CENTRE FOR
CYBERSECURITY
BELGIUM

CyberFundamentals

ESSENTIAL

Version: 01.03.2023

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Table of Contents

Introduction

The **CyberFundamentals Framework** is a set of concrete measures to:

- protect data,
- significantly reduce the risk of the most common cyber-attacks,
- increase an organisation's cyber resilience.

The requirements and guidance are complemented with the relevant insights included in NIST/CSF framework, ISO 27001/ISO 27002, IEC 62443 and the CIS Critical security Controls (ETSI TR 103 305-1).

The coding of the requirements corresponds with the codes used in the NIST CSF Framework. Since not all NIST CSF requirements are applicable, some codes that do exist in the NIST CSF framework may be missing.

The framework and the proportional approach of the assurance levels are validated by practitioners in the field and using anonymized real-world cyber-attack information provided by the federal Cyber Emergency Response Team (CERT - the operational service of the Centre for Cybersecurity Belgium).

The **CyberFundamentals Framework** is built around five core functions: identify, protect, detect, respond, and recover. These functions allow, regardless of the organization and industry, to promote communication around cybersecurity among both technical practitioners and stakeholders so that cyber-related risks can be incorporated into the overall risk management strategy of the organization.

- **Identify**
  Know important cyber threats to your most valuable assets. Essentially, you can't protect what you don't know exists. This function helps develop an organizational understanding of how to manage cyber security risks related to systems, people, assets, data, and capabilities.
- **Protect**
  The protect function focuses on developing and implementing the safeguards necessary to mitigate or contain a cyber risk.
- **Detect**
  The purpose of the Detect function is to ensure the timely detection of cyber security events.
- **Respond**
  The Respond function is all about the controls that help respond to cyber security incidents. The Respond function supports the ability to contain the impact of a potential cyber security incident.
- **Recover**
  The Recover function focuses on those safeguards that help maintain resilience and restore services that have been affected by a cyber security incident.

To respond to the severity of the threat an organisation is exposed to, in addition to the starting level ***Small***, 3 assurance levels are provided: ***Basic, Important and Essential***.

The **starting level Small** allows an organisation to make an initial assessment. It is intended for micro-organisations or organisations with limited technical knowledge.

The **assurance level Basic** contains the standard information security measures for all enterprises. These provide an effective security value with technology and processes that are generally already available. Where justified, the measures are tailored and refined.

Building on the Basic level, security measures are supplemented to protect organisations from increased cyber risks to achieve a higher level of assurance.

The **assurance level Important** is designed to minimise the risks of targeted cyber-attacks by actors with common skills and resources in addition to known cyber security risks.

The **assurance level Essential** goes a step further to also respond to the risk of advanced cyber-attacks by actors with extensive skills and resources.

Several controls require particular attention; These measures are labelled as **- key measure -**.

The framework is a living document and will continue to be updated and improved considering the feedback received from stakeholders, evolving risk of specific cybersecurity threats, availability of technical solutions and progressive insight.

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

ID.AM-1: Physical devices and systems used within the organization are inventoried.

An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.

Guidance

- This inventory includes fixed and portable computers, tablets, mobile phones, Programmable Logic Controllers (PLCs), sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices.
- This inventory must include all assets, whether or not they are connected to the organization's network.
- The use of an IT asset management tool could be considered.

The inventory of assets associated with information and information processing facilities shall reflect changes in the organization's context and include all information necessary for effective accountability.

Guidance

- Inventory specifications include for example, manufacturer, device type, model, serial number, machine names and network addresses, physical location…
- Accountability is the obligation to explain, justify, and take responsibility for one's actions, it implies answerability for the outcome of the task or process.
- Changes include the decommissioning of material.

When unauthorized hardware is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.

Guidance

- Any unsupported hardware without an exception documentation, is designated as unauthorized.
- Unauthorized hardware can be detected during inventory, requests for support by the user or other means.

Mechanisms for detecting the presence of unauthorized hardware and firmware components within the organization's network shall be identified.

Guidance

- Where safe and feasible, these mechanisms should be automated.
- There should be a process to address unauthorized assets on a frequently basis; The organization may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1
IEC 62443-2-1:2010, Clause 4.2.3.4
IEC 62443-3-3:2013, SR 7.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.9, 5.11, 7.9, 8.1

ID.AM-2: Software platforms and applications used within the organization are inventoried.

An inventory that reflects what software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.

Guidance

- This inventory includes software programs, software platforms and databases, even if outsourced (SaaS).
- Outsourcing arrangements should be part of the contractual agreements with the provider.
- Information in the inventory should include for example: name, description, version, number of users, data processed, etc.
- A distinction should be made between unsupported software and unauthorized software.
- The use of an IT asset management tool could be considered.

The inventory of software platforms and applications associated with information and information processing shall reflect changes in the organization's context and include all information necessary for effective accountability.

Guidance

The inventory of software platforms and applications should include the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date.

Individuals who are responsible and who are accountable for administering software platforms and applications within the organization shall be identified.

When unauthorized software is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.

Guidance

- Any unsupported software without an exception documentation, is designated as unauthorized.
- Unauthorized software can be detected during inventory, requests for support by the user or other means.

Mechanisms for detecting the presence of unauthorized software within the organization's ICT/OT environment shall be identified.

Guidance

- Where safe and feasible, these mechanisms should be automated.
- There should be a process to regularly address unauthorised assets; The organization may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.9

ID.AM-3: Organizational communication and data flows are mapped.

Information that the organization stores and uses shall be identified.

Guidance

- Start by listing all the types of information your business stores or uses. Define “information type” in any useful way that makes sense to your business. You may want to have your employees make a list of all the information they use in their regular activities. List everything you can think of, but you do not need to be too specific. For example, you may keep customer names and email addresses, receipts for raw material, your banking information, or other proprietary information.
- Consider mapping this information with the associated assets identified in the inventories of physical devices, systems, software platforms and applications used within the organization (see ID.AM-1 & ID.AM-2).

All connections within the organization's ICT/OT environment, and to other organization-internal platforms shall be mapped, documented, approved, and updated as appropriate.

Guidance

- Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection.
- Configuration management can be used as supporting asset.
- This documentation should not be stored only on the network it represents.
- Consider keeping a copy of this documentation in a safe offline environment (e.g. offline hard disk, paper hardcopy, …).

The information flows/data flows within the organization’s ICT/OT environment, as well as to other organization-internal systems shall be mapped, documented, authorized, and updated when changes occur.

Guidance

- With knowledge of the information/data flows within a system and between systems, it is possible to determine where information can and cannot go.
- Consider:
    - Enforcing controls restricting connections to only authorized interfaces.
    - Heightening system monitoring activity whenever there is an indication of increased risk to organization's critical operations and assets.
    - Protecting the system from information leakage due to electromagnetic signals emanations.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.14

ID.AM-4: External information systems are catalogued.

The organization shall map, document, authorize and when changes occur, update, all external services and the connections made with them.

Guidance

- Outsourcing of systems, software platforms and applications used within the organization is covered in ID.AM-1 & ID.AM-2
- External information systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls, or the determination of the effectiveness of implemented controls on those systems i.e., services that are run in cloud, SaaS, hosting or other external environments, API (Application Programming Interface)…
- Mapping external services and the connections made to them and authorizing them in advance avoids wasting unnecessary resources investigating a supposedly non-authenticated connection to external systems.

The flow of information to/from external systems shall be mapped, documented, authorized, and update when changes occur.

Guidance

Consider requiring external service providers **to** identify and document the functions, ports, protocols, and services necessary for the connection services.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Annex A (see ISO 27002**)**
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.12, 7.9

ID.AM-5: Resources are prioritized based on their classification, criticality, and business value.

The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.

Guidance

- Determine organization's resources (e.g., hardware, devices, data, time, personnel, information, and software):
  - What would happen to my business if these resources were made public, damaged, lost…?
  - What would happen to my business when the integrity of resources is no longer guaranteed?
  - What would happen to my business if I/my customers couldn't access these resources? And rank these resources based on their classification, criticality, and business value.
- Resources should include enterprise assets.
- Create a classification for sensitive information by first determining categories, e.g.
  - Public - freely accessible to all, even externally
  - Internal - accessible only to members of your organization
  - Confidential - accessible only to those whose duties require access.
- Communicate these categories and identify what types of data fall into these categories (HR data, financial data, legal data, personal data, etc.).
- Consider the use of the Traffic Light Protocol (TLP).
- Data classification should apply to the three aspects: C-I-A
- Consider implementing an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3
IEC 62443-2-1:2010, Clause 4.2.3.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.12, 7.9

ID.AM-6: Cybersecurity roles, responsibilities, and authorities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners.
- key measure -

Guidance

It should be considered to:

- Describe security roles, responsibilities, and authorities: who in your organization should be consulted, informed, and held accountable for all or part of your assets.
- Provide security roles, responsibilities, and authority for all key functions in information/cyber security (legal, detection activities…).
- Include information/cybersecurity roles and responsibilities for third-party providers with physical or logical access to the organization's ICT/OT environment.

The organization shall appoint an information security officer.

Guidance

The information security officer should be responsible for monitoring the implementation of the organization's information/cyber security strategy and safeguards.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.3, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.2, 5.4, 5.23, 5.24, 6.2, 6.5, 8.24

The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

ID.BE-1: The organization's role in the supply chain is identified and communicated.

The organization's role in the supply chain shall be identified, documented, and communicated.

Guidance

- The organisation should be able to clearly identify who is upstream and downstream of the organisation and which suppliers provide services, capabilities, products and items to the organisation.
- The organisation should communicate its position to its upstream and downstream so that it is understood where they sit in terms of critical importance to the organisation's operations.

The organization shall protect its ICT/OT environment from supply chain threats by applying security safeguards as part of a documented comprehensive security strategy.

Guidance

No additional guidance on this topic.

References

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.19, 5.20, 5.21, 5.22

ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.

The organization's place in critical infrastructure and its industry sector shall be identified and communicated.

Guidance

The organisation covered by NIS legislation has a responsibility to know the other organisations in the same sector in order to work with them to achieve the objectives set by NIS for that particular sector.

References

IEC 62443-2-1:2010, Clause 4.2.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1

ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.

Priorities for organization's business, objectives, and activities shall be established and communicated.

Guidance

- Organizational mission, objectives and activities should be determined and prioritized.
- Information protection needs should be determined, and the related processes revised as necessary, until an achievable set is obtained.

References

IEC 62443-2-1:2010, Clause 4.2.2, 4.2.3.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.1, 5.2, 6.1, 7.4, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.1

ID.BE-4: Dependencies and critical functions for delivery of critical services are established.

Dependencies and mission-critical functions for the delivery of critical services shall be identified, documented, and prioritized according to their criticality as part of the risk assessment process.

Guidance

Dependencies and business critical functions should include support services.

References

IEC 62443-2-1:2010, Clause 4.2.3.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.1, 8, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 7.11, 7.12, 8.6

ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).

To support cyber resilience and secure the delivery of critical services, the necessary requirements are identified, documented and their implementation tested and approved.

Guidance

- Consider implementing resiliency mechanisms to support normal and adverse operational situations (e.g., failsafe, load balancing, hot swap).
- Consider aspects of business continuity management in e.g. Business Impact Analyse (BIA), Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).

Information processing & supporting facilities shall implement redundancy to meet availability requirements, as defined by the organization and/or regulatory frameworks.

Guidance

- Consider provisioning adequate data and network redundancy (e.g. redundant network devices, servers with load balancing, raid arrays, backup services, 2 separate datacentres, fail-over network connections, 2 ISP's…).
- Consider protecting critical equipment/services from power outages and other failures due to utility interruptions (e.g. UPS & NO-break, frequent test, service contracts that include regular maintenance, redundant power cabling, 2 different power service providers...).

Recovery time and recovery point objectives for the recovery of essential ICT/OT system processes shall be defined.

Guidance

- Consider applying the 3-2-1 back-up rule to improve RPO and RTO (maintain at least 3 copies of your data, keep 2 of them at separate locations and one copy should be stored at an off-site location).
- Consider implementing mechanisms such as hot swap, load balancing and failsafe to increase resilience.

References

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.29, 7.5, 8.14

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

ID.GV-1: Organizational cybersecurity policy is established and communicated.

Policies and procedures for information security and cyber security shall be created, documented, reviewed, approved, and updated when changes occur.

Guidance

- Policies and procedures used to identify acceptable practices and expectations for business operations, can be used to train new employees on your information security expectations, and can aid an investigation in case of an incident. These policies and procedures should be readily accessible to employees.
- Policies and procedures for information- and cybersecurity should clearly describe your expectations for protecting the organization's information and systems, and how management expects the company's resources to be used and protected by all employees.
- Policies and procedures should be reviewed and updated at least annually and every time there are changes in the organization or technology. Whenever the policies are changed, employees should be made aware of the changes.

An organization-wide information security and cybersecurity policy shall be established, documented, updated when changes occur, disseminated, and approved by senior management.

Guidance

The policy should include, for example:

- The identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Guidance on role profiles along with their identified titles, missions, tasks, skills, knowledge, competences is available in the "European Cybersecurity Skills Framework Role Profiles" by ENISA. (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles)
- The coordination among organizational entities responsible for the different aspects of security (i.e., technical, physical, personnel, cyber-physical, information, access control, media protection, vulnerability management, maintenance, monitoring)
- The coverage of the full life cycle of the ICT/OT systems.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14
IEC 62443-2-1:2010, Clause 4.3.2.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4, 5, 7.5, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.1

ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood, and managed.

Legal and regulatory requirements regarding information/cybersecurity, including privacy obligations, shall be understood, implemented, and managed.

Guidance

- There should be regular reviews to ensure the continuous compliance with legal and regulatory requirements regarding information/cybersecurity, including privacy obligations.
- This requirement also applies to contractors and service providers.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.4.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1, 4.2, 7.4, 7.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.31, 5.32, 5.33, 5.34

ID.GV-4: Governance and risk management processes address cybersecurity risks.

As part of the company's overall risk management, a comprehensive strategy to manage information security and cybersecurity risks shall be developed and updated when changes occur.

Guidance

This strategy should include determining and allocating the required resources to protect the organization’s business-critical assets.

Information security and cybersecurity risks shall be documented, formally approved, and updated when changes occur.

Guidance

Consider using Risk Management tools.

References

IEC 62443-2-1:2010, Clause 4.2.3, 4.4.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

ID.RA-1: Asset vulnerabilities are identified and documented.

Threats and vulnerabilities shall be identified.

Guidance

- A vulnerability refers to a weakness in the organization's hardware, software, or procedures. It is a gap through which a bad actor can gain access to the organization's assets. A vulnerability exposes an organization to threats.
- A threat is a malicious or negative event that takes advantage of a vulnerability.
- The risk is the potential for loss and damage when the threat does occur.

A process shall be established to monitor, identify, and document vulnerabilities of the organisation's business critical systems in a continuous manner.

Guidance

- Where safe and feasible, the use of vulnerability scanning should be considered.
- The organization should establish and maintain a testing program appropriate to its size, complexity, and maturity.

To ensure that organization's operations are not adversely impacted by the testing process, performance/load testing and penetration testing on the organization's systems shall be conducted with care.

Guidance

Consider validating security measures after each penetration test.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 7
IEC 62443-2-1:2010, Clause 4.2.3, 4.2.3.9, 4.2.3.12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6, 7, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.36, 8.8

ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.

A threat and vulnerability awareness program that includes a cross-organization information-sharing capability shall be implemented.

Guidance

A threat and vulnerability awareness program should include ongoing contact with security groups and associations to receive security alerts and advisories. (Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations).This contact can include the sharing of information about potential vulnerabilities and incidents. This sharing capability should have an unclassified and classified information sharing capability.

It shall be identified where automated mechanisms can be implemented to make security alert and advisory information available to relevant organization stakeholders.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14
IEC 62443-2-1:2010, Clause 4.2.3, 4.2.3.9, 4.2.3.12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.2, 7.4, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.6

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

The organization shall conduct risk assessments in which risk is determined by threats, vulnerabilities and impact on business processes and assets.

Guidance

- Keep in mind that threats exploit vulnerabilities.
- Identify the consequences that losses of confidentiality, integrity and availability may have on the assets and related business processes.

The organization shall conduct and document risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence.

Guidance

- Risk assessment should include threats from insiders and external parties.
- Qualitative and/or quantitative risk analysis methods (MAPGOOD, ISO27005, CIS RAM, …) can be used together with software tooling.

Risk assessment results shall be disseminated to relevant stakeholders.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 7, 10
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.1, 6.1, 7.4, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.8

ID.RA-6: Risk responses are identified and prioritized.

A comprehensive strategy shall be developed and implemented to manage risks to the organization's critical systems, that includes the identification and prioritization of risk responses.

Guidance

- Management and employees should be involved in information- and cybersecurity.
- It should be identified what the most important assets are, and how they are protected.
- It should be clear what impact will be if these assets are compromised.
- It should be established how the implementation of adequate mitigation measures will be organized.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 7, 10
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.1, 6.1.3, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.8

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.

A cyber risk management process that identifies key internal and external stakeholders and facilitates addressing risk-related issues and information shall be created, documented, reviewed, approved, and updated when changes occur.

Guidance

External stakeholders include customers, investors and shareholders, suppliers, government agencies and the wider community.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 7, 10
IEC 62443-2-1:2010, Clause 4.3.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.1, 5.2, 6.1.3, 8.3, 9.3

ID.RM-2: Organizational risk tolerance is determined and clearly expressed.

The organization shall clearly determine its risk appetite.

Guidance

Determination and expression of risk tolerance (risk appetite) should be in line with the policies on information security and cybersecurity, to facilitate demonstration of coherence between policies, risk tolerance and measures.

References

IEC 62443-2-1:2010, Clause 4.3.2.6.5
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.1, 5.2, 6.1.3, 7.4, 8.3, 9.3

ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

The organization's role in critical infrastructure and its sector shall determine the organization's risk appetite.

Guidance

No additional guidance on this topic.

References

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.1, 5.2, 6.1.3, 8.3, 9.3

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.

The organization shall document, review, approve, update when changes occur, and implement a cyber supply chain risk management process that supports the identification, assessment, and mitigation of the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains.

Guidance

No additional guidance on this topic.

References

IEC 62443-2-1:2010, Clause 4.3.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.1, 5.3, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.19, 5.20, 5.21, 5.22

ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.

The organization shall conduct cyber supply chain risk assessments at least annually or when a change to the organization's critical systems, operational environment, or supply chain occurs; These assessments shall be documented, and the results disseminated to relevant stakeholders including those responsible for ICT/OT systems.

Guidance

This assessment should identify and prioritize potential negative impacts to the organization from the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains.

A documented list of all the organization's suppliers, vendors and partners who may be involved in a major incident shall be established, kept up-to-date and made available online and offline.

Guidance

This list should include suppliers, vendors and partners contact information and the services they provide, so they can be contacted for assistance in the event of an outage or service degradation.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.1, 5.3, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.19, 5.20, 5.21, 5.22

ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

Based on the results of the cyber supply chain risk assessment, a contractual framework for suppliers and external partners shall be established to address sharing of sensitive information and distributed and interconnected ICT/OT products and services.

Guidance

- Entities not subject to the NIS legislation should consider business critical suppliers and third-party partners only.
- Keep in mind that GDPR requirements need to be fulfilled when business information contains personal data (applicable on all levels), i.e. security measures need to be addressed in the contractual framework.

Contractual 'information security and cybersecurity' requirements for suppliers and third-party partners shall be implemented to ensure a verifiable flaw remediation process, and to ensure the correction of flaws identified during 'information security and cybersecurity' testing and evaluation.

- Key measure -

Guidance

- Information systems containing software (or firmware) affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) should be identified.
- Newly released security relevant patches, service packs, and hot fixes should be installed, and these patches, service packs, and hot fixes are tested for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation should be incorporated into configuration management as an emergency change.

The organization shall establish contractual requirements permitting the organization to review the 'information security and cybersecurity' programs implemented by suppliers and third-party partners.

- Key measure -

Guidance

No additional guidance on this topic.

References

IEC 62443-2-1:2010, Clause 4.3.2.6.4, 4.3.2.6.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.19, 5.20, 5.21, 5.22

ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

The organization shall review assessments of suppliers' and third-party partner's compliance with contractual obligations by routinely reviewing audits, test results, and other evaluations.

Guidance

Entities not subject to the NIS legislation could limit themselves to business-critical suppliers and third-party partners only.

The organization shall review assessments of suppliers' and third-party partner's compliance with contractual obligations by routinely reviewing third-party independent audits, test results, and other evaluations.

Guidance

The depth of the review should depend on the criticality of delivered products and services.

References

IEC 62443-2-1:2010, Clause 4.3.2.6.7
IEC 62443-3-3:2013, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, 9.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.22

ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.

The organization shall identify and document key personnel from suppliers and third-party partners to include them as stakeholders in response and recovery planning activities.

Guidance

Entities not subject to the NIS legislation could limit themselves to business-critical suppliers and third-party partners only.

The organization shall identify and document key personnel from suppliers and third-party partners to include them as stakeholders in testing and execution of the response and recovery plans.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 18
IEC 62443-2-1:2010, Clause 4.3.2.5.7, 4.3.4.5.11
IEC 62443-3-3:2013, SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6.1.3, 8.1, 8.3, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.29

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.

Identities and credentials for authorized devices and users shall be managed.
- key measure -

Guidance

Identities and credentials for authorized devices and users could be managed through a password policy. A password policy is a set of rules designed to enhance ICT/OT security by encouraging organization's to (Not limitative list and measures to be considered as appropriate):

- Change all default passwords.
- Ensure that no one works with administrator privileges for daily tasks.
- Keep a limited and updated list of system administrator accounts.
- Enforce password rules, e.g. passwords must be longer than a state-of-the-art number of characters with a combination of character types and changed periodically or when there is any suspicion of compromise.
- Use only individual accounts and never share passwords.
- Immediately disable unused accounts.
- Rights and privileges are managed by user groups.

Identities and credentials for authorized devices and users shall be managed, where feasible through automated mechanisms.

Guidance

- Automated mechanisms can help to support the management and auditing of information system credentials.
- Consider strong user authentication, meaning an authentication based on the use of at least two authentication factors from different categories of either knowledge (something only the user knows), possession (something only the user possesses) or inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way to protect the confidentiality of the authentication data.

System credentials shall be deactivated after a specified period of inactivity unless it would compromise the safe operation of (critical) processes.

Guidance

- To guarantee the safe operation, service accounts should be used for running processes and services.
- Consider the use of a formal access procedure for external parties.

For transactions within the organization's critical systems, the organization shall implement:

- multi-factor end-user authentication (MFA or "strong authentication").
- certificate-based authentication for system-to-system communications

Guidance

Consider the use of SSO (Single Sign On) in combination with MFA for the organization's internal and external critical systems.

The organization's critical systems shall be monitored for atypical use of system credentials. Credentials associated with significant risk shall be disabled.

Guidance

- Consider limiting the number of failed login attempts by implementing automatic lockout.
- The locked account won't be accessible until it has been reset or the account lockout duration elapses.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.16, 5.17, 5.18, 8.2, 8.5

PR.AC-2: Physical access to assets is managed and protected.

Physical access to the facility, servers and network components shall be managed.

Guidance

- Consider to strictly manage keys to access the premises and alarm codes. The following rules should be considered:
  - Always retrieve an employee's keys or badges when they leave the company permanently.
  - Change company alarm codes frequently.
  - Never give keys or alarm codes to external service providers (cleaning agents, etc.), unless it is possible to trace these accesses and restrict them technically to given time slots.
- Consider to not leaving internal network access outlets accessible in public areas. These public places can be waiting rooms, corridors...

Physical access shall be managed, including measures related to access in emergency situations.

Guidance

- Physical access controls may include, for example lists of authorized individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, monitoring of facility access, camera surveillance.
- The following measures should be considered:
  - Implement a badge system and create different security zones.
  - Limit physical access to servers and network components to authorized personnel.
  - Log all access to servers and network components.
- Visitor access records should be maintained, reviewed and acted upon as required.

Physical access to critical zones shall be controlled in addition to the physical access to the facility.

Guidance

E.g. production, R&D, organization's critical systems equipment (server rooms…)

Assets related to critical zones shall be physically protected.

Guidance

- Consider protecting power equipment, power cabling, network cabling, and network access interfaces from accidental damage, disruption, and physical tampering.
- Consider implementing redundant and physically separated power systems for organization's critical operations.

References

IEC 62443-2-1:2010, Clause 4.3.3.3.2, 4.3.3.3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 7.1, 7.2, 7.3, 7.5, 7.6, 7.8, 7.9, 7.10, 7.12, 7.14, 8.1

PR.AC-3: Remote access is managed.

The organisation's wireless access points shall be secured.

Guidance

Consider the following when wireless networking is used:

- Change the administrative password upon installation of a wireless access points.
- Set the wireless access point so that it does not broadcast its Service Set Identifier (SSID).
- Set your router to use at least WiFi Protected Access (WPA-2 or WPA-3 where possible), with the Advanced Encryption Standard (AES) for encryption.
- Ensure that wireless internet access to customers is separated from your business network.
- Connecting to unknown or unsecured / guest wireless access points, should be avoided, and if unavoidable done through an encrypted virtual private network (VPN) capability.
- Manage all endpoint devices (fixed and mobile) according to the organization's security policies.

Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment shall be identified, documented, and implemented.

- key measure -

Guidance

Consider the following:

- Remote access methods include, for example, wireless, broadband, Virtual Private Network (VPN) connections, mobile device connections, and communications through external networks.
- Login credentials should be in line with company's user authentication policies.
- Remote access for support activities or maintenance of organizational assets should be approved, logged, and performed in a manner that prevents unauthorized access.
- The user should be made aware of any remote connection to its device by a visual indication.

Remote access to the organization's critical systems shall be monitored and cryptographic mechanisms shall be implemented where determined necessary.

Guidance

This should include that only authorized use of privileged functions from remote access is allowed.

The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).
- key measure -

Guidance

Enforce MFA (e.g. 2FA) on Internet-facing systems, such as email, remote desktop, and Virtual Private Network (VPNs).

The security of connections with external systems shall be verified and framed by documented agreements.

Guidance

Access from pre-defined IP addresses could be considered.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.14, 6.7, 7.9, 8.1, 8.5, 8.20

PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

Access permissions for users to the organization's systems shall be defined and managed.
- key measure -

Guidance

The following should be considered:

- Draw up and review regularly access lists per system (files, servers, software, databases, etc.), possibly through analysis of the Active Directory in Windows-based systems, with the objective of determining who needs what kind of access (privileged or not), to what, to perform their duties in the organization.
- Set up a separate account for each user (including any contractors needing access) and require that strong, unique passwords be used for each account.
- Ensure that all employees use computer accounts without administrative privileges to perform typical work functions. This includes separation of personal and admin accounts.
- For guest accounts, consider using the minimal privileges (e.g. internet access only) as required for your business needs.
- Permission management should be documented in a procedure and updated when appropriate.
- Use 'Single Sign On' (SSO) when appropriate.

Where feasible, automated mechanisms shall be implemented to support the management of user accounts on the organisation's critical systems, including disabling, monitoring, reporting and deleting user accounts.

Guidance

Consider separately identifying each person with access to the organization's critical systems with a username to remove generic and anonymous accounts and access.

Account usage restrictions for specific time periods and locations shall be considered in the organization's security access policy and applied accordingly.

Guidance

Specific restrictions can include, for example, restricting usage to certain days of the week, time of day, or specific durations of time.

It shall be identified who should have access to the organization's business's critical information and technology and the means to get access.
- key measure -

Guidance

Means to get access may include: a key, password, code, or administrative privilege.

Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (the principle of Least Privilege).
- key measure -

Guidance

- The principle of Least Privilege should be understood as the principle that a security architecture should be designed so that each employee is granted the minimum system resources and authorizations that the employee needs to perform its function.
- Consider to:
    - Not allow any employee to have access to all the business's information.
    - Limit the number of Internet accesses and interconnections with partner networks to the strict necessary to be able to centralize and homogenize the monitoring of exchanges more easily.
    - Ensure that when an employee leaves the business, all access to the business's information or systems is blocked instantly.

Separation of duties shall be ensured in the management of access rights.

Guidance

Separation of duties includes, for example:

- dividing operational functions and system support functions among different roles.
- conducting system support functions with different individuals.
- not allow a single individual to both initiate and approve a transaction (financial or otherwise).
- ensuring that security personnel administering access control functions do not also administer audit functions.

Nobody shall have administrator privileges for daily tasks.
- key measure -

Guidance

Consider the following:

- Separate administrator accounts from user accounts.
- Do not privilege user accounts to effectuate administration tasks.
- Create unique local administrator passwords and disable unused accounts.
- Consider prohibiting Internet browsing from administrative accounts.

Privileged users shall be managed, monitored and audited.

Guidance

No additional guidance on this topic.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.3, 5.15, 8.2, 8.3, 8.4, 8.18

PR.AC-5: Network integrity (network segregation, network segmentation…) is protected.

Firewalls shall be installed and activated on all the organization's networks.
- key measure -

Guidance

Consider the following:

- Install and operate a firewall between your internal network and the Internet. This may be a function of a (wireless) access point/router, or it may be a function of a router provided by the Internet Service Provider (ISP).
- Ensure there is antivirus software installed on purchased firewall solutions and ensure that the administrator's log-in and administrative password is changed upon installation and regularly thereafter.
- Install, use, and update a software firewall on each computer system (including smart phones and other networked devices).
- Have firewalls on each of your computers and networks even if you use a cloud service provider or a virtual private network (VPN). Ensure that for telework home network and systems have hardware and software firewalls installed, operational, and regularly updated.
- Consider installing an Intrusion Detection / Prevention System (IDPS). These devices analyse network traffic at a more detailed level and can provide a greater level of protection.

Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.
- key measure -

Guidance

- Consider creating different security zones in the network (e.g. basic network segmentation through VLAN's or other network access control mechanisms) and control/monitor the traffic between these zones.
- When the network is "flat", the compromise of a vital network component can lead to the compromise of the entire network.

Where appropriate, network integrity of the organization's critical systems shall be protected by
(1) Identifying, documenting, and controlling connections between system components.
(2) Limiting external connections to the organization's critical systems.
- key measure -

Guidance

Boundary protection mechanisms include, for example, routers, gateways, unidirectional gateways, data diodes, and firewalls separating system components into logically separate networks or subnetworks.

The organization shall implement, where feasible, authenticated proxy servers for defined communications traffic between the organization's critical systems and external networks.

Guidance

No additional guidance on this topic.

The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where appropriate.
- key measure -

Guidance

Consider implementing the following recommendations:

- Separate your public WIFI network from your business network.
- Protect your business WIFI with state-of-the-art encryption.
- Implement a network access control (NAC) solution.
- Encrypt connections to your corporate network.
- Divide your network according to security levels and apply firewall rules. Isolate your networks for server administration.
- Force VPN on public networks.
- Implement a closed policy for security gateways (deny all policy: only allow/open connections that have been explicitly pre-authorized).

The organization shall ensure that the organization's critical systems fail safely when a border protection device fails operationally.

Guidance

No additional guidance on this topic.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.14, 8.20, 8.22, 8.26

PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.

The organization shall implement documented procedures for verifying the identity of individuals before issuing credentials that provide access to organization's systems.

Guidance

No additional guidance on this topic.

The organization shall ensure the use of unique credentials bound to each verified user, device, and process interacting with the organization's critical systems; make sure that they are authenticated, and that the unique identifiers are captured when performing system interactions.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 5, 6
IEC 62443-2-1:2010, Clause 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7,5, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.3, 5.15, 8.2, 8.3, 8.18

PR.AC-7: Identities are proofed, bound to credentials and asserted in interactions.

The organization shall perform a documented risk assessment on organization's critical system transactions and authenticate users, devices, and other assets (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
- Key measure -

Guidance

Consider a security-by-design approach for new systems; For existing systems a separate risk assessment should be used.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 5, 6, 9, 12, 13
IEC 62443-2-1:2010, Clause 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9
IEC 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6.1, 7.5, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.16, 5.17, 5.34, 8.5

The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

PR.AT-1: All users are informed and trained.

Employees shall be trained as appropriate.

Guidance

- Employees include all users and managers of the ICT/OT systems, and they should be trained immediately when hired and regularly thereafter about the company's information security policies and what they will be expected to do to protect company's business information and technology.
- Training should be continually updated and reinforced by awareness campaigns.

The organization shall incorporate insider threat recognition and reporting into security awareness training.

Guidance

Consider to:

- Communicate and discuss regularly to ensure that everyone is aware of their responsibilities.
- Develop an outreach program by gathering in a document the messages you want to convey to your staff (topics, audiences, objectives, etc.) and your communication rhythm on a calendar (weekly, monthly, one-time, etc.). Communicate continuously and in an engaging way, involving management, IT colleagues, the ICT service provider and HR and Communication managers.
- Cover topics such as: recognition of fraud attempts, phishing, management of sensitive information, incidents, etc. The goal is for all employees to understand ways to protect company information.
- Discuss with your management, your ICT colleagues, or your ICT service provider some practice scenarios (e.g. what to do if a virus alert is triggered, if a storm cuts off the power, if data is blocked, if an account is hacked, etc.), determine what behaviours to adopt, document and communicate them to all your staff. The central point of contact in the event of an incident should be known to all.
- Organize a simulation of a scenario to test your knowledge. Consider performing the exercise for example at least once a year.

The organization shall implement an evaluation method to measure the effectiveness of the awareness trainings.

Guidance

No additional guidance on this topic.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.2, 7.4, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 6.3, 8.7

PR.AT-2: Privileged users understand their roles and responsibilities.

Privileged users shall be qualified before privileges are granted, and these users shall be able to demonstrate the understanding of their roles, responsibilities, and authorities.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 14, 16
IEC 62443-2-1:2010, Clause 4.3.2.4.2, 4.3.2.4.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.3, 7.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.2, 6.3

PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.

The organization shall establish and enforce security requirements for business-critical third-party providers and users.

Guidance

Enforcement should include that 'third party stakeholder'-users (e.g. suppliers, customers, partners) can demonstrate the understanding of their roles and responsibilities.

Third-party providers shall be required to notify any personnel transfers, termination, or transition involving personnel with physical or logical access to organization's business critical system's components.

Guidance

Third-party providers include, for example, service providers, contractors, and other organizations providing system development, technology services, outsourced applications, or network and security management.

The organization shall monitor business-critical service providers and users for security compliance.

Guidance

Third party audit results can be used as audit evidence.

The organization shall audit business-critical external service providers for security compliance.

Guidance

Third party audit results can be used as audit evidence.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14
IEC 62443-2-1:2010, Clause 4.3.2.4.2, 4.3.2.4.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.3, 8.1, 9.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.2, 5.4, 5.12, 6.3

PR.AT-4: Senior executives understand their roles and responsibilities.

Senior executives shall demonstrate the understanding of their roles, responsibilities, and authorities.

Guidance

Guidance on role profiles along with their identified titles, missions, tasks, skills, knowledge, competences is available in the "European Cybersecurity Skills Framework Role Profiles" by ENISA. (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles)

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14, 17
IEC 62443-2-1:2010, Clause 4.3.2.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1, 4.2, 5.3, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.2, 5.4, 5.12, 6.3

PR.AT-5: Physical security and cybersecurity personnel understand their roles and responsibilities.

The organization shall ensure that personnel responsible for the physical protection and security of the organization's critical systems and facilities are qualified through training before privileges are granted, and that they understand their responsibilities.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14
IEC 62443-2-1:2010, Clause 4.3.2.4.2, 4.3.2.4.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.3, 7.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.2, 6.3

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

PR.DS-1: Data-at-rest is protected.

The organization shall protect its critical system information determined to be critical/ sensitive while at rest.

Guidance

- Consider using encryption techniques for data storage, data transmission or data transport (e.g., laptop, USB).
- Consider encrypting end-user devices and removable media containing sensitive data (e.g. hard disks, laptops, mobile device, USB storage devices, …). This could be done by e.g. Windows BitLocker®, VeraCrypt, Apple FileVault®, Linux® dm-crypt,…
- Consider encrypting sensitive data stored in the cloud.
- Implement dedicated safeguards to prevent unauthorized access, distortion, or modification of system data and audit records (e.g. restricted access rights, daily backups, data encryption, firewall installation).
- Encrypt hard drives, external media, stored files, configuration files and data stored in the cloud.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.10

PR.DS-2: Data-in-transit is protected.

The organization shall protect its critical system information determined to be critical when in transit.

Guidance

If you send sensitive documents or emails, you may want to consider encrypting those documents and/or emails with appropriate, supported, and authorized software tools.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3
IEC 62443-3-3:2013, SR 3.1, SR 3.8, SR 4.1, SR 4.**2**
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.10, 5.14, 8.20, 8.26

PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.

Assets and media shall be disposed of safely.

Guidance

- When eliminating tangible assets like business computers/laptops, servers, hard drive(s) and other storage media (USB drives, paper…), ensure that all sensitive business or personal data are securely deleted (i.e. electronically "wiped") before they are removed and then physically destroyed (or re-commissioned). This is also known as "sanitization" and thus related to the requirement and guidance in PR.IP-6.
- Consider installing a remote-wiping application on company laptops, tablets, cell phones, and other mobile devices

The organization shall enforce accountability for all its business-critical assets throughout the system lifecycle, including removal, transfers, and disposition.

Guidance

Accountability should include:

- The authorization for business-critical assets to enter and exit the facility.
- Monitoring and maintaining documentation related to the movements of business-critical assets.

The organization shall ensure that disposal actions are approved, tracked, documented, and verified.

Guidance

Disposal actions include media sanitization actions (See PR.IP-6).

The organization shall ensure that the necessary measures are taken to deal with loss, misuse, damage, or theft of assets.

Guidance

This can be done by policies, processes & procedures (reporting), technical & organizational means (encryption, Access Control (AC), Mobile Device Management (MDM), monitoring, secure wipe, awareness, signed user agreement, guidelines & manuals, backups, inventory update …).

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1
IEC 62443-2-1:2010, Clause 4.3.3.3.9, 4.3.4.4.1
IEC 62443-3-3:2013, SR 4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.10, 7.10, 7.14

PR.DS-4: Adequate capacity to ensure availability is maintained.

Capacity planning shall ensure adequate resources for organization's critical system information processing, networking, telecommunications, and data storage.

Guidance

No additional guidance on this topic.

The organization's critical systems shall be protected against denial-of-service attacks or at least the effect of such attacks will be limited.

Guidance

No additional guidance on this topic.

Audit data from the organization's critical systems shall be moved to an alternative system.

Guidance

Be aware that log services can become a bottleneck and hinder the correct functioning of the source systems.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.1, 8.1, Annex A (see ISO 27002**)**
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.14, 8.32

PR.DS-5: Protections against data leaks are implemented.

The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected.

Guidance

- Consider implementing dedicated protection measures (restricted access rights, daily backups, data encryption, installation of firewalls, etc.) for the most sensitive data.
- Consider frequent audit of the configuration of the central directory (Active Directory in Windows environment), with specific focus on the access to data of key persons in the company.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3
IEC 62443-3-3:2013 SR 5.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.3, 5.10, 5.13, 5.14, 5.15, 6.1, 6.2, 6.5, 6.6, 7.5, 7.6, 7.8, 8.2, 8.3, 8.4, 8.18, 8.20, 8.22, 8.24, 8.26

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.

The organization shall implement software, firmware, and information integrity checks to detect unauthorized changes to its critical system components during storage, transport, start-up and when determined necessary.

Guidance

State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

The organization shall implement automated tools where feasible to provide notification upon discovering discrepancies during integrity verification.

Guidance

No additional guidance on this topic.

The organization shall implement automatic response capability with pre-defined security safeguards when integrity violations are discovered.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2, 7
IEC 62443-3-3:2013, SR 3.1, SR 3.3, SR 3.4, SR 3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.7, 8.19, 8.26, 8.32

PR.DS-7: The development and testing environment(s) are separate from the production environment.

The development and test environment(s) shall be isolated from the production environment.

Guidance

- Any change one wants to make to the ICT/OT environment should first be tested in an environment that is different and separate from the production environment (operational environment) before that change is effectively implemented . That way, the effect of those changes can be analysed and adjustments can be made without disrupting operational activities.
- Consider adding and testing cybersecurity features as early as during development (secure development lifecycle principles).

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 16,
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.31

PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.

The organization shall implement hardware integrity checks to detect unauthorized tampering to its critical system's hardware.

Guidance

State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

The organization shall incorporate the detection of unauthorized tampering to its critical system's hardware into the organization incident response capability.

Guidance

No additional guidance on this topic.

References

IEC 62443-2-1:2010, Clause 4.3.4.4.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 7.13

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles.

The organization shall develop, document, and maintain a baseline configuration for its business-critical systems.
- key measure -

Guidance

- This control includes the concept of least functionality.
- Baseline configurations include for example, information about organization's business critical systems, current version numbers and patch information on operating systems and applications, configuration settings/parameters, network topology, and the logical placement of those components within the system architecture.
- Network topology should include the nerve points of the IT/OT environment (external connections, servers hosting data and/or sensitive functions, DNS services security, etc.).

The organization shall configure its business-critical systems to provide only essential capabilities. Therefore, the baseline configuration shall be reviewed, and unnecessary capabilities shall be disabled.

Guidance

- Configuration of a system to provide only organization-defined mission essential capabilities is known as the “concept of least functionality”.
- Capabilities include functions, ports, protocols, software, and/or services.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.19, A.8.32

PR.IP-2: A System Development Life Cycle to manage systems is implemented.

The system and application development life cycle shall include security considerations.

Guidance

- System and application development life cycle should include the acquisition process of the organization's business critical systems and its components.
- Vulnerability awareness and prevention training for (web application) developers, and advanced social engineering awareness training for high-profile roles should be considered.
- When hosting internet facing applications the implementation of a web application firewall (WAF) should be considered.

The development process for critical systems and system components shall cover the full design cycle and shall provide a description of the functional properties of security controls, and design and implementation information for security-relevant system interfaces.

Guidance

The development cycle includes:

- All development phases: specification , design, development, implementation.
- Configuration management for planned and unplanned changes and change control during the development.
- Flaw tracking & resolution.
- Security testing.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 16
IEC 62443-2-1:2010, Clause 4.3.4.3.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.8, 8.25, 8.27

PR.IP-3: Configuration change control processes are in place.

Changes shall be tested and validated before being implemented into operational systems.

Guidance

No additional guidance on this topic.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.19, 8.32

For planned changes to the organization's critical systems, a security impact analysis shall be performed in a separate test environment before implementation in an operational environment.

Guidance

No additional guidance on this topic.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.19, 8.32

PR.IP-4: Backups of information are conducted, maintained, and tested.

Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides.

- key measure -

Guidance

- Organization's business critical system's data includes for example software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, etc.
- Consider a regular backup and put it offline periodically.
- Recovery time and recovery point objectives should be considered.
- Consider not storing the organization's data backup on the same network as the system on which the original data resides and provide an offline copy. Among other things, this prevents file encryption by hackers (risk of ransomware).

The reliability and integrity of backups shall be verified and tested on regular basis.

Guidance

This should include regular testing of the backup restore procedures.

Backup verification shall be coordinated with the functions in the organization that are responsible for related plans.

Guidance

- Related plans include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Cyber Incident response plans.
- Restoration of backup data during contingency plan testing should be provided.

A separate alternate storage site for system backups shall be operated and the same security safeguards as the primary storage location shall be employed.

Guidance

An offline backup of your data is ideally stored in a separate physical location from the original data source and where feasible offsite for extra protection and security.

Critical system backup shall be separated from critical information backup.

Guidance

Separation of critical system backup from critical information backup should lead to a shorter recovery time.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.29, 5.33, 8.13

PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.

The organization shall define, implement, and enforce policy and procedures regarding emergency and safety systems, fire protection systems, and environment controls for its critical systems.

Guidance

The below measures should be considered:

- Protect unattended computer equipment with padlocks or a locker and key system.
- Fire suppression mechanisms should take the organization's critical system environment into account (e.g., water sprinkler systems could be hazardous in specific environments).

The organization shall implement fire detection devices that activate and notify key personnel automatically in the event of a fire.

Guidance

No additional guidance on this topic.

References

IEC 62443-2-1:2010, Clause 4.3.3.3.1, 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1, 6.1, 7.1, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 7.5, 7.8, 7.11, 7.12

PR.IP-6: Data is destroyed according to policy.

The organization shall ensure that its critical system's data is destroyed according to policy.

Guidance

- Disposal actions include media sanitization actions (See PR.DS-3)
- There are two primary types of media in common use:
  - Hard copy media (physical representations of information)
  - Electronic or soft copy media (the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment…)

Sanitation processes shall be documented and tested.

Guidance

- Sanitation processes include procedures and equipment.
- Consider applying non-destructive sanitization techniques to portable storage devices.
- Consider sanitation procedures in proportion to confidentiality requirements.

References

IEC 62443-2-1:2010, Clause 4.3.4.4.4
IEC 62443-3-3:2013, SR 4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.10, 7.10, 7.14

PR.IP-7: Protection processes are improved.

The organization shall incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process updates (continuous improvement).

Guidance

No additional guidance on this topic.

The organization shall implement independent teams to assess the protection process(es).

Guidance

- Independent teams may include internal or external impartial personnel.
- Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, or management of the organization's critical system under assessment or to the determination of security control effectiveness.

The organization shall ensure that the security plan for its critical systems facilitates the review, testing, and continual improvement of the security protection processes.

Guidance

No additional guidance on this topic.

References

IEC 62443-2-1:2010, Clause 4.4.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 9, 10.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.27

PR.IP-8: Effectiveness of protection technologies is shared.

The organization shall collaborate and share information about its critical system's related security incidents and mitigation measures with designated partners.

Guidance

No additional guidance on this topic.

Communication of effectiveness of protection technologies shall be shared with appropriate parties.

Guidance

No additional guidance on this topic.

The organization shall implement, where feasible, automated mechanisms to assist in information collaboration.

Guidance

No additional guidance on this topic.

References

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.4, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.27

PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

Incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) shall be established, maintained, approved, and tested to determine the effectiveness of the plans, and the readiness to execute the plans.

Guidance

- The incident response plan is the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack.
- Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information.
- Maintaining essential functions despite system disruption, and the eventual restoration of the organization's systems, should be addressed.
- Consider defining incident types, resources and management support needed to effectively maintain and mature the incident response and contingency capabilities.

The organization shall coordinate the development and the testing of incident response plans and recovery plans with stakeholders responsible for related plans.

Guidance

Related plans include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber incident response plans, and Occupant Emergency Plans.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1, 4.2, 6, 8, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.24, 5.29

PR.IP-11: Cybersecurity is included in human resources practices (deprovisioning, personnel screening…).

Personnel having access to the organization's most critical information or technology shall be verified.

Guidance

- The access to critical information or technology should be considered when recruiting, during employment and at termination.
- Background verification checks should take into consideration applicable laws, regulations, and ethics in proportion to the business requirements, the classification of the information to be accessed and the perceived risks

Develop and maintain a human resource information/cyber security process that is applicable when recruiting, during employment and at termination of employment.

Guidance

The human resource information/cyber security process should include access to critical information or technology; background verification checks; code of conduct; roles, authorities, and responsibilities…

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1, 4.2, 7.1, 7.3, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.4, 5.11, 6.1, 6.2, 6.3, 6.4, 6.5

PR.IP-12: A vulnerability management plan is developed and implemented.

The organization shall establish and maintain a documented process that allows continuous review of vulnerabilities and strategies to mitigate them.

Guidance

- Consider inventorying sources likely to report vulnerabilities in the identified components and distribute updates (software publisher websites, CERT website, ENISA website).
- The organization should identify where its critical system's vulnerabilities may be exposed to adversaries.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2, 4, 5, 16, 18
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6, 8, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.36, 6.8, 8.8, 8.32

Maintenance and repair of industrial control and information system components are performed consistent with policies and procedures.

PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

Patches and security updates for Operating Systems and critical system components shall be installed.

- key measure -

Guidance

The following should be considered:

- Limit yourself to only install those applications (operating systems, firmware, or plugins) that you need to run your business and patch/update them regularly.
- You should only install a current and vendor-supported version of software you choose to use. It may be useful to assign a day each month to check for patches.
- There are products which can scan your system and notify you when there is an update for an application you have installed. If you use one of these products, make sure it checks for updates for every application you use.
- Install patches and security updates in a timely manner.

The organization shall plan, perform, and document preventive maintenance and repairs on its critical system components according to approved processes and tools.

Guidance

The following should be considered:

- Perform security updates on all software in a timely manner.
- Automate the update process and audit its effectiveness.
- Introduce an internal patching culture on desktops, mobile devices, servers, network components, etc. to ensure updates are tracked.

The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.

- Key measure -

Guidance

This requirement mainly focuses on OT/ICS environments.

The organization shall enforce approval requirements, control, and monitoring of maintenance tools for use on its critical systems.

Guidance

Maintenance tools can include hardware/software diagnostic test equipment, hardware/software packet sniffers and laptops.

Maintenance tools and portable storage devices shall be inspected when brought into the facility and shall be protected by anti-malware solutions so that they are scanned for malicious code before they are used on organization's systems.
- Key measure -

Guidance

No additional guidance on this topic.

The organization shall verify security controls following hardware and software maintenance or repairs/patching and take action as appropriate.
- Key measure -

Guidance

No additional guidance on this topic.

References

IEC 62443-2-1:2010, Clause 4.3.3.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.2, 7.1, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 7.2, 7.9, 7.10, 7.13

PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

Remote maintenance shall only occur after prior approval, monitoring to avoid unauthorised access, and approval of the outcome of the maintenance activities as described in approved processes or procedures.

Guidance

No additional guidance on this topic.

The organization shall require that diagnostic services pertaining to remote maintenance be performed from a system that implements a security capability comparable to the capability implemented on the equivalent organization's critical system.

Guidance

No additional guidance on this topic.

The organization shall make sure that strong authenticators, record keeping, and session termination for remote maintenance is implemented.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 7
IEC 62443-2-1:2010, Clause 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.2, 7.1, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.19, 5.22, 7.13

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

Logs shall be maintained, documented, and reviewed.
- key measure -

Guidance

- Ensure the activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) is enabled.
- Logs should be backed up and saved for a predefined period.
- The logs should be reviewed for any unusual or unwanted trends, such as a large use of social media websites or an unusual number of viruses consistently found on a particular computer. These trends may indicate a more serious problem or signal the need for stronger protections in a particular area.

The organization shall ensure that the log records include an authoritative time source or internal clock time stamp that are compared and synchronized to an authoritative time source.

Guidance

Authoritative time sources include for example, an internal Network Time Protocol (NTP) server, radio clock, atomic clock, GPS time source.

The organization shall ensure that audit processing failures on the organization's systems generate alerts and trigger defined responses.

Guidance

The use of System Logging Protocol (Syslog) servers can be considered.

The organization shall enable authorized individuals to extend audit capabilities when required by events.

Guidance

No additional guidance on this topic.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 9.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.15, 8.17, 8.34

PR.PT-2: Removable media is protected, and its use restricted according to policy.

The usage restriction of portable storage devices shall be ensured through an appropriate documented policy and supporting safeguards.

Guidance

No additional guidance on this topic.

Portable storage devices containing system data shall be controlled and protected while in transit and in storage.

- key measure -

Guidance

Protection and control should include the scanning of all portable storage devices for malicious code before they are used on organization's systems.

The organization should technically prohibit the connection of removable media unless strictly necessary; in other instances, the execution of autoruns from such media should be disabled.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 10
IEC 62443-3-3:2013, SR 2.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.1, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.10, 5.12, 5.13, 7.7, 7.10

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.

The organization shall configure the business-critical systems to provide only essential capabilities.

Guidance

Consider applying the principle of least functionality to access systems and assets (see also PR.AC-4).

The organization shall disable defined functions, ports, protocols, and services within its critical systems that it deems unnecessary.

Guidance

No additional guidance on this topic.

The organization shall implement technical safeguards to enforce a deny-all, permit-by-exception policy to only allow the execution of authorized software programs.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 7
IEC 62443-2-1:2010, Clause 4.3.3.5, 4.3.3.6, 4.3.3.7
IEC 62443-3-3:2013, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.1, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.15

PR.PT-4: Communications and control networks are protected.

Web and e-mail filters shall be installed and used.

Guidance

- E-mail filters should detect malicious e-mails, and filtering should be configured based on the type of message attachments so that files of the specified types are automatically processed (e.g. deleted).
- Web-filters should notify the user if a website may contain malware and potentially preventing users from accessing that website.

The organization shall control the information flows/data flows within its critical systems and between interconnected systems.

Guidance

Consider the following:

- Information flow may be supported, for example, by labelling or colouring physical connectors as an aid to manual hook-up.
- Inspection of message content may enforce information flow policy. For example, a message containing a command to an actuator may not be permitted to flow between the control network and any other network.
- Physical addresses (e.g., a serial port) may be implicitly or explicitly associated with labels or attributes (e.g., hardware I/O address). Manual methods are typically static. Label or attribute policy mechanisms may be implemented in hardware, firmware, and software that controls or has device access, such as device drivers and communications controllers.

The organization shall manage the interface for external communication services by establishing a traffic flow policy, protecting the confidentiality and integrity of the information being transmitted; This includes the review and documenting of each exception to the traffic flow policy.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 10, 12, 13
IEC 62443-3-3:2013, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.14, 8.20, 8.26

Anomalous activity is detected and the potential impact of events is understood.

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

The organization shall ensure that a baseline of network operations and expected data flows for its critical systems is developed, documented, and maintained to track events.
- key measure -

Guidance

- Consider enabling local logging on all your systems and network devices and keep them for a certain period, for example up to 6 months.
- Ensure that your logs contain enough information (source, date, user, timestamp, etc.) and that you have enough storage space for their generation.
- Consider centralizing your logs.
- Consider deploying a Security Information and Event Management tool (SIEM) that will facilitate the correlation and analysis of your data.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 8, 13
IEC 62443-2-1:2010, Clause 4.4.3.3
ISO/IEC 27001:2012, Clause 8.1, 9.1, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.37, 8.20, 8.21, 8.32

DE.AE-2: Detected events are analysed to understand attack targets and methods.

The organization shall review and analyse detected events to understand attack targets and methods.

Guidance

No additional guidance on this topic.

The organization shall implement automated mechanisms where feasible to review and analyse detected events.

Guidance

Consider reviewing your logs regularly to identify anomalies or abnormal events.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 8, 13, 15
IEC 62443-2-1:2010, Clause 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
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, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, 9.1, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.24, 5.25, 8.15

DE.AE-3: Event data are collected and correlated from multiple sources and sensors.

The activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.
- key measure -

Guidance

- Logs should be backed up and saved for a predefined period.
- The logs should be reviewed for any unusual or unwanted trends, such as a large use of social media websites or an unusual number of viruses consistently found on a particular computer. These trends may indicate a more serious problem or signal the need for stronger protections in a particular area.

The organization shall ensure that event data is compiled and correlated across its critical systems using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Guidance

No additional guidance on this topic.

The organization shall integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; its critical system's monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 3, 8, 10, 13, 15
IEC 62443-3-3:2013, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, 9.1, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.28, 8.15

DE.AE-4: Impact of events is determined.

Negative impacts to organization’s operations, assets, and individuals resulting from detected events shall be determined and correlated with risk assessment outcomes.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 13
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, 9.1, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.25

DE.AE-5: Incident alert thresholds are established.

The organization shall implement automated mechanisms and system generated alerts to support event detection and to assist in the identification of security alert thresholds.

Guidance

No additional guidance on this topic.

The organization shall define incident alert thresholds.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 13
IEC 62443-2-1:2010, Clause 4.2.3.10
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, 9.1, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.25

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

DE.CM-1: The network is monitored to detect potential cybersecurity events.

Firewalls shall be installed and operated on the network boundaries and completed with firewall protection on the endpoints.

Guidance

- Endpoints include desktops, laptops, servers...
- Consider, where feasible, including smart phones and other networked devices when installing and operating firewalls.
- Consider limiting the number of interconnection gateways to the Internet.

The organization shall monitor and identify unauthorized use of its business-critical systems through the detection of unauthorized local connections, network connections and remote connections.

- key measure -

Guidance

- Monitoring of network communications should happen at the external boundary of the organization's business critical systems and at key internal boundaries within the systems.
- When hosting internet facing applications the implementation of a web application firewall (WAF) should be considered.

The organization shall conduct ongoing security status monitoring of its network to detect defined information/cybersecurity events and indicators of potential information/cybersecurity events.

Guidance

Security status monitoring should include:

- The generation of system alerts when indications of compromise or potential compromise occur.
- Detection and reporting of atypical usage of organization's critical systems.
- The establishment of audit records for defined information/cybersecurity events.
- Boosting system monitoring activity whenever there is an indication of increased risk.
- Physical environment, personnel, and service provider.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 8, 10, 13
IEC 62443-2-1:2010, Clause 4.3.3.3.8
IEC 62443-3-3:2013, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.22, 8.15, 8.30

The physical environment of the facility shall be monitored for potential information/cybersecurity events.

Guidance

No additional guidance on this topic.

DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.

The physical access to organization's critical systems and devices shall be, on top of the physical access monitoring to the facility, increased through physical intrusion alarms, surveillance equipment, independent surveillance teams.

Guidance

It is recommended to log all visitors.

References

IEC 62443-2-1:2010, Clause 4.3.3.3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.22, 7.1, 7.2, 8.15, 8.30

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.

Endpoint and network protection tools to monitor end-user behaviour for dangerous activity shall be implemented.

Guidance

Consider deploying an Intrusion Detection/Prevention system (IDS/IPS).

Endpoint and network protection tools that monitor end-user behaviour for dangerous activity shall be managed.

Guidance

- Consider using a centralized log platform for the consolidation and exploitation of log files.
- Consider to actively investigate the alerts generated because of suspicious activities and take the appropriate actions to remediate the threat, e.g. through the deployment of a security operations centre (SOC).

Software usage and installation restrictions shall be enforced.

Guidance

Only authorized software should be used, and user access rights should be limited to the specific data, resources and applications needed to complete a required task (least privilege principle).

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 8, 13, 15
IEC 62443-3-3:2013, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.15

DE.CM-4: Malicious code is detected.

Anti-virus, -spyware, and other -malware programs shall be installed and updated.
- key measure -

Guidance

- Malware includes viruses, spyware, and ransomware and should be countered by installing, using, and regularly updating anti-virus and anti-spyware software on every device used in company's business (including computers, smart phones, tablets, and servers).
- Anti-virus and anti-spyware software should automatically check for updates in "real-time" or at least daily followed by system scanning as appropriate.
- It should be considered to provide the same malicious code protection mechanisms for home computers (e.g. teleworking) or personal devices that are used for professional work (BYOD).

The organization shall set up a system to detect false positives while detecting and eradicating malicious code.

Guidance

No additional guidance on this topic.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.7

DE.CM-5: Unauthorized mobile code is detected.

The organization shall define acceptable and unacceptable mobile code and mobile code technologies; and authorize, monitor, and control the use of mobile code within the system.

Guidance

- Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Mobile code technologies include for example Java applets, JavaScript, HTML5, WebGL, and VBScript.
- Decisions regarding the use of mobile code in organizational systems should be based on the potential for the code to cause damage to the systems if used maliciously. Usage restrictions and implementation guidance should apply to the selection and use of mobile code installed.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 10
IEC 62443-3-3:2013 SR 2.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.19

DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.

All external connections by vendors supporting IT/OT applications or infrastructure shall be secured and actively monitored to ensure that only permissible actions occur during the connection.

Guidance

This monitoring includes unauthorized personnel access, connections, devices, and software.

External service providers' conformance with personnel security policies and procedures and contract security requirements shall be monitored relative to their cybersecurity risks.

Guidance

No additional guidance on this topic.

References

IEC 62443-2-1:2010, Clause 4.3.3.3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.22, 8.15, 8.30

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.

The organization's business critical systems shall be monitored for unauthorized personnel access, connections, devices, access points, and software.

Guidance

- Unauthorized personnel access includes access by external service providers.
- System inventory discrepancies should be included in the monitoring.
- Unauthorized configuration changes to organization's critical systems should be included in the monitoring.

Unauthorized configuration changes to organization's systems shall be monitored and addressed with the appropriate mitigation actions.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 2, 8, 13, 15
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.1, 7.5, 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.22, 8.15, 8.30

DE.CM-8: Vulnerability scans are performed.

The organization shall monitor and scan for vulnerabilities in its critical systems and hosted applications ensuring that system functions are not adversely impacted by the scanning process.

Guidance

Consider the implementation of a continuous vulnerability scanning program; Including reporting and mitigation plans.

The vulnerability scanning process shall include analysis, remediation, and information sharing.

Guidance

No additional guidance on this topic.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.8, 8.29

Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

DE.DP-2: Detection activities comply with all applicable requirements.

The organization shall conduct detection activities in accordance with applicable federal and regional laws, industry regulations and standards, policies, and other applicable requirements.

Guidance

No additional guidance on this topic.

References

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.3, 7.4, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.34, 5.36, 8.8

DE.DP-3: Detection processes are tested.

The organization shall validate that event detection processes are operating as intended.

Guidance

- Validation includes testing.
- Validation should be demonstrable.

References

IEC 62443-2-1:2010, Clause 4.4.3.2
IEC 62443-3-3:2013, SR 3.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.3, 7.4, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.29

DE.DP-4: Event detection information is communicated.

The organization shall communicate event detection information to predefined parties.

Guidance

Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, mobile device connection, altered configuration settings, contrasting system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, use of Voice over Internet Protocol (VoIP), and malware disclosure.

References

IEC 62443-2-1:2010, Clause 4.3.4.5.9
IEC 62443-3-3:2013, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.3, 7.4, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 6.8

DE.DP-5: Detection processes are continuously improved.

Improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned, shall be incorporated into detection process revisions.

Guidance

- This results in a continuous improvement of the detection processes.
- The use of independent teams to assess the detection process could be considered.

The organization shall conduct specialized assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the organization's critical systems.

Guidance

These activities can be outsourced, preferably to accredited organizations.

References

IEC 62443-2-1:2010, Clause 4.4.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.3, 7.4, 8.1, 9, 10.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.27

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

RS.RP-1: Response plan is executed during or after an incident.

An incident response process, including roles, responsibilities, and authorities, shall be executed during or after an information/cybersecurity event on the organization's critical systems.

Guidance

- The incident response process should include a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack.
- The roles, responsibilities, and authorities in the incident response plan should be specific on involved people, contact info, different roles and responsibilities, and who makes the decision to initiate recovery procedures as well as who will be the contact with appropriate external stakeholders.
- It should be considered to determine the causes of an information/cybersecurity event and implement a corrective action in order that the event does not recur or occur elsewhere (an infection by malicious code on one machine did not have spread elsewhere in the network). The effectiveness of any corrective action taken should be reviewed. Corrective actions should be appropriate to the effects of the information/cybersecurity event encountered.

References

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
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, 8.3, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.26

Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

RS.CO-1: Personnel know their roles and order of operations when a response is needed.

The organization shall ensure that personnel understand their roles, objectives, restoration priorities, task sequences (order of operations) and assignment responsibilities for event response.

Guidance

Consider the use the CCB Incident Management Guide to guide you through this exercise and consider bringing in outside experts if needed. Test your plan regularly and adjust it after each incident.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5, 7.3, 7.4, 8.1, 8.3, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.2, 5.24, 6.3

RS.CO-2: Incidents are reported consistent with established criteria.

The organization shall implement reporting on information/cybersecurity incidents on its critical systems in an organization-defined time frame to organization-defined personnel or roles.

Guidance

All users should have a single point of contact to report any incident and be encouraged to do so.

Events shall be reported consistent with established criteria.

Guidance

Criteria to report should be included in the incident response plan.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.5
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5, 7.3, 7.4, 8.1, 8.3, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.5, 6.8

RS.CO-3: Information is shared consistent with response plans.

Information/cybersecurity incident information shall be communicated and shared with the organization's employees in a format that they can understand.

Guidance

No additional guidance on this topic.

The organization shall share information/cybersecurity incident information with relevant stakeholders as foreseen in the incident response plan.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.3, 7.4, 8.1, 8.3, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 6.8

RS.CO-4: Coordination with stakeholders occurs consistent with response plans.

The organization shall coordinate information/cybersecurity incident response actions with all predefined stakeholders.

Guidance

- Stakeholders for incident response include for example, mission/business owners, organization's critical system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.
- Coordination with stakeholders occurs consistent with incident response plans.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.5
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.3, 7.4, 8.1, 8.3, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.6, 5.26

RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

The organization shall share information/cybersecurity event information voluntarily, as appropriate, with external stakeholders, industry security groups… to achieve broader information/cybersecurity situational awareness.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.3, 7.4, 8.1, 8.3, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.6

Analysis is conducted to ensure effective response and support recovery activities.

RS.AN-1: Notifications from detection systems are investigated.

The organization shall investigate information/cybersecurity-related notifications generated from detection systems.

Guidance

No additional guidance on this topic.

The organization shall implement automated mechanisms to assist in the investigation and analysis of information/cybersecurity-related notifications.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
IEC 62443-3-3:2013 SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 9.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.26, 8.15

RS.AN-2: The impact of the incident is understood.

Thorough investigation and result analysis shall be the base for understanding the full implication of the information/cybersecurity incident.

Guidance

- Result analysis can involve the outcome of determining the correlation between the information of the detected event and the outcome of risk assessments. In this way, insight is gained into the impact of the event across the organization.
- Consider including detection of unauthorized changes to its critical systems in its incident response capabilities.

The organization shall implement automated mechanisms to support incident impact analysis.

Guidance

Implementation could vary from a ticketing system to a Security Information and Event Management (SIEM).

References

IEC 62443-2-1:2010, Clause 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1, 4.2, 9.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.25, 5.27

RS.AN-3: Forensics are performed.

The organization shall provide on-demand audit review, analysis, and reporting for after-the-fact investigations of information/cybersecurity incidents.

Guidance

No additional guidance on this topic.

The organization shall conduct forensic analysis on collected information/cybersecurity event information to determine root cause.

Guidance

Consider determining the root cause of an incident. If necessary, use forensics analysis on collected information/cybersecurity event information to achieve this.

References

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/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1, 4.2, 9, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.28

RS.AN-4: Incidents are categorized consistent with response plans.

Information/cybersecurity incidents shall be categorized according to the level of severity and impact consistent with the evaluation criteria included the incident response plan.

Guidance

- It should be considered to determine the causes of an information/cybersecurity incident and implement a corrective action in order that the incident does not recur or occur elsewhere.
- The effectiveness of any corrective action taken should be reviewed.
- Corrective actions should be appropriate to the effects of the information/cybersecurity incident encountered.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6, 8.3, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.25

RS.AN-5: Processes are established to receive, analyse, and respond to vulnerabilities disclosed to the organization from internal and external sources.

The organization shall implement vulnerability management processes and procedures that include processing, analysing and remedying vulnerabilities from internal and external sources.
- key measure -

Guidance

Internal and external sources could be e.g. internal testing, security bulletins, or security researchers.

The organization shall implement automated mechanisms to disseminate and track remediation efforts for vulnerability information, captured from internal and external sources to key stakeholders.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6, 7.5, 8.3, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.8

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities

RS.MI-1: Incidents are contained.

RS.MI-2: Incidents are mitigated.

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.

The organization shall implement an incident handling capability for information/cybersecurity incidents on its business-critical systems that includes preparation, detection and analysis, containment, eradication, recovery, and documented risk acceptance.

Guidance

A documented risk acceptance deals with risks that the organization assesses as not dangerous to the organization's business critical systems and where the risk owner formally accepts the risk (related with the risk appetite of the organization)

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.6
IEC 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6, 7.5, 8.3, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.26, 8.7, 8.8

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities

RS.IM-1: Response plans incorporate lessons learned.

The organization shall conduct post-incident evaluations to analyse lessons learned from incident response and recovery, and consequently improve processes/procedures/technologies to enhance its cyber resilience.

Guidance

Consider bringing involved people together after each incident and reflect together on ways to improve what happened, how it happened, how we reacted, how it could have gone better, what should be done to prevent it from happening again, etc.

Lessons learned from incident handling shall be translated into updated or new incident handling procedures that shall be tested, approved and trained.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control
IEC 62443-2-1:2010, Clause 4.3.4.5.10, 4.4.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6.1, 8.3, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.26, 5.27

RS.IM-2: Response and Recovery strategies are updated.

The organization shall update the response and recovery plans to address changes in its context.

Guidance

The organization's context relates to the organizational structure, its critical systems, attack vectors, new threats, improved technology, environment of operation, problems encountered during plan implementation/execution/testing and lessons learned.

References

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6.1, 8.3, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.27

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.

A recovery process for disasters and information/cybersecurity incidents shall be developed and executed as appropriate.

Guidance

- A process should be developed for what immediate actions will be taken in case of a fire, medical emergency, burglary, natural disaster, or an information/cyber security incident.
- The process should consider:
  - Roles and Responsibilities, including of who makes the decision to initiate recovery procedures and who will be the contact with appropriate external stakeholders.
  - What to do with company's information and information systems in case of an incident. This includes shutting down or locking computers, moving to a backup site, physically removing important documents, etc.
  - Who to call in case of an incident.

The essential organization's functions and services shall be continued with little or no loss of operational continuity and continuity shall be sustained until full system restoration.

Guidance

No additional guidance on this topic.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 11
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.26

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

RC.IM-1: Recovery plans incorporate lessons learned.

The organization shall incorporate lessons learned from incident recovery activities into updated or new system recovery procedures and, after testing, frame this with appropriate training.

Guidance

No additional guidance on this topic.

References

IEC 62443-2-1:2010, Clause 4.4.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.27

RC.IM-2: Recovery strategies are updated.

This requirement is combined with RS.IM-2.

Guidance

No additional guidance on this topic.

References

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.6

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

RC.CO-1: Public relations are managed.

The organization shall centralize and coordinate how information is disseminated and manage how the organization is presented to the public.

Guidance

Public relations management may include, for example, managing media interactions, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and e-mail requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of information provided to the media, ensuring personnel are familiar with public relations and privacy policies.

A Public Relations Officer shall be assigned.

Guidance

The Public Relations Officer should consider the use of pre-define external contacts (e.g. press, regulators, interest groups).

References

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5, 7.4, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.6

RC.CO-2: Reputation is repaired after an incident.

The organization shall implement a crisis response strategy to protect the organization from the negative consequences of a crisis and help restore its reputation.

Guidance

Crisis response strategies include, for example, actions to shape attributions of the crisis, change perceptions of the organization in crisis, and reduce the negative effect generated by the crisis.

References

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5, 7.4, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.6

RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

The organization shall communicate recovery activities to predefined stakeholders, executive and management teams.

Guidance

Communication of recovery activities to all relevant stakeholders applies only to entities subject to the NIS legislation.

References

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5, 7.4, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.6

Annex A: List of key measures for the assurance level 'Basic'

PROTECT

PR.AC-1:	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.

(1) Identities and credentials for authorized devices and users shall be managed.

PR.AC-3:	Remote access is managed.

(2) The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).

PR.AC-4:	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

(3) Access permissions for users to the organization's systems shall be defined and managed.
(4) It shall be identified who should have access to the organization's business's critical information and technology and the means to get access.
(5) Employee access to data and information shall be limited to the systems and specific information they need to do their jobs.
(6) Nobody shall have administrator privileges for daily tasks.

PR.AC-5:	Network integrity is protected (e.g., network segregation, network segmentation).

(7) Firewalls shall be installed and activated on all the organization's networks.
(8) Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.

PR.IP-4:	Backups of information are conducted, maintained, and tested.

(9) Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides.

PR.MA-1:	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

(10) Patches and security updates for Operating Systems and critical system components shall be installed.

PR.PT-1:	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

(11) Logs shall be maintained, documented, and reviewed.

DETECT

DE.AE-3: Event data are collected and correlated from multiple sources and sensors.

(12) The activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.

DE.CM-4: Malicious code is detected.

(13) Anti-virus, -spyware, and other -malware programs shall be installed and updated.

Annex B: List of additional key measures for the assurance level 'Important' and 'Essential'

The list below is **in addition** to the key measures for the assurance level 'Basic'.

IDENTIFY

ID.AM-6: Cybersecurity roles, responsibilities, and authorities for the entire workforce and third-party stakeholders are established.

(1) Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners.

PROTECT

PR.AC-3: Remote access is managed.

(2) Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment shall be identified, documented, and implemented.

PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).

(3) Where appropriate, network integrity of the organization's critical systems shall be protected by (1) identifying, documenting, and controlling connections between system components and (2) Limiting external connections to the organization's critical systems.

(4) The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where appropriate.

PR.DS-5: Protections against data leaks are implemented.

(5) The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected.

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles.

(6) The organization shall develop, document, and maintain a baseline configuration for its business-critical systems.

DETECT

DE.CM-1: The network is monitored to detect potential cybersecurity events.

(7) The organization shall monitor and identify unauthorized use of its business-critical systems through the detection of unauthorized local connections, network connections and remote connections.

RESPOND

RS.AN-5:	Processes are established to receive, analyse, and respond to vulnerabilities disclosed to the organization from internal and external sources.

(8) The organization shall implement vulnerability management processes and procedures that include processing, analysing and remedying vulnerabilities from internal and external sources.

Annex C: List of additional key measures for the assurance level 'Essential'

The list below is **in addition** to the key measures for the assurance levels 'Basic' and 'Important'.

IDENTIFY

ID.SC-3: Cybersecurity roles, responsibilities, and authorities for the entire workforce and third-party stakeholders are established.

(1) Contractual 'information security and cybersecurity' requirements for suppliers and third-party partners shall be implemented to ensure a verifiable flaw remediation process, and to ensure the correction of flaws identified during 'information security and cybersecurity' testing and evaluation.

(2) The organization shall establish contractual requirements permitting the organization to review the 'information security and cybersecurity' programs implemented by suppliers and third-party partners

PROTECT

PR.AC-7: Identities are proofed and bound to credentials and asserted in interactions.

(3) The organization shall perform a documented risk assessment on organization's critical system transactions and authenticate users, devices, and other assets (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

(4) The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.

(5) Maintenance tools and portable storage devices shall be inspected when brought into the facility and shall be protected by anti-malware solutions so that they are scanned for malicious code before they are used on organization's systems.

(6) The organization shall verify security controls following hardware and software maintenance or repairs/patching and take action as appropriate.

PR.PT-2: Removable media is protected, and its use restricted according to policy.

(7) Portable storage devices containing system data shall be controlled and protected while in transit and in storage.

DETECT

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

(8) The organization shall ensure that a baseline of network operations and expected data flows for its critical systems is developed, documented, and maintained to track events.

Disclaimer

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

This document contains technical information written mainly in English. This information related to the security of networks and information systems is addressed to IT services which use the English terms of computer language. A translation into Dutch, French or German of this technical information is also made available by the CCB.

The CCB accepts **no responsibility for the content** of this document.
The information provided:

- is exclusive of a general nature and do not intend to take into consideration all particular situations.
- is not necessarily exhaustive, precise, or up to date on all points.

Responsible editor

Centre for Cybersecurity Belgium
Mr. De Bruycker, Director General
Rue de la Loi, 18
1000 Brussels

Legal depot

D/2023/14828/001