NIS2 Supply Chain Certification

NIS2-SC10 BASIC

Version 3.2
December 15, 2025

NIS2 SUPPLY CHAIN

Contents

This is the NIS2-QM10 Basic standard, belonging to the NIS2 Supply Chain certification, an integral part of the Compliance and Certification Scheme of NIS2 Supply Chain and the Quality Innovation Foundation
Version 3.1 © 2025

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

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

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

1. Organisational measures

1.2 Information security policy formulation and management approval

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

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

Goal

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

Focus points

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

Mapping indication

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

1.3 Assignment of responsibility for information security

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

Goal

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

Focus points

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

Mapping indication

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

1.6.1 Overview of information

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

Goal

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

Focus points

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

Mapping indication

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

1.6.2 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 appointed, who is responsible for its protection.

Goal

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

Focus points

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

Mapping indication

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

1.8 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

1.14 Access Privilege Management

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

Goal

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

Focus points

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

Mapping indication

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

1.23 ICT preparation for business continuity

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

Goal

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

Focus points

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

Mapping indication

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

1.26 Securing the supply chain together

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

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

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

Goal

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

Focus points

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

Mapping indication

ISO 27001: A.5.21

2. People-oriented measures

2.2 Cybersecurity education for directors and employees

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

Goal

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

Focus points

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

Mapping indication

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

2.6 Working from home or hybrid in a safe way

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

Goal

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

Focus points

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

Mapping indication

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

2.7 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

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

Mapping indication

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

3. Physical measures

3.9 Define Access Control

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

Goal

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

Focus points

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

Mapping indication

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

4. Technological measures

4.1 Security and management of user devices

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

Goal

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

Focus points

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

4.4 Malware Control and Prevention

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

Goal

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

Focus points

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

Mapping indication

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

4.5 Backup and recovery

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

Goal

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

Focus points

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

Mapping indication

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

4.7 Keeping software on assets up to date

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

Goal

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

Focus points

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

Mapping indication

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

4.10 Implement authentication methods

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

Goal

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

Focus points

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

Mapping indication

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

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

Although the measures included in the NIS2 Supply Chain certification and related overview of measures have been developed by experts and have been compiled with the greatest possible care, no guarantees are given as to the correctness, completeness, reliability, suitability, or availability with respect to the NIS2 Supply Chain certification and the information, products, services, or related graphics contained therein. The use of the NIS2 Supply Chain certification and related overview of measures is entirely at the risk of the user. Any liability for damage, direct or indirect, arising out of or in any way connected with the use of the NIS2 Supply Chain certification and related overview of measures is excluded. The NIS2 Supply Chain certification Mapping indication overview may contain references to other standards, including ISO 27001 and NEN 7510, for information purposes only and to identify possible connections or areas of overlap. These references do not imply any association with or endorsement of the contents of the other standards. The NIS2 Supply Chain certification and related overview of measures and the other standards mentioned are separate and unique documents. All rights with respect to other standards mentioned in the document belong to their respective owners. The NIS2 Supply Chain certification and related summary of measures are protected by copyright. No part of this standard may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission.