CyFun®

ESSENTIAL

CYBERFUNDAMENTALS

Version 2025-10-01

TABLE OF CONTENTS

PROTECT 29

INTRODUCTION

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

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

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

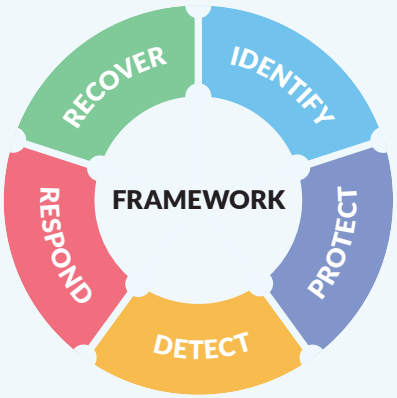
The coding of the requirements corresponds with the codes used in the NIST CSF Framework. Since not all NIST CSF requirements are applicable, some codes that do exist in the NIST CSF framework may be missing.

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

The **CyberFundamentals Framework** is built around five core functions: identify, protect, detect, respond, and recover. Regardless of the organisation and industry, these functions make it possible to promote communication around cybersecurity among technical practitioners and stakeholders alike, so that cyber-related risks can be incorporated into the overall risk management strategy of the organisation.

Identify

Being aware of important cyber threats to your most valuable assets. Essentially, you can't protect what you don't know exists. This function helps develop an organisational understanding of how to manage cybersecurity 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 cybersecurity events.

Respond

The Respond function is all about the controls that help respond to cybersecurity incidents. The Respond function supports the ability to contain the impact of a potential cybersecurity incident.

Recover

The Recover function focuses on those safeguards that help maintain resilience and restore services that have been affected by a cybersecurity incident.

To respond to the severity of the threat an organisation is exposed to, and in addition to the starting level ***Small***, three assurance levels are also 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 that includes 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 and thereby achieve a higher level of assurance.

The **assurance level *Important*** is designed to minimise known cybersecurity risks and the risks of targeted cyberattacks by actors with common skills and resources

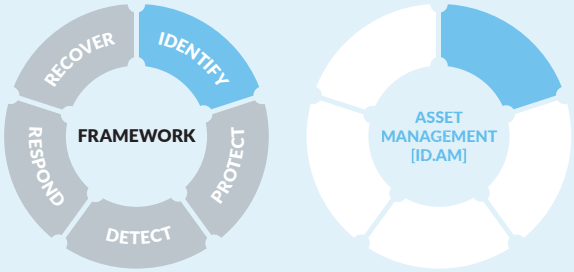
The **assurance level *Essential*** goes a step further to also respond to the risk of advanced cyberattacks by actors with extensive skills and resources.

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 in response to the feedback received from stakeholders, the evolving risk of specific cybersecurity threats, the availability of technical solutions and progressive insight.

IDENTIFY

Identify



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

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

An inventory of assets associated with information and information processing facilities within the organisation 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 organisation'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 organisation's context and include all information necessary for effective accountability.

Guidance

- Inventory specifications include for example, the 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 unauthorised 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 a documented exception, is designated as unauthorised.
- Unauthorised hardware can be detected during inventory, requests for support by the user or other means.

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

Guidance

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

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

An inventory that reflects what software platforms and applications are being used in the organisation 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 unauthorised 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 organisation'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 organisation shall be identified.

Guidance

No additional guidance on this topic.

When unauthorised 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 unauthorised.
- Unauthorised software can be detected during inventory, requests for support by the user or other means.

Mechanisms for detecting the presence of unauthorised software within the organisation'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 organisation may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

ID.AM-3 Organisational communication and data flows are mapped.

Information that the organisation 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 organisation (see ID.AM-1 & ID.AM-2).

All connections within the organisation's ICT/OT environment, and to other organisation-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 organisation's ICT/OT environment, as well as to other organisation-internal systems shall be mapped, documented, authorised, and updated when changes occur.

Guidance

- By having a 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 authorised interfaces only.
  - Heightening system monitoring activity whenever there is an indication of increased risk to the organisation's critical operations and assets.
  - Protecting the system from information leakage due to electromagnetic signals emanations.

ID.AM-4 External information systems are catalogued.

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

Guidance

- The outsourcing of systems, software platforms and applications used within the organisation is covered in ID.AM-1 & ID.AM-2
- External information systems are systems or components of systems for which organisations 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 authorising 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, authorised, and updated when changes occur.

Guidance

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

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

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

Guidance

- Determine the organisation'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 or 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? You should also 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 organisation
  - 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.

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 organisation shall be documented, reviewed, authorised, and updated and alignment with organisation-internal roles and external partners.

Guidance

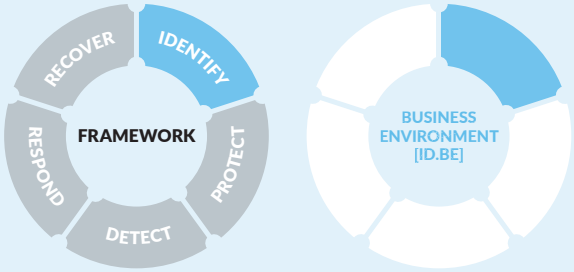
You should consider working through the following tasks:

- Describe security roles, responsibilities, and authorities: who in your organisation 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/cybersecurity (legal, detection activities...).
- Include information/cybersecurity roles and responsibilities for third-party providers with physical or logical access to the organisation's ICT/OT environment.

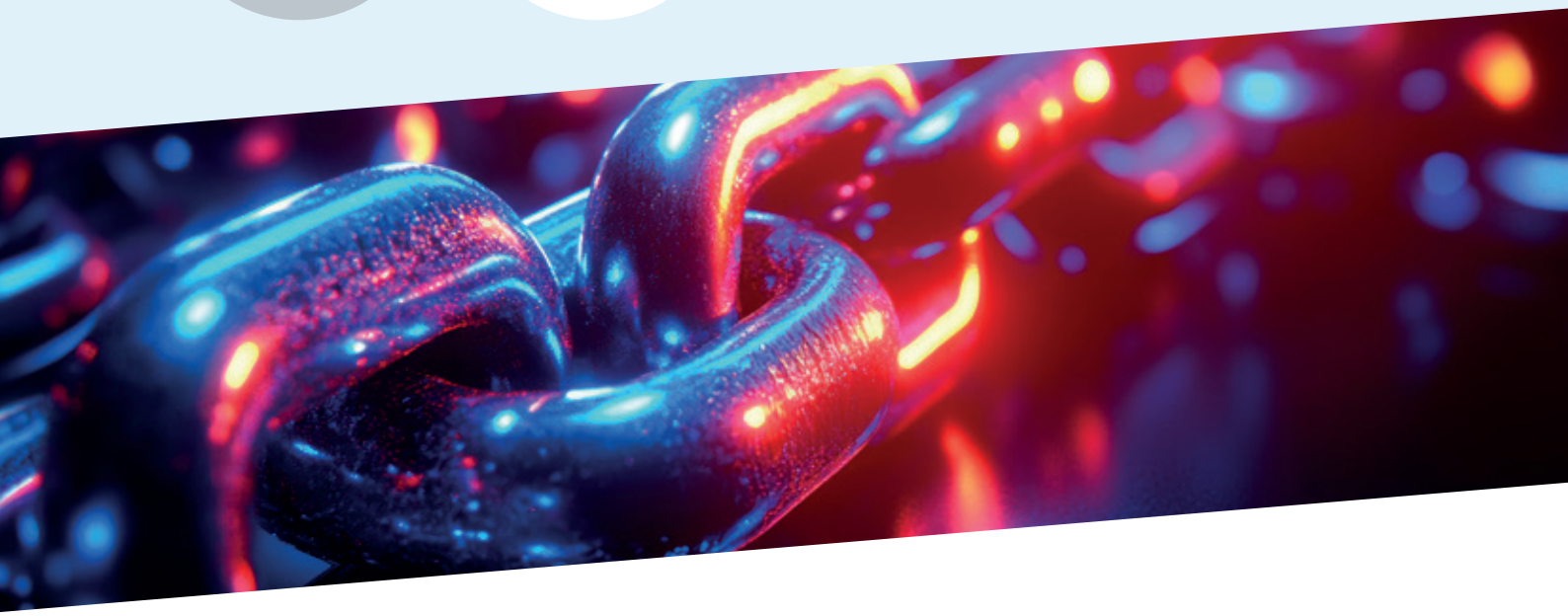
The organisation shall appoint an information security officer.

Guidance

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



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



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

The organisation'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 those entities know where they stand in terms of their critical importance to the organisation's operations.

The organisation 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.

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

The organisation'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.

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

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

Guidance

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

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 prioritised according to their criticality as part of the risk assessment process.

Guidance

Dependencies and business-critical functions should include support services.

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 the Business Impact Analysis (BIA), Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP), for example.

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

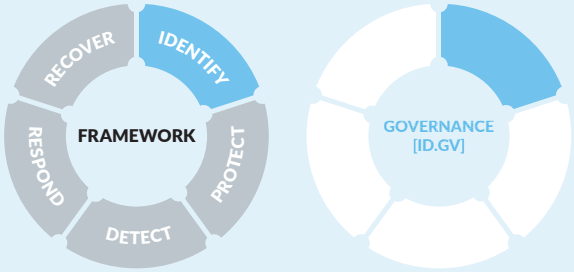
Guidance

- Consider provisioning adequate data and network redundancy (e.g. redundant network devices, servers with load balancing, raid arrays, backup services, two separate datacentres, fail-over network connections, two ISPs...).
- 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, two 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.



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

ID.GV-1 Organisational cybersecurity policy is established and communicated.

Policies and procedures for information security and cybersecurity 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 with regard to your information security expectations, and can aid an investigation in the event of an incident. These policies and procedures should be readily accessible to employees.
- Policies and procedures for information security and cybersecurity should clearly describe your expectations for protecting the organisation'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 organisation or technology. Whenever the policies are changed, employees should be made aware of the changes.

An organisation-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 organisational 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 organisational 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.

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.

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.

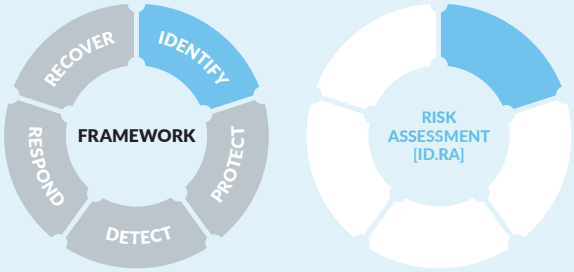
Guidance

This strategy should include determining and allocating the required resources to protect the organisation'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.



The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational 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 organisation's hardware, software, or procedures. It is a gap through which a bad actor can gain access to the organisation's assets. A vulnerability exposes an organisation 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

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

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

Guidance

Consider validating security measures after each penetration test.

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

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

Guidance

A threat and vulnerability awareness programme should include ongoing contact with security groups and associations in order 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 organisations).This contact can include the sharing of information about potential vulnerabilities and incidents. This sharing capability should include a facility to share unclassified and classified information.

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

Guidance

No additional Guidance on this topic.

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

The organisation 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 organisation 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

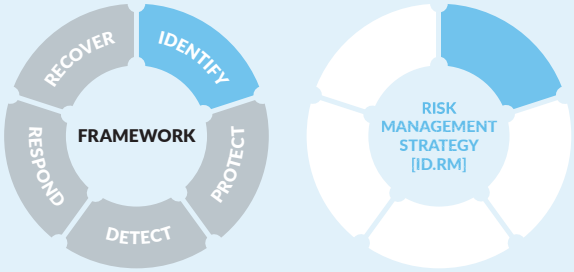
No additional Guidance on this topic.

ID.RA-6 Risk responses are identified and prioritised.

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

Guidance

- Management and employees should be involved in information security 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 organised.



The organisation'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 organisational 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.

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

The organisation shall clearly determine its risk appetite.

Guidance

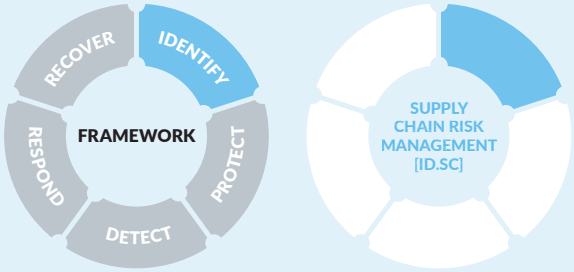
The determination and expression of risk tolerance (risk appetite) should be in line with the policies on information security and cybersecurity, as this will make it easier to demonstrate coherence between policies, risk tolerance and measures.

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

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

Guidance

No additional Guidance on this topic.



The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation 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 organisational stakeholders.

The organisation 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.

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

The organisation shall conduct cyber supply chain risk assessments at least annually or when a change to the organisation'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 prioritise potential negative impacts to the organisation from the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains.

A documented list of all the organisation'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.

ID.SC-3 Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organisation'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 whenever business information contains personal data (applicable on all levels), i.e. security measures need to be addressed within 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.

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

Guidance

No additional Guidance on this topic.

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 organisation 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 organisation 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.

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

The organisation 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 organisation 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.

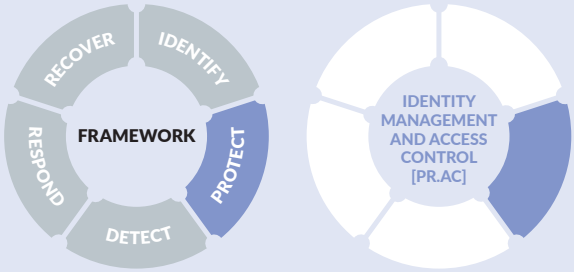
Guidance

No additional Guidance on this topic.


Username
Password
Protected
Balance:
5.367.50 $

PROTECT

Protect



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

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

Identities and credentials for authorised devices and users shall be managed.

Guidance

Identities and credentials for authorised devices and users could be managed by means of a password policy. A password policy is a set of rules designed to enhance ICT/OT security by encouraging organisation's to: (This list is not exhaustive and the measures listed should be considered, as appropriate)

- Change all default passwords.
- Ensure that no one works with administrator privileges when performing 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 whenever 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 authorised 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 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). These must be independent, in that the breach of one must not compromise the reliability of the others. Strong user authentication must be designed in such a way as 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 organisation's critical systems, the organisation 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 organisation's internal and external critical systems.

The organisation'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.

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 strictly managing 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 technically restrict them to given time slots.
- Consider to not leaving internal network access outlets accessible in public areas. These public places include waiting rooms, corridors, for example.

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

Guidance

- Physical access controls may include, for example lists of authorised individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, the monitoring of facility access, and 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 authorised 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, the organisation'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 organisation's critical operations.

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 Wi-Fi 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, connection should be made using an encrypted virtual private network (VPN) capability.
- Manage all endpoint devices (fixed and mobile) in accordance with the organisation's security policies.

Usage restrictions, connection requirements, implementation Guidance, and authorisations for remote access to the organisation's critical systems environment shall be identified, documented, and implemented.

Guidance

Consider the following:

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

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

Guidance

This should include a restriction to ensure that privileged functions can only be used via remote access when authorised.

When accessed remotely, the organisation's networks shall be secured, including through the use of multi-factor authentication (MFA).

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.

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

Access permissions for users to the organisation's systems shall be defined and managed.

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), and to what, in order to perform their duties in the organisation.
- Set up a separate account for each user (including any contractors needing access) and require that strong, unique passwords to be used for each account.
- Ensure that all employees use computer accounts without administrative privileges to perform typical work functions. This includes the 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 organisation'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 organisation's security access policy and applied accordingly.

Guidance

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

It shall be identified who should have access to the organisation's business's critical information and technology and is given the means to obtain access.

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).

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 authorisations that they need to perform their job role.
- Consider:
  - Not allowing any employee to have access to all the business's information.
  - Limiting the number of Internet accesses and interconnections with partner networks to those that are strictly necessary to be able to centralise and homogenise the monitoring of exchanges more easily.
  - Ensuring 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 using different individuals.
- Not allowing 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.

Guidance

Consider the following:

- Separate administrator accounts from user accounts.
- Do not privilege user accounts to perform 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.

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

Firewalls shall be installed and activated on all the organisation's networks.

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 that anti-virus software has been 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 teleworking purposes, home networks and systems have hardware and software firewalls installed are 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, the network integrity of the organisation's critical systems shall be protected by incorporating network segmentation and segregation.

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

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

Guidance

No additional Guidance on this topic.

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

Guidance

Consider implementing the following recommendations:

- Separate your public Wi-Fi network from your business network.
- Protect your business Wi-Fi 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-authorised).

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

Guidance

No additional Guidance on this topic.

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

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

Guidance

No additional Guidance on this topic.

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

Guidance

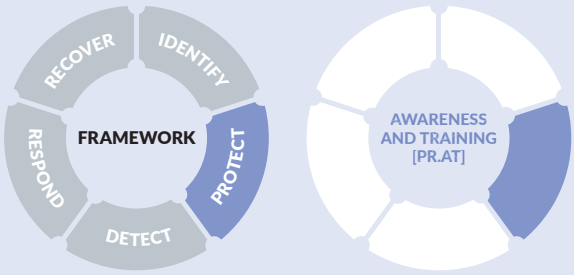
No additional Guidance on this topic.

PR.AC-7 Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organisational risks)

The organisation shall perform a documented risk assessment on its 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 organisational risks).

Guidance

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



The organisation'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 on the subject of 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 organisation 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 programme 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.
- Organise a simulation of a scenario to test your knowledge. Consider performing the exercise for example at least once a year, for example.

The organisation shall implement an evaluation method to measure the effectiveness of the awareness training.

Guidance

No additional Guidance on this topic.

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 their understanding of their roles, responsibilities, and authorities.

Guidance

No additional Guidance on this topic.

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

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

Guidance

Enforcement should include a requirement 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 components of the organisation's business-critical systems.

Guidance

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

The organisation shall monitor business-critical service providers and users in relation to security compliance.

Guidance

Third party audit results can be used as audit evidence.

The organisation shall audit business-critical external service providers in relation to security compliance.

Guidance

Third party audit results can be used as audit evidence.

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

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

Guidance

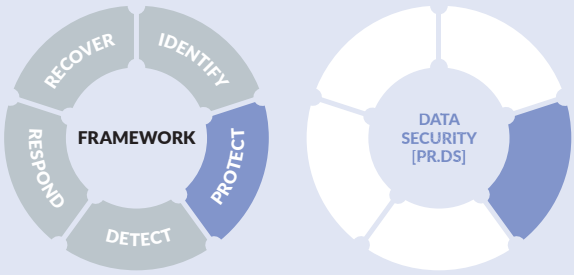
Guidance on role profiles along with their identified titles, missions, tasks, skills, knowledge, competences is available in the "European Cybersecurity Skills Framework Role Profiles" by ENISA. (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles)

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

The organisation shall ensure that personnel responsible for the physical protection and security of the organisation'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.



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

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

The organisation 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 using solutions such as Windows BitLocker®, VeraCrypt, Apple FileVault®, Linux® dm-crypt,...
- Consider encrypting sensitive data stored in the cloud.
- Implement dedicated safeguards to prevent unauthorised 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.

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

The organisation shall protect its critical system information that is deemed 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 using appropriate, supported, and authorised software tools.

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 such as 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 the devices or media themselves are removed and then physically destroyed (or re-commissioned). This is also known as "sanitisation" and therefore relates 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 organisation shall enforce accountability for all its business-critical assets throughout the system life cycle, including removal, transfers, and disposition.

Guidance

Accountability should include:

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

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

Guidance

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

The organisation 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 & organisational means (encryption, Access Control (AC), Mobile Device Management (MDM), monitoring, secure wipe, awareness, signed user agreement, guidelines & manuals, backups, inventory update …).

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

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

Guidance

No additional Guidance on this topic.

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

Guidance

No additional Guidance on this topic.

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

Guidance

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

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

The organisation shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorised 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 performing frequent audits of the configuration of the central directory (Active Directory in Windows environment), specifically focusing on the access to data of key persons in the company.

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

The organisation shall implement software, firmware, and information integrity checks to detect unauthorised changes to its critical system components during storage, transport, start-up and whenever this is deemed necessary.

Guidance

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

Where feasible, the organisation shall implement automated tools to provide notification upon discovering discrepancies during integrity verification.

Guidance

No additional Guidance on this topic.

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

Guidance

No additional Guidance on this topic.

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 life cycle principles).

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

The organisation shall implement hardware integrity checks to detect unauthorised tampering with its critical system's hardware.

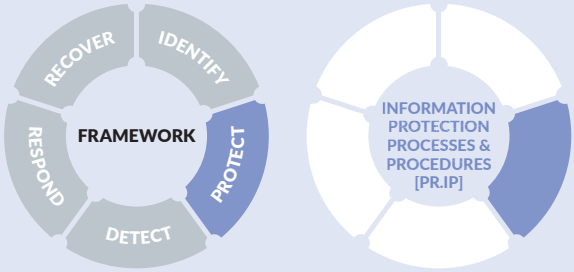
Guidance

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 organisation shall incorporate the detection of unauthorised tampering with its critical system's hardware into the organisation's incident response capability.

Guidance

No additional Guidance on this topic.



Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational 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 organisation shall develop, document, and maintain a baseline configuration for its business-critical systems.

Guidance

- This control includes the concept of least functionality.
- Baseline configurations include for example, information about the organisation'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 organisation shall configure its business-critical systems to provide only essential capabilities. The baseline configuration shall therefore be reviewed, and unnecessary capabilities shall be disabled.

Guidance

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

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

- The system and application development life cycle should include the acquisition process of the organisation'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.

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.

In the case of planned changes to the organisation'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.

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

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

Guidance

- Examples of the organisation's business critical system's data include 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 organisation'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 organisation that are responsible for related plans.

Guidance

- Examples of related plans include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Cyber Incident response plans.
- Provision should be made for the restoration of backup data during contingency plan testing.

A separate alternative 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 to ensure extra protection and security.

Critical system backup shall be separated from critical information backup.

Guidance

Separating critical system backups from critical information backups should lead to a shorter recovery time.

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

The organisation 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 measures listed below should be considered:

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

The organisation 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.

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

The organisation shall ensure that data from its critical systems are destroyed in accordance with policy.

Guidance

- Disposal actions include media sanitisation 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 on hard drives, in random access memory (RAM), read-only memory (ROM) and on disks, memory devices, phones, mobile computing devices, networking equipment...)

Sanitisation processes shall be documented and tested.

Guidance

- Sanitisation processes include procedures and equipment.
- Consider applying non-destructive sanitisation techniques to portable storage devices.
- Consider sanitisation procedures in proportion to the confidentiality requirements.

PR.IP-7 Protection processes are improved.

The organisation 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 organisation 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 organisation's critical system under assessment or with regard to determining the effectiveness of security controls.

The organisation 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.

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

The organisation shall collaborate and share information about security incidents and mitigation measures concerning its critical system with designated partners.

Guidance

No additional Guidance on this topic.

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

Guidance

No additional Guidance on this topic.

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

Guidance

No additional Guidance on this topic.

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 cyberattack.
- 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 organisation's systems, should be addressed.
- Consider defining incident types, resources and management support that are needed to effectively maintain and mature the incident response and contingency capabilities.

The organisation 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.

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

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

Guidance

- Access to critical information or technology should be considered when recruiting, during employment and upon 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/cybersecurity process that is applicable when recruiting, during employment and upon termination of employment.

Guidance

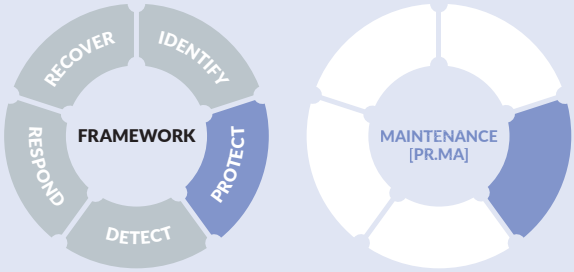
The human resource information/cybersecurity process should include access to critical information or technology; background verification checks; code of conduct; roles, authorities, and responsibilities...

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

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

Guidance

- Consider drawing up an inventory of sources likely to report vulnerabilities in the identified components and distribute updates (software publisher websites, CERT website, ENISA website).
- The organisation should identify where the vulnerabilities of its critical system may be exposed to adversaries.



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

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

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

Guidance

The following should be considered:

- 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 that 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 organisation shall plan, perform, and document preventive maintenance and repairs on its critical system components in accordance with 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 organisation shall prevent the unauthorised removal of maintenance equipment containing critical system information relating to the organisation.

Guidance

This requirement mainly focuses on OT/ICS environments.

The organisation shall enforce requirements for the approval, 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 the organisation's systems.

Guidance

No additional Guidance on this topic.

The organisation shall verify security controls following hardware and software maintenance or repairs/patching and take action as appropriate.

Guidance

No additional Guidance on this topic.

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

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

Guidance

No additional Guidance on this topic.

The organisation 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 critical system of the organisation.

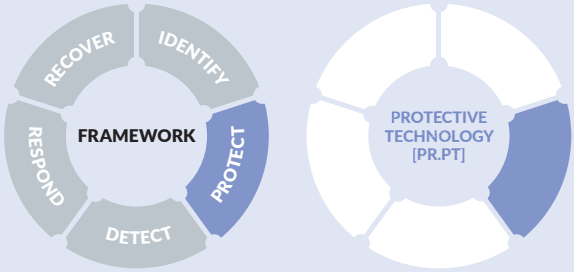
Guidance

No additional Guidance on this topic.

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

Guidance

No additional Guidance on this topic.



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.

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

Guidance

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

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

Guidance

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

The organisation shall enable authorised individuals to extend audit capabilities when required by events.

Guidance

No additional Guidance on this topic.

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

The usage restriction of portable storage devices shall be ensured by means of 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.

Guidance

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

The organisation 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.

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

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

Guidance

No additional Guidance on this topic.

The organisation shall implement technical safeguards to enforce a deny-all, permit-by-exception policy to ensure that only authorised software programs are executed.

Guidance

No additional Guidance on this topic.

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 prevent users from accessing that website.

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

Guidance

Consider the following:

- The information flow may be supported, for example, by labelling or colouring physical connectors as an aid to manual hook-up.
- Inspecting the content of messages 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 access to devices, such as device drivers and communications controllers.

The organisation 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 reviewing and documenting each exception to the traffic flow policy.

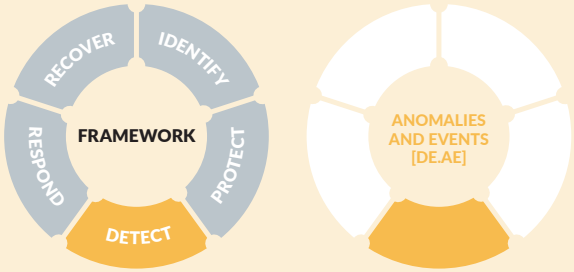
Guidance

No additional Guidance on this topic.


WARNING!
SYSTEM WARNING

DETECT

Detect



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

Guidance

- Consider enabling local logging on all your systems and network devices and retain the logs 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 them, once generated.
- Consider centralising your logs.
- Consider deploying a Security Information and Event Management tool (SIEM) that will facilitate the correlation and analysis of your data.

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

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

Guidance

No additional Guidance on this topic.

Where feasible, the organisation shall implement automated mechanisms to review and analyse detected events.

Guidance

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

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.

Guidance

- Logs should be backed up and saved for a predefined period.
- The logs should be reviewed to identify 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 organisation shall ensure that event data are 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 organisation shall integrate events analysis, where feasible including the analysis of vulnerability scanning information, performance data, its monitoring of its critical system, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.

Guidance

No additional Guidance on this topic.

DE.AE-4 Impact of events is determined.

Negative impacts on the organisation'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.

DE.AE-5 Incident alert thresholds are established.

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

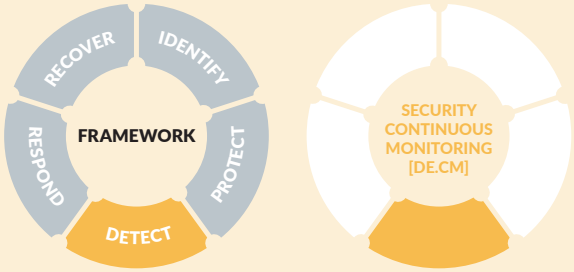
Guidance

No additional Guidance on this topic.

The organisation shall define incident alert thresholds.

Guidance

No additional Guidance on this topic.



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 smartphones and other networked devices when installing and operating firewalls.
- Consider limiting the number of interconnection gateways to the Internet.

The organisation shall monitor and identify the unauthorised use of its business-critical systems by detecting unauthorised local connections, network connections and remote connections.

Guidance

- The monitoring of network communications should take place at the external boundary of the organisation'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 organisation 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:

- Generating system alerts when indications of compromise or potential compromise occur.
- The detection and reporting of atypical usage of the organisation'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.

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.

In addition to physical monitoring of access to the facility, physical access to the organisation's critical systems and devices shall be supervised by means of physical intrusion alarms, surveillance equipment, and independent surveillance teams.

Guidance

Organisations are recommended to maintain a log of all visitors.

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 centralised logging platform for the consolidation and exploitation of log files.
- Consider actively investigating the alerts generated as a result of suspicious activities and take the appropriate actions to remediate the threat, e.g. by deploying a security operations centre (SOC).

Software usage and installation restrictions shall be enforced.

Guidance

Only authorised 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).

DE.CM-4 Malicious code is detected.

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

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 the 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.
- Organisations should consider providing the same malicious code protection mechanisms for home computers (e.g. for teleworking purposes) or for personal devices that are used to perform work of a professional nature (BYOD).

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

Guidance

No additional Guidance on this topic.

DE.CM-5 Unauthorised mobile code is detected.

The organisation shall define acceptable and unacceptable mobile code and mobile code technologies and authorise, 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 items such as Java applets, JavaScript, HTML5, WebGL, and VBScript.
- Decisions regarding the use of mobile code in organisational 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.

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.

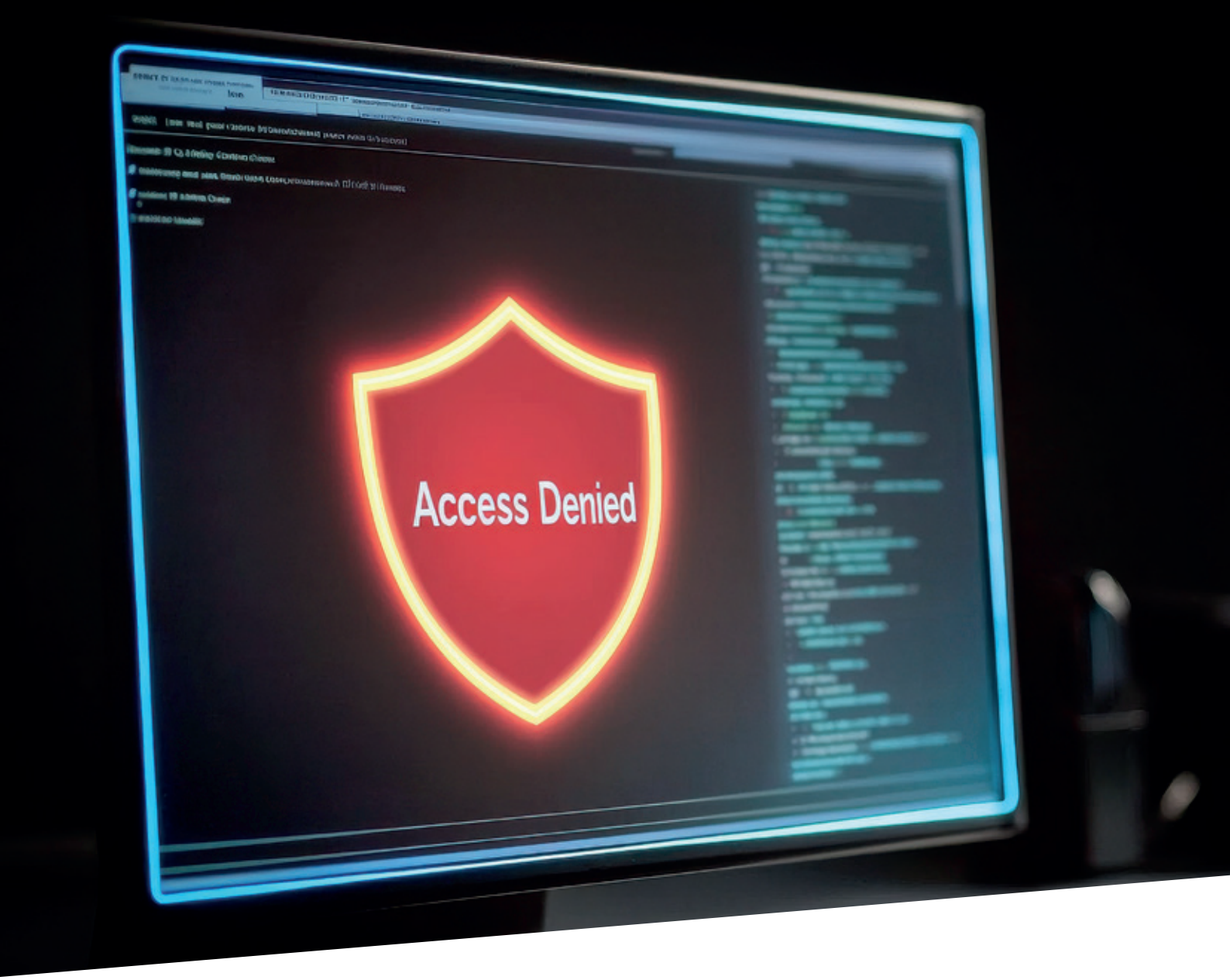
Guidance

This monitoring includes access by unauthorised personnel, and unauthorised 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.



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

The organisation's business critical systems shall be monitored to detect access by unauthorised personnel, and unauthorised connections, devices, access points, and software.

Guidance

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

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

Guidance

No additional Guidance on this topic.

DE.CM-8 Vulnerability scans are performed.

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

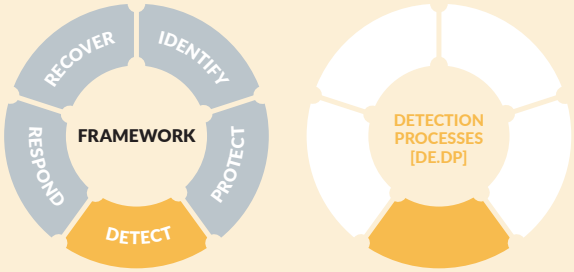
Guidance

Consider implementing 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.



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 organisation 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.

DE.DP-3 Detection processes are tested.

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

Guidance

- Validation includes testing.
- Validation should be demonstrable.

DE.DP-4 Event detection information is communicated.

The organisation shall communicate event detection information to predefined parties.

Guidance

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

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

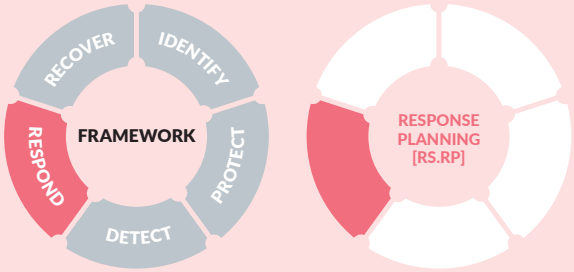
The organisation shall conduct specialised assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing of the organisation's critical systems.

Guidance

These activities can be outsourced, preferably to accredited organisations.

RESPOND

Respond



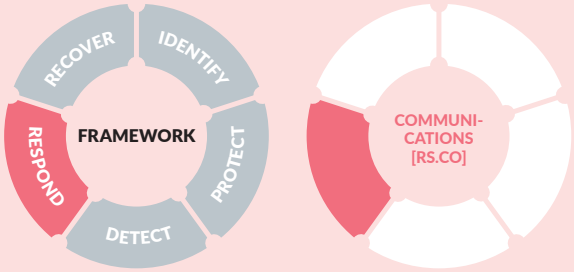
Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

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 organisation'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 cyberattack.
- The roles, responsibilities, and authorities in the incident response plan should be specific with regard to the people involved, contact information, different roles and responsibilities, and with regard to 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 event/ cybersecurity event encountered.



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 organisation shall ensure that personnel understand their roles, objectives, restoration priorities, task sequences (order of operations) and assignment responsibilities when responding to an event.

Guidance

Consider using 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.

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

The organisation shall implement reporting on information/cybersecurity incidents in its critical systems within an organisation-defined timeframe to organisation-defined personnel or roles.

Guidance

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

Events shall be reported in a manner consistent with established criteria.

Guidance

The criteria to report should be included in the incident response plan.

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

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

Guidance

No additional Guidance on this topic.

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

Guidance

No additional Guidance on this topic.

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

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

Guidance

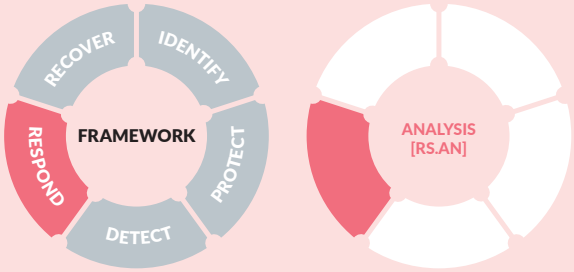
- Stakeholders for incident response purposes include mission/business owners, the organisation's critical system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.
- Coordination with stakeholders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

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

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

Guidance

No additional Guidance on this topic.



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

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

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

Guidance

No additional Guidance on this topic.

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

Guidance

No additional Guidance on this topic.

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

Thorough investigation and result analysis shall form the basis for understanding the full implication of the information security or 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 organisation.
- Consider including detection of unauthorised changes to its critical systems in its incident response capabilities.

The organisation 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).

RS.AN-3 Forensics are performed.

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

Guidance

No additional Guidance on this topic.

The organisation shall conduct forensic analysis of information collected following an information security/cybersecurity event to determine the root cause.

Guidance

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

RS.AN-4 Incidents are categorised consistent with response plans.

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

Guidance

- Organisations should consider determining the causes of an information security or cybersecurity incident and implementing 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.

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

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

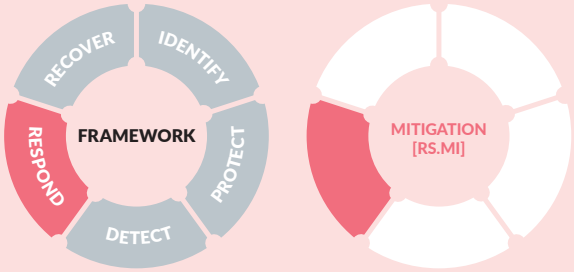
Guidance

Internal and external sources could include internal testing, security bulletins or security researchers.

The organisation shall implement automated mechanisms to track remediation efforts in response to vulnerability information, captured from internal and external sources, and disseminate them to key stakeholders.

Guidance

No additional Guidance on this topic.



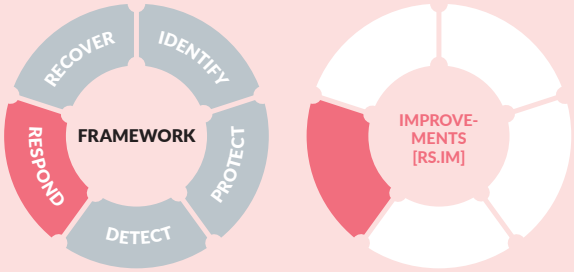
Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities

RS.MI-1 Incidents are contained.

The organisation 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

Documented risk acceptance deals with risks that the organisation assesses as not dangerous to its business-critical systems and with regard to which the risk owner formally accepts the risk (in line with the risk appetite of the organisation)



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

RS.IM-1 Response plans incorporate lessons learned.

The organisation 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

After each incident, consider bringing the persons involved together and reflecting 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

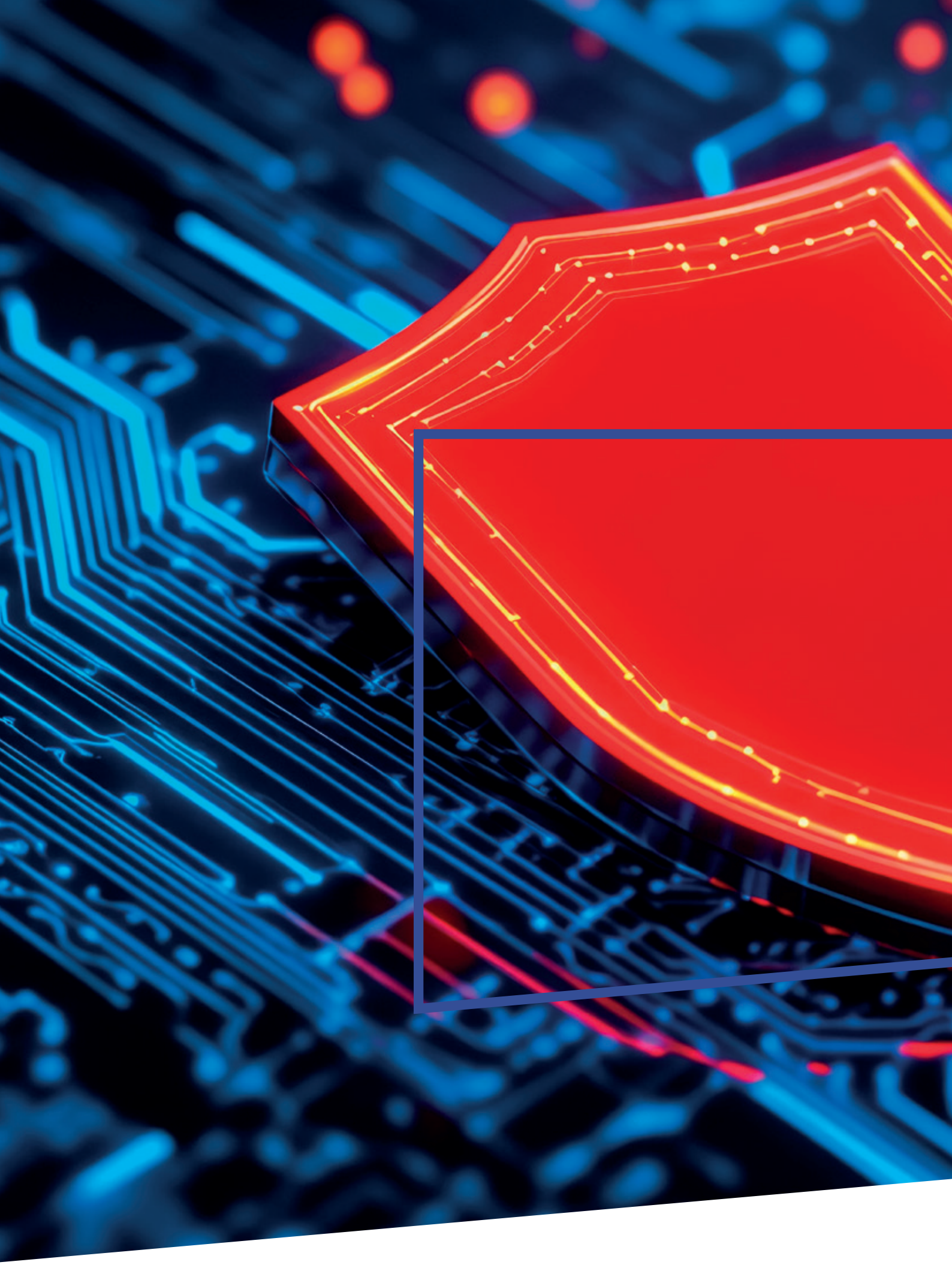
No additional Guidance on this topic.

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

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

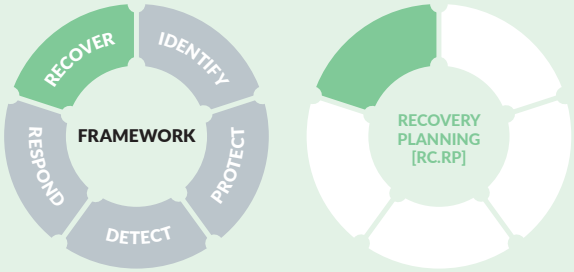
Guidance

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



RECOVER

Recover



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.

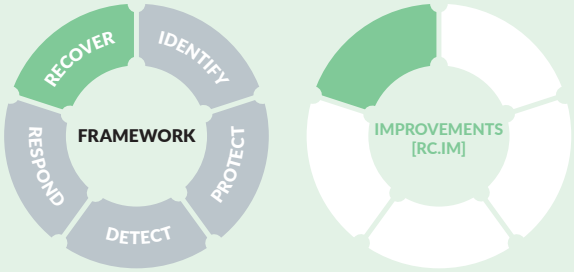
Guidance

- A process should be developed to determine what immediate actions will be taken in the event of a fire, medical emergency, burglary, natural disaster, or an information security/cybersecurity 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 the 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 the event of an incident.

The organisation's essential functions and services shall be continued with little or no loss of operational continuity and continuity shall be sustained until the system is fully restored.

Guidance

No additional Guidance on this topic.



Recovery planning and processes are improved by incorporating lessons learned into future activities.

RC.IM-1 Recovery plans incorporate lessons learned.

The organisation shall incorporate lessons learned from incident recovery activities into updated or new system recovery procedures and, after testing, provide appropriate training to ensure it is embedded.

Guidance

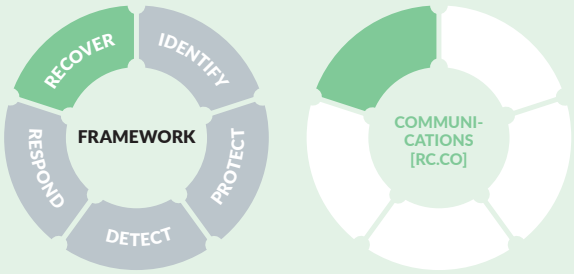
No additional Guidance on this topic.

RC.IM-2 Recovery strategies are updated.

This requirement is combined with RS.IM-2.

Guidance

No additional Guidance on this topic.



Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

RC.CO-1 Public relations are managed.

The organisation shall centralise and coordinate how information is disseminated and manage how the organisation 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 that 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-defined external contacts (e.g. press, regulators, interest groups).

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

The organisation shall implement a crisis response strategy to protect the organisation 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 organisation in crisis, and reduce the negative effect generated by the crisis.

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

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

Guidance

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

ANNEX

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 authorised devices, users, and processes.

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

PR.AC-3 Remote access is managed.

(2) When accessed remotely, the organisation's networks shall be secured, including through the use of multi-factor authentication (MFA).

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

(3) Access permissions for users to the organisation's systems shall be defined and managed.

(4) It shall be identified who should have access to the organisation's business-critical information and technology and how they should obtain 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 (network segregation, network segmentation…) is protected.

(7) Firewalls shall be installed and activated on all the organisation's networks.

(8) Where appropriate, the network integrity of the organisation'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 organisation'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 organisational 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, anti-spyware, and other anti-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 organisation shall be documented, reviewed, authorised updated, and aligned with internal roles within the organisation and external partners.

PROTECT

PR.AC-3 Remote access is managed.

(2) Usage restrictions, connection requirements, implementation Guidance, and authorisations for remote access to the organisation'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 organisation's critical systems shall be protected by (1) identifying, documenting, and controlling connections between system components and (2) limiting external connections to the organisation's critical systems.

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

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

(5) The organisation shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points whenever unauthorised access and activities, including data leakage, are detected.

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

(6) The organisation 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 organisation shall monitor and identify the unauthorised use of its business-critical systems by detecting unauthorised local connections, network connections and remote connections.

RESPOND

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

(8) The organisation 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 Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organisation's cybersecurity program and Cyber Supply Chain Risk Management Plan.

(1) Contractual 'information security and cybersecurity' requirements for suppliers and third-party partners shall be implemented in order 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 organisation shall establish contractual requirements permitting the organisation 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 organisation shall perform a documented risk assessment on the organisation'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 organisational risks).

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

(4) The organisation shall prevent the unauthorised removal of maintenance equipment containing critical system information pertaining to the organisation.

(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 organisation's systems.

(6) The organisation 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 organisation 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 relating 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:

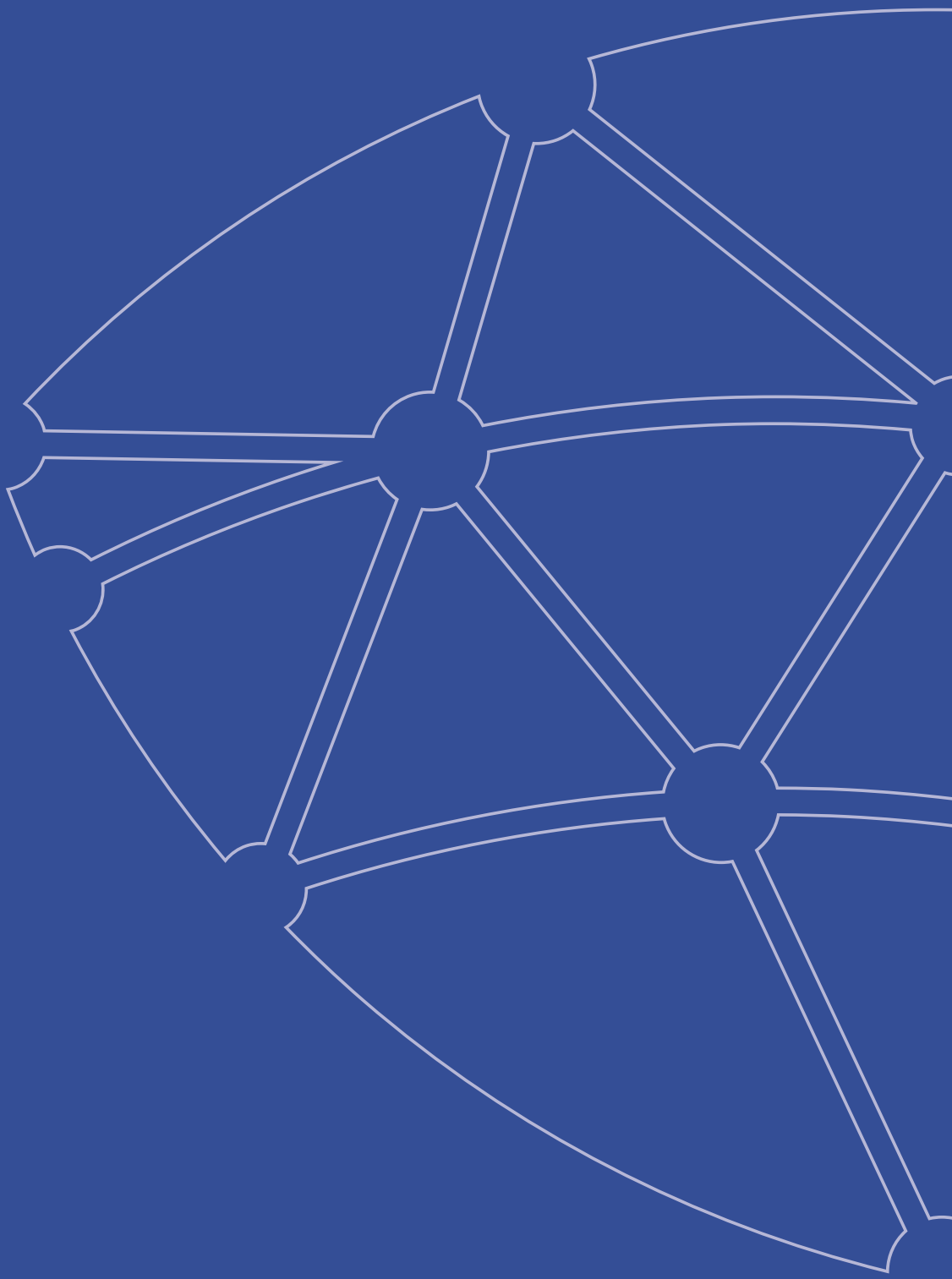
- is exclusively of a general nature and is not intended to take into consideration all particular situations.
- is not necessarily exhaustive, precise, or up to date on all points.

Responsible editor

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

Legal depot

D/2023/14828/001



Centre pour la Cybersécurité Belgique

Rue de la Loi, 18

1000, Bruxelles