NIS2 Quality Mark

NIS2-QM20 SUBSTANTIAL

Version 3.2
December 15, 2025

NIS2 QUALITY MARK

Contents

Substantial standard , belonging to the NIS2 Quality Mark, an integral part of the Compliance and Certification Scheme of NIS2 Quality Mark and the Quality Innovation Foundation
Version 3.1 © 2025

There are more standards aimed at increasing cyber resilience. To guide this process and potentially prevent duplicate efforts, each standard includes a mapping indication so that the reader can see how each component of the standard may relate to other authoritative standards in Europe, particularly ISO standard 27001.

***Mapping indication:** The measure shows similarities to another standard but cannot be considered completely identical. It serves as a tool to identify overlapping areas without losing the unique characteristics of the standards.*

As for the measures from the ISO standard 27001: the 'A' referred to is the numbering from Annex A of the 27001 standard. This is leading for 27001.

1. Organisational measures

1.2 Information security policy formulation and management approval

The organisation's management should formulate a policy that sets out strategic objectives for protecting the availability, integrity and confidentiality of information from cyber threats. The policy is approved by management and communicated to relevant employees.

The organisation shall formulate specific policies based on the cyber security strategy that support proactive preparedness and protection against incidents and cyber threats. The policies shall provide clarity on standard practices such as access security, application management, IT management, network management and backup management. The policies shall be approved by appropriate management and communicated to relevant employees.

Goal

Preventing information security incidents from occurring due to employees feeling insufficient urgency and being given frameworks for protecting the availability, integrity and confidentiality of information against cyber threats.

Focus points

- Develop a detailed information security policy that includes standard practices and procedures. This policy should be formally approved by management and shared with all stakeholders.
- Ensure regular updates, password changes, installation management, access restrictions, and data backups . These practices support proactive protection against incidents and threats.
- Clearly define who is responsible for initiating and deciding on cybersecurity measures. Formal administrative approval of the policy is essential for compliance and implementation.
- The policy should be reviewed and updated regularly, especially when significant changes occur in the organisation or the external threat environment. This guarantees ongoing effectiveness and relevance .

Mapping indication

ISO 27001: A. 5.1
IEC 62443-2-1: 2010, Clause 4.2.2, 4.2.3.6
NIST SP 800-53: PL-1 - Policy and procedures

1.3 Assignment of responsibility for information security

The organisation must define and assign tasks and responsibilities for cybersecurity. The responsibilities for initiating and deciding on cybersecurity measures are known to those responsible. At least one individual is designated as the primary person accountable for the whole of the organisation's cybersecurity.

Goal

Preventing information security incidents from occurring because necessary actions are not carried out, are not carried out properly, or are not carried out on time, due to lack of clarity about responsibilities.

Focus points

- Define and assign clear roles and responsibilities for information security to all employees. This helps ensure a coordinated and consistent approach to security practices across the organisation. There should be a specific person responsible for overall information security.
- Document and communicate information security roles and responsibilities to all employees. This provides clarity and helps employees better understand their roles and responsibilities. Training and support should be available to ensure employees can effectively contribute to information security.
- Regularly evaluate and review assigned roles and responsibilities to ensure they continue to align with the organisation's changing needs and risks. This includes adapting responsibilities as organisational or technology changes and continually informing employees about their role in information security.

Mapping indication

ISO 27001: A.5.2
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1: 2010, Clause 4.3.2.3.3
NIST SP 800-53: PM-1 - Information security program plan

1.6.1 Overview of information

The organisation must establish and maintain an overview of business information categories. For each category, an owner (manager) is designated, responsible for safeguarding the information within that category.

Goal

Preventing information security incidents from occurring due to unidentified and unowned information, and therefore insufficiently protected.

Focus points

- Inventory all information data within the organisation, such as customer data, contracts and financial administration. This overview helps to identify and effectively secure all information.
- Establish an information register that contains all types of information, including storage locations, forms (digital or paper) and retention periods. This register must complete, correct and current.
- Designate owners/managers for specific categories of information in the registry. These individuals are responsible for the management and security of their assigned information.
- Check and update the information register regularly to ensure that it remains complete and up-to-date. This ensures that the information is properly managed and protected.

Mapping indication

ISO 27001: A.5.9
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2
IEC 62443-2-1:2010, Clause 4.2.3.4 IEC 62443-3-3:2013 SR 7.8

1.6.2 Overview of ICT assets

The organisation must establish and maintain an ICT assets overview, including servers, data storage systems and firewalls. For each asset (or group of assets), a designated owner (manager) is assigned, responsible for its protection.

Goal

Preventing information security incidents from occurring due to unidentified and unowned ICT assets, and therefore insufficiently protected.

Focus points

- Create an inventory of all ICT assets within the organisation, such as computers, servers, data storage systems and firewalls. This overview helps to effectively manage and secure all ICT assets.
- Create an inventory list of all ICT assets, including their locations, descriptions and date of acquisition. Ensure that this list is complete, correct and up to date.
- Designate owners/managers for each ICT asset on the inventory list. These individuals are responsible for the management, security and maintenance of their assigned ICT assets.
- Check and update the inventory list regularly to ensure that it is always up to date. This guarantees a reliable basis for the management and security of the ICT assets.

Mapping indication

ISO 27001: A.5.9
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2
IEC 62443-2-1:2010, Clause 4.2.3.4 IEC 62443-3-3:2013 SR 7.8

1.7 Acceptable use of information and related assets

The organisation shall establish and communicate rules for the safe use of information and related assets such as computers, laptops, telephones, storage media and business applications.

Goal

To reduce the likelihood of employees causing information security incidents due to ignorance, inexperience, carelessness, inaccuracy or indifference in handling information and related assets.

Focus points

- Establish clear rules and procedures for the secure use of information and related assets, such as computers, laptops, telephones, storage media and business applications. This helps prevent misuse and ensures the integrity of the information.
- Monitor and enforce compliance with established rules and procedures. Ensure that mechanisms are in place to detect violations and take appropriate action when necessary.
- Regularly evaluate and update policies and procedures to ensure they remain aligned with the latest security standards and the changing needs of the organisation. This ensures that the measures remain effective and up-to-date.

Mapping indication

ISO 27001 A.5.10
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3
IEC 62443-3-3:2013, SR 3.4, SR 4.1
NIST SP 800-53: AC-2 - Account Management .

1.8 Returning company assets after use

The organisation must use a procedure and checklist to ensure that employees and temporary workers return company assets (such as laptops, telephones, key cards and keys) after termination or change of their employment, contract or agreement.

Goal

To prevent an information security incident from occurring due to a company asset falling into the wrong hands or being used unsafely following termination or change of an employment relationship, contract or agreement.

Focus points

- Create an inventory of all company assets that employees use, such as computers, smartphones and other equipment. This helps in managing and reclaiming company assets when an employee leaves the organisation.
- Establish a clear procedure and checklist for returning company assets when an employee leaves. This procedure should describe step-by-step what needs to be done to ensure that all assets are returned correctly.
- Designate a responsible person or department to oversee the return process. This person or department will ensure that the procedure is followed and that all assets are actually returned.
- Review and update the procedure and checklist regularly to ensure it remains up-to-date and aligned with current business practices and technologies. This will ensure an effective delivery process and help ensure information security.

Mapping indication

ISO 27001 A.5.11

1.9 Classifying information

The organisation must maintain an overview of different categories of business information that have the same level of confidentiality in a classification scheme. For each category, it has been determined how the business information in question must be treated and protected to ensure its confidentiality. For each category, it has also been determined whether the business information in question must be labeled to make it more recognisable to employees.

Goal

An information classification scheme helps to establish rules for handling and protecting certain types of information. Labeling can reduce the chance of an information security incident occurring because an employee does not know how to handle a certain type of information.

Focus points

- Create a classification scheme that defines different categories for information, such as "public," "internal," and "highly confidential." This helps to systematically label and manage information based on its sensitivity and security needs.
- Label all information within the organisation according to the established classification scheme. This ensures that employees can see at a glance how to handle different types of information and what protective measures are needed.
- Communicate the classification scheme and associated procedures clearly to all employees. This promotes awareness and compliance with the security guidelines for information handling.
- Regularly review and update the classification scheme and procedures to ensure they remain consistent with the changing needs of the organisation and the latest security standards. This ensures that the classification and protection of information remains up-to-date and effective.

Mapping indication

ISO 27001 A.5.12
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 12
NIST SP 800-53: RA-2 - Security categorization

1.13 User Registration and Deregistration

The organisation shall define and implement a procedure for creating, modifying and timely deleting of all types of accounts used by registered employees and temporary workers.

Goal

Preventing an information security incident from occurring because a person or system is incorrectly or wrongly registered and therefore does not have the correct access rights.

Focus points

- Establish a procedure for registering, modifying and deleting employee user accounts. This ensures that the identity lifecycle is properly managed and documented.
- Define and assign clear roles and responsibilities for managing user accounts. This helps ensure that each step in the identity lifecycle is properly executed and controlled.
- Ensure that identity data, such as usernames, email addresses and employee numbers, are unique and well-secured. This is essential for authentication and authorisation within the organisation and helps prevent unauthorised access.
- Communicate the procedures and responsibilities around identity data management to all employees. This promotes compliance and awareness of the importance of good identity management within the organisation.

Mapping indication

ISO 27001: A.5.16
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 3, 4, 5, 12, 13
IEC 62443-2-1:2010, Clause 4.3.3.5.1, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
NIST SP 800-53: IA-2 - Identification and authentication (organisational users).

1.14 Access Privilege Management

The organisation shall implement a procedure to ensure that access rights are properly granted, modified, and removed. Records shall be maintained showing who has been granted logical and physical access rights and the date on which they were revoked.

Goal

Prevent an information security incident from occurring due to access rights being wrongly or incorrectly assigned to a user's account.

Focus points

- Register who has access to which information and assets, and define both logical and physical access rights. This helps to control and monitor access rights within the organisation.
- Establish a procedure and checklist for granting, changing and revoking access rights. This ensures that access rights are managed in a structured and consistent manner**.**
- When an employment relationship is terminated, ensure that all accounts are closed properly, and all access rights are revoked. This prevents unauthorised access after departure of a colleague.
- Create an authorisation matrix that makes clear which access rights belong to which role. Evaluate and update the authorisation matrix regularly to ensure that it remains up-to-date and matches the current roles and responsibilities within the organisation. This ensures that the access rights are always correct and relevant.

Mapping indication

ISO 27001: A.5.18
NIST SP 800-53: AC-2 - Account Management.

1.15 Protection of information in cooperation with suppliers

The organisation must define processes and procedures that enable the organisation to determine whether services and products from suppliers sufficiently meet the information security requirements of the organisation. If necessary, appropriate measures are taken to manage the risks.

Goal

Preventing an information security incident from occurring as a result of using defective services or products from a supplier.

Focus points

- Inventory the information security risks associated with the use of products and services from suppliers. This helps to identify possible threats and weaknesses.
- Assess the identified risks and prioritize them based on their severity and impact. This ensures that the most critical risks are addressed first.
- Take appropriate measures to mitigate the identified risks, such as implementing security protocols, updating contractual agreements, and working with suppliers to improve their security standards.
- Clearly communicate the established procedures and security measures to all relevant employees and suppliers. This promotes compliance and ensures that everyone is aware of the expectations and requirements for information security in the cooperation with suppliers.

Mapping indication

ISO 27001 A.5.19
IEC 62443-2-1:2010, Clause 4.3.4.2

1.20 Guidelines for dealing with information security incidents (cybersecurity incidents)

A plan should be drawn up that clearly states how the organisation deals with a suspected or confirmed breach of the availability, integrity or confidentiality of information. The plan clearly states who is responsible for each task.

Goal

Preventing information security incident handling from being inefficient, which could lead to the consequences of incidents to become unnecessarily large.

Focus points

- Develop an Incident Response Plan (IRP) that clearly describes how the organisation will handle information security incidents. This plan should include detailed steps for identifying, reporting, and resolving incidents.
- Define and assign clear roles and responsibilities for information security incident management. Ensure that everyone in the organisation knows who is responsible for which tasks in the event of an incident.
- Communicate the processes and responsibilities from the IRP to all employees. This ensures that everyone is aware of the procedures and knows what is expected of them in the event of an incident.
- Regularly test and evaluate the effectiveness of the Incident Response Plan. This helps to identify any weaknesses in the approach and ensures that the organisation remains prepared for new and emerging threats.

Mapping indication

ISO 27001: 5.24
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.2.5.7, 4.3.4.5.11
NIST SP 800-53: IR-8 - Incident response plan

1.23 ICT preparation for business continuity

The organisation must develop a plan that includes ICT continuity requirements, including objectives for the maximum recovery time of essential information systems. Technical and organisational measures are implemented to meet the ICT continuity requirements in the event of a disruption.

Goal

Prevent recovery times and data loss of essential information systems from not sufficiently aligning with the organisation's business continuity objectives in the event of a disruption.

Focus points

- Set objectives and continuity requirements for business continuity in the event of unexpected events, such as cyber attacks. This helps to be operational again quickly and minimize the impact on business operations.
- Develop a detailed business continuity plan that includes backup management, contingency planning, and crisis management. This plan should clearly describe how the organisation can continue its operations during and after an incident.
- Implement and maintain ICT readiness based on the established objectives and continuity requirements. This ensures that the technical infrastructure is ready to respond to disruptions.
- Test ICT readiness regularly to ensure that all systems and procedures work effectively during an incident. This ensures that the organisation can recover quickly and efficiently from unforeseen events.

Mapping indication

ISO 27001 A.5.30
NIST SP 800-53: CP-2 - Contingency Plan.

1.26 Securing the supply chain together

For the supply chain, the organisation must implement appropriate and proportionate technical, operational and organisational measures to prevent risks to the security of network and information systems. The measures for the supply chain must be based on an all-hazards approach that encompasses the protection of networks, information systems and the physical environment.

The focus should be on suppliers that pose risks to business continuity, particularly where they affect the Protected Interests ("crown jewels"): essential data, services, processes or systems whose compromise could cause significant harm.

The organisation must identify business risks associated with the use of suppliers' products and services within its policy. The organisation must set out this policy in writing and demonstrably apply it. Relevant agreements on digital resilience within the supply chain must be contractually established with suppliers. The corresponding measures must be demonstrably assured through proportionate certification or audits carried out by the organisation itself or by independent auditors.

Goal

To maintain the organisation's business processes and ensure the availability, integrity, and confidentiality of its information.

Focus points

- Identify the risks associated with your key suppliers (particularly those with an impact on the Protected Interests ("crown jewels")) to understand the threats to your organisation. This helps in identifying vulnerabilities within the supply chain.
- Establish agreements with suppliers on digital security, applying proportional and achievable standards in relation to the level of risk. This ensures that all parties follow the same practices and procedures to minimise cyber threats.
- Require suppliers to demonstrate their compliance with the requested standard. This may be done by providing a valid certificate or, if this is not yet available, by supplying evidence within the six-month initiation phase that they are actively working towards obtaining certification. Final certification must then be provided within one year.
- Inform recipients (individuals or organisations) in a timely manner about the control measures they can take in the event of a significant cyber threat within the organisation. This ensures a coordinated and effective response to potential threats.
- Review and update the risk assessment and supplier agreements annually.

Mapping indication

ISO 27001 A.5.21

1.27 Collecting evidence

The organisation must determine for which types of incidents which evidence must be collected and secured in order to determine the cause or to provide evidence to third parties.

Goal

Preventing the organisation from suffering damage because, after an information security incident, no information is available to determine the cause or to provide (legal) evidence to third parties.

Focus points

- Establish procedures for identifying, collecting and preserving evidence in the event of an information security incident. This ensures that there is a standardised approach that employees can follow in the event of an incident.
- Communicate these procedures clearly to all employees so that everyone knows how and when to collect evidence. This ensures a uniform approach within the organisation and contributes to an effective response to incidents.
- Determine and implement concrete measures to ensure an appropriate level of information security during an incident. This includes measures for availability, integrity and confidentiality of information.
- Regularly evaluate and update procedures and controls to ensure they remain up-to-date and aligned with the latest security standards and threats. This ensures that the organisation can respond effectively to incidents and maintain the integrity of evidence.

Mapping indication

ISO 27001 A.5.28
IEC 62443-3-3:2013, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1

ISO 27001 5.29
NIST SP 800-53: CP-2 - Contingency Plan.

2. People-oriented measures

2.2 Cybersecurity education for directors and employees

The organisation's directors and officers should receive training or instruction to help them identify and assess cybersecurity risks. Employees of the organisation should receive cybersecurity education and training appropriate to their roles and should be tested on their knowledge of the organisation's rules and procedures.

Goal

Preventing information security incidents from occurring due to a lack of awareness of information security risks, or a lack of knowledge of organisational rules and procedures.

Focus points

- Ensure that directors and executives receive training or courses to identify and assess cybersecurity risks. This strengthens their ability to take appropriate security measures and ensure a secure information environment.
- Implement video training modules and other forms of education for employees on digital security. This ensures that all employees are aware of the risks of information processing and know how to minimize them.
- Organise training courses that are tailored to specific functions within the organisation. This ensures that each employee has the right knowledge and skills required for their role in protecting information.
- Regularly test employee knowledge and policy compliance. This helps ensure that the knowledge gained is applied effectively and that employees adhere to established security guidelines.

Mapping indication

ISO 27001 A.6.3
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14, 16
IEC 62443-2-1:2010, Clause 4.3.2.4.2
NIST SP 800-53: AT-3 – Role-based training

2.6 Working from home or hybrid in a safe way

The organisation must formulate and communicate rules for safe information processing at remote locations. The organisation ensures that all employees know the rules for working at remote locations.

Goal

Prevent information security incidents from occurring due to employees accessing, processing or storing information in an insecure manner while working at remote locations.

Focus points

- Establish clear rules for secure information processing outside the physical business location, such as at home or at remote locations. This helps to sensitive facts at protect in return for cyber incidents.
- Implement security measures specifically for remote and hybrid work, such as using VPNs, encryption, and strong passwords. This will ensure data remains secure no matter where employees are located.
- Ensure all employees are aware of the rules and security measures for remote working. This can be done through training and regular communication on the latest safety guidelines.
- Regularly review and update the security measures and guidelines for home and hybrid working. This ensures that the measures remain effective and respond to new cyber threats.

Mapping indication

ISO 27001: A.6.7
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 5, 6, 13
IEC 62443-2-1:2010, Clause 4.3.3.6.6, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.13, SR 2.6
NIST SP 800-53: AC-17 - Remote Access.

2.7 Recording and reporting of information security events

The organisation shall make it clear to all employees how observed or suspected information security events can be reported promptly and through appropriate communication channels.

Goal

Prevent potential information security incidents from not being addressed or prevented in a timely manner because employees do not report observed or suspected information security events or report them too late.

Focus points

- Provide a clear and simple procedure for reporting cyber incidents so employees can quickly and effectively report threats to information security.
- Agree on the channels to be used for notifications, such as email, WhatsApp and telephone, to ensure a fast and reliable response.
- Consider using a digital reporting system or a specific app for more extensive and detailed reporting of cyber incidents. This can help to systematically record and follow up on reports.
- Ensure that there is a central reporting point within the organisation, such as the service desk or IT team, that is responsible for receiving and handling reports of information security incidents.

Mapping indication

ISO 27001: A. 6.8
IEC 62443-2-1:2010, Clause 4.3.4.5.9 IEC 62443-3-3:2013, SR 6.1
NIST SP 800-53: IR-6 - Incident Reporting.

3. Physical measures

3.5 Confidential Policy regarding Desks and Screens

The organisation shall formulate and communicate policies for locking active computer screens and removing paper and storage media containing confidential information from unattended workstations. The organisation shall ensure that all employees are aware of and comply with the policies for unattended workstations.

Goal

Prevent an information security incident from occurring due to someone misusing easily accessible information or an unlocked screen in an unattended workplace.

Focus points

- Establish clear rules for a " Clear Desk" policy, requiring employees are to securely store all paper documents and removable storage media when they leave their workstation. This prevents that sensitive information unattended and accessible stays.
- Implement a " Clear Screen" policy that requires computer screens to be locked when left unattended. This includes setting automatic screen locks after a specified period of inactivity.
- Communicate the Clear Desk and Clear Screen policies clearly to all employees and ensure regular repetition of their importance. This will increase awareness and ensure that everyone adheres to the rules.
- Monitor and enforce compliance with the Clear Desk and Clear Screen policies through regular checks and audits. This helps ensure that the rules are followed consistently, and that confidential information remains protected.

Mapping indication

ISO 27001: A.7.7

3.8 Safely Dispose or Reuse Company Equipment

The organisation must define and implement a process for the safe disposal or reuse of corporate devices that contain embedded storage media. The rules make it clear that sensitive data and software must be deleted or overwritten before a corporate device can be disposed of or reused.

Goal

Prevent an information security incident from occurring by removing or reusing a device that was found to contain information and/or licensed software.

Focus points

- Create a checklist for securely removing or overwriting sensitive information and software from storage media devices. This checklist will help verify that all sensitive data has been completely removed before the equipment is replaced or reused.
- Define clear rules and procedures for securely wiping data from devices such as computers, tablets and phones. This prevents sensitive information from accidentally being left behind and falling into the wrong hands.
- Communicate these policies and procedures to all employees and provide regular training on secure data disposal. This will promote compliance and ensure everyone is aware of the correct steps.
- Implement and use reliable software tools for secure data erasure or overwriting. Ensure that these tools are regularly updated and meet the latest security standards.

Mapping indication

ISO 27001: A.7.14
IEC 62443-2-1:2010, Clause 4.3.4.4.4 IEC 62443-3-3:2013, SR 4.2
NIST SP 800-53: MP-6 - Media Sanitization.

3.9 Define Access Control

Based on predefined roles, the organisation should determine the access rights appropriate to each role, limited to the needs of that role.

Goal

Preventing information security incidents from occurring due to individuals having unnecessary access to certain information or other company resources.

Focus points

- Establish clear access rules that determine who has access to which sensitive information and assets. This helps prevent unauthorised access and ensures security.
- Create an autorisation matrix that makes clear which access rights belong to which role. Evaluate and update the authorisation matrix regularly to ensure that it remains up-to-date and matches the current roles and responsibilities within the organisation. This ensures that the access rights are always correct and relevant.
- Register and monitor access to sensitive assets so you know who accessed them and when. This provides a detailed overview and helps detect unauthorised access.
- Regularly evaluate and update access policies and security controls to ensure they remain effective and aligned with changing business needs and threat landscape.

Mapping indication

ISO 27001: A.5.15
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 6, 7, 12, 13, 16
IEC 62443-2-1:2010, Clause 4.3.3.7.3
IEC 62443-3-3:2013, SR 2.1
NIST SP 800-53: AC-3 – Access enforcement.

4. Technological measures

4.1 Security and management of user devices

Corporate devices used by employees and contractors (such as PCs, laptops, phones and tablets) must be secured against unauthorised use, unauthorised installation of software and unauthorised changes to security settings.

Goal

Prevent an information security incident from occurring due to a user device being insufficiently secured, or the corporate network being insufficiently secured against insecure user devices.

Focus points

- Maintain an up-to-date list of all user devices within the organisation and continuously monitor security configurations. This helps to stay one step ahead of potential threats and ensure devices are as secure as possible.
- Implement measures such as laptop encryption, restricting admin rights and requiring strong passwords and PINs. This will ensure that employee devices are well protected against cyber incidents.
- Communicate clear rules and security requirements for the use of user devices to all employees. Ensure everyone is aware of the procedures for protecting their devices and the risks of unautorised access.
- Regularly manage and update the security settings of all devices, including installing software updates and enforcing security protocols. This ensures that devices are always well protected against new threats.

Mapping indication

ISO 27001: A.8.1

4.4 Malware Control and Prevention

The organisation shall implement anti-malware measures, including technical measures for the timely detection and neutralisation of malware.

Goal

Preventing an information security incident from occurring due to malware compromising the availability, integrity or confidentiality of information.

Focus points

- Install and maintain reliable anti-malware software, virus scanners and spam filters on all systems within the organisation. This helps to protect the digital environment from malicious software and unwanted e-mails.
- Consider using encryption for important documents and sensitive information. This ensures that even if unauthorised access is obtained, the information cannot be read without the correct encryption keys.
- Train employees regularly to recognize and prevent malware attacks. This increases awareness of the risks and ensures that everyone in the organisation knows how to safely deal with digital threats.
- Have a policy and procedure in place to combat malware, including regularly updating security software and performing system scans. This ensures that malware protection remains up-to-date and effective against new threats.

Mapping indication

ISO 27001: A.8.7
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 10, 13
IEC 62443-2-1:2010, Clause 4.3.4.3.8
IEC 62443-3-3:2013, SR 3.2
NIST SP 800-53: SI-3 - Malicious code protection.

4.5 Backup and recovery

Backups of information and systems should be made according to a defined backup plan. Backups are tested to ensure they are valid when they are needed.

Goal

Preventing critical information from becoming permanently unavailable due to a malicious attack, human error, disaster, or other cause.

Focus points

- Set up a comprehensive backup policy according to the 3-2-1 system, where you keep three copies of the data on two different media, one copy of which is offsite. This ensures that the data remains safe and accessible in the event of a disaster.
- Make regular backups of all important data and systems, such as customer data, financial administration and databases. This ensures that a recent copy is always available in case of data loss.
- test backups for reliability to ensure they are working correctly, and that data can be restored if necessary. This prevents surprises when a recovery is necessary.
- Clearly communicate responsibilities within the backup process, including who is responsible for performing, monitoring, and testing backups. This will ensure a structured approach and prevent data loss due to human error.

Mapping indication

ISO 27001 A.8.13
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 11
IEC 62443-2-1:2010, Clause 4.3.4.3.9
IEC 62443-3-3:2013, SR 7.3, SR 7.4
NIST SP 800-53: CP-9 – System backup

4.7 Keeping software on assets up to date

The organisation shall define and implement a policy for keeping software on all assets up to date and secure at all times.

Goal

Preventing an information security incident from occurring due to an unpatched software vulnerability.

Focus points

- Implement procedures for automatically updating software on all computers and devices. This ensures that updates are installed as quickly as possible without requiring manual intervention by employees.
- Establish guidelines for safely updating software, including the frequency and methods for installing updates. This helps protect systems from new threats and vulnerabilities.
- Communicate the importance of regular software updates to all employees and ensure they are aware of the procedures. This will promote compliance and ensure all devices are kept up to date.
- Work with external vendors to update operational systems as needed and ensure that the integrity and operation of the systems is maintained. This can improve efficiency and ensure that updates are performed correctly and in a timely manner.

Mapping indication

ISO 27001: A.8.19
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 7, 4, 12
IEC 62443-2-1:2010, Clause 4.3.4.3.2, 4.3.4.3.3
IEC 62443-3-3:2013, SR 7.6

4.9 Network segmentation

The organisation shall establish and implement rules for segmenting groups of users, information systems, and information services in the organisation's networks.

Goal

Network segmentation improves information security by isolating sensitive data and critical systems, limiting unauthorised access, and minimizing the impact of cyberattacks. This prevents threats from spreading throughout the network and helps with targeted protection of specific network areas.

Focus points

- Split the network into specific segments, such as separate WiFi segments, VLANs, Firewalls, or Subnets. This helps isolate problems in one part of the network and prevents them from affecting the entire network.
- Establish clear rules and procedures for network segmentation, defining how and why segments are created. This provides a structured and targeted approach to network management.
- Work with your IT vendor to implement network segmentation. This will ensure that segmentation is done correctly and meets the latest security standards.
- Regularly evaluate and update network segmentation to ensure it continues to meet the changing needs of the organisation and new security challenges. This guarantees that the network effective and safe stays.

Mapping indication

ISO 27001: A.8.22
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 7, 12, 16
IEC 62443-2-1:2010, Clause 4.3.3.4
IEC 62443-3-3:2013, SR 3.1, SR 3.8

4.10 Implement authentication methods

The organisation must ensure that the authentication methods used are appropriate for the sensitivity of the information being accessed. At a minimum, MFA must be implemented for accounts with administrative rights, when accessing systems with sensitive information, and for all users who log in via the Internet.

Goal

Preventing an information security incident from occurring due to an insecure authentication method being used when logging in.

Focus points

- Implement multi-factor authentication (MFA) for all accounts with administrative rights and access to systems with sensitive business information. This provides an additional layer of security that makes unauthorised access more difficult.
- Use authentication methods that are appropriate for the sensitivity of the information and systems being accessed. Always equip critical systems with MFA or continuous authentication solutions to strengthen security.
- Ensure that users who log in via the internet also use MFA. This protects the systems from attacks where passwords may be compromised.
- Secure communication channels such as voice, video and text communication with secure protocols. Ensure that emergency communication systems are also well secured to ensure reliable communication during incidents.

Mapping indication

ISO 27001: A.8.5
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 5, 6, 13
IEC 62443-2-1:2010, Clause 4.3.3.6.6, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.13, SR 2.6
NIST SP 800-53: IA-2 - Identification and authentication (organisational users).

4.11 Log files

The organisation shall record and analyse log files of relevant events. Based on a risk assessment, the organisation has determined what are relevant events and how the recorded log files should be analysed.

Goal

Prevent important information security events from being detected too late, or from not being detected because the necessary log files are not available.

Focus points

- Establish rules for creating, storing, and protecting log files. This ensures that all activities, exceptions, and errors are carefully recorded and protected from unauthorised access and modification.
- Implement a central repository for log files where they can be stored securely and easily accessed for analysis. This will increase efficiency in investigating irregularities and taking corrective action.
- Regularly analyse log files to detect anomalous behavior in networks, systems, and applications at an early stage. This helps to proactively identify and address potential threats and security incidents.
- Synchronize the system time of all systems that keep logs to UTC time. This ensures consistency in timekeeping and facilitates log analysis.
- Monitor and restrict access to logs to prevent unauthorised changes. Ensure logs are retained for at least 30 days to ensure sufficient historical data is available for in-depth analysis.

Mapping indication

ISO 27001: A.8.15
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 3, 4, 8
IEC 62443-2-1:2010, Clause 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.4
IEC 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
NIST SP 800-53: AU-2 – Event logging.

5. OT measures

5.1 Register of all OT assets

The organisation shall establish and maintain a list of OT assets, including relevant configuration data, such as software versions and patch levels. An owner (manager) shall be appointed for each asset.

Goal

Preventing information security incidents from occurring due to unidentified and unowned OT assets, and therefore not being managed securely.

Focus points

- Establish a detailed register of all OT assets within the organisation, including both hardware and software components. This provides a complete overview of all operational technologies in use.
- Also, document in the registry the specific software versions and current patch levels of each OT component. This helps identify potential security risks and ensures that all systems are up to date.
- Create an overview of all network connections and external links to the corporate network. This provides insight into the entire OT infrastructure and helps manage both internal and external security risks.
- Review and update the register regularly to ensure that all information remains accurate and up-to-date. This is essential for identifying emerging risks in a timely manner and effectively managing OT assets.

Mapping indication

BIACS:

121, 124: 2.8.2.1 Change measures in a controlled manner.
50: 2.4.2.1 Network connection measures.
132: 2.9.2.1 Management and maintenance measures.

5.2 Determine the dependency on OT assets

The organisation must define for each OT asset how dependent the organisation is on it, what the probability of failure is, and what the impact is in the event of a failure.

Goal

Identifying risks associated with OT system failures in order to manage these risks with appropriate controls and priority.

Focus points

- Identify per OT system how critical it is to the operational processes of the organisation. This helps to prioritize the management and security of these systems.
- Perform a risk analysis for each OT system, assessing the likelihood of failure and the potential impact to the organisation. Use the probability x impact formula to quantify and prioritize risks.
- Document the findings of the risk analysis in an overview that clearly indicates which OT systems are most critical to the organisation. This overview supports strategic decisions about maintenance and investments.
- Keep the overview of dependencies and risks up-to-date by regularly reviewing the risk analysis. This ensures that the organisation remains prepared for changes in the technology or business environment that may affect the dependency on certain OT systems.

Mapping indication

BIACS:

130: 2.9.2.1 Management and maintenance measures.
139: 2.10.2 Backup measures.

5.4 Backups of OT systems

Backups of OT systems should be made according to a defined backup plan. Backups are tested to ensure they are valid when they are to be used.

Goal

Prevent OT systems from becoming unavailable due to malicious attack, human error, disaster, or other cause.

Focus points

- Make regular backups of the configuration settings and operational parameters of all OT systems. This ensures that the systems can be quickly and effectively restored after technical problems or a cyber attack.
- test the backups you have created to verify that they are functioning correctly and can actually be restored. This ensures that the backups are reliable and can be used in the event of an incident.
- Ensure that backups are updated regularly to reflect the latest configurations and operational parameters. This prevents outdated information from being restored, which could lead to further problems.
- Store backups in a secure location, separate from operational systems, to minimize the risk of data loss due to physical damage or cyberattacks. This contributes to the continuity and security of the organisation.

Mapping indication

BIACS:

143, 144, 145: 2.10.2 Backup measures

5.5 Recovery plan OT systems

The organisation must develop a business continuity plan that includes continuity requirements for disruptions, including the accepted recovery time of essential OT systems. Technical and organisational measures are implemented to meet the OT continuity requirements in the event of a disruption. The effectiveness of these measures has been tested.

Goal

Preventing the recovery times of essential OT systems from not sufficiently matching the continuity objectives of the organisation in the event of a disruption.

Focus points

- Create a detailed recovery plan that outlines the steps for quickly and effectively recovering systems after a failure or cyberattack. This plan should also clearly define the roles and responsibilities of all stakeholders, including external parties.
- Perform periodic tests of the recovery plan to verify that the process is effective and that all necessary resources, such as configurations, documentation, and spare parts, are available. If performing actual tests is too risky, perform a dry run or simulation to test the recovery process without actually affecting the systems.
- Document and communicate the recovery plan to all relevant employees and external parties. This ensures that everyone knows exactly what needs to be done during an incident and that the continuity of the business processes is guaranteed.
- Evaluate and update the recovery plan regularly, especially after major system updates or upgrades. This ensures that the plan remains up-to-date and can be effectively applied in the event of any future outages or attacks.

Mapping indication

BIACS:

40, 41: 2.3.2 Security incident measures and incident response plan.

5.11 OT system overview and additional information

The organisation shall establish and maintain an overview of all OT systems, including information on hardware, software, firmware, configurations, security settings, suppliers and maintenance. An owner (manager) is appointed for each OT system.

Goal

For an organisation, an overview of OT systems and their specific information is important for information security, because it provides insight into possible vulnerabilities. This facilitates risk management, incident response and the protection of critical infrastructure against cyber attacks or technical failures.

Focus points

- Keep accurate records of versions and revisions of all OT equipment and components in use. This is essential to respond quickly and effectively to security issues and to ensure that updates are performed efficiently.
- Document vendor information for each OT device, including manufacturer and contact information. This allows the organisation to quickly obtain support, receive updates, and learn about known issues or vulnerabilities.
- Update the overview of versions, revisions and vendor information regularly, especially after system updates or when new equipment is installed. This ensures that the organisation always has the most up-to-date information.
- Use this information to optimize maintenance planning and anticipate potential problems. This helps minimize risks and ensure continuity of operational processes.

Mapping indication

BIACS:

121, 124: 2.8.2.1 Change measures in a controlled manner.
132: 2.9.2.1 Management and maintenance measures.

6. IT measures

6.1 Access to source code

The organisation shall protect access to source code and software libraries from unauthorised access and unwanted modification.

Goal

Preventing an information security incident from occurring due to unauthorised or improperly configured access to source code or software libraries.

Focus points

- Implement strict version control for source code, so that all changes are accurately tracked. This ensures that developers can always fall back on previous versions and that the full history of changes is visible.
- Implement robust access control mechanisms for the source code, allowing only authorised individuals access to specific parts of the code. This prevents unauthorised access and protects the integrity of the software.
- Use a reliable version control system such as Git, SVN, or BitBucket, and leverage features such as branching and CI/CD pipelines to ensure the quality and security of your source code.
- Monitor and evaluate the effectiveness of version control and access control on a regular basis. Ensure that these mechanisms remain up-to-date and comply with the latest security standards, so that the integrity and security of the software is continuously guaranteed.

Mapping indication

ISO 27001: 8.4

6.3 Developing secure software

The organisation shall establish best practices for developing secure software. Compliance with these best practices shall be monitored.

Goal

Prevent a bug, logical error or other vulnerability from being present in software created by the organisation and leading to an information security incident when the software is used.

Focus points

- Ensure that architecture guidelines are consistently applied throughout the development process. This ensures that the software is scalable, maintainable and of high quality.
- Follow OWASP guidelines, especially the OWASP Top 10, when developing web applications. This helps identify and mitigate the biggest security risks, making the software more secure against cyber threats.
- Integrate the architecture guidelines and OWASP guidelines into the development process by means of design patterns and best practices. This not only promotes security, but also the efficiency and quality of software development.
- Monitor and evaluate compliance with these guidelines and recommendations on a regular basis. Ensure developers are kept up to date with the latest architecture guidelines and OWASP updates so that software continues to meet the highest security standards.

Mapping indication

ISO 27001: A.8.27

6.9 Software Delivered Overview

The organisation must establish and maintain an overview of all customers who use software created by the organisation. This overview should clearly indicate which customer is using which version of each software product.

Goal

An up-to-date overview of customers and their software versions helps the organisation to quickly identify vulnerable or outdated software, efficiently apply security patches and manage incidents. This minimizes security risks and provides better protection against potential threats to customers.

Focus points

- Create a detailed customer database where you record which software and versions are used by each customer. This helps in accurately planning maintenance, updates and license management.
- Link customer information to specific software versions and licenses, so you can effectively monitor which customers have access to which software. This is crucial for managing licenses and adhering to contractual agreements.
- Use the collected data to analyse the impact of new versions, patches, or updates. This allows you to understand the scope of changes and provide targeted support to customers who may be affected.
- Regularly update and check the customer database to ensure that all information remains up-to-date. This ensures an efficient maintenance process and helps minimize errors in license management and software updates.

Mapping indication

No Mapping indication available.

6.12 Customer coordination of new software and updates

The organisation shall define and implement a process for installing new software versions or patches in consultation with customers.

Goal

Preventing information security incidents from occurring due to insufficient coordination with customers regarding the installation of new software or patches.

Focus points

- Identify the target group of customers who need the new version or patch, and establish a timeline for the rollout. This helps minimize the impact on customers and provides a structured approach to rolling out updates.
- Proactively inform customers about the availability, content and benefits of the new version or patch. Provide clear instructions for implementation if necessary, so that customers are well prepared for the changes.
- Automate as much as possible the process of distributing and installing new versions and patches. This reduces the time needed to implement improvements and reduces the risk of errors during installation.
- Provide a standardised release and patching roadmap that includes the identification, communication, and distribution phases. This ensures a consistent process that is efficient and effective in rolling out improvements to customers.

Mapping indication

No Mapping indication available.

Copyright

Explanation of Mapping indication

Our cybersecurity standard is the result of extensive collaboration between a diverse team of cybersecurity experts. This multidisciplinary team included representatives from NIS2 organisations, SMEs, independent cybersecurity specialists, and auditors. This diverse composition ensured that our standard encompasses a wide range of perspectives and expertise, resulting in a unique and highly valuable approach to cybersecurity. While our standard may overlap with other cybersecurity standards in some areas, users should understand that our standard is a standalone product developed to address the specific needs and challenges of modern businesses. The content and approach of our standard may therefore differ from other standards, even if some similarity exists. It is important to emphasize that our standard is designed to encompass cybersecurity best practices, based on the insights and experiences of our diverse team members. Therefore, users should view our standard as a unique tool designed to maximize value and effectiveness for organisations striving for improved cybersecurity.

Disclaimer