CyFun®

CyberFundamentals 2025

Version 2025-10-01

TABLE OF CONTENTS

INTRODUCTION

The CyberFundamentals Framework is a framework owned by the Centre for Cybersecurity Belgium (CCB). The Framework is a set of concrete measures and offers a clear, step-by-step approach that helps organisations to:

- protect their data,
- significantly reduce their risk of the most common cyber-attacks,
- and improve their cyber resilience.

The requirements, also known as controls or measures, are supported by relevant insights from the NIST Cybersecurity Framework[1], ISO 27001/ISO 27002, IEC 62443 and the CIS Critical security Controls (ETSI TR 103 305-1).

The Framework is built around **six core functions**: govern, identify, protect, detect, respond and recover. These six functions support clear communication across all areas of the organisation, technical and non-technical, making it easier to understand, discuss, and manage cyber risks. By using a common language, they help integrate cybersecurity into broader business decisions and the overall risk management strategy.

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.

- **Govern**: Ensures that cybersecurity is treated as a strategic priority, not just a technical issue. It sets clear expectations, policies, responsibilities and authorities, and makes sure these are communicated and reviewed across the organisation.
- **Identify**: Helps build a clear understanding of what matters most to the organisation, such as systems, people, assets, data, and the processes and tools that support operations. This function helps recognise potential cyber threats and lays the foundation for informed decisions about managing cybersecurity risks.
- **Protect**: Involves putting safeguards in place to reduce the chance of a cyber incident or limit its impact. This includes technical measures, processes, and awareness efforts.

- **Detect**: Supports the ability to notice cybersecurity events quickly. Early detection helps reduce harm and allows for faster response.
- **Respond**: Covers the actions taken when a cybersecurity incident occurs. It helps contain the issue, coordinate communication, and reduce disruption.
- **Recover**: Focuses on restoring affected services and operations after an incident. It also includes learning from the event to improve future resilience.

The CyberFundamentals Framework uses a proportional assurance model with three assurance levels: *Basic*, *Important* and *Essential*, preceded by an entry level: *Small*.

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

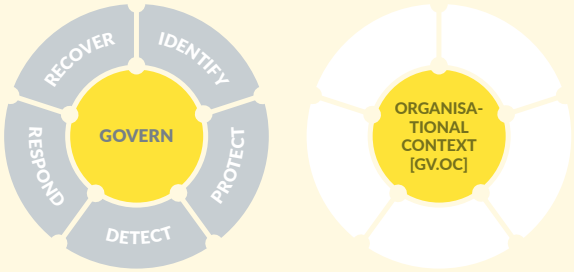
The assurance level **Basic** includes information and cyber security requirements applicable for all organisations. It provides a reliable level of protection by using technologies and processes that are generally already available. Where appropriate, these requirements can be adapted and improved to better match the organisation's specific needs.

Based on common types of cyber-attacks, some requirements are marked as **key measure**  .
These shall be addressed at this assurance level.


POLICIES

GOVERN

Govern



The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organisation's cybersecurity risk management decisions are understood

GV.OC-03 Legal, regulatory, and contractual requirements regarding cybersecurity are understood and managed

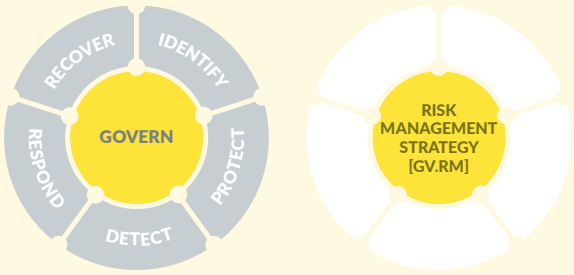
GV.OC-03.1 Legal and regulatory requirements regarding information and cybersecurity shall be identified and implemented.

Implementation guidance

The goal of this control is to ensure that legal, regulatory, and contractual requirements related to information security and cybersecurity are identified, monitored, and implemented.

To achieve this goal, the following should be considered:

- A process should be established to track and apply relevant legal and regulatory requirements related to both information security and cybersecurity.
- These requirements should be integrated into all relevant policies, procedures, and operational practices.
- The areas that should be covered include, but are not limited to:
  - Risk assessments and protection of information systems
  - Incident response, business continuity, and crisis management
  - Supply chain security and secure system development
  - Vulnerability management and secure configuration
  - Security awareness and training
  - Cryptographic controls and secure communications
  - Emergency communication systems
  - Access control, asset management, and Multi-Factor Authentication (MFA)
  - Coordinated vulnerability disclosure
  - (...)



The organisation's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions

GV.RM-03 Cybersecurity risk management activities and outcomes are included in enterprise risk management processes

GV.RM-03.1 As part of the organisation-wide risk management strategy, a comprehensive strategy to manage information and cybersecurity risks shall be developed and updated when changes occur.

Implementation guidance

This control focuses on the creation and maintenance of a specific strategy for managing information and cybersecurity risks. It ensures that the organisation has a dedicated, actionable plan that evolves with the threat landscape.

To make this happen, the following should be considered:

- An organisation-wide risk management strategy includes an expression of the security risk tolerance for the organisation, security risk mitigation strategies, acceptable risk assessment methodologies, a process for evaluating security risk across the organisation with respect to the organisation's risk tolerance, and approaches for monitoring risk over time.
- Information and Cybersecurity risks should be aggregated and managed alongside other organisation risks (e.g., compliance, financial, operational, regulatory, reputational, safety).
- The information and cybersecurity risk management strategy should include identifying and allocating the necessary resources to protect the organisation's business-critical assets.
- This is the cybersecurity-specific implementation of the broader vision defined in GV.RM-04.1

Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated

GV.RR-04 Cybersecurity is included in human resources practices

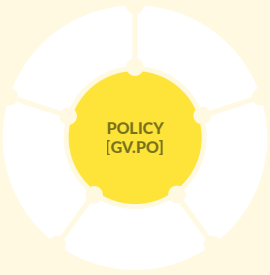
GV.RR-04.1 **Personnel with access to the organisation's most critical information or technology shall be authenticated.**

Implementation guidance

The goal of this control is protecting critical assets by ensuring only authenticated personnel can access them.

To achieve this, the following should be considered:

- "Authenticated" means the user must technically prove their identity at the point of access, ideally using MFA or stronger methods, not just be validated during onboarding.
- The access to critical information or technology should be considered during recruitment, onboarding, during employment, change of function and when offboarding (termination of employment).
- Background verification checks should be conducted prior to onboarding new personnel for sensitive roles, and background checks should be periodically repeated for personnel with such roles. Background verification checks should however take into account applicable laws, regulations, and ethics in proportion to the business requirements, the classification of the information to be accessed and the perceived risks.
- Cybersecurity expertise should *be recognised as a valuable asset in recruitment*, training, and retention decisions.



Organisational cybersecurity policy is established, communicated, and enforced

GV.PO-01 Policy for managing cybersecurity risks is established based on organisational context, cybersecurity strategy, and priorities and is communicated and enforced

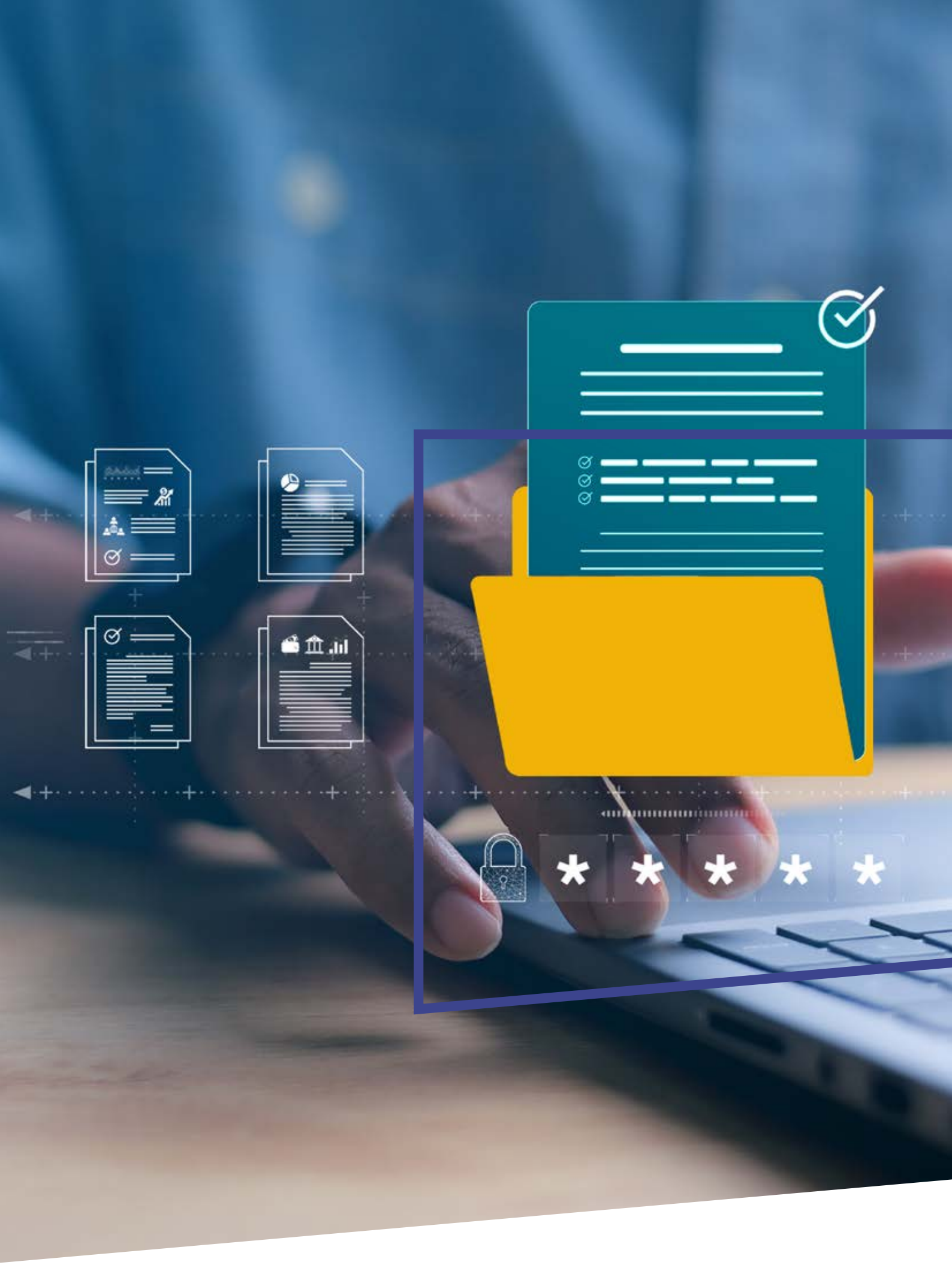
GV.PO-01.1 Policies and procedures for managing information and cybersecurity shall be established, documented, reviewed, approved, updated when changes occur, communicated and enforced.

Implementation guidance

This control sets the foundation for how all information and cybersecurity policies and procedures should be managed. It emphasises the governance lifecycle, from creation to enforcement, and ensures alignment with the organisation's strategic direction.

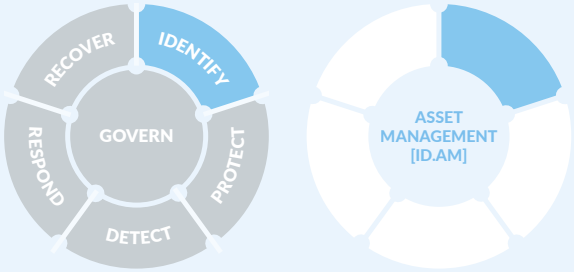
To effectively implement this control, consider the following practices:

- Develop clear and practical policies, processes, and procedures which:
  - Define acceptable behaviours and expectations for protecting the organisation's information and systems.
  - Outline how management expects employees to use and safeguard company resources.
- Ensure employee awareness by communicating these policies, processes, and procedures:
  - During onboarding of new personnel.
  - Whenever significant updates or changes are made.
  - Maintain accessibility by making all relevant documents easily available to employees.
- Review and update regularly (e.g. annually) to reflect:
  - Organisational changes, such as mergers, acquisitions, or new contractual obligations.
  - Technological developments, such as the adoption of artificial intelligence or new security tools.
- Define risk assessment criteria within the organisation's risk management policy:
  - The entity should establish and document clear criteria for determining the probability and impact of risks.
  - These criteria should be tailored to the organisation's specific context and used consistently to evaluate and prioritise cybersecurity risks. This ensures that risk-based decisions are aligned with the organisation's overall strategy and risk appetite.



IDENTIFY

Identify



Assets (e.g., data, hardware, software, systems, facilities, services, people) 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-01 Inventories of hardware managed by the organisation are maintained

ID.AM-01.1 An inventory of physical and virtual infrastructure assets — such as hardware, network devices, and cloud-hosted environments — that support information processing shall be documented, reviewed, and updated as changes occur.

Implementation guidance

The goal of this control is to ensure that critical systems and services remain available by implementing redundancy in line with organisational, legal, and regulatory availability requirements.

While ID.AM-01.1 focuses on the infrastructure layer, this control is closely linked to ID.AM-02.1 which tracks the software and services that run on top of it, such as applications, platforms, and digital tools. Together, they provide a full picture of the organisation's technology environment.

To achieve the goal of ID.AM-01.1, the following should be considered:

- Organisations should identify and document all physical and virtual infrastructure assets that support information processing, including servers, workstations, network devices, storage systems, and cloud-hosted resources.
- The inventory should include key attributes such as asset type, location, owner, configuration, and lifecycle status.
- Organisations should consider automated asset discovery and management tools where possible to ensure accuracy and real-time updates.
- The inventory should be reviewed and updated regularly, especially following changes such as deployments, decommissions, or relocations.
- The inventory should be accessible to relevant stakeholders and should be integrated with risk management and incident response processes.

ID.AM-02 Inventories of software, services, and systems managed by the organisation are maintained

ID.AM-02.1 An inventory of software, digital services, and business systems used within the organisation shall be documented, reviewed, and updated as changes occur.

Implementation guidance

This control ensures that all software, digital services, and business systems used within the organisation are identified, tracked, and regularly updated. It focuses on the functional and intangible parts of the technology environment, such as applications, platforms, and cloud services, that operate on or interact with the underlying infrastructure. Keeping this inventory up-to-date supports operational continuity, strengthens security, and helps meet compliance requirements.
It is closely linked to ID.AM-01.1, which covers the physical and virtual infrastructure (such as servers, network devices, and cloud environments) that supports these systems.
Together, both controls provide a complete view of the organisation's technology landscape, from the foundational infrastructure to the applications and services that deliver business value.

To achieve this goal, the following steps should be considered:

- Identify Software and Services
  The inventory should include all applications, cloud services, APIs, and business systems (e.g. ERP, CRM, HR platforms).
- Record Key Information
  Each entry should include version, owner, purpose, licence type, and deployment environment.
- Use Automation Where Possible
  Automated discovery tools should be used to accurately detect and update software and services.
- Maintain a Software Bill of Materials (SBOM)
  An SBOM should be maintained for critical or internally developed software to track components and dependencies.
- Keep the Inventory up-to-date
  The inventory should be reviewed and updated regularly, especially after installations, upgrades, or removals.
- Align with Infrastructure Inventory (ID.AM-01.1)
  Software records should be linked to the infrastructure they run on to provide a complete view of the technology environment.

ID.AM-05 Assets are prioritised based on classification, criticality, resources, and impact on the mission

ID.AM-05.1 The organisation's assets shall be prioritised based on classification, criticality, and business value.

Implementation guidance

The goal of this control is to ensure that all organisational assets, such as devices, systems, services, data, and business processes, are prioritised based on their classification, criticality, and business value.
This prioritisation helps direct protection efforts toward the most important assets, supporting operational continuity, security, and compliance.

To make this happen, the following steps should be considered:

- Asset Identification
  All relevant assets, including devices, systems, software, cloud services, data, employees, and business processes, should be identified and recorded in a central inventory.
- Asset Classification
  Each asset should be classified based on its role:
  - Primary assets should be defined as those directly supporting core business functions.
  - Secondary assets should be defined as those that support, protect, or enable primary assets.
- Criticality Assessment
  - The organisation should assess how critical each asset is to business continuity.
  - The assessment should consider potential impacts such as operational disruption, financial loss, legal or regulatory consequences, safety risks, and reputational damage.
- Prioritisation Method
  A consistent scoring or ranking method should be used to prioritise assets based on classification, criticality, and business value.
- Ownership Assignment
  Each asset should have an assigned owner responsible for maintaining accurate and up-to-date information.
- Regular Review
  Asset classifications and priorities should be reviewed at least annually or when significant changes occur (e.g. new systems, business restructuring).
- Documentation and Evidence
  - The asset register should include classification, prioritisation criteria, assigned owners, and evidence of regular reviews.
  - Definitions of primary and secondary assets should be clearly documented.

ID.AM-07 Inventories of data and corresponding metadata for designated data types are maintained

ID.AM-07.1 Data that the organisation stores and uses shall be identified.

Implementation guidance

The goal of this control is to ensure that all data stored and used by the organisation is clearly identified. This supports proper data management, protection, and alignment with business and regulatory requirements.

To achieve this goal, the following should be considered:

- Data Identification
  All types of data, regardless of format, location, or system, should be identified and recorded.
- Data Classification
  Identified data should be classified using standard categories such as:
  - Public
  - Internal
  - Confidential
  - Restricted
- Data-to-Asset Mapping
  Data should be linked to the assets that store or process it, including physical devices, systems, software, and applications listed in the inventories from ID.AM-01 and ID.AM-02.
- Documentation and Maintenance
  Data types, classifications, and associated assets should be documented and regularly updated to reflect changes in the environment.

ID.AM-08 Systems, hardware, software, services, and data are managed throughout their life cycles

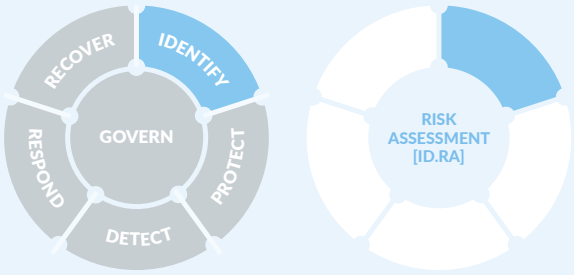
ID.AM-08.2 Patches and security updates for Operating Systems and critical system components shall be installed.

Implementation guidance

The goal of this control is to ensure that operating systems and critical system components are kept secure and up-to-date by installing patches and security updates in a timely and controlled manner.

To achieve this goal, the following should be considered:

- Timely Updates
  Patches and security updates should be installed as soon as possible, especially for critical systems.
- Industrial Systems
  Firmware updates for industrial assets (e.g. PLCs, HMIs) should be included in the patching process.
- Centralised Management
  A Centralised patch management system should be used to automate and streamline patch deployment.
- Testing Before Deployment
  - Patches should be tested in a controlled environment to avoid disruptions.
  - A test environment should closely mirror the production setup.
- Phased Rollouts
  - Where appropriate, test groups, pilot users, and phased rollouts should be used.
  - A rollback procedure should be in place in case issues arise.
- Trusted Sources Only
  - Patches should only be downloaded from verified, trusted sources.
  - Links in emails or advertisements should be avoided.
- Minimal Software Footprint
  Only essential applications should be installed. These should be regularly patched and updated.
- Safe Update Practices
  - Automatic updates should be enabled when connected to trusted networks.
  - Updates should not be performed over untrusted networks (e.g. public Wi-Fi).
- Supported Software Only
  - Only vendor-supported and up-to-date software versions should be used.
  - End-of-life (EOL) software should be decommissioned as soon as possible.
- Regular Checks
  If automatic updates are not possible, a regular schedule (e.g. monthly) should be set to manually check for and install updates.
- Update Monitoring Tools
  Tools that notify about available updates should be configured to monitor all installed applications.



The cybersecurity risk to the organisation, assets, and individuals is understood by the organisation

ID.RA-01 Vulnerabilities in assets are identified, validated, and recorded

ID.RA-01.1 Threats and vulnerabilities shall be identified in all relevant assets, including software, network and system architectures, and facilities that house critical computing assets.

Implementation guidance

The goal of this control is to help organisations mitigate cybersecurity risks by identifying threats and vulnerabilities in their critical assets. This includes software, networks, systems, and physical locations that support essential computing operations.

To support this objective, organisations should:

- Understand Key Concepts
  - A **vulnerability** is a weakness in hardware, software, or procedures that could be exploited.
  - A **threat** is an event or actor that may try to exploit a vulnerability.
  - A **risk** is the possible impact if a threat successfully exploits a vulnerability.
- Identify Relevant Assets
  All critical systems, applications, networks, and facilities should be listed and documented.
- Respond to Vulnerabilities
  - Organisations should act on vulnerabilities that are reported by trusted sources (e.g., vendors, service providers, government advisories).
  - At the basic level, active scanning is not required, but known vulnerabilities should be addressed promptly.
- Be Aware of Threats
  - Organisations should stay informed about common threats relevant to their sector (e.g., phishing, ransomware, supply chain risks).
  - Threat awareness can come from government advisories, industry news, or sector-specific guidance.
- Maintain a Simple Risk Register
  A basic list of known threats and vulnerabilities should be kept, to support decision-making and planning.
- Review Periodically
  This list should be reviewed when new systems are added or when there are major changes in the threat landscape.

ID.RA-05 Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritisation

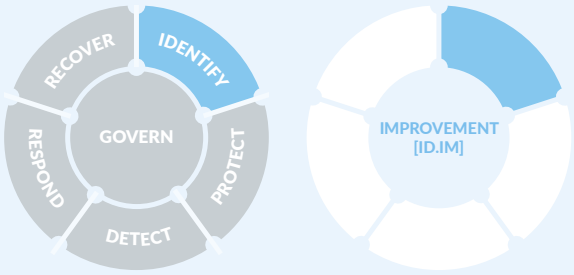
ID.RA-05.1 The organisation shall conduct risk assessments in which risk is determined by threats, vulnerabilities and the impact on business processes and assets.

Implementation guidance

The goal of this control is to ensure that risk assessments are conducted by evaluating threats, vulnerabilities, and their potential impact on business processes and assets. This supports informed decision-making and effective risk mitigation.

To achieve this goal, the following should be considered:

- Identify Threats and Vulnerabilities
  Assessments should include threats and vulnerabilities across software, network and system architectures, and facilities housing critical computing assets.
- Evaluate Business Impact
  The potential impact on business operations, services, and assets should be analysed to determine the severity of each risk.
- Include Human Factors
  Human behaviour should be considered when designing and applying security policies, especially in operational technology (OT) environments.
- Document and Review
  Risk assessments should be documented, regularly reviewed, and updated to reflect changes in systems, operations, or the threat landscape.



Improvements to organisational cybersecurity risk management processes, procedures and activities are identified across all CyFun® Functions

ID.IM-03 Improvements are identified from execution of operational processes, procedures, and activities

ID.IM-03.1 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.

Implementation guidance

The goal of this control is to enhance cyber resilience by learning from incidents. After each incident, the organisation should analyse what happened, how it was handled, and what can be improved in processes, procedures, or technologies.

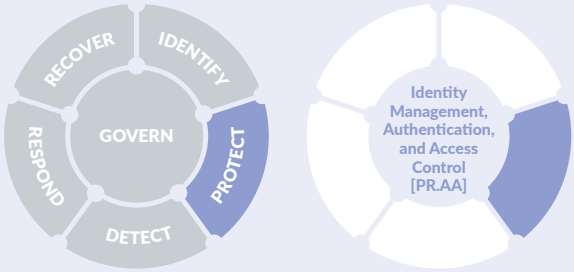
To achieve this goal, the following should be considered:

- Conduct Post-Incident Reviews
  A structured evaluation should be held after each incident, involving all relevant participants.
- Reflect on Key Questions
  The review should explore:
  - What happened and why
  - How the response was managed
  - What worked well and what didn't
  - What actions should be taken to prevent recurrence
- Document Lessons Learned
  Findings from the review should be documented and shared with relevant teams.
- Update Policies and Procedures
  Cybersecurity policies, processes, and procedures should be reviewed and updated regularly, at least annually, to reflect lessons learned.
- Improve Tools and Capabilities
  Where applicable, technologies and response tools should be adapted or upgraded based on insights from the incident.


Username
Password
Protected
Balance
5,367.50 $

PROTECT

Protect



Access to physical and logical assets is limited to authorised users, services, and hardware and managed commensurate with the assessed risk of Unauthorised access

PR.AA-01 Identities and credentials for authorised users, services, and hardware are managed by the organisation

PR.AA-01.1 Identities and credentials for authorised users, services, and hardware shall be managed.

Implementation guidance

The goal of this control is to ensure that identities and credentials for authorised users, services, and hardware are properly managed to prevent unauthorised access and support secure operations in both ICT and OT environments.

To achieve this goal, the following should be considered:

- Access Requests and Authorisation
  - Access should be formally requested, documented, and approved by system or data owners.
  - Access rights should follow the principle of least privilege.
- Identity and Credential Management
  - Individual user accounts should be used; sharing passwords should be avoided.
  - Default passwords should be changed before systems are activated.
  - Unused accounts should be disabled immediately.
  - Administrator accounts should be limited, reviewed regularly, and not used for daily tasks.
- Password Policy
  - Strong password rules should be enforced.
  - Passwords should be changed regularly or immediately after suspected compromise.
  - A formal password policy should be in place (See also: CyFun® Toolbox on www.cyfun.eu).
  - Rights and privileges should be assigned through user groups.
- Device and Hardware Identity
  - Each authorised device should have a unique identifier (e.g. MAC address, serial number).
  - Devices should be physically labelled to support inventory and maintenance.
- Shared Access to PLCs/HMIs (OT-Specific Measures)
  - If individual accounts are not feasible, the principle of least privilege should still apply.
  - A secure jump server or HMI front-end should be used to control access, log activity, and add authentication layers.

- Secure Remote Access
  - Technical requirements for remote access should be clearly defined and documented.
  - Secure methods such as VPNs, encrypted protocols (e.g. SSH, TLS), and multi-factor authentication (MFA – see also PR.AA-03.2) should be used.
  - Remote access should be monitored and logged.

PR.AA-03 Users, services, and hardware are authenticated

PR.AA-03.1 All wireless access points used by the organisation, including those providing guest access, shall be securely configured, managed, and monitored to prevent unauthorised access and ensure network integrity.

Implementation guidance

The goal of this control is to ensure that all wireless access points, including those for guest use, are securely configured, managed, and monitored to prevent unauthorised access and protect network integrity.

To achieve this goal, the following should be considered:

- General Wireless Security
  - Default administrative credentials should be changed immediately after installation.
  - SSID broadcasting should be disabled unless operationally necessary.
  - Strong encryption protocols (e.g. WPA2 or WPA3 with AES) should be used.
  - Physical access to wireless access points should be restricted.
  - Firmware should be updated regularly to address known vulnerabilities.
  - Wireless networks should be monitored for unauthorised access points and suspicious activity.
- Guest Wi-Fi Security
  - Guest networks should be isolated from internal systems using VLANs or separate SSIDs.
  - Bandwidth and access restrictions should be applied to guest networks.
  - Captive portals should be used to display terms of use and optionally log guest access.
  - Sensitive data should not be stored or transmitted over guest networks.
  - Guest Wi-Fi should be disabled when not in use or outside business hours, if feasible.
- Endpoint and User Practices
  - Devices connecting to wireless networks should comply with endpoint security policies.
  - VPNs should be used when connecting to unknown or unsecured networks.
  - Wi-Fi credentials should follow password policies that enforce complexity and regular updates.

PR.AA-03.2 **Multi-Factor Authentication (MFA) shall be required to access the organisation's networks remotely.**

Implementation guidance

The goal of this control is to protect the organisation's networks by requiring multi-factor authentication (MFA) for all remote access, thereby reducing the risk of unauthorised access and credential-based attacks.

To achieve this goal, the following should be considered:

- General MFA Enforcement
  - MFA should be enforced on all internet-facing systems, including email, VPNs, RDP, cloud services, and web portals.
  - All remote access, including access by third-party vendors and contractors, should require MFA.
- MFA Technology Selection
  - MFA methods should be selected based on security strength, phishing resistance, and operational fit.
  - Common options include:
    - Hardware TOTP (Time-based One-Time Password) tokens — secure, limited phishing resistance
    - Authenticator apps (software TOTP) — widely used, moderate security
    - Passkeys — passwordless, user-friendly, cryptographically secure
    - FIDO2 (platform or hardware-based – Fast Identity Online 2) — strong cryptographic authentication
    - Push-based apps — convenient, but may be vulnerable to push fatigue
  - SMS and email-based MFA should be avoided due to security weaknesses.
- Supporting Security Measures
  - Strong password policies should be enforced alongside MFA.
  - Users should be trained to log out of sessions explicitly.
  - Anti-malware tools and platforms should be kept up-to-date.
  - Regular phishing awareness training should be conducted.
- OT-Specific MFA Considerations *(see also PR.AA-01.1)*
  - Shared Access to PLCs/HMIs
    - If individual accounts are not feasible, the principle of least privilege should be applied.
    - A secure jump server or HMI front-end should be used to control access, log activity, and add an authentication layer.
  - Secure Remote Access to OT Systems
    - Technical and procedural requirements for remote access should be clearly defined.
    - Secure protocols (e.g. VPN, SSH, TLS) should be used.
    - MFA should be enforced for all remote OT access, especially for third-party suppliers.
    - Just-In-Time (JIT) access controls should be used to grant temporary, time-limited access.
    - All remote access should be logged and monitored.
  - Integration and Compatibility
    - The MFA solution should be compatible with both IT and OT systems.
    - Integration should be tested in OT environments to avoid disruptions.
    - Where direct integration is not possible, secure intermediary platforms (e.g. jump servers) should be used.

PR.AA-05 Access permissions, entitlements, and authorisations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties

PR.AA-05.1 Access permissions, rights, and authorisations shall be defined, managed, enforced and reviewed.

Implementation guidance

The goal of this control is to ensure that access permissions, rights, and authorisations are clearly defined, properly managed, consistently enforced, and regularly reviewed to protect systems and data from unauthorised access.

To achieve this goal, the following should be considered:

- Access Definition and Management
  - Access lists for systems (e.g. files, servers, software, databases) should be created and reviewed regularly.
  - Reviews should be supported by tools such as Active Directory analysis.
  - Permission management procedures should be documented and updated as needed.
- Access Review and Revocation
  - Logical and physical access rights should be reviewed periodically and whenever roles change or individuals leave the organisation.
  - Unnecessary privileges should be revoked immediately.
- User Account Practices
  - Each user, including contractors, should have a separate account to ensure accountability.
  - Where technically feasible, appropriate authentication measures should be applied.
  - Guest accounts should be restricted to minimum required privileges (e.g. internet access only).
  - Single Sign-On (SSO) should be used where appropriate.
- Authorisation Criteria
  Authorisation decisions should consider characteristics such as geolocation, time of access, and the security posture of the requesting device.
- OT-Specific Considerations
  - In environments where individual accounts are not technically feasible — such as shared access to PLCs or HMIs, access should be limited to essential functions only, and enforced through secure methods like a jump server or HMI front-end that logs activity, restricts access by role or time, and adds an extra authentication layer (e.g. badge or PIN).
  - Authentication methods should align with the capabilities of OT systems.
  - Access to OT systems should be logged and monitored where possible.

PR.AA-05.2 **It shall be determined who needs access to the organisation's business-critical information and technology and the means to gain access.**

Implementation guidance

The goal of this control is to determine who requires access to the organisation's business-critical information and technology, and to define the secure means by which this access is granted.

To achieve this goal, the following should be considered:

- Access Determination and Restriction
  - Access rights should be limited to only those individuals who need them to perform their roles.
  - A zero trust model should be considered for both IT and OT environments, requiring verification before granting access.
- Means of Access
  - Access methods should include secure mechanisms such as keys, passwords, codes, or administrative privileges.
  - These methods should be managed and monitored to prevent misuse.
- Cyber Health of Endpoints
  - Devices such as laptops, smartphones, and tablets should meet security standards before connecting to the production network.
  - Endpoint health should be verified by checking for:
    - Up-to-date antivirus software
    - Absence of malware
    - Installation of the latest security patches
  - Only compliant devices should be allowed to access critical systems and data.
- OT-Specific Considerations
  - In OT environments, access to control systems should be limited to essential personnel.
  - Secure access methods (e.g. jump servers, role-based restrictions) should be used where individual accounts are not feasible.
- Reference
  For practical tools and templates, refer to the Access Policy template in the CyFun® Toolbox on www.cyfun.eu

PR.AA-05.3 **Access rights, privileges and authorisations shall be restricted to the systems and specific information needed to perform the tasks (the principle of Least Privilege).**

Implementation guidance

The goal of this control is to ensure that access rights, privileges, and authorisations are restricted to only the systems and specific information needed to perform assigned tasks, following the principle of least privilege.

To achieve this goal, the following should be considered:

- Apply Least Privilege
  - Access rights should be limited to the minimum necessary for users, systems, and services.
  - Accounts should start with low privileges, and be elevated only when justified.
  - Just-in-time access should be used to limit the duration of elevated privileges.
- Define and Manage Permissions
  - Access rights should be clearly defined based on roles and responsibilities.
  - An inventory of accounts and their permissions should be maintained and kept up to date.
  - Separate accounts should be used for contractors and third parties to ensure traceability.

- Enforce Access Controls
  - Role-based or attribute-based access control models should be implemented where feasible.
  - Internet access points and external connections should be limited to what is strictly necessary.
- Harden Systems
  - Systems should be hardened to support access control by:
    - Disabling unused ports and services
    - Restricting Bluetooth where not needed
    - Limiting legacy protocols such as FTP unless securely configured
- Review and Adapt Access
  - Access rights should be reviewed regularly and adjusted based on role changes, project completion, or security assessments.
  - Access should be revoked immediately when no longer needed.
- OT-Specific Considerations
  In OT environments, access control should still follow the principle of least privilege. Where technical limitations exist, previously defined OT access control measures (see PR.AA-01.1 and PR.AA-05.1) should be applied to ensure secure and traceable access.

PR.AA-05.4 No one shall have administrative privileges for routine day-to-day tasks.

Implementation guidance

The goal of this control is to prevent the use of administrative privileges for routine, day-to-day tasks, thereby reducing the risk of misuse or exploitation by attackers.

To ensure this goal is met, the organisation should consider the following:

- Account Separation and Privilege Management
  - Administrative and general user accounts should be strictly separated.
  - Dedicated administrator accounts should be used only for system management and administrative tasks.
  - User accounts should not have administrative privileges.
- Access Restrictions and Security Measures
  - Unique local administrator passwords should be created for each system.
  - Unused accounts should be promptly disabled.
  - Internet browsing from administrative accounts should be prohibited to reduce exposure to web-based threats.
- OT-Specific Considerations
  - In OT environments, administrative access should be limited to essential personnel and functions.
  - Where shared access is necessary, secure access methods (e.g. jump servers, session logging) should be used to enforce accountability and reduce risk.

PR.AA-06 Physical access to assets is managed, monitored, and enforced commensurate with risk

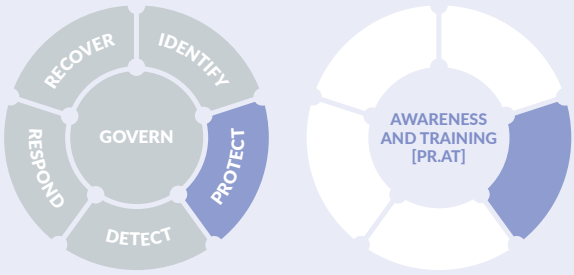
PR.AA-06.1 Physical access to all organisational assets, including critical zones, shall be managed, monitored, and enforced based on risk.

Implementation guidance

The goal of this control is to ensure that physical access to all organisational assets, especially in critical zones, is managed, monitored, and enforced based on risk to prevent unauthorised entry and protect sensitive systems.

To support this goal, the following actions should be taken:

- Access Control Measures
  - Keys, badges, and alarm codes should be strictly managed.
  - Employee access credentials should be collected immediately upon departure.
  - Alarm codes should be changed regularly.
  - External service providers (e.g. cleaners) should only receive access when necessary, and it should be:
    - Time-limited using technical controls
    - Logged electronically for traceability
- Physical Security Enhancements
  - Critical zones should be protected with physical controls such as:
    - Surveillance cameras
    - Security guards
    - Locked doors and gates
    - Alarm systems
  - These controls should be placed strategically to monitor and restrict access.
- Network Access Protection
  Internal network ports (e.g. Ethernet) should not be exposed in unsecured areas such as waiting rooms, corridors, or reception zones.
- OT-Specific Considerations
  - Physical access to OT environments (e.g. control rooms, cabinets, field devices) should be limited to authorised personnel only.
  - Access should be logged and monitored, and physical barriers should be used where feasible.
- Reference
  For practical tools and templates, refer to the Access Policy in the CyFun® Toolbox on www.cyfun.eu.



The organisation's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks

PR.AT-01 Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind

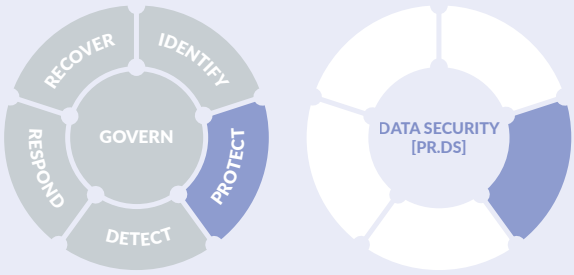
PR.AT-01.1 The organisation shall establish and maintain a cybersecurity awareness and training programme to ensure that all personnel understand how to perform their tasks securely and responsibly.

Implementation guidance

The goal of control PR.AT-01.1 is to ensure everyone in the organisation understands how to work securely by providing regular, clear, and practical cybersecurity training that reduces human risk and supports safe behaviour in both IT and OT environments.

To achieve this goal, the following should be considered:

- **Basic Training Should Be Provided to All**
  Cybersecurity awareness training should be given to all employees, contractors, partners, and suppliers, including those in Operational Technology (OT) environments.
- **Training Should Cover Common Threats**
  Topics such as phishing, weak passwords, social engineering, and OT-specific risks (e.g. USB misuse, remote access threats) should be included.
- **Training Should Start Early and Be Repeated Regularly**
  Training should be provided during onboarding and refreshed at least annually. Ongoing updates and reminders should reinforce key messages.
- **Multiple Channels Should Be Used**
  Awareness should be raised through structured sessions, campaigns, posters, newsletters, and interactive tools.
- **Consequences of Non-Compliance Should Be Explained**
  The impact of violating cybersecurity policies should be clearly communicated, both for individuals and the organisation.
- **Training Should Align with Policies and Best Practices**
  Content should reflect internal cybersecurity policies, expected behaviours, and protection measures. Recognised frameworks like ENISA's AR-in-a-Box should guide programme design.
- **OT-Specific Risks Should Be Addressed**
  Training should be tailored to include the unique responsibilities and risks faced by personnel working with industrial control systems and other OT assets.
- **Content Should Be Kept Up to Date**
  Training materials should be regularly reviewed and updated to reflect new threats and lessons learned from incidents.



Data are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information

PR.DS-01 The confidentiality, integrity, and availability of data-at-rest are protected

PR.DS-01.9 Enterprise assets shall be disposed of safely.

Implementation guidance

The goal of this control is to ensure that all enterprise assets are disposed of in a secure and controlled manner, to prevent unauthorised access to sensitive business, personal, or operational data.

To support this goal, the organisation should consider to:

- Sanitise Data Before Disposal
  Sensitive data should be securely removed ("wiped") from all assets, such as computers, servers, hard drives, USB drives, mobile devices, and paper documents, before retirement, reassignment, repair, or replacement.
- Use Appropriate Destruction Methods
  Suitable methods should be available for destroying paper records, digital storage media, and other physical data carriers.
- Enable Remote Wiping for Mobile Devices
  Remote wiping capabilities should be enabled on laptops, tablets, phones, and other mobile devices to protect data if lost or stolen.
- Manage Expired Domain Names Carefully
  Expired domains should be protected, as they are often targeted by cyber-criminals. The following practices should be considered:
  - Enable auto-renewal or renew domains for at least ten years.
  - Communicate domain changes clearly and manage transitions internally.
  - Set auto-replies for emails sent to old domains.
  - Update online references and cloud service settings.
  - Change or delete accounts registered with old domains.
  - Keep login email addresses current and enable MFA.
  - Avoid using non-approved cloud storage for sensitive data.
- Follow Asset Management Best Practices
  Guidance from trusted sources, such as the Asset Management policy template in the CyFun® Toolbox on www.cyfun.eu, should be used to support secure disposal.
- Include OT Assets in Disposal Planning
  OT systems and devices should be included in disposal procedures, ensuring operational data and configurations are securely removed before decommissioning.

PR.DS-11 Backups of data are created, protected, maintained, and tested

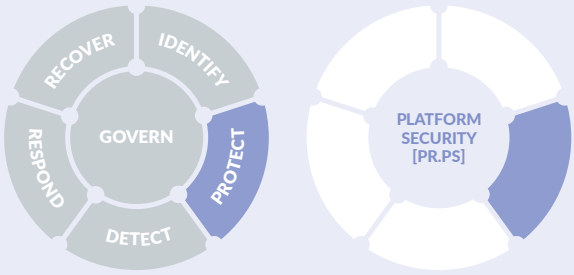
PR.DS-11.1 Backups for the organisation's business-critical data shall be performed and stored on a different system from the device on which the original data resides.

Implementation guidance

The goal of this control is to ensure that business-critical data is regularly backed up and securely stored on a separate system to protect against data loss, system failure, or cyberattacks such as ransomware.

To support this goal, the organisation should:

- Back Up Critical Data and Systems
  Backups should include:
  - Business-critical data (e.g. customer records, financial and operational data).
  - System data such as software configurations, device settings, documentation, and application backups.
- Define a Backup Strategy
  - Critical data should be backed up continuously or in near-real time.
  - Other important data should be backed up at regular, agreed intervals.
  - Backups should be stored on a system that is physically or logically separate from the original data source. This means they must not reside on the same device, server, or storage array as the original data. Ideally, backups should be stored in a different security zone, network segment, or even offsite location to ensure they remain accessible and uncompromised in the event of system failure, ransomware, or other incidents affecting the primary environment.
- Ensure Network Separation
  - Backups should not be stored on the same network as the original systems.
  - At least one backup copy should be kept completely offline or air-gapped to ensure recovery in the event of a network breach or ransomware attack.
- Plan for Recovery
  Recovery Time Objective (RTO – how quickly systems must be restored) and Recovery Point Objective (RPO – how much data loss is acceptable) should be defined and reviewed regularly to ensure timely and effective restoration.
- Include OT Environments
  Backup strategies should cover OT systems, including control system configurations, operational data, and device settings critical to industrial operations.



The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organisation's risk strategy to protect their confidentiality, integrity, and availability

PR.PS-04 Log records are generated and made available for continuous monitoring

PR.PS-04.1 Logs shall be maintained, documented, and monitored.

Implementation guidance

The goal of this control is to ensure that logs are consistently maintained, documented, and monitored to support visibility, accountability, and early detection of anomalies or threats.

To support this goal, the organisation should:

- Enable Logging Across Systems
  All operating systems, applications, services (including cloud-based), and security tools (e.g. firewalls, antivirus) should be configured to generate log records.
- Include a Variety of Log Types
  Logs should include, where applicable: audit logs, event logs, application logs, security logs, system logs, and maintenance logs.
- Protect Log Data
  Logs should be protected from unauthorised access using encryption and access controls.
- Back Up and Retain Logs
  Log backups should be performed regularly and retained for a predefined period, based on business needs or regulatory requirements.
- Review Logs for Anomalies
  Logs should be reviewed to detect unusual patterns or behaviours, such as repeated malware detections or excessive access to non-business websites.
- Define Retention Periods
  Retention periods for logs should be clearly defined. Sector-specific requirements should be taken into account.
- Support Monitoring and Accountability
  Monitoring should be in place to provide visibility into system activity and support effective auditing and incident response.
- Include OT Systems
  Logging practices should extend to OT environments, including industrial control systems, where logs can help detect operational anomalies or unauthorised access attempts.

PR.PS-05 Installation and execution of unauthorised software are prevented

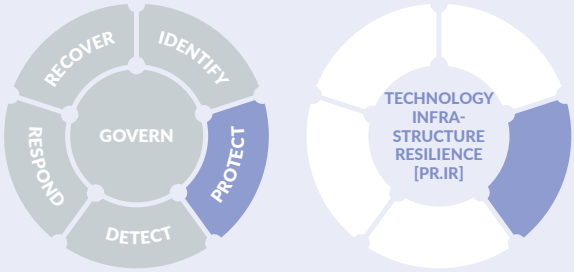
PR.PS-05.1 Web and e-mail filters shall be installed and used.

Implementation guidance

The goal of this control is to reduce the risk of malware infections, phishing attacks, and data breaches by implementing and maintaining effective web and email filtering solutions.

To support this goal, the organisation should:

- **Implement Web Filtering**
  Web filters should be used to control access to websites based on:
  - Predefined allow/block lists (e.g. by URL or domain)
  - Real-time content analysis to detect malicious or inappropriate content
  - Techniques such as URL filtering, content filtering, DNS filtering, and client- or server-side filtering
- **Configure Email Filtering**
  Email filters should be configured to:
  - Block spam, phishing attempts, and malicious attachments or links
  - Categorise incoming emails (e.g. newsletters, social media alerts) to reduce clutter and improve awareness
  - Scan for known threats and suspicious patterns to enhance email security
- **Keep Filters Updated**
  Filtering rules and threat databases should be updated regularly to respond to evolving threats.
- **Integrate with Security Policies**
  Web and email filtering should align with the broader organisational security policies and awareness efforts.
- **Include OT Considerations**
  In OT environments, internet and email access should be restricted to only what is operationally necessary. Filtering should be applied to any systems with external connectivity to prevent exposure to threats.



Security architectures are managed with the organisation's risk strategy, to protect asset confidentiality, integrity, and availability, and organisational resilience

PR.IR-01 Networks and environments are protected from unauthorised logical access and usage

PR.IR-01.1 Firewalls shall be installed, configured, and actively maintained on all networks used by the organisation to protect against unauthorised access and cyber threats.

Implementation guidance

The goal of this control is to ensure that all networks used by the organisation are protected against unauthorised access and cyber threats through the installation, configuration, and active maintenance of firewalls.

This control focuses on the installation, configuration, and maintenance of network-based firewalls to prevent unauthorised access by monitoring and controlling traffic entering or leaving the network (focus: control and prevention). In contrast, control DE.CM-01.1 addresses host-based firewalls, which help detect threats that bypass the network perimeter by monitoring traffic to and from individual devices (focus: visibility and detection).

To implement this control, the organisation should:

- Protect the Network Perimeter
  - A firewall should be installed between the internal network and the internet. This may be integrated into a wireless access point, router, or ISP-provided device.
  - Firewalls should be configured based on a baseline security policy using the principle of "deny all by default, allow only exceptions."
- Secure Endpoint Devices
  - A software firewall should be installed and regularly updated on all endpoint devices, including laptops, smartphones, and other networked systems.
  - Local firewalls should remain active even when using VPNs or cloud services.
- Secure Home and Remote Work Environments
  - Home networks used for teleworking should use routers with built-in firewalls, which should be enabled, securely configured, and kept up to date.
  - Software firewalls should be active and updated on all remote work devices.
  - Default administrator credentials on home routers should be changed and updated regularly.
- Protect Operational Technology (OT) Environments
  - Remote access to OT systems should be treated as third-party access, not standard teleworking.
  - A clear separation between IT and OT networks should be enforced.
  - When IT-to-OT access is necessary, it should pass through a secure jump host located in a dedicated DMZ.
- Enhance Detection with IDPS
  An Intrusion Detection and Prevention System (IDPS) should be considered to monitor and analyse network traffic for suspicious activity and enhance overall protection.

PR.IR-01.2 **To safeguard critical systems, organisations shall implement network segmentation and segregation aligned with trust boundaries and asset criticality, thereby limiting threat propagation and enforcing strict access control**

Implementation guidance

The goal of this control is to limit the spread of cyber threats and enforce strict access control by implementing network segmentation and segregation based on trust boundaries and the criticality of systems.

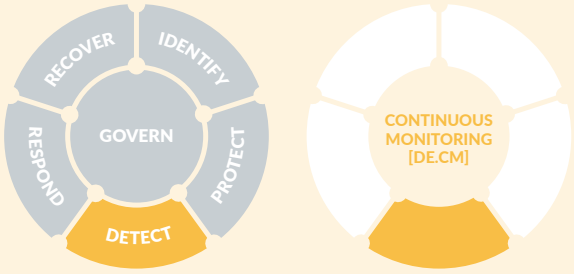
To implement this control, the following should be considered:

- Define Security Zones
  Networks should be divided into distinct zones (e.g. office, production, guest, mobile). Traffic between zones should be monitored and controlled, for example using firewalls.
- Align Segmentation with Trust and Criticality
  Segmentation should reflect which users and systems are trusted and how critical each asset is. Only essential communication between zones should be allowed, following the principle of least privilege.
- Avoid Flat Networks
  Flat networks should be avoided, as compromising one system could expose the entire environment. Segmentation should help contain threats within a single zone.
- Separate IT and OT Environments
  In environments with industrial systems (OT), office and production networks should be separated. Guest and mobile networks should not have direct access to internal office or production systems. Segmentation should follow the IEC 62443 standard, in particular requirements SR 5.1 to SR 5.3.
- Use VLANs with Caution
  VLANs should be used only as part of a broader defence-in-depth strategy. They should not be relied on alone to meet Security Level 2 requirements under IEC 62443-3-3. VLANs should be combined with firewalls, access controls, and monitoring.
- Enforce Segmentation with Firewalls
  Firewalls should be configured to block all traffic by default and allow only specific, approved connections. Segmentation and segregation should be enforced through well-maintained firewall rules, in line with control PR.IR-01.1.
- Clarify Segmentation vs. Segregation
  - Segmentation should be used to logically divide networks and control traffic between zones.
  - Segregation should be applied where systems have to be isolated, with no direct communication unless explicitly permitted.


WARNING!
SYSTEM WARNING

DETECT

Detect



Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events

DE.CM-01 Networks and network services are monitored to find potentially adverse events

DE.CM-01.1 Firewalls shall be installed and operated at the network boundaries, including end-point firewalls.

Implementation guidance

The goal of this control is to enhance visibility and detection of threats at the device level, particularly those that may bypass traditional network perimeter defences.

This control focuses on the use of host-based firewalls to detect threats that may bypass the network perimeter, by monitoring and controlling traffic to and from individual devices (focus: visibility and detection). In contrast, control PR.IR-01.1 addresses network-based firewalls, which are designed to prevent unauthorised access by managing traffic entering or leaving the network (focus: control and prevention).

To achieve this goal, the following should be considered:

- Define Endpoints Broadly
  Include desktops, laptops, servers, smartphones, and where feasible, OT (Operational Technology) components like PLCs and HMIs, as well as IoT devices.
- Deploy Host-Based Firewalls
  Ensure firewalls are installed, active, and properly configured on all endpoint devices. These firewalls help detect and block suspicious activity directly on the device, even when it is connected to secure networks or VPNs.
- Segment Network Assets
  Group systems based on their criticality or function (e.g. put public-facing services like email, web, and VPN servers in a DMZ).
- Use Predefined Firewall Rules
  Establish rules to filter both inbound and outbound traffic, thereby helping to detect anomalies or malicious behaviour.
- Limit Internet Gateways
  Reduce the number of interconnection points to the internet to minimise exposure and simplify monitoring.

DE.CM-01.2 Anti-virus, -spyware, and other -malware programs shall be installed and updated.

Implementation guidance

The goal of this control is to ensure that all organisational devices (IT and OT assets) are protected against malicious software, by deploying and regularly updating anti-malware tools.

To achieve this goal, consider the following:

- Scope of Protection
  - IT Devices: Install anti-malware software on all user and system devices, including desktops, laptops, servers, smartphones, and tablets.
  - OT Devices: Extend protection to OT assets such as PLCs, HMIs, SCADA servers, and engineering workstations, where technically feasible.
- Update and Scanning Practices
  - IT: Configure anti-malware tools to update in real-time or at least daily, followed by automated or scheduled scans.
  - OT: Carefully plan updates and scans to avoid operational disruption. Use maintenance windows and test updates before deployment.
- Tailored Solutions for OT
  - Use lightweight or OT-specific anti-malware tools that are compatible with real-time systems.
  - For legacy or resource-constrained OT devices, consider:
    - Application whitelisting
    - Network-based malware detection
    - Use specialised tools that quietly monitor industrial systems to spot unusual or suspicious activity, without interfering with how the systems operate (passive monitoring).
- Remote Work and BYOD
  - Apply the same protection standards to:
    - Home computers used for teleworking
    - Personal devices (BYOD) used for professional tasks
  - Use endpoint protection platforms to enforce policies across all devices.
- Centralised Management and Monitoring
  - Use Centralised tools to manage anti-malware configurations, updates, and alerts across both IT and OT environments.
  - Integrate malware alerts into the organisation's broader security monitoring and incident response processes.
- Continuous Improvement
  - Regularly review and test anti-malware effectiveness.
  - Update policies and tools based on emerging threats and lessons learned from incidents.

DE.CM-03 Personnel activity and technology usage are monitored, to find potentially adverse events

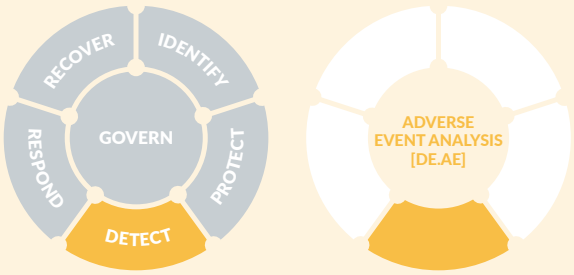
DE.CM-03-1 End point and network protection tools to monitor end-user behaviour for dangerous activity shall be implemented.

Implementation guidance

The goal of this control is to ensure that the organisation can detect and respond to risky or suspicious behaviour by users on both devices and networks. This helps identify threats such as malware infections, misuse of systems, or attempts to bypass security controls — whether caused by external attackers or insiders.

To achieve this goal, the following should be considered:

- Organisations should consider using a combination of modern security tools that work together to provide a full picture of user and system activity:
  - Intrusion Detection and Prevention Systems (IDPS): These tools monitor network traffic and can block or alert on suspicious activity, such as hacking attempts or exploitation of vulnerabilities.
  - Web Application Firewalls (WAFs) and API Gateways: These help protect online applications and services by filtering harmful traffic and preventing unauthorised access.
- In addition, a layered approach using advanced detection and response tools can provide real-time visibility and faster response:
  - Endpoint Detection and Response (EDR): Monitors activity on individual devices (like laptops or servers) to detect threats such as malware or unauthorised access.
  - Network Detection and Response (NDR): Analyses network traffic to identify unusual patterns, such as lateral movement or hidden attacks.
  - Identity Threat Detection and Response (ITDR): Focuses on detecting misuse of user accounts, such as stolen credentials or insider threats.
  - User and Entity Behaviour Analytics (UEBA): Uses machine learning to understand normal behaviour and detect anomalies that may indicate a threat.
- These tools are part of a modern, layered security strategy and are often referenced in industry best practices and frameworks such as the Security Operations Centre (SOC) Visibility Triad introduced by Gartner.



Anomalies, indicators of compromise, and other potentially adverse events are analysed to characterise the events and detect cybersecurity incidents

DE.AE-03 Information is correlated from multiple sources

DE.AE-03.1 The logging functionality of protection and detection tools shall be enabled. Logs shall be backed up and retained for a predefined period and regularly reviewed to identify unusual or potentially harmful activity.

Implementation guidance

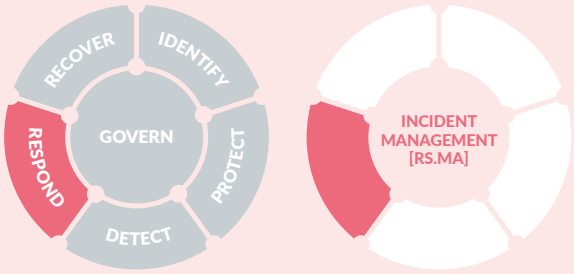
The goal of this control is to make sure security tools have logging turned on, logs are kept for a set time, and regularly checked to spot unusual or harmful activity. This helps to detect threats early and take action. Examples of such tools include firewalls, antivirus software, endpoint detection, and intrusion detection systems.

To achieve this goal, the following should be considered:

- Logs should be stored securely and retained according to a defined retention schedule, based on applicable legal, regulatory, or operational needs.
- Event detection tools and solutions should be configured to generate automated alerts for suspicious or harmful activity.
- A documented procedure should be in place for regularly reviewing logs and dashboards to support timely detection and response.
- Log reviews should include checks for patterns such as repeated malware infections, abnormal network traffic, or excessive access to non-business-related websites.
- If such patterns are identified, follow-up actions should be defined, such as strengthening specific security controls, updating detection rules, or conducting targeted awareness training.

RESPOND

Respond



Responses to detected cybersecurity incidents are managed

RS.MA-01 The incident response plan is executed in coordination with relevant third parties once an incident is declared

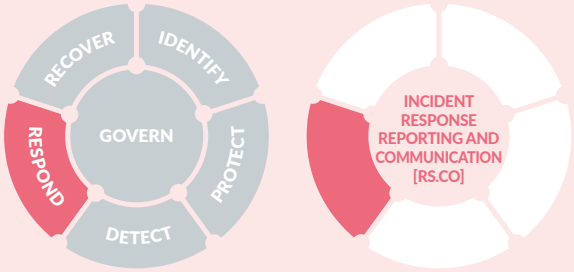
RS.MA-01.1 An incident response plan, including defined roles, responsibilities, and authorities, shall be executed during or after a cybersecurity event affecting the organisation's critical systems.

Implementation guidance

The goal of this control is to ensure that a well-defined incident response plan is executed during or after a cybersecurity event affecting the organisation's critical systems, enabling timely detection, containment, communication, and recovery.

To support this goal, the organisation should:

- **Develop a Documented Response Plan**
  The plan should include predefined instructions and procedures to detect cybersecurity incidents, respond effectively, and support the recovery of critical systems.
- **Include Detection Capabilities**
  Detection technologies should be in place to automatically report confirmed incidents and trigger response actions.
- **Define Roles, Responsibilities, and Authorities**
  The plan should clearly identify:
  - Who is involved in the response
  - Contact details for key personnel
  - Who has the authority to initiate recovery
  - Who is responsible for external communication (e.g. regulators, partners, media)
- **Review and Update the Plan Regularly**
  The plan should be reviewed and updated to reflect changes in the threat landscape, organisational structure, or lessons learned from past incidents.
- **Test the Plan Through Exercises**
  Simulations and tabletop exercises should be conducted to validate the plan's effectiveness and identify areas for improvement.
- **Include OT Environments**
  The plan should address incident response in OT systems, including coordination with safety protocols, isolation of affected industrial assets, and restoration of operational processes.



Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies

RS.CO-02 Internal and external stakeholders are notified of incidents

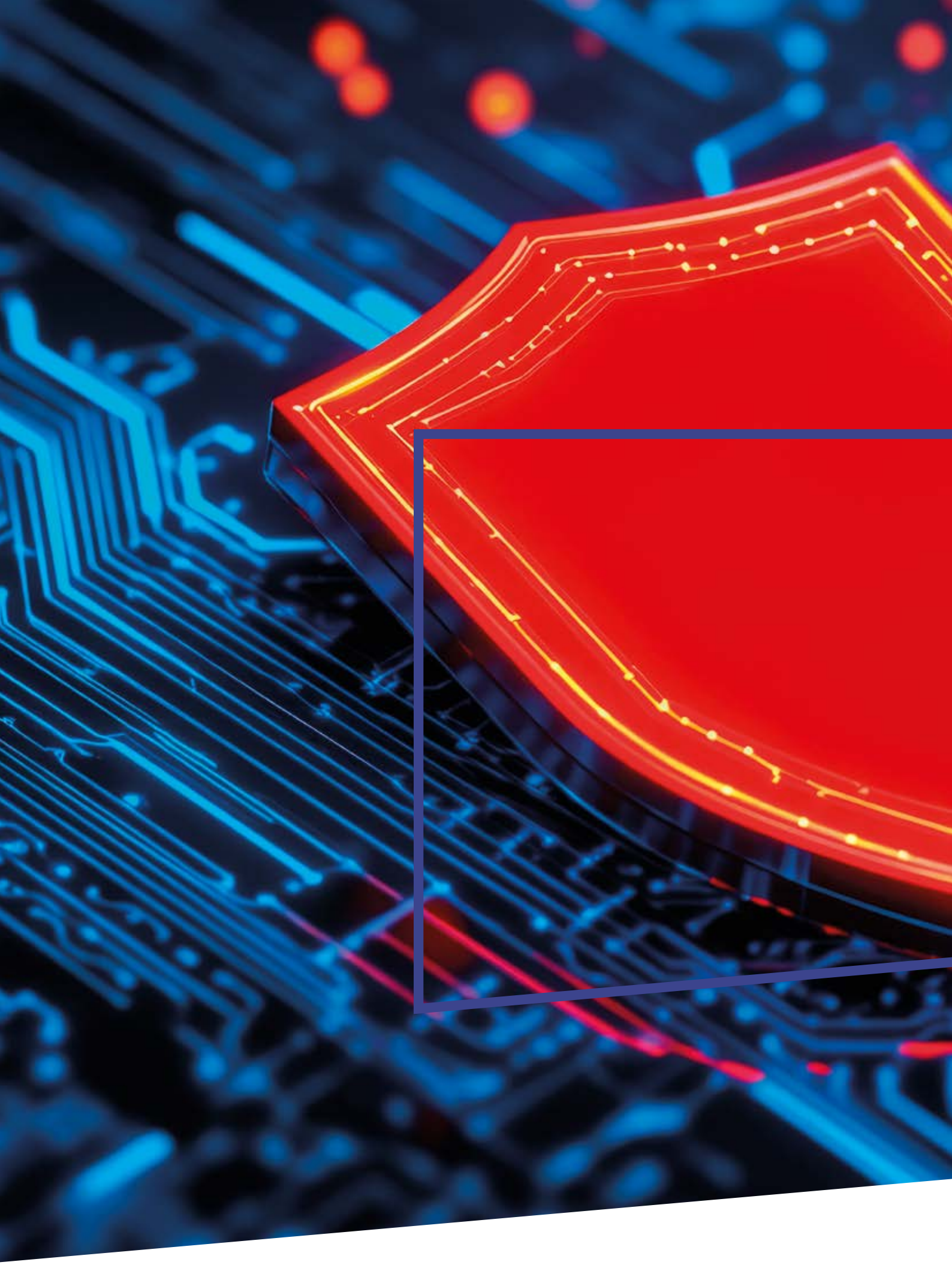
RS.CO-02.1 Information about cybersecurity incidents shall be communicated to employees in a way that is clear and easy to understand.

Implementation guidance

The goal of this control is to ensure that all employees are informed about cybersecurity incidents in a timely and understandable manner, so they can respond appropriately and help reduce risks.

To achieve this:

- An Incident Response Plan (IRP) should be in place. This plan outlines how the organisation will respond to cybersecurity incidents, including who is responsible for what and how to escalate different types of threats.
- The IRP should include a communication protocol that explains how to share accurate and relevant information with employees quickly and efficiently during an incident.
- The plan should define the communication channels to be used, such as email, internal messaging platforms, phone calls, or a dedicated incident portal.
- Templates for incident messages should be prepared in advance. These templates should include key details like the type of incident, how serious it is, which systems are affected, and what actions employees should take.
- Messages should be written in clear, simple language that avoids technical terms, so all employees can understand what is happening and what is expected of them.
- Senior management should receive high-level summaries that explain the impact of the incident, the risks involved, and the steps being taken to resolve it.



RECOVER

Recover

Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents

RC.RP-01 The recovery portion of the incident response plan is executed once initiated from the incident response process

RC.RP-01.1 A recovery process for disasters and information/cybersecurity incidents shall be developed and executed.

Implementation guidance

The goal of this control is to ensure the organisation can respond quickly and effectively to disasters, information security incidents, and cybersecurity events by developing and executing a structured recovery process that protects people, systems, and data.

To support this goal, the organisation should:

- Develop a Recovery Process
  A documented process should guide immediate actions in the event of a fire, medical emergency, theft, natural disaster, or information/cybersecurity incident.
- Define Roles and Responsibilities
  The recovery process should specify who is authorised to initiate recovery procedures and who will communicate with external stakeholders.
- Protect Information and Systems
  The process should include steps for securing information and systems, such as shutting down or locking devices, switching to backup sites, or securing physical documents.
- Establish Contact Procedures
  A list of internal and external contacts should be maintained and included in the recovery plan for quick access during an incident.
- Ensure Awareness and Readiness
  Individuals with recovery responsibilities should be familiar with the recovery plan and understand the authorisations required to carry out each step.
- Integrate with the Incident Response Plan
  The recovery process should be part of or aligned with the broader Incident Response Plan (IRP) to ensure consistency and coordination.
- Include OT Environments
  Recovery planning should address OT systems, including procedures for restoring industrial operations, securing control systems, and coordinating with safety protocols.
- Plan for Future Enhancements
  This control serves as a foundation for more advanced recovery planning, as further developed in control RC.RP-06.1 (assurance level Important).

ANNEX

ANNEX A: LIST OF KEY MEASURES FOR THE ASSURANCE LEVEL 'BASIC'

Identify

ID.AM-08 Systems, hardware, software, services, and data are managed throughout their lifecycles

ID.AM-08.2 Patches and security updates for operating systems and critical system components shall be installed.

Protect

PR.AA-01 Identities and credentials for authorised users, services, and hardware are managed by the organisation

PR.AA-01.1 Identities and credentials for authorised users, services, and hardware shall be managed.

PR.AA-03 Users, services, and hardware are authenticated

PR.AA-03.2 Multi-Factor Authentication (MFA) shall be required to access the organisation's networks remotely.

PR.AA-05 Access permissions, entitlements, and authorisations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties

PR.AA-05.1 Access permissions, rights, and authorisations shall be defined, managed, enforced and reviewed.

PR.AA-05.2 It shall be determined who needs access to the organisation's business-critical information and technology and the means to gain access.

PR.AA-05.3 Access rights, privileges and authorisations shall be restricted to the systems and specific information needed to perform the tasks (the principle of Least Privilege).

PR.AA-05.4 No-one shall have administrative privileges for routine day-to-day tasks.

PR.DS-11 Backups of data are created, protected, maintained, and tested

PR.DS-11.1 Backups for the organisation's business critical data shall be performed and stored on a different system from the device on which the original data resides.

PR.PS-04 Log records are generated and made available for continuous monitoring

PR.PS-04.1 Logs shall be maintained, documented, and monitored.

PR.IR-01 Networks and environments are protected from unauthorised logical access and usage

PR.IR-01.1 Firewalls shall be installed, configured, and actively maintained on all networks used by the organisation to protect against unauthorised access and cyber threats.

PR.IR-01.2 To safeguard critical systems, organisations shall implement network segmentation and segregation aligned with trust boundaries and asset criticality, thereby limiting threat propagation and enforcing strict access control.

Detect

DE.CM-01 Networks and network services are monitored to find potentially adverse events

DE.CM-01.2 Anti-virus, -spyware, and other -malware programs shall be installed and updated.

DE.AE-03 Information is correlated from multiple sources

DE.AE-03.1 The logging functionality of protection and detection tools shall be enabled. Logs shall be backed up and kept for a predefined period, and regularly reviewed to identify unusual or potentially harmful activity.

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 the CCB.

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

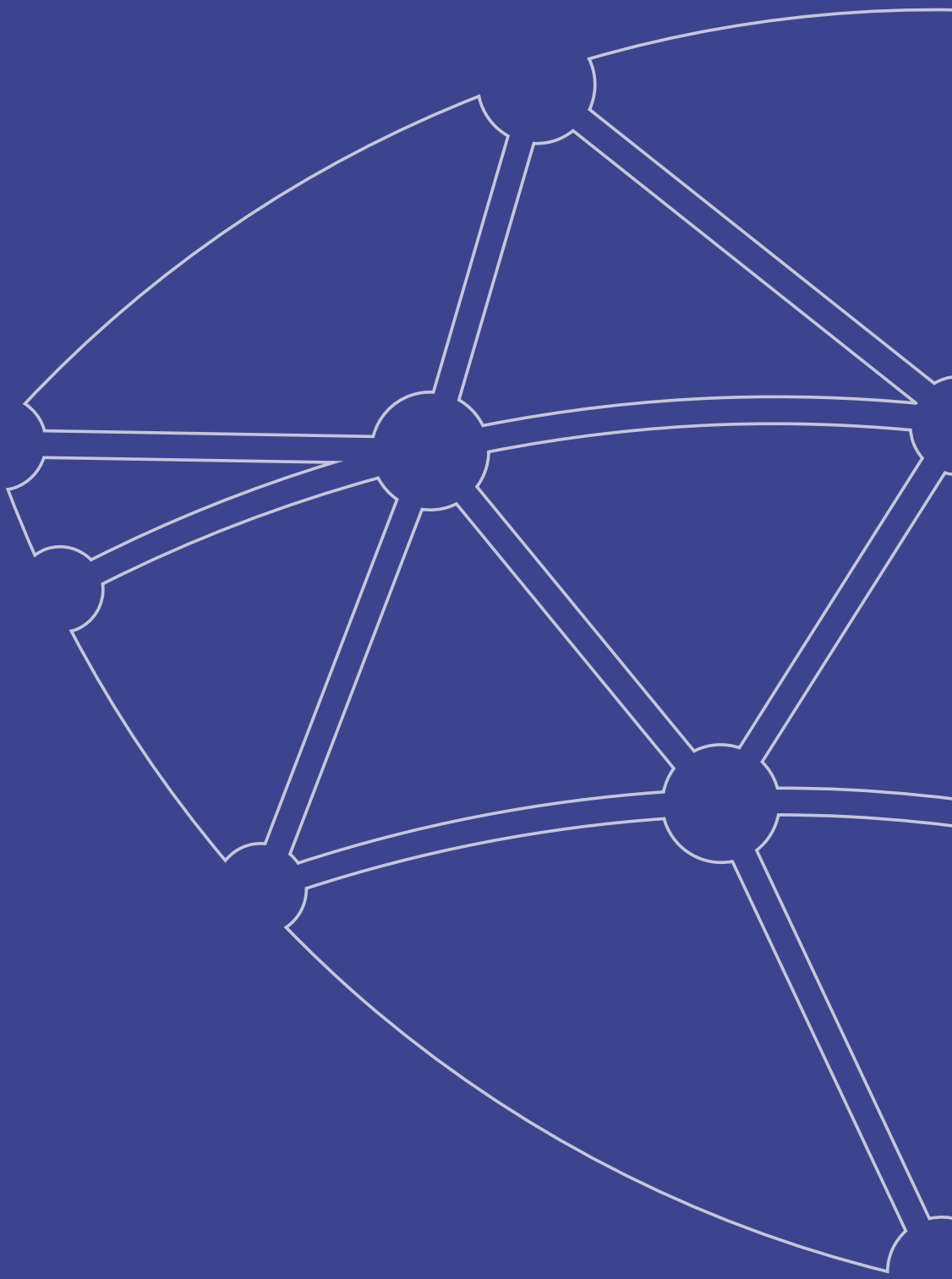
- is exclusively of a general nature and is not intended to take into consideration all particular situations.
- is not necessarily exhaustive, precise, or up to date on all points.

Responsible editor

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

Legal depot

D/2025/14828/002



Centre for Cybersecurity Belgium

Rue de la Loi, 18

1000 Brussels