated and centralised tools to handle known threats (such as malware).** **a)** Use antivirus/antimalware products, ideally a centrally managed solution, to detect and block known malware that can exploit vulnerabilities in email clients and document readers etc. **b)** Also use IDS/IPS functionality on clients and servers. **c)** Incidents from these tools should be logged, see principle 3.2 – Establish security monitoring.

Supplementary information

Defences against malware must be able to operate in dynamic environments, support large-scale automation, receive rapid updates, and be integrated with the processes for incident management. The defences must also be distributed to a number of potential attack points in order to detect malware, prevent lateral movement and control/block harmful execution of code.

Important threat and vulnerability notices are published on the NSM website, see [2]. Similar warnings are also distributed by commercial providers and software suppliers.

Links

[1] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[2] (Norwegian) NSM: NCSC varsler: https://nsm.no/varsler
[3] UK NCSC: Antivirus and other security software: https://www.ncsc.gov.uk/collection/mobile-device-guidance/antivirus-and-other-security-software
[4] CIS: CSC 7 – Continuous Vulnerability Management: https://www.cisecurity.org/controls/cis-controls-list

3.2. Establish security monitoring

Aim of the principle: The organisation monitors its ICT systems and collects relevant data to detect security incidents and perform data analysis.

Why is this important?

Collecting and analysing security relevant data can help detect security incidents early, evaluate the extent of the damage and the nature of the incident, and understand the sequence of events. The availability of sufficient data can be key to the organisation being able to restore to a desired state and prevent similar future incidents. It is also important to the subsequent investigation.

A lack of security monitoring and detection in information systems along with inadequate analysis of security-relevant data allow attackers to hide their presence, actions and activities in the organisation's information systems. If an organisation knows that its systems and machines have been infiltrated, but hasn`t established adequate security monitoring, it will be blind to the details of the incident.

Recommended measures: Establish security monitoring

ID	Description
3.2.1	**Determine a strategy and guidelines for security monitoring.** The following should be described: **a)** Purpose and usage of collected data. **b)** Which data to collect. **c)** Secure storage of data

	(including storage and processing of data related to legal processes). **d)** Capacity planning for collected data. **e)** Access control of collected data. **f)** Collation of logs from the organisation's different devices and services. **g)** Deletion of data. **h)** Audit frequency for the strategy (at least once a year and on particular occasions, e.g. after a major event such as a cyberattack).
3.2.2	**Comply with laws, regulations and the organisation's guidelines on security monitoring. a)** Determine which laws and regulations the organisation is required to comply with. **b)** Decide how long collected data can be stored. **c)** Inform staff of what is being collected, what it will be used for and how the data will be processed.
3.2.3	**Decide which parts of the ICT system to monitor.** This could be: **a)** The most critical parts of the system or the parts which contain the most confidential information (operating system, database and application). **b)** Operating systems on devices. **c)** Internal gateways where data flows through. **d)** Gateways between internal and external systems, e.g. to the internet. **e)** Security products (AVS, IDS, IPS, FW etc.) in the information systems. **f)** Systems for backup and restore.
3.2.4	**Decide which data is security-relevant and should be collected.** With regard to the parts of the system described in 3.2.3, one should collect the following as a minimum: **a)** Data relating to access control (successful and unsuccessful log-in attempts), and **b)** Administration and security logs from devices and services in the ICT systems. With regard to clients, one should record the following as a minimum: **c)** attempts to run unknown software (cf. 2.3.2), and **d)** attempts to seek privilege escalation.
3.2.5	**Verify that the monitoring is working as intended**. **a)** Check that log settings are working and that the collection works as expected. **b)** Ensure that all systems which regularly store security-relevant data have sufficient storage space so that crucial data is not lost. **c)** Use a standardised format so that data can easily be read by third-party log analysis tools.
3.2.6	**Prevent manipulation of monitoring-data**. **a)** Archive and sign logs digitally at regular intervals to ensure log integrity. **b)** Ensure sufficient access control for logs and implement functionality to detect attempted manipulation or deletion of logs. **c)** Ensure that all components are synchronised with a single time source. **d)** Gather and consolidate relevant monitoring-data and make available for analysis (see principle 3.3 – Analyse data from security monitoring).
3.2.7	**Review the security relevant monitoring-data regularly and, if necessary, reconfigure the monitoring** in line with the strategy so that only relevant data is collected and preserved. Remove collected data which no longer has operational or security relevance.

Supplementary information

It is important to identify the organisation's most critical systems and data so that monitoring, collection and detection is done in the right places in the information systems. It is important to be able to detect unauthorised actions, security breaches and security threats as early as possible in order to minimise, if not prevent, damage.

Identifying critical systems and data is necessary to be able to collect relevant information about systems and activities that can help detect incidents.

Unwanted activity in an organisation's network is difficult to detect, and once the threat actors get a foothold, they will attempt to mask most of their activities as legitimate traffic. Security-relevant data

should therefore be used to get an idea of what constitutes a desired state so that non-conformities can be identified. The increasing use of end-to-end encryption by threat actors means that collecting data from end points should be a priority along with the collection of general network traffic.

Logs are important in incident management and for the rational operation of information systems, but they must be protected and protected well. Security-relevant data can contain confidential information about individual staff members, and the need for storage and access must always be weighed up against the need for privacy.

Security monitoring of clients is often overlooked. A large number of attacks begin when the end user processes emails or surfs the internet. We often find that important client logs are missing that could help understand the early stages of an incident. For that reason, more detailed data from clients is often needed, see 3.2.4.

Security-relevant data should help maintain the authenticity, confidentiality, integrity, availability, accountability and trust of the information systems. The data must be collected and treated in a way that instils confidence in what the log says, in that one is collecting what is to be collected, and in that the data has not been manipulated. The security-relevant data should only be used to maintain security in the ICT system and should be stored for long enough so that one can detect and identify unwanted activity following an incident. When determining how long to store data for, one should also consider the fact that the data could potentially be relevant to a future investigation, damage assessments and trend analyses.

To be able to use security-relevant data effectively, the data should be *centralised and consolidated* so that it can be evaluated and analysed and enable one to mount the right response to a security incident.

Links

[1] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[2] UK NCSC: Logging and monitoring https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes
[3] UK NCSC: Introduction to logging for security purposes: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/monitoring
[4] AUS GOV: Guidelines for System Monitoring: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring

3.3. Analyse data from security monitoring

Aim of the principle: The organisation detects harmful activities that affect information systems, data and services by analysing security-relevant data.

Why is this important?

Detecting unauthorised actions and security incidents can be difficult, and in some cases it is down to luck, an observant user or an external tip-off. Systematic processing by collating and analysing collected data will improve chances of detecting incidents. The analysis will also help to understand incidents across structures and components in the ICT system.

The organisation should be capable of identifying known threats in its infrastructure, have the skills needed to use automated tools, and understand how to fully utilise the tools. The tools should analyse the information gathered in principle 3.2 to verify indicators of compromise (IoCs).

Recommended measures: Analyse data from security monitoring

ID	Description

3.3.1	**Create a plan for analysing data from security monitoring**, including:
	• Determining whether the organisation is capable of building its own analytics expertise or whether to buy it.
	• Priority, frequency and resources spent on analytics.
	• Tools, services and mechanisms for searching, processing and analysing.
	• Administration and further development, including:
	  ○ signature-based tools
	  ○ desired state of the information system
	  ○ methodology and automated processing of collected security-relevant data
	  ○ reconfigure tool for collecting security-relevant data
	  ○ analytics tools, technology and algorithms for applied machine learning
	• Reporting.
	• Incident management.

3.3.2	**Establish and maintain expertise on the desired state of the organisation's information systems** to be able to detect changes or abnormalities that could indicate unauthorised actions. The desired state needs to be managed over time and should reflect any restructuring, reorganisation, acquisitions, mergers, staff redundancies and changes to the operational concept. Knowledge of the information systems should be good enough that it is possible to identify anomalies that represent a threat. This could include: • Data flow in breach of permitted data flow as per principle 2.5 – Control data flow • Data flow at abnormal times and which is not deemed normal traffic. • Abnormal volumes of data flowing through the network.
3.3.3	**Select tools that support manual and automated searches including criteria based alerts**. The tool should be able to automatically collate data from different sources to determine more easily whether the incident is genuine (i.e. not a false positive) as well as its scope and nature. Use

	knowledge of the desired state (see 3.3.2) and threats (see 3.3.4) to improve the tools' searches and alert criteria. This will help to detect unknown threats at an earlier stage.
3.3.4	**Obtain and process threat information from relevant sources** and use it to evaluate potential security incidents. This could be data from past attacks or threat information from the authorities, sector CERTs, comparable organisations or open sources.
3.3.5	**Continually assess whether the collected data is sufficiently relevant and detailed**.
3.3.6	**Establish a procedure for escalating alerts**, whom to report to, which data to make available and to whom when managing an incident.
3.3.7	**Use analytics tools, technology and algorithms** (e.g. applied machine learning) to help detect and communicate unknown threats and abnormalities in the security-relevant data.

Supplementary information

Organisations should be able to utilise the results from the security monitoring, see principle 3.2 – Establish security monitoring. Such capabilities may be retained in-house or purchased. Organisations should also partner with relevant sector CERTs for analytics support and incident support.

Threat information can be obtained in a variety of formats, volumes and qualities. It can be collected from open discussion forums, partners, service subscriptions or internal sources. Threat information must be processed further once it has been received in order to identify what is relevant to the organisation's ICT systems.

Organisations should also be able to *identify unknown threats* by combining in-depth knowledge about their own systems with vulnerabilities, threat assessment for their respective sectors. Some attackers will make a great effort to avoid detection by standard monitoring systems such as antivirus software and signature-based intrusion detection systems (IDSs).

To help process large quantities of data and detect unauthorised events, the organisation should also consider using applied machine learning – implementing known algorithms to help identify abnormalities in the security-relevant data.

To ensure a swift and effective analysis and notification process based on the collected data, the organisation should obtain automated analytics tools which are then continually calibrated based on threshold values, knowledge of the organisation's desired state, or knowledge of the threats that exist in the digital space. The "desired state" describes what constitutes a "clean network" and which settings and data flow are normal during day-to-day operations.

It is important to identify irregularities and incidents early in order to be able to detect and respond to cyberattacks (see category 4 – Respond and).

Organisations should continually improve their expertise on the processing of security-relevant data, including system specific knowledge, use of tools, threats and methods for detecting unauthorised events.

Links

[1] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[2] NCSC UK: Cyber Assessment Framework - C1 Security monitoring: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/c-1-security-monitoring

3.4. Perform penetration tests

Aim of the principle: The organisation tests elements in its defence mechanisms (technology, processes and personnel) by simulating the targets and actions of an attacker.

Why is this important?

ICT systems are in constant change and development and are regularly challenged by attackers. Organisations should therefore regularly test their defence capabilities in order to verify established security measures, identify shortcomings and evaluate their preparedness. Attackers often exploit weaknesses in an organisation's routines. Examples of weaknesses include:

- Too long between the time of a security fix being issued by the provider, and the time of the actual installation of the fix by the customer.
- Generous access rights combined with weak authentication mechanisms (e.g. weak passwords).
- Inadequate configuration of devices in the ICT system.
- Inability to understand the organisation's value chains and dependencies between systems.

A penetration test will provide deeper insights by demonstrating in practice the risk posed by vulnerabilities. Using different attack vectors and tools ensures a better evaluation of the organisation's security barriers and defence mechanisms.

Recommended measures: Perform penetration tests

ID	Description
3.4.1	**Plan penetration testing with defined goals and scope**. **a)** Identify important parts of the information system that should be emphasised during testing. **b)** Identify individual systems or components which are so critical that they must be excluded from the testing. They could be parts of the ICT infrastructure which are vital to maintaining organisation-critical services or which are incapable of withstanding a penetration test (e.g. centralised industrial control systems).
3.4.2	**Involve relevant stakeholders in advance.** Adapt the type of information being issued and to whom according to the goals and scope of the testing. For example, it will often be appropriate to inform external system monitoring providers prior to testing, but not necessarily users and system management personnel.
3.4.3	**Use vulnerability scanning tools and attack tools.** Vulnerability scanning can be used as a starting

	point for the test, while attack tools are used to exploit identified vulnerabilities.
3.4.4	**Perform regular penetration testing (at least annually) to identify vulnerabilities.** Penetration tests should be carried out **a)** from outside the organisation's network barriers (e.g. from the internet or via wireless communication near the organisation's premises) in order to simulate an external attack, and **b)** from inside the barriers (e.g. in the internal network) in order to simulate internal attacks from a compromised client/server or disloyal employee.
3.4.5	**Test the organisation´s routines for detection and preparedness** e.g. when performing penetration tests. Testing frequency will depend on the organisation's needs, but tests should be performed at least every two years to maintain adequate skill levels amongst the personnel involved.
3.4.6	**Communicate the results of penetration tests to relevant stakeholders.** **a)** Reports on penetration tests and ICT preparedness exercises should meet the organisation's needs. **b)** The tests should be documented with a summary (management summary) and a list of findings and suggested improvements.

Supplementary information

Penetration tests are controlled cyberattacks designed to test the resilience of ICT systems through targeted searches and analysis and attempted exploitation of discovered vulnerabilities. The actions of a malicious actor are simulated, but the tests take place within a limited time frame in parts of the systems. We often distinguish between two types of tests.

Testing the organisation's systems and components to identify and exploit vulnerabilities. The purpose of this test is to identify the most serious weaknesses and then rectify them. It is common to take a broad approach in order to identify as many vulnerabilities as possible within the given time frame and scope. A penetration test can demonstrate how attackers can gain access to confidential information and take control of parts of the ICT infrastructure or specific services.

Testing the organisation's capacity for detection and response.
The aim is to test the organisation's capability to identify and respond to a cyberattack by simulating an actual attack. This type of testing is often more targeted and does not aim to find as many vulnerabilities as possible.

Links

[1] (Norwegian) NSM: Inntrengingstesting
https://nsm.no/tjenester/inntrengingstjenester
[2] UK NCSC: Penetration testing
https://www.ncsc.gov.uk/guidance/penetration-testing
[3] CIS: CSC 18 – Penetration Testing:
https://www.cisecurity.org/controls/cis-controls-list

4. Respond and recover

4.1. Prepare the organisation for incidents

Aim of the principle: The organisation has implemented effective processes for incident management in order to quickly detect, control, minimise the damage and effectively remove the cause of the incident. This includes restoring the integrity of the systems and networks.

Why is this important?

Cyberattacks are common and something that all organisations should prepare for. Even large, technically sophisticated organisations with extensive resources find it difficult to keep up with the frequency and complexity of cyberattacks. The question is not "if" an organisation will fall victim to a successful cyberattack, but too often "when". Without a plan and a process for dealing with incidents, it will be difficult for the organisation to limit the damage and return to its desired state.

Once an incident has occurred, it is too late to create good procedures, reporting routines, data collection, management responsibilities and communication strategies. These must be prepared and rehearsed regularly to enable the organisation to understand, respond and return to its desired state.

Recommended measures: Prepare the organisation for incidents

ID	Description
4.1.1	**Establish plans for incident management** which meet the need for business continuity at times of preparedness and crisis. This should include **a)** a set of requirements for restoring ICT functions, ICT services and ICT systems based on an analysis of the consequences for the organisation (BIA – business impact analysis), **b)** a description of roles and responsibilities for relevant personnel, **c)** required training of relevant personnel, **d)** categorization regime for incidents and threshold values for activating the crisis management team, **e)** requirements for testing and exercising plans and personnel. **f)** Revise and update plans regularly, at least once a year and after an exercise, major incident or attack.
4.1.2	**Perform a business impact analysis.** This should include: **a)** prioritising vital business functions and their required security levels, **b)** identified dependencies of ICT functions, ICT services, ICT systems etc., **c)** criteria for restoration time, loss of data and service levels.
4.1.3	**Describe roles and responsibilities for personnel involved in incident management**. This includes: **a)** personnel with important responsibilities, e.g. IT manager, application manager, platform manager etc., **b)** managers with decision-making responsibilities at various levels, and **c)** emergency personnel available outside ordinary working hours and during holidays. **d)** Ensure sufficient training and exercising for personnel according to plans.
4.1.4	**Establish agreements with relevant third parties** in order to provide support if required during an incident. Third parties could be sector-specific computer emergency response teams, IT specialists

	in various fields, equipment and software providers etc.
4.1.5	**Determine which communication channels to use in the event of an incident. a)** Distribute contact information on relevant personnel. **b)** Create a plan for alternative communication channels. **c)** Create an internal and external communication plan for incidents.
4.1.6	**Test and rehearse the plans regularly so that they are established. a)** Exercises should include relevant subcontractors. **b)** Exercises should include testing of procedures for detection and preparedness, see 3.4.5.

Supplementary information

To avoid delays, the need to obtain approvals, discussions, etc. it is an advantage to adopt a pre-approved response pattern. Then the organisation can react quicker when incidents occur. For example, cut the organisation's internet access when situation X occurs, impose highly restrictive firewall rules when situation Y occurs, etc. These plans need to be approved by the management, not just IT.

What to do if a cyberattack is detected outside working hours?

- How quickly can the organisation mobilise a response?
- Is the organisation's phone list up to date?
- Has the organisation paid subcontractors and support staff who can step in at short notice?
- What does the organisation do if key personnel are on holiday abroad?

If self-propagating malware has been detected, one needs to act quickly to prevent extensive damage. An organisation might have only an hour or two from detecting the malware to deciding a course of action.

- Should we shut down traffic between various network zones in the organisation?
- Should we cut power to central servers?
- Do we have any services that need to be isolated from other ICT infrastructure?
- Will the response functions work if the information systems are down?
- Will backup copies work if we have to delete all our servers?

Good planning, up-to-date and well tested plans and 24/7 monitoring can be do or die for an organisation when a cyberattack occurs.

Links

[1] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[2] (Norwegian) NSM: Rammeverk for håndtering av hendelser: https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/
[3] UK NCSC: Incident Management: https://www.ncsc.gov.uk/collection/incident-management
[4] UK NCSC: Incident Management 10 steps: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/incident-management

[5] UK NCSC: Planning your response to cyber incidents: https://www.ncsc.gov.uk/collection/board-toolkit/planning-your-response-to-cyber-incidents
[6] UK NCSC: Small business guidance - Response & Recovery: Step 1: Prepare for incidents https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery/step-1-prepare-for-incidents
[7] ISO/IEC 27035-1 Information security incident management – Part 1: Principles of incident management: https://www.iso.org/standard/78973.html
[8] ISO/IEC 27035-2 Information security incident management – Part 2: Guidelines to plan and prepare for incident response: https://www.iso.org/standard/78974.html

4.2. Assess and categorize incidents

Aim of the principle: The organisation assesses and categorize incidents correctly and swiftly so that they can be dealt with efficiently, are prioritized correctly and involves the correct resources and personnel.

Why is this important?

Correct assessment and categorization of incidents is important so that the organisation can allocate resources effectively and resolve the issue within required time. If it takes too long between the incident being detected and then reported, prioritised and dealt with, the extent of the damage, resource use and restoration time can become significant. Incorrect categorization can lead the organisation to spending a great deal of time and effort on insignificant events, while more important incidents go under the radar.

If the right decision-makers are not involved, the incident could escalate and spread because reactive measures are not taken quickly enough. If the malware is complex, few people will be able to identify the actual extent of the damage until after the event. Many organisations will need to seek external expertise.

Recommended measures: Assess and categorize incidents

ID	Description
4.2.1	**Review log data and collect relevant data on the incident to create a good basis for making decisions.** This could involve obtaining and collating data from multiple sources, performing tests or taking measurements in order to verify or disprove an incident. The method and scope will depend on the type of incident.
4.2.2	**Determine the severity level of the incident** in accordance with adopted plans, see 4.1.1. **a)** Determine whether the incident is a potential or confirmed security incident or a false alarm. **b)** Categorize the incident in accordance with the organisation's categorization regime (4.1.1.d). **c)** Involve relevant roles (4.1.3). **d)** Activate response plans if the nature of the incident requires it.

4.2.3	**Inform relevant stakeholders.** This could be sector-specific computer emergency response teams, IT specialists in various fields, equipment and software providers, the management, end users, the media etc. See 4.1.3–4.1.4.

Supplementary information

When an incident occurs there will always be a discussion about whether to shut down services, implement measures or just sit tight and observe in order to understand what is happening. This is an extremely difficult decision to make and one that requires competent observers. Get the decision wrong, and it can cause extensive damage. Shutting down a service will have consequences for the organisation's deliverables, and shutting down too early can make it difficult to tidy up afterwards. Organisations should seek to involve all relevant resources when making the decision.

Links

[1] UK NCSC: Small Business Guide - Response & Recovery: Step 2: Identify what's happening https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery/step-2-identify-what-s-happening

4.3. Control and manage incidents

Aim of the principle: The organisation manages incidents correctly using appropriate resources to minimise the spread and consequences, and the desired secure state is maintained or effectively restored.

Why is this important?

When an incident occurs, one should keep calm while swiftly alerting and involving the right people. If the organisation is unable to determine which parts of its infrastructure are affected and how to best manage the extent of the cyberattack, the consequences can be catastrophic.

Stick to adopted procedures based on the incident categorization, and involve personnel with specialist expertise on the ICT system and its day-to-day operation. Irrespective of the type of incident, a number of common principles will apply. Investigate the spread and potential consequences. Keep the event data and situational awareness up to date for the duration of the incident. Prepare for a potential escalation as well as concurrent incidents and ensure a good flow of communication between the parties involved.

Reactive measures should be taken as soon as sufficient information is available. All activities and decisions should be logged so that one later can evaluate the sequence of events. Internal and external parties affected by the incident should be kept up to date. Once an incident has occurred,

trust in services, systems and ICT infrastructure will obviously weaken. Effective incident management will help restore that trust.

Recommended measures: Control and manage incidents

ID	Description
4.3.1	**Identify extent and impact on business processes.** Identify the impact of the incident on underlying ICT functions, ICT services and ICT systems. See 4.1.2.
4.3.2	**Determine whether the incident is under control and take the necessary reactive measures**. If the extent increases and appears to be having serious consequences for the organisation's business processes, one should implement crisis response activities by escalating to the crisis management team. Examples of reactive measures are: • Allocating internal and external personnel to manage the incident. • Encapsulating and blocking the intruder to prevent spreading. • Terminating threatening or compromised activities in the system, e.g. by shutting down compromised internal servers which can be used for further attacks.
4.3.3	**Log all activities, results and relevant decisions** for subsequent analysis. **a)** Establish a timeline of the organisation's own and the threat actor's activities. **b)** Update event data and situational awareness continuously in order to manage the incident in the best possible way. **c)** Secure electronic evidence for malware analysis and potential legal processes, see also principle 3.2 – Establish security monitoring.
4.3.4	**Launch recovery plan during or after the incident**. Measures will depend on the type of incident, but could include: • Reactivating redundant resources lost or damaged during the incident. • Reinstalling hardware and software on affected components. • Restoring configuration settings, to include any necessary adjustments. • Restoring services halted during the incident. The ICT systems should be rebuilt to a better state than they were in before the incident occurred ("build back better"). More information in [1].
4.3.5	**Co-ordinate and communicate with internal and external stakeholders while managing the incident.** This could be the organisations system management team, the executive management, in-house departments and other organisation's that may be affected by the incident. Organisations should also adopt a media strategy for incidents that may be of interest to the media and wider public.

4.3.6	**Perform necessary activities after the incident**. The severity of the incident and the organisation's expertise and capacity will determine which activities are required and whether they should be conducted by internal or external personnel. It could involve:
	• Investigation to determine the root cause of the incident, including:
	  ○ Type of malware
	  ○ Threat actor
	  ○ Attack vector
	  ○ Tools
	  ○ How the sequence of events unfolded, and how the threat actor behaved.
	• Preparing a summary that the management can understand and act on.
	• Communication with relevant parties, including sector-specific computer emergency response

	teams and/or NSM NCSC.

Supplementary information

The response will depend on the type of incident. For example, there is a difference between incidents that have only just occurred and are escalating and incidents that have gone on for some time and are now in a “stable” phase.

- Scenario 1: In the event of extensive spread and damage by malware such as self-propagating cryptoviruses: act immediately to stop the attack!
- Scenario 2: If “someone” has gained a foothold inside the organisation over time: wait, observe, understand, act. If the organisation is under attack by an advanced threat actor with a good foothold, taking the wrong action can cause the actor to go into hibernation or use less visible attack methods. This will make it more difficult to determine the extent of the damage, obtain evidence and remove the actor.

One rule of thumb is that one has 2 hours from “something” happening abroad until you need to make a decision for your organisation on how to act.

Links

[1] NSM: Security measures against ransomware and other malware attacks (particularly recommendation category 2 and 7): www.nsm.no/ransomware
[2] (Norwegian) NSM: Samleside mot digital utpressing (løspengeangrep): nsm.no/digitalutpressing
[3] UK NCSC: Small Business Guide: Response & Recovery: Step 3: Resolve the incident https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery/step-3--resolve-the-incident
[4] UK NCSC: Small Business Guide: Response & Recovery: Step 4: Report the incident https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery/step-4--report-the-incident-to-wider-stakeholders

4.4. Evaluate and learn from incidents

Aim of the principle: The organisation learns from incidents and improves its security measures, incident processes and staff training and updates prevailing procedures.

Why is this important?

Once an incident has been dealt with in full and the case is closed, it is important that the organisation quickly identifies and learns from what has happened and ensures that its conclusions are reviewed and acted on. Failure to do so means a great deal of knowledge and experience is lost, and one may end up making the same mistakes again the next time an incident occurs. One may be able to identify

new vulnerabilities or a need for new or improved security measures to prevent situations from arising in the future.

Recommended measures: Evaluate and learn from incidents

ID	Description
4.4.1	**Identify experiences and lessons learnt from incidents**, both things that worked and things that could be improved.
4.4.2	**Review identified compromised security measures** to prevent a similar incident from occurring. Determine whether the established measures are adequate for the organisation's risk tolerance.
4.4.3	**Assess the effectiveness of processes, procedures, reporting formats and organisational structures related to incident response.** Review regularly, also after an incident, and update based on any lessons learnt.
4.4.4	**Communicate and share findings with relevant stakeholders**, and use actual stories from the incident response to train and raise awareness amongst staff.

Supplementary information

When evaluating an incident, one will usually end up with a number of potential improvements and measures. They can often be divided into three categories:

1. The need for updated or new risk assessments. This could be due to changing threat or vulnerability information.
2. Organisational and procedural measures. This could be changes to incident management plans, processes, procedures, reporting formats, organisational structures etc.
3. Technological, physical or human measures such as better technical tools for detecting incidents, updated security guidelines or awareness campaigns aimed at users.

Links

[1] UK NCSC: Small Business Guide: Response & Recovery: Step 5: Learn from the incident https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery/step-5--learn-from-the-incident

Norwegian National Security Authority

www.nsm.no/ict-sp

24/00704