NIS2 Quality Mark

NIS2-QM30 HIGH

Version 3.0
October 16, 2024

NIS2 QUALITY MARK

Contents

This is the NIS2-QM30 High 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 3.0 © 2024

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 ensures continued effectiveness and relevance.

Mapping indication

ISO 27001: A.5.1 – Information security policies.
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 - Roles and responsibilities
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

1.4 Management Direction

The organisation's management must explicitly require all employees, including all new employees, to work in accordance with the organisation's information security policies and procedures.

Goal

Preventing information security incidents from occurring due to management's insufficient (visible) support for the communicated rules and procedures regarding information security.

Focus points

- Actively involve management in the monitoring and compliance of information security measures. Management should receive regular reports and ensure that all employees are familiar with the requirements and are involved in their implementation.
- Clearly communicate to all employees the importance of information security and the specific policies and procedures that must be followed. Ensure that sufficient resources, such as time, money and training, are made available to ensure compliance with information security policies.

Mapping indication

ISO 27001 A.5.4 – Management responsibilities.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 6
IEC 62443-2-1:2010, Clause 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3

1.5 Security Threat Assessment and Understanding

The organisation should regularly consult appropriate sources to stay informed about threats that may be relevant to information security. Additional measures are taken as needed to protect against new or changing threats.

Goal

Preventing an information security incident from occurring because the organisation missed threat information that was available.

Focus points

- Ensure that the organisation actively collects information about potential information security threats, both by human analysts and by automated systems. This helps to get a broad overview of possible risks.
- Perform thorough analyses of the collected threat information to understand the meaning and impact of the threats. Ensure that employees are adequately trained to perform these analyses and recognize relevant signals.
- Use the analysed threat information to develop your own threat profiles and use them to strengthen information security. Document the measures taken to demonstrate that the threat information is used effectively.
- Regularly evaluate the threat assessment and analysis process to ensure it remains up-to-date and aligned with the changing threat environment. This promotes a proactive approach to information security within the organisation.

Mapping indication

ISO 27001: A.5.7 - Threat intelligence and analysis.
NIST SP 800-53: RA-5 - Vulnerability monitoring and scanning.

1.6.1 Information Overview

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

- Provide a complete and reliable overview of all information, assets and assets of the organisation, including customer data, contracts, personnel, machines, equipment and buildings. This overview helps to effectively manage and secure these resources.
- Establish an information register in which all information data is documented, including where the information is stored, in what form, who works with it, and how long it should be kept. This ensures structured management of information.
- Assign clear owners or administrators for each component within the information repository. These individuals are responsible for the proper management and security of their assigned information and assets.
- Review and update the policy and information register regularly to ensure that it is always complete, correct and up to date. This ensures that the security measures remain up to date and effective.

Mapping indication

ISO 27001: A.5.9 – Inventory of information and other related assets.
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 ICT Assets Overview

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

- Inventory 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 – Inventory of information and other related assets.
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 network equipment and cloud services. This helps prevent misuse and ensures the integrity of the information.
- Communicate these rules and procedures effectively to all employees so that everyone is aware of how to use information and assets safely. This promotes compliance and awareness within the organisation.
- 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 - Acceptable use of information and other related assets.
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

Preventing 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

- Inventory 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 - Return of company assets.

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 - Classification of information.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 12
NIST SP 800-53: RA-2 - Security categorization

1.11 Transferring information within the organisation and to third parties

The organisation must establish rules that make clear which resources and external parties may be used for the secure transfer of confidential information within the organisation, and between the organisation and other parties. The organisation ensures that employees are aware of the rules for transferring information.

Goal

Preventing an information security incident from occurring as a result of insecure, incorrect or unreliable transmission of information.

Focus points

- Establish clear rules and procedures for the secure transfer of information, both internally within the organisation and externally to third parties. This ensures that the availability, integrity and confidentiality of information is guaranteed during the transfer.
- Communicate the established rules and procedures to all employees and, if necessary, to external parties such as customers and suppliers. This promotes compliance and ensures that everyone is aware of the correct ways to transfer information securely.
- Distinguish between different types of information transmission, such as electronic (email, social networks), physical (paper documents, USB sticks) and oral transmission (telephone conversations, face-to-face conversations). This helps specify security measures for each transmission method.
- Regularly check that the rules and procedures are effectively followed and that they are up to date. This ensures that the information transfer remains consistently secure, even when new means of communication or threats emerge.

Mapping indication

ISO 27001 A.5.14 - Transfer of information.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 12
IEC 62443-2-1:2010, Clause 4.2.3.4
NIST SP 800-53: SC-8 - Transmission confidentiality and integrity .

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 policies and procedures for managing identity data, including the registration, modification and deletion of this data. This ensures structured management of the identity of personnel throughout the entire lifecycle.
- Define and assign clear roles and responsibilities for managing the authentication process and identity lifecycle. This ensures that the process is well managed and that each step is performed accurately.
- Ensure that policies and procedures cover all aspects of identity management, such as usernames, email addresses and employee numbers. This will help ensure secure and consistent authentication across the organisation.
- Communicate policies and procedures to all relevant employees to ensure everyone is aware of the correct processes and responsibilities. This promotes compliance and helps manage identity data effectively.

Mapping indication

ISO 27001: A.5.16 – Identity management.
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 properly closed and all access rights are revoked. This prevents unauthorised access after an employee has left.
- Regularly evaluate and update the authorisation matrix to ensure it remains up-to-date and aligned with current roles and responsibilities within the organisation. This ensures that access rights are always correct and relevant.

Mapping indication

ISO 27001: A.5.18 – Access rights.
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 - Information security in supplier relationships.
IEC 62443-2-1:2010, Clause 4.3.4.2

1.16 Ensuring information security in agreements with suppliers

The organisation must define processes and procedures that enable the organisation to determine whether the guarantees offered by suppliers sufficiently meet the information security requirements of the organisation. If necessary, additional agreements are agreed upon.

Goal

Preventing information security incidents from occurring as a result of unclear information security agreements with suppliers.

Focus points

- Establish clear security requirements and responsibilities in agreements with suppliers. This ensures that both parties know exactly what is required to ensure information security and who is responsible for its implementation.
- Make concrete agreements with suppliers about the measures that are jointly taken to mitigate cyber risks. This helps to effectively address existing security risks and guarantee the security of shared information.
- Ensure that employees who draft agreements with suppliers have sufficient knowledge of information security and the relevant legislation. This prevents important security aspects from being overlooked when concluding contracts.
- Use a checklist to check whether all necessary security measures are included in the agreements and whether logical access rights are properly recorded. This helps to systematically record agreements and prevents suppliers from having too much freedom in choosing security measures.

Mapping indication

ISO 27001: A.5.20 - Addressing information security issues in supplier agreements.
IEC 62443-2-1:2010, Clause 4.3.2.6.4, 4.3.2.6.7.

1.18 Supervision, evaluation and change management of supplier services

The organisation must use a risk assessment to decide which service suppliers need extra monitoring. These selected suppliers are regularly evaluated to check if the reliability and security of their services meet both the agreed-upon terms and the organisation's current requirements.

Goal

Preventing an information security incident from occurring due to an unexpected change in a supplier’s approach to information security or service provision.

Focus points

- Conduct regular reviews and evaluations of suppliers' information security practices and services, either through internal audits or external audits, to ensure compliance with contractual security requirements.
- Establish a clear process for monitoring and managing changes to vendor services. This helps ensure that any changes to their business operations or security measures do not negatively impact information security.
- Document information security practices and service standards in vendor agreements. This makes them easier to audit and provides a clear basis for evaluations.
- Systematically evaluate the results of supplier assessments and take action on deficiencies. This can range from conducting corrective interviews to terminating contracts, if necessary, to ensure the organisation's level of security.

Mapping indication

ISO 27001: A.5.22 - Monitoring, reviewing and controlling changes to supplier services.
IEC 62443-2-1:2010, Clause 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14.

1.19 Keeping information secure when using cloud services

The organisation shall define processes that enable the organisation to determine whether safeguards provided by cloud service providers adequately meet the organisation's information security requirements.

Goal

Preventing the use of a cloud service from leading to information security incidents or non-compliance with contractual or legal obligations.

Focus points

- Establish clear processes for purchasing, using, managing and terminating cloud services. This ensures that all aspects of cloud use within the organisation are structured and secure.
- Define and document the responsibilities of both the organisation and the Cloud Service Providers (CSPs). This helps to avoid misunderstandings and ensures that security measures are applied consistently.
- Conduct regular evaluations of the performance and security of the CSPs to ensure they continue to meet the organisation's information security requirements. This can be done through scheduled check-ins and reviews from various departments such as IT and procurement.
- Develop a specific process for safely terminating cloud services, including support for moving from one CSP to another. This process should take into account the challenges of data transfer and system adaptation, so that business continuity is maintained.

Mapping indication

ISO 27001:5.23 - Information security for the use of cloud services.

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 cause 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 - Planning and preparation for information security incident management.
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

1.21 Recording, assessment and handling of information security incidents

The organisation shall assess events relating to information security to determine whether they constitute incidents. Incidents relating to the availability, integrity or confidentiality of information shall be recorded and handled in accordance with documented procedures.

Goal

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

Focus points

- Record each information security event and determine whether it is an anomaly, event or incident. This helps to correctly categorize and prioritize security issues and contributes to an effective security strategy.
- Carefully assess each unusual event to determine whether action is required. This ensures that not every event is treated as an incident unnecessarily, but that attention is paid to potential risks.
- Handle incidents according to established procedures and ensure that all steps, from registration to handling, are well documented. This guarantees a structured and consistent approach to security incidents.
- Report all incidents and deviations to management, so that there is insight into the security situation and adjustments can be made at a strategic level if necessary. This ensures good communication and management involvement in information security.

Mapping indication

ISO 27001:5.25 - Assessment and decision-making on information security events.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 13
NIST SP 800-53: IR-4 - Incident handling.

1.22 Incident reporting to external parties

The organisation has and uses a documented procedure to report incidents relating to the availability, integrity or confidentiality of information to external parties, in accordance with legal and contractual requirements.

Goal

Preventing reputational or financial damage from occurring because the handling of information security incidents is not sufficiently aligned with the legal and contractual obligations relevant to the organisation.

Focus points

- Establish clear procedures for reporting and responding to information security incidents, including steps for both inside and outside regular business hours. This helps the organisation respond to incidents quickly and effectively, minimizing their impact.
- Ensure that incidents with significant consequences, such as major operational disruptions or financial damage, are reported to the CSIRT and the competent authorities in a timely manner. This contributes to a coordinated and legally compliant approach to serious incidents.
- Communicate the established procedures clearly to all employees, so that everyone knows how to act in the event of a cyber incident. This increases preparedness and ensures that incidents are dealt with adequately, regardless of when they occur.
- Provide new employees with targeted training on procedures for dealing with information security incidents. This ensures that they too are well prepared to respond to security incidents and contribute to the overall security of the organisation.

Mapping indication

ISO 27001:5.26 - Information security incident assessment and resolution.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.1
NIST SP 800-53: IR-4 - Incident handling.

1.23 ICT preparation for business continuity

The organisation must develop a business continuity 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 - ICT readiness for business continuity.
NIST SP 800-53: CP-2 - Contingency Plan.

1.24 Objective assessment of the information security approach

The organisation must conduct an independent assessment at planned intervals to determine whether the information security approach is sufficiently meeting the information security objectives as set out in the information security policy. If it is found that the strategy is inadequate, management will take corrective measures.

Goal

To ensure that the organisation continues to implement an appropriate and effective approach to information security management.

Focus points

- Schedule regular independent assessments, such as external audits, to verify the organisation's compliance with information security requirements. This helps to obtain an objective evaluation of current measures and processes.
- Establish clear audit criteria that auditors can use to assess the effectiveness of information security controls and business continuity. This ensures a structured and consistent assessment.
- Ensure that the auditors have the appropriate competencies and knowledge of the sector in which the organisation operates. This ensures that the assessment is thorough and relevant, and that the recommendations are valuable to the organisation.
- Implement improvements based on the results of the audits. This ensures that the organisation continuously improves its information security practices and business continuity plans and adapts to new challenges and threats.

Mapping indication

ISO 27001:5.35 - Independent assessment of information security.
NIST SP 800-53: CA-2 - Control assessments.

1.25 Independent assessment of information security

The organisation must conduct an independent assessment at planned intervals to determine whether the organisation is operating in accordance with the requirements of the NIS2 Quality Mark standard, and in accordance with the organisation's own information security requirements in the form of internal rules, agreements, processes and procedures.

Goal

Preventing information security incidents from occurring due to insufficient compliance with or application of rules, agreements, processes and procedures.

Focus points

- Establish a clear information security policy, including vulnerability reporting procedures, and ensure that these are regularly tested for currency and compliance. This will help maintain a consistent and effective level of security across the organisation.
- Check at fixed times whether all agreements and rules from the information security policy are strictly adhered to. This ensures that the information within the organisation remains safe and that potential weak points are identified in time.
- Report the results of these checks and tests to management. This promotes management involvement and ensures that necessary actions can be taken quickly to strengthen information security.
- Regularly assess the effectiveness of the management measures laid down in the information security policy. This ensures that the measures continue to meet the changing demands and threats in the digital environment.

Mapping indication

ISO 27001: 5.36 - Compliance with information security policies, rules and standards.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2, 4, 5, 16, 18

1.26 Securing the supply chain together

The organisation must determine the information security risks associated with the use of ICT products and ICT services from suppliers, or from suppliers further down the supply chain. Relevant agreements regarding information security in the ICT supply chain have been agreed with the organisation's suppliers.

Goal

Preventing an information security incident from occurring as a result of using a defective service or product from suppliers, or from suppliers deeper in the supply chain.

Focus points

- Assess the risks of your key suppliers to understand the threats to your organisation. This helps identify weak points in the supply chain.
- Make joint agreements with suppliers on digital security. This ensures that all parties follow the same standards and procedures to minimize cyber threats.
- Inform recipients (individuals or organisations) in a timely manner about the control measures they can take in the event of a significant cyber threat in the organisation. This ensures a coordinated and effective response to potential threats.
- Evaluate and update the risk inventory and agreements made with suppliers regularly. This ensures that the security measures remain up-to-date and are effective against new threats.

Mapping indication

ISO 27001: A.5.21 – Information security management in the ICT supply chain.

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 - Collection of evidence.
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 - Information security during a disruption.
NIST SP 800-53: CP-2 - Contingency Plan.

2. People-oriented measures

2.1 Confidentiality obligation in employment contracts

All forms of employment contracts must include a confidentiality obligation.

Goal

Prevent an employee from sharing confidential information with unauthorised persons and thereby causing an information security incident.

Focus points

- Include explicit information security responsibilities for employees in all employment contracts. This ensures that all employees are aware of their obligations and what is expected of them to ensure information security.
- Include a code of conduct in employment contracts that includes specific information security guidelines. This will make the contract more transparent and provide detailed instructions for adhering to security protocols.
- Ensure that information security responsibilities are clearly communicated to all employees, including temporary workers, contractors and volunteers. This helps maintain a uniform standard for information security across the organisation.
- Regularly check whether the provisions in the employment contracts are up-to-date and in line with current information security requirements and standards. This ensures that the agreements remain relevant and effectively contribute to the security of the organisation.

Mapping indication

ISO 27001: A.6.2 - Employment contract.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 6
IEC 62443-2-1:2010, Clause 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3

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 - Information security awareness, education and training.
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

2.4 Ongoing confidentiality obligations after termination or change of employment relationship

It must be agreed with employees and temporary workers that a duty of confidentiality continues to apply after termination or change of their employment, contract or agreement.

Goal

Preventing an information security incident from occurring because someone feels free to share sensitive company information after termination or modification of an employment relationship, contract or agreement.

Focus points

- Include in the employment contract which responsibilities and tasks in the area of information security continue to apply after the departure or change of function of an employee. This helps to ensure the security of sensitive information, even after someone leaves the organisation.
- Communicate clearly with departing or internally moving employees about their ongoing responsibilities, such as confidentiality and the correct handling of confidential data. This ensures that they are aware of their obligations, even after the termination or change of their employment.
- Ensure that procedures are in place to maintain these ongoing responsibilities, for example by including a confidentiality agreement in the exit interview or by providing written confirmations. This provides a legal framework that protects the organisation from potential data breaches or misuse of information.
- Regularly check whether the agreements on continuing responsibilities are still up-to-date and effective, and adjust them if necessary. This ensures that the organisation remains protected, regardless of changes in staff composition.

Mapping indication

ISO 27001: A.6.5 - Responsibilities after termination or change of employment.
NIST SP 800-53: PS-4 - Personnel Termination.

2.5 Confidentiality Agreements

The organisation must ensure that employees and contractors sign a confidentiality agreement, which stipulates that confidential information exchanged during the collaboration may not be disclosed to third parties.

Goal

Prevent an employee or temporary worker from sharing confidential information with unauthorised persons and thereby causing an information security incident.

Focus points

- Formulate clear data protection agreements that specifically address how information is to be handled and the obligations of employees and other data subjects. Ensure that these agreements include both confidentiality and non-disclosure aspects, depending on the sensitivity of the information.
- Ensure that all employees and relevant stakeholders sign these agreements before accessing sensitive information. This provides legal certainty and emphasizes the responsibility of all parties to handle information with care.
- Implement a process to regularly review and update data protection agreements. This can be done through annual reviews or internal audits to ensure that the agreements remain up to date and in line with changing requirements and circumstances.
- Use a digital system to send reminders for periodic reviews and updates of the agreements. This helps to remain consistent in ensuring data protection within the organisation.

Mapping indication

ISO 27001: A.6.6 - Confidentiality or nondisclosure agreements.

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 protect sensitive data from 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, regardless of 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 - Remote working.
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 Information Security Event Reporting

The organisation shall make it clear to all employees how to report observed or suspected information security events 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

- Incidents or vulnerabilities that threaten information security must be quickly detected and communicated, especially during the development and maintenance of network and information systems.
- Ensure that cyber incident reporting can be done easily and quickly via internal communication channels such as email, WhatsApp, and telephone for an immediate response.
- Consider implementing a digital reporting system or app to enable detailed reporting of information security threats and rapid response.
- Ensure that all employees have clear instructions on how to report security issues, and that these reports are received and handled by a designated reporting point within the organisation.

Mapping indication

ISO 27001: A.6.8 - Reporting of information security events.
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.

2.8 Background checks on candidates for employment

The organisation shall establish and implement rules for conducting background checks on candidates for employment prior to their employment with the organisation. The scope and thoroughness of these checks will align with the information security risks related to the specific roles being filled.

Goal

Preventing information security incidents from occurring due to employees proving to be insufficiently competent, reliable or motivated.

Focus points

- Ensure that a thorough background check is performed before hiring new employees or assigning existing employees to confidential tasks. This helps to minimize business risk and ensures that only appropriate individuals have access to sensitive information.
- Formulate detailed rules and procedures for conducting background checks. Clearly define specific checks required for different functions or responsibilities, such as checking credentials, work history, and requesting a Certificate of Good Conduct (VOG).
- Explicitly include screening requirements for sensitive functions in the security policy. This policy should be reviewed and adjusted regularly to continue to meet the changing requirements of the organisation and legislation.
- Designate one or two individuals who are authorised and competent to perform these background checks. Ensure that these individuals are knowledgeable about privacy and employment laws and regulations, and that they take ethical considerations into account when performing the checks.

Mapping indication

ISO 27001: A.6.1 - Screening.
NIST SP 800-53: PS-3 - Personnel Screening.

3. Physical measures

3.1 Physical access security

The organisation shall design and implement appropriate physical security for sites, buildings, offices and spaces based on a risk assessment. The design shall take into account the organisation's need to be able to grant or prevent specific access within an environment.

Goal

Preventing an information security incident from occurring due to an unauthorised person gaining access to a site, building, office or space.

Focus points

- Ensure that all security zones within the organisation are clearly defined, so that important information and assets are optimally protected. Security zones can be both physical, such as secure rooms, and digital, such as shielded network segments.
- Ensure strict physical access control by implementing processes and resources that ensure controlled access to areas and buildings. Restrict access to certain areas only to those with the appropriate authorisations.
- Perform a comprehensive risk assessment to identify specific information security risks within the organisation. Use the results to tailor access security measures that effectively address these risks.

Mapping indication

ISO 27001: A.7.1 - Physical security zones.
IEC 62443-2-1:2010, Clause 4.3.3.3.2, 4.3.3.3.8
NIST SP 800-53: PE-2 - Physical access authorisations.

ISO 27001: A.7.2 - Physical access control.
IEC 62443-2-1:2010, Clause 4.3.3.3.2, 4.3.3.3.8
NIST SP 800-53: PE-3 - Physical access control.

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 to are to securely store all paper documents and removable storage media when they leave their workstation. This prevents sensitive information from being left unattended and accessible.
- 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 - 'Clear Desk' and 'Clear Screen'.

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 - Safe disposal or reuse of equipment.
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 Defining 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.
- Implement strict physical security measures for critical assets such as servers and patch cabinets. This can include building access controls, camera surveillance and secure server rooms.
- 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 – Access control.
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 unauthorised 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 - User Endpoint Devices.

4.2 Special Access Privileges

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

Goal

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

Focus points

- Carefully document which individuals or groups within the organisation have special access rights, so that it is always clear who has access to specific parts of systems or platforms.
- Implement a procedure for assigning and using special access privileges, with restrictions in place to ensure that only the appropriate individuals or processes obtain and use these rights.
- Maintain an up-to-date overview of all privileged accounts and clearly communicate the rules surrounding their use to the employees involved, so that everyone is aware of the responsibilities that these accounts entail.
- Establish procedures for timely deactivation of privileged accounts and regular password changes, paying special attention to accounts assigned to third-party vendors, to ensure the security of sensitive information.

Mapping indication

ISO 27001: A.8.2 - Special access rights.
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

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 - Protection against malware.
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 offsite. This guarantees 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.
- Periodically 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 ensures a structured approach and prevents data loss due to human error.

Mapping indication

ISO 27001: A.8.13 - Backup of information.
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

4.6 Redundant implementation of ICT infrastructure

The organisation must determine which parts of the ICT infrastructure require redundancy based on business continuity objectives and ICT continuity objectives (see 1.23). These redundant implementations must be deployed and tested to ensure they meet continuity objectives.

Goal

Preventing the recovery times of essential information systems from not sufficiently matching the organisation's business continuity objectives in the event of a disruption.

Focus points

- Determine the minimum required availability for the information processing facilities within the organisation and ensure that this is clearly established so that you know what requirements the systems must meet.
- Ensure that all information processing facilities have sufficient redundancy so that they continue to function even if a component fails and meet the specified availability requirements.
- Implement redundancy methods such as data storage in multiple locations or automatic failover to a backup system to ensure that key systems and services remain operational in the event of a failure.
- Regularly monitor and test the redundancy mechanisms to ensure that they are effective and actually ensure the continuity of the information processing facilities.

Mapping indication

ISO 27001: A.8.14 - Redundancy of information processing facilities.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 2
IEC 62443-2-1:2010, Clause 4.3.3.3.9, 4.3.4.4.1
IEC 62443-3-3:2013, SR 4.2, SR 7.1, SR 7.2

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 - Installing software on operational systems.
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

4.8 Manage and secure networks

The organisation must define and assign responsibilities for managing and configuring networks and network devices. All network devices are listed in an inventory and have an owner (administrator). The inventory is maintained and contains relevant information about the network devices.

Goal

Prevent information security incidents from occurring due to under-managed or incorrectly configured networks or network devices.

Focus points

- Ensure that network components and devices are properly secured so that information within your networks remains protected from unwanted access and attacks. This includes implementing strong security measures such as firewalls, encryption, and access control.
- Continuously monitor the behavior of your networks to quickly detect suspicious activities and potential security incidents. Analyse these incidents thoroughly to determine the cause and take appropriate measures to prevent future problems.
- Document and update network configurations accurately when changes are made. This helps to maintain an up-to-date overview of the network infrastructure and makes it easier to detect and resolve issues.
- Consider network automation to streamline routine tasks such as updating configurations and checking network status. This reduces the chance of human error and makes network management more efficient and secure.

Mapping indication

ISO 27001: A.8.20 - Security of network components.
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

4.9 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 ensures that the network remains effective and secure.

Mapping indication

ISO 27001: A.8.22 – Network segmentation.
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 company-sensitive 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 - Secure authentication.
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 – Logging.
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.

4.12 Cryptography and Encryption

Based on a risk assessment, the organisation should establish and implement rules that clarify in which cases stored and transmitted information must be secured with a specific form of cryptography. These rules also clarify how cryptographic keys must be stored securely.

Goal

Preventing an information security incident from occurring due to an unauthorised person gaining access to readable information stored or transmitted.

Focus points

- Establish a policy on cryptography and encryption to ensure a secure digital environment and communications, describing clear procedures for the use and control of encryption protocols such as TLS and HTTPS. Ensure that this policy is regularly reviewed for effectiveness.
- Implement TLS and HTTPS to ensure the security of data transmission over the Internet, encrypting all sensitive information during online communication and protecting it from unauthorised access. Verify that the organisation has established policies for cryptography and encryption that meet established security standards
- Ensure that all TLS certificates comply with established security standards, including a minimum key length of 2048 bits. Strictly monitor certificate validity periods and ensure timely renewal to prevent security risks.
- Periodically check all email domains for appropriate security measures such as DNSSEC, DKIM, DMARC, and SPF, and resolve critical issues quickly to ensure email communications remain secure.

Mapping indication

ISO 27001: A.8.24 – Cryptographic measures.
NIST SP 800-53: SC-13 - Cryptographic protection

4.14 Finding and repairing technical vulnerabilities in a timely manner

The organisation shall define and assign responsibilities for the timely finding, recording and repairing of technical vulnerabilities in networks and information systems under the organisation's management.

Goal

Preventing an information security incident from occurring due to an undiscovered technical vulnerability.

Focus points

- Identify and document technical vulnerabilities in the information systems on a regular basis, such as software bugs or misconfigurations. Ensure that there is a clear process for detecting these vulnerabilities, including who is responsible for this and what tools or methods are used.
- Carefully evaluate the exposure and risk of each identified vulnerability by determining how likely it is to be exploited and what the impact would be to the organisation. Prioritize vulnerabilities based on this evaluation to decide which mitigations to take first.
- Implement the correct measures to fix the vulnerabilities quickly and effectively, such as applying software updates or patches. Make sure that these measures are tested before they are put into production to prevent unexpected problems.
- Ensure an ongoing process to identify and address emerging vulnerabilities, including regular monitoring of external sources such as security bulletins. Keep the process current through periodic reviews and updates to procedures so that emerging threats can be effectively addressed.

Mapping indication

ISO 27001: A.8.8 - Technical vulnerability management.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 7, 10
NIST SP 800-53: RA-5 - Vulnerability monitoring and scanning.

4.15 Controlled implementation of changes

The organisation shall define and implement a process for the controlled implementation of changes to networks and information systems under the organisation's control. The process shall include a mandatory analysis of the potential impact on the availability, integrity and confidentiality of information.

Goal

Preventing an information security incident from occurring as a result of an inadequately prepared change to networks and information systems managed by the organisation.

Focus points

- Establish procedures to ensure information security when implementing changes to systems that process information, such as computers, but also for managing networks and information systems throughout their lifecycle. Ensure that these procedures are followed to ensure the security and integrity of the systems, especially for non-standard changes.
- Define how changes to systems are to be implemented, and develop a policy that covers the entire lifecycle of network and information systems, from development to disposal. This policy should ensure consistent security measures throughout the life of the systems.
- Ensure that all persons responsible for managing changes are adequately trained in ensuring information security. This is crucial, especially when emergency changes or non-standard changes occur that may introduce unexpected risks.
- Document and evaluate all changes, including the impact on information security. Ensure that emergency changes are managed properly and that an evaluation is always performed after the emergency procedure to assess the effects on security and to make the necessary adjustments.

Mapping indication

ISO 27001: A.8.32 - Change management.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 5, 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
NIST SP 800-53: CM-3 - Configuration change control.

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 systems

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 asset how critical it is to the organisation's operational processes. This helps to prioritize the management and security of these systems.
- Perform a risk analysis for each OT asset, 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 assets 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 assets.

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.
- Periodically 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.

5.6 Segmentation of OT networks

The organisation shall establish and implement rules for segmenting the organisation's OT 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

- Ensure that the network within the organisation is divided into separate segments, with each segment specifically equipped with the correct access rights. This limits access to sensitive information and prevents a potential threat from spreading unchecked across the entire network.
- Work with separate network segments within the network to ensure protection of sensitive information and increase cyber resilience. This helps build a layered defense strategy, making it harder for malicious actors to attack the entire network.
- Regularly check that the networks within the organisation are divided into separate segments with specific access rights, especially in critical parts of the network. This ensures that the segmentation remains effective and that sensitive information is always adequately protected.
- Ensure that network segmentation is well documented so that everyone involved knows exactly how the segments are set up and what access rights apply. This promotes consistent management and prevents unauthorised access to sensitive segments of the network.

Mapping indication

BIACS:
29, 31, 51: 2.4.2.1 Network connection measures

5.8 Remote access to critical OT systems

The organisation shall use a server that acts as a secure access point for remote access to critical OT systems under the organisation's control. The server in question shall have an owner (administrator) who is responsible for its security.

Goal

Using a secure access point reduces the risk of unauthorised access to internal OT systems by centralizing and restricting external access. This reduces the attack surface, improves control and monitoring of access attempts, and increases the overall security of the OT network.

Focus points

- Ensure that remote access to critical systems such as ICS and SCADA is only possible via a central access point, a so-called Jump Host, to minimize the risks of unauthorised access.
- Implement strict procedures and controls, such as two-factor authentication and encryption, to ensure the security of remote access. These measures ensure that only authorised users can access the network via the Jump Host.
- Monitor and log all activities that occur via the Jump Host. This allows for early detection and response to suspicious activity, contributing to the overall security of the network.
- Make sure the Jump Host itself is well secured, with regular updates and audits, to prevent it from becoming the weak link in the security chain.

Mapping indication

BIACS:
22, 28, 33: 2.2.2.2 Technical measures for logical access

5.9 Installing OT patches

The organisation shall establish and assign responsibilities for the timely application of critical patches to systems within OT networks under the organisation's management.

Goal

Patching in OT networks is crucial to close vulnerabilities that expose systems to cyberattacks. OT networks, which often power industrial processes and critical infrastructure, typically have outdated systems with limited security. Unpatched systems can lead to disruptions, production downtime and dangerous situations. Because OT systems often operate 24/7, patch management is complex but necessary to ensure both security and business continuity.

Focus points

- Ensure there is a detailed overview of all software and systems used within the organisation so that it is clear when patches need to be applied to close security holes.
- Perform periodic scans on all systems within the OT infrastructure to identify and manage potential security risks early.
- Carefully analyse the results of these scans and follow up by installing the required patches on all relevant systems as soon as possible.
- Ensure that responsibility for patch and scan management is clearly assigned, for example through vendor agreements, to ensure that the security of OT systems is always maintained.

Mapping indication

BIACS:
73, 74, 75, 76, 77: 2.5.2.3 Patching measures

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 the 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 - Source code access control.

6. 2 Keeping the program code and external components up to date

Organisations that develop applications must ensure that program code, including external components such as libraries and frameworks, is regularly updated with the latest security updates. This is documented in a formal process, with updates performed and documented within a set timeframe. The process is periodically evaluated and checked for compliance.

Goal

Keeping program code and external components up to date with the latest security updates helps close security holes and prevent new threats. Doing this consistently reduces the risk of data leaks, unauthorised access, and other security incidents.

Focus points

- Ensure that the program code, including third party components, is regularly updated to fix known vulnerabilities and ensure information security.
- Implement a system, such as Github's Dependabot, to continuously monitor for security updates and patches for both custom code and third-party components.
- Periodically evaluate the integration of third party components to ensure that they do not introduce unnecessary security risks.
- Document and track all updates and patches carefully to ensure that the program code always remains current and secure.

Mapping indication

No Mapping indication available.

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, vulnerability or logical error from being present in an application created by the organisation, and from leading to an information security incident when the application 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 - Secure system architecture and technical challenges.

6.4 Information security awareness in application development

Organisations that develop applications should ensure that developers are aware of the information security risks associated with developing applications and using those applications to process information.

Goal

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

Focus points

- Ensure that everyone within the organisation receives regular training and awareness sessions on information security, so that they are well informed about the risks and the importance of secure practices.
- Promote knowledge and use of security standards such as OWASP, CIS Controls or SANS Top 20 Critical Security Controls among employees to strengthen security practices within the organisation.
- Actively encourage employee involvement in adopting security standards so they understand how their actions contribute to the overall security of the organisation.
- Regularly evaluate and update security awareness programs to ensure they remain relevant and aligned with current security risks and standards.

Mapping indication

ISO 27001: A.6.3 - Information security awareness, education and training.
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-2 - Literacy training and awareness .

6.5 Testing the security of applications

Organisations that develop (or have developed) applications must first set requirements for the security of the applications with a view to their use in practice. When testing a developed application, not only the user aspects are tested, but also the security aspects of the application.

Goal

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

Focus points

- Ensure that the organisation regularly performs independent quality assessments and external audits, such as PEN testing, to ensure the security of systems and data. This helps to check the integrity and security of new functionalities and to address potential vulnerabilities in a timely manner.
- Record the findings of these tests and audits in a standardised manner, for example by ranking them according to the Common Vulnerability Scoring System (CVSS), so that vulnerabilities can be addressed on a prioritized basis.
- Take proactive action based on the results of the tests and audits to remediate identified vulnerabilities and strengthen overall security.
- Use the insights gained from these tests and audits to improve future developments and ensure security continuity within the organisation.

Mapping indication

ISO 27001: A.8.29 - Security testing during development and acceptance.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 10
IEC 62443-2-1:2010, Clause 4.2.3.1, 4.2.3.7
NIST SP 800-53: SA-11 - Developer security testing and evaluation.

6.6 Outsourced software development

When the development of custom software is (partly) outsourced to an external party, the organisation actively monitors the development activities and determines whether the delivered software meets the information security requirements.

Goal

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

Focus points

- When outsourcing software development, make sure you map out the information security measures your partners are taking. It is crucial to know what steps the external software developers are taking to ensure the security of your data and systems.
- Define clear security requirements and communicate them to your external software developers. This helps to ensure that the developed software meets established security standards, such as OWASP, CIS Controls or the SANS Top 20.
- Perform regular assessments of the security measures of the external developers. This can be done by means of audits and other checks to verify that the security requirements are being met and that there are no shortcomings in the delivered software.
- Please note that in offshoring, the priority given to security can vary. It is important to manage these risks well and ensure that all parties involved adhere to the same security standards.

Mapping indication

ISO 27001: A.8.3 - Restriction of access to information.
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

6.7 Separation of development, test, acceptance and production

Organisations that develop applications (or have them developed) must ensure that development and test environments remain separate from production environments, for example by using separate virtual or physical environments, in combination with separate access rights.

Goal

Preventing an information security incident from occurring as a result of an unauthorised or unintended change to a production environment by a developer or tester.

Focus points

- Ensure that development, test, acceptance, and production environments are clearly separated to minimize risk and ensure security. This means that each environment must be isolated so that changes or tests in one environment cannot affect the others.
- Implement strict controls and procedures to prevent unauthorised access between the different environments. By carefully managing access, you prevent errors or unwanted changes from occurring in the production environment, which is essential for the continuity and security of your systems.
- Use a separate acceptance environment where test scenarios are executed that closely mimic the production environment. This ensures that any issues are discovered early and resolved before new features or changes are implemented in production.
- Regular evaluations of the separation between these environments and the associated controls help ensure the integrity of the entire system and that the appropriate measures are still effective.

Mapping indication

ISO 27001: A.8.31 - Separation of development, test, and production environments.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 16

6.8 Procedures and methods for deploying software

Organisations that install or have software installed on their operational systems must implement procedures and measures to do this in a safe and controlled manner.

Goal

Preventing an information security incident from occurring as a result of uncontrolled installation of software on an operational system, with consequences for both business continuity and the security of the operational systems.

Focus points

- Ensure that there are documented procedures and methodologies for deploying software, where Infrastructure as Code (IAC) can play an important role. This ensures a standardised and controlled deployment, ensuring the consistency and security of software installations.
- Apply Infrastructure as Code (IAC) to automate and make the deployment process repeatable. This not only helps maintain information security but also ensures efficient and error-free installation of software solutions.
- Implement regular reviews and updates of deployment procedures to ensure they continue to meet the latest security standards and technologies. This contributes to the continuous improvement of the quality and security of software installations.
- Ensure that everyone on the team is familiar with software deployment procedures and methods, and provide training as needed. This will strengthen the organisation's adherence to and effectiveness of standardised deployment processes.

Mapping indication

No Mapping indication available.

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.

6.10 Maintaining an overview of delivered equipment and software

The organisation must maintain an accurate inventory of all equipment and software delivered to customers and record it in an up-to-date and documented overview of the IT landscape. This overview should be reviewed and updated periodically. The process must ensure that proactive maintenance is carried out and that security updates are applied to customers in a timely manner.

Goal

An accurate inventory of equipment and software helps identify vulnerabilities, manage risks effectively, and ensure timely security updates. This reduces the likelihood of security incidents and strengthens the overall security of the IT landscape.

Focus points

- Maintain an accurate inventory of all delivered equipment and software, including versions, to have a complete overview of the customers' IT landscape. This overview is crucial for effective management, proactive maintenance and the timely application of security updates.
- Create a detailed inventory list that tracks exactly which equipment and software is in use at each customer, including versions. This makes it easier to plan maintenance and implement updates, reducing the risk of security issues and unauthorised use.
- Ensure that the inventory list is always up to date by updating it immediately when changes are made. This reduces the risk of errors and helps maintain the reliability and security of the IT infrastructure.
- Implement a system for automatically updating the inventory list so that changes to equipment and software are immediately recorded. This ensures that the inventory list remains accurate and helps to proactively manage security risks.

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 about installing 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