CyFun®

SMALL BASIC **IMPORTANT** ESSENTIAL

CyberFundamentals 2025

Version 2025-10-01

TABLE OF CONTENTS

PROTECT   57

DETECT   93

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 recognize 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*.

| SMALL | BASIC | IMPORTANT | ESSENTIAL |

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 cybersecurity 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.

In the assurance level **Important**, Basic security measures are strengthened to help reduce known cyber risks and limit the impact of attacks carried out by threat actors with limited resources and skills.

Controls related to **management aspects** have to be reviewed during every certification audit – whether it is an initial audit, a surveillance audit, or a recertification audit – when auditing the CyFun® "Essential" assurance level. These controls correspond to the management system principles that ISO/IEC 17021-1 requires certification bodies to assess when auditing any type of management system.

Based on common types of cyber-attacks, certain requirements are identified as **key measure**. These shall be addressed at this assurance level, in addition to the key measures already required at the assurance level Basic.

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-01 The organisational mission is understood and informs cybersecurity risk management

GV.OC-01.1 The organisation's mission shall be established, communicated and shall form the basis for information and cybersecurity risk management.

Implementation guidance

The goal of this control is to ensure that the organisation's mission is clearly defined and communicated, and that it serves as the foundation for managing information and cybersecurity risks. Understanding the mission helps identify which risks could interfere with achieving strategic objectives.

To achieve this goal, the following should be considered:
- The organisation's mission should be communicated through materials such as vision and mission statements, service strategies, or marketing documents. This helps guide risk identification and prioritisation.
- Business processes and strategic goals should be developed with consideration for information security and cybersecurity. This includes understanding how risks may affect operations, assets, individuals, partners, or broader societal interests.
- The need to protect sensitive information, including personal data, should be assessed based on the organisation's mission and how its systems and services operate.
- The mission and related business processes should be reviewed regularly, for example once a year, to ensure they remain relevant and continue to support effective risk management.

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

GV.OC-03.2 Legal, regulatory, and contractual obligations related to information and cybersecurity shall be continuously managed to ensure they remain accurate, up to date, and effectively applied.

Implementation guidance

The goal of this control is to ensure that legal and regulatory requirements related to information and cybersecurity are continuously managed, kept up to date, and effectively applied across the organisation.

To achieve this goal, the following should be considered:
- A structured process should be in place to manage legal and regulatory requirements related to information and cybersecurity on an ongoing basis.
- These requirements should be documented, regularly reviewed, and updated to reflect changes in laws and regulations.
- The organisation's approach to compliance should be clearly defined, including roles, responsibilities, and accountability.
- Mechanisms should be implemented to monitor changes in the legal and regulatory landscape. Such changes should trigger a review of relevant policies, procedures, and controls to ensure continued compliance.
- Evidence of compliance activities should be maintained to support audits and demonstrate due diligence.

GV.OC-04 **Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organisation are understood and communicated**

GV.OC-04.1 The organisation shall identify, document, and communicate the critical objectives, capabilities, and services relied upon by external stakeholders, prioritise them based on criticality, and integrate this prioritisation into the risk assessment process

Implementation guidance

The goal of this control is to ensure that the organisation understands which critical services, capabilities, and objectives are essential to external stakeholders, prioritises them based on their importance, and includes them in the risk assessment process.

To achieve this goal, the following should be considered:
· The focus of this control is on what the organisation delivers to others, in other words, the services and functions that external stakeholders depend on (the downstream supply chain, such as customers, partners, or end users).
· Critical services and the internal functions that support them should be clearly identified.
· Criteria should be defined to determine how important each service or capability is, from both internal and external perspectives.
· A business impact analysis can help identify which assets and operations are vital to achieving key objectives, and what the consequences would be if they were disrupted.
· Resilience goals, such as how quickly critical services should recover during disruptions, should be established and communicated.

GV.OC-04.2 The organisation shall define and document cybersecurity requirements for essential operations, validate them through testing and audits, maintain records of results and corrective actions, and regularly update requirements based on evolving risks

Implementation guidance

The goal of this control is to ensure that essential operations are protected by clearly defined and tested security measures, and that these measures remain effective and up to date as risks evolve.

To achieve this goal, the following actionable steps should be considered:
· **Identification & Documentation**
  · Define critical services and their dependencies (e.g. systems, suppliers) through a structured risk assessment.
  · Document security and operational requirements, including regulatory and industry-specific needs (e.g. CyFun®, ISO/IEC 27001, IEC 62443).
· **Validation & Approval**
  · Establish governance processes for reviewing and approving identified security requirements.
  · Assign accountability to relevant stakeholders (e.g. security teams, compliance officers, senior management).
· **Testing & Assurance**
  · Conduct penetration tests, vulnerability assessments, and incident simulations to validate implementation.
  · Ensure audits are performed to assess effectiveness and identify gaps in security measures.
  · Implement corrective actions where deficiencies are found, ensuring continuous improvement.

- Record-Keeping & Compliance
  - Maintain detailed documentation of testing procedures, results, approvals, and corrective measures.
  - Align security frameworks with regulatory obligations to ensure compliance and governance oversight.
- Continuous Review & Adaptation
  - Regularly reassess requirements in response to evolving threats, incidents, and regulatory changes.
  - Ensure governance bodies oversee updates and improvements to maintain long-term cyber resilience.

GV.OC-05 Outcomes, capabilities, and services that the organisation depends on are understood and communicated

GV.OC-05.1 **The organisation shall identify, document, and communicate its role in the supply chain, including the external capabilities, services, and dependencies it relies on (upstream), as well as its interactions with downstream stakeholders.**

Implementation guidance

The goal of this control is to ensure the organisation identifies, documents, and communicates its role within the supply chain by understanding the external capabilities, services, and dependencies it relies on (upstream), while also recognising its interactions with downstream stakeholders.

This control focuses primarily on the upstream supply chain, what the organisation depends on from others, while maintaining alignment with GV.OC-04, which addresses what the organisation delivers to others. Together, they provide a complete view of supply chain dependencies and responsibilities.

To support this control, the following should be considered:
- The organisation's role in the supply chain should be clearly defined, including both what is delivered to others (downstream) and what is received from external sources (upstream).
- Dependencies on external resources — such as facilities, cloud providers, and suppliers of services, products, or capabilities — should be identified and documented.
- These dependencies should be mapped to related business functions and organisational assets to understand their impact on operations.
- Particular attention should be given to external dependencies that represent potential points of failure for critical services or capabilities.
- This information should be shared with relevant personnel and stakeholders to support risk management, continuity planning, and coordinated response.
- Communication channels should be established to ensure that supply chain roles and dependencies are clearly understood across the organization and with key partners.

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

GV.RM-01 **Risk management objectives are established and agreed to by organisational stakeholders**

GV.RM-01.1 Information/cybersecurity objectives shall be identified, agreed to by organisational stakeholders and approved by senior management

Implementation guidance

To support this objective, organisations should:
- Follow the risk management principles outlined in ISO/IEC 27005, which provide guidance on identifying, assessing, and mitigating information security risks. Specifically:
  - Clause 6.1 should be used to establish a structured risk assessment process.
  - Clause 6.3 should guide the definition of appropriate risk treatment strategies.
- Update near-term and long-term information and cybersecurity objectives during annual strategic planning and in response to major organisational changes.
- In OT-sector organisations, senior management should consider health, safety, and environmental factors when identifying risks.
- Establish measurable (SMART) objectives for information and cybersecurity (e.g., improving user training quality, ensuring adequate protection for industrial control systems).
- Use these objectives to measure and manage risk and performance across the organisation.

GV.RM-02 **Risk appetite and risk tolerance statements are established, communicated, and maintained**

GV.RM-02.1 Risk appetite and risk tolerance statements shall be defined, documented, approved by senior management, communicated, and maintained.

Implementation guidance

The goal of GV.RM-02.1 is to ensure that an organisation has a clear and actionable understanding of its risk boundaries, which helps guide decision-making and risk management practices.

The following should be considered to reach this goal:
- Risk appetite is the amount and type of risk an organisation is willing to take or accept, and is strategic/ qualitative (Source: ISO/IEC 27005).
- Risk tolerance is the acceptable deviation from the level set by the risk appetite and business objectives, and is tactical/quantitative (source: ISACA).
- The organisation's risk appetite should take into account its role in critical infrastructure and its sector.
- Organisations in the OT sector should take into account health, safety & environment priorities in the definition of their risk appetite.
- Risk appetite statements should be translated into specific, measurable, and broadly understandable risk tolerance statements (SMART).
- Organisational objectives and risk appetite should be periodically refined based on known risk exposure and residual risk.
- With AR-in-a-Box, ENISA, the European Union Agency for Cybersecurity, provides organisations with the essential tools and resources to effectively raise cybersecurity awareness within their operations. This ENISA-Do-It-Yourself Toolbox contains a C-level guide.

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

> **GV.RM-03.2** Information and Cybersecurity risks shall be documented, as part of the enterprise risk management processes, formally approved by senior management, and updated when changes occur.

Implementation guidance

This control should ensure that the strategy is put into action through structured processes. It focuses on operational and governance level, ensures accountability and traceability of risks, and emphasises formal processes and oversight.

The following actionable components should be considered while implementing this control:
Systematic Risk Identification
- Goal: Proactively identify information and cybersecurity risks across the organisation.
- Actions:
  - Regular risk assessments should be conducted using methods like threat modelling, risk workshops, and vulnerability scans.
  - Risks related to all digital and physical assets (hardware, software, data, networks) should be included in the asset inventory, along with key metadata (location, owner, usage).
  - Leverage sources such as:
    - Security incident logs
    - Penetration test results
    - Regulatory requirements
    - Industry threat intelligence
- Consider involving cross-functional teams (IT/OT, legal, compliance, business units).
- Tools to Consider:
  - Risk assessment templates
  - Threat intelligence platforms (e.g., MISP, Recorded Future)
  - Asset inventories and data flow diagrams

Risk Documentation in the ERM Framework
- Goal: Ensure cybersecurity risks are integrated into the broader Enterprise Risk Management (ERM) process.
- Actions:
  - Consider using a centralised risk register or GRC tool to document:
    - Risk description
    - Likelihood and impact
    - Risk owner
    - Controls in place
    - Residual risk
    - Treatment plan
  - Cybersecurity risk management should be aligned with strategic business objectives to ensure relevance and support.
- Tools to Consider:
  - GRC platforms
  - Excel/SharePoint (for smaller organisations)

Formal Approval and Senior Management Involvement
- Goal: Ensure leadership oversight and accountability in risk decisions.
- Actions:
  - Risk assessments and treatment plans should be presented to a Risk Committee or Executive Board.
  - Consider including cybersecurity risks in quarterly risk reports.
  - Formal sign-off should be obtained on:
    - Risk acceptance
    - Mitigation plans
    - Budget allocations

- Tools to Consider:
  - Board reporting templates
  - Risk dashboards
  - Meeting minutes with documented approvals

Communication and Awareness
- Goal: Ensure all relevant stakeholders are informed and engaged.
- Actions:
  - Clear lines of communication should be established for cybersecurity risks, including those from suppliers and third parties.
  - Approved risks and mitigation strategies should be communicated to relevant teams.
  - Awareness should be promoted through training, briefings, and internal communications.
- Tools to Consider:
  - Internal communication platforms (e.g., Teams, Slack)
  - Risk communication plans
  - Stakeholder maps

Continuous Monitoring and Updates
- Goal: Keep risk information current and responsive to change.
- Actions:
  - Continuous monitoring should be implemented to detect changes in the threat landscape or organisational environment.
  - Consider defining triggers for updates, such as:
    - New threats or vulnerabilities
    - Changes in business processes or IT systems
    - Regulatory changes
  - A change management process should be established that includes updating cybersecurity documentation.
  - Regular reviews should be conducted (e.g., quarterly or twice a year) of documented risks.
- Tools to Consider:
  - Change management systems
  - Continuous monitoring tools
  - Risk review calendars

This control operationalises GV.RM-03.1 by embedding cybersecurity risks into the Enterprise Risk Management (ERM) framework and ensuring governance and accountability.

GV.RM-04 **Strategic direction that describes appropriate risk response options is established and communicated**

GV.RM-04.1 **A high-level plan or vision shall be formally established and clearly communicated to everyone involved on how to manage risks, including the different strategies the organisation can employ to deal with identified risks based on risk appetite or risk tolerance level.**

Implementation guidance
The aim of this control is to set the strategic foundation for risk management, including:
- Risk tolerance and appetite,
- Strategic direction for managing risks (e.g., mitigate, transfer, accept),
- Ensuring alignment across departments.
- Ensuring that everyone in the organisation understands the big picture of how risks are approached and managed

The control focus on:
- Strategic and organisational -level risk management.
- Establishing a formal, overarching vision or plan.
- Communicating risk management strategies (e.g., avoid, mitigate, transfer, accept).
- Applies to all types of risks, not just cybersecurity.

In relation to the controls GV.RM-03.1, GV.RM-03.2 and GV.RM-05.1, this control is the starting point; it defines the organisation's risk philosophy, including appetite and tolerance, which guides all other activities.

GV.RM-05 Lines of communication across the organisation are established for cybersecurity risks, including risks from suppliers and other third parties

GV.RM-05.1 **To support the high-level risk management vision, the organisation shall establish clear lines of communication for cybersecurity risks, including those arising from suppliers and third parties.**

Implementation guidance

The aim of this control is to ensure that cybersecurity and information security risk information is shared effectively across the organisation and with external parties.

This control focus on operational and tactical communication is specific to cybersecurity risks and emphasises communication channels (e.g., reporting, escalation, coordination), including external risks from suppliers and third parties.

Consider the following elements when implementing this control:
- Define Communication Roles and Responsibilities
  Assign clear ownership for reporting, escalating, and responding to cybersecurity risks across departments and with third parties.
- Establish Communication Channels
  Use structured channels such as email groups, ticketing systems, incident response platforms, or collaboration tools (e.g. Teams, Slack) for timely risk communication.
- Include Third Parties
  Integrate suppliers and partners into the communication process through contractual clauses, shared reporting protocols, or joint incident response plans.
- Document and Train
  Maintain a communication protocol or playbook and train relevant staff on how and when to report cybersecurity risks.
- Review and Improve
  Periodically test and review communication effectiveness through tabletop exercises or post-incident reviews.

This control supports the implementation of GV.RM-03.2 by ensuring that identified and documented risks are communicated to the right stakeholders, enabling timely response and coordination.

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

GV.RR-02 **Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced**

GV.RR-02.1 Information security and cybersecurity roles, responsibilities and authorities for employees, suppliers, customers, and partners shall be documented, reviewed, authorised, kept up to date, communicated, and coordinated internally and externally.

Implementation guidance

The goal of this control is to ensure all internal and external parties understand and fulfil their cybersecurity roles, responsibilities and authorities, reducing gaps, overlaps, and delays in incident response and compliance.

It should be considered to:
- Describe security roles, responsibilities, and authorities: who in the organisation should be consulted, informed, held responsible and accountable for all or part of the enterprise assets. Use of the RACI model can be considered. Guidance can also be found in the ENISA European Cybersecurity Skills Framework Role Profiles (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles).
- Include risk management roles, responsibilities, and authorities.
- Include information/cybersecurity responsibilities and performance requirements in personnel descriptions.
- Clearly articulate information/cybersecurity responsibilities within operations, risk functions, and internal audit functions.
- Identify one or more specific roles or positions that will be responsible and accountable for planning, resourcing, and executing information/cybersecurity supply chain risk management activities.
- Follow the previous guideline, extend internal security roles, responsibilities, and authorities to the information/cybersecurity supply chain risk management roles, responsibilities, and authorities.
- Develop roles, responsibilities, and authorities for suppliers, customers, and business partners to address shared responsibilities for applicable information/cybersecurity risks, and integrate them into organisational policies and applicable third-party agreements.
- Internally communicate information/cybersecurity supply chain risk management roles and responsibilities for third parties.
- Establish rules and protocols for information sharing and reporting processes between the organisation and its suppliers.

- Consider a clear distinction between IT (Information Technology) and OT (Operational Technology) in the implementation of this control by taking the following into account:
  - Roles and Responsibilities
    - IT: Define roles such as system administrator, network security analyst, incident responder.
    - OT: Define roles such as control system engineer, OT cybersecurity lead, plant operator.
  - Documentation and Review
    - Ensure both IT and OT roles are documented separately but aligned.
    - Review cycles may differ: IT (quarterly/annually), OT (aligned with maintenance windows).
  - Authorisation and Updates
    - Ensure both IT and OT documentation is approved by relevant leadership (e.g., CIO for IT, Plant Manager for OT).
    - Updates in OT may require change control procedures due to safety implications.
  - Communication and Coordination
    - Internal: Ensure IT and OT teams have joint incident response plans.
    - External: Include suppliers and partners specific to OT (e.g., ICS vendors) and IT (e.g., cloud providers).

GV.RR-03   Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies

GV.RR-03-1   Sufficient resources shall be allocated in line with the cybersecurity risk strategy, roles, responsibilities and policies.

Implementation guidance

The goal of this control is to ensure that cybersecurity is effectively supported by aligning resource allocation (which may include staff, budget, technology) with strategic priorities, roles, and policies.

To make this happen, the following should be considered:
- Periodic management reviews should be conducted to ensure that those with cybersecurity risk management responsibilities have the necessary authority.
- Resource allocation and investment should be determined in line with the organisation's risk appetite
- Adequate and sufficient people, processes and technical resources should be ensured to support the cybersecurity strategy
- Expert personnel should have the specialised knowledge and skills required for OT security to enable collaboration with OT engineers so that alerts are interpreted accurately and threats are responded to effectively.

GV.RR-03-2 The organisation shall assign roles and responsibilities for reviewing and updating response and recovery plans, ensuring they reflect changes in the risk environment and remain effective.

Implementation guidance

The goal of this control is to ensure response and recovery plans remain effective by assigning roles and responsibility for their regular review and adaptation to evolving risks.

To implement this control, the following elements should be considered:
- **Define and Assign Responsibilities**
  - Assign clear roles for maintaining, reviewing, and updating response and recovery plans.
  - Ensure responsible individuals have the authority and resources to act on identified changes.
  - Designate a central coordinator or team to oversee the update process and ensure accountability.
- **Understand and Monitor Organisational Context**
  - Regularly assess internal and external factors such as:
    - Organisational structure and critical systems
    - Emerging threats and vulnerabilities
    - Regulatory changes and market dynamics
    - Lessons learned from incidents, tests, or exercises
- **Update Plans Based on Contextual Changes**
  - Revise plans to reflect:
    - New or evolving threats
    - Changes in technology or infrastructure
    - Operational challenges or gaps identified during testing
  - Updates may include contact lists, communication protocols, escalation paths, and resource allocations.
- **Communicate and Train**
  - Ensure all relevant stakeholders are informed of updates.
  - Provide training or briefings to clarify roles and responsibilities in the revised plans.
- **Test and Improve**
  - Conduct regular exercises and simulations to validate the effectiveness of updated plans.
  - Use results to identify gaps and drive continuous improvement.
- **Continuous Review Cycle**
  - Establish a review schedule (e.g. quarterly or after major changes).
  - Integrate plan updates with broader risk management and governance processes.

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.

GV.RR-04.2   **A cybersecurity process for human resources shall be developed and maintained applicable at recruitment, during employment and at termination of employment.**

Implementation guidance

The goal of this control is to ensure cybersecurity risks are managed throughout the employee lifecycle by integrating security into HR processes, from hiring to termination.

To make this happen, the following should be considered:
- Cybersecurity risk management considerations should be integrated into human resources processes (e.g., personnel screening, onboarding, change notification, offboarding)
- The human resource cybersecurity process should include access to critical information or technology; background verification checks; code of conduct; roles, authorities, and responsibilities …
- Obligations for personnel to be aware of, adhere to and uphold security policies in relation to their role should be defined and enforced.
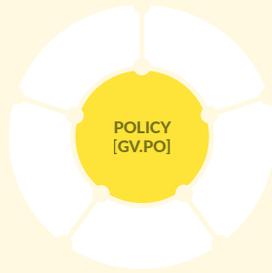
Organisational cybersecurity policy is established, communicated, and enforced

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.

GV.PO-01.2 **Organisational-wide information and cybersecurity policies and procedures shall include the use of cryptography and, where appropriate, encryption, reflect changes in requirements, threats, technology and organisational roles, and be approved by senior management, who oversee its implementation.**

This control builds further on GV.PO-01.1 and focuses on the content and oversight of the cyber- and information security policies themselves. It ensures that specific technical topics (such as cryptography and encryption) are addressed, policies are responsive to change and Senior leadership is actively involved in approval and oversight.

Consider the following elements to be covered:
· **Define Scope & Objectives**
  Ensure policies apply organisation-wide and align with business and risk priorities.
· **Include Cryptography & Encryption**
  · Address encryption at-rest/in-transit, key management, and approved algorithms.
  · Define where encryption is required (e.g., personal data, remote access).
· **Keep Policies Current**
  Update policies to reflect changes in:
  · Legal/regulatory requirements
  · Threat landscape
  · Technology
  · Organisational structure
· **Senior Management Oversight**
  · Require formal approval by senior leadership.
  · Assign a policy owner (e.g., CISO) to oversee implementation and compliance.
· **Assign Roles & Responsibilities**
  · Use ENISA ECSF Role Profiles
    https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles) to:
    · Define cybersecurity roles (e.g., Policy Officer, Risk Manager)
    · Align tasks, skills, and competencies
· **Communicate & Train**
  Disseminate policies and provide role-specific training.
· **Monitor & Enforce**
  Use technical controls and audits to ensure compliance.

Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organisational stakeholders

---

GV.SC-02 **Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally**

GV.SC-02.1 **Third-party providers shall notify any transfer, termination or transition of personnel with physical or logical access to business-critical system elements of the organisation.**

Implementation guidance

The goal of this control is to ensure continuity and security of critical systems by requiring third-party providers to report personnel changes affecting access.

To achieve this goal, the following should be considered:
- Third-party providers include, for example, service providers, contractors, and other organisations providing system development, technology services, outsourced applications, or network and security management.
- Rules and protocols for information sharing between the organisation and its suppliers and sub-tier suppliers should be defined in contractual agreements.

GV.SC-05 Requirements to address cybersecurity risks in supply chains are established, prioritised, and integrated into contracts and other types of agreements with suppliers and other relevant third parties

GV.SC-05.1 Requirements for addressing cybersecurity risks and the sharing of sensitive information in supply chains shall be established, prioritised, integrated into contracts and other types of formal agreements, and enforced.

Implementation guidance

The goal of this control is to establish and enforce cybersecurity and sensitive data handling requirements in supply chain agreements, by integrating them into contracts and prioritising them based on risk.

To make this happen, the following should be considered:
- Contractual agreements and other types of formal agreements with suppliers and other relevant third parties should define expectations, responsibilities, and security requirements.
- Key elements of these agreements include information sharing between the organisation and its suppliers and sub-tier suppliers, security controls, incident response, and required compliance with standards and regulations.
- Security requirements should be set for suppliers, products and services that are proportionate to the criticality and potential consequences if compromised.
- All cybersecurity and supply chain requirements that third parties must comply with, should be included in standard contractual language (i.e., pre-drafted, commonly used terms and clauses that ensure consistency, compliance, and clarity). The contract should also specify how compliance with these requirements will be verified.
- Consider to include in the enforcement that third-party providers and users (e.g. suppliers, customers, partners) should be able to demonstrate the understanding of their roles and responsibilities.
- Consider defining security requirements in service-level agreements (SLAs) for monitoring suppliers for acceptable security performance throughout the supplier relationship lifecycle.
- Consider to contractually require suppliers to vet their employees and guard against insider threats.
- Consider to contractually require suppliers to provide evidence of performing acceptable security practices through, for example, self-assessment (e.g. CyFun®), conformance to known standards, verifications (e.g. CyFun®), certifications (e.g. CyFun®), or inspections.
- Keep in mind that GDPR requirements must be met if business information contains personal data (applicable at all levels), i.e. safeguards should be included in the contractual framework.

GV.SC-07 The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritised, assessed, responded to, and monitored over the course of the relationship

GV.SC-07.1 The risks posed by a supplier, its products and services and other third parties shall be identified, documented, prioritised, mitigated and assessed at least annually and when changes occur during the relationship.

Implementation guidance

The goal of this control is to ensure that risks related to suppliers, their products and services, and other third parties are continuously identified, assessed, prioritised, and managed throughout the relationship, especially when changes occur in critical systems.

To achieve this goal:
- **Tailored Risk Assessments**
  Assessment formats and frequencies should be adapted based on the supplier's reputation and the criticality of the products or services provided, including OT components.
- **Broader Risk Considerations**
  Risk evaluations should include potential service disruptions and concentration risks that could impact operations or OT environments.
- **Evidence of Compliance**
  Suppliers should provide evidence of compliance with contractual cybersecurity requirements, such as self-assessments (e.g. CyFun®), certifications, warranties, test results, labels, or third-party audit reports.
- **Ongoing Monitoring**
  Critical suppliers should be monitored throughout the relationship using inspections, audits, tests, or other evaluation methods to ensure security obligations remain fulfilled.
- **Risk Profile Updates**
  Changes in supplier services, products, or performance should trigger a reassessment of their risk profile and criticality, especially when OT systems are involved.
- **Business Continuity Planning**
  An action plan should be in place to address unexpected supplier disruptions and maintain operational continuity.

GV.SC-08   **Relevant suppliers and other third parties are included in incident planning, response, and recovery activities**

GV.SC-08.1	**The organisation shall identify and document key personnel from relevant suppliers and other third parties to include them in incident planning, response, and recovery activities.**

Implementation guidance

The goal of this control is to strengthen incident preparedness and recovery by ensuring that key personnel from critical suppliers and third parties are identified and actively integrated into response planning and execution.

To achieve this goal:
- **Establish Communication Protocols**
  Clear rules and procedures should be defined for reporting incident status and coordinating response and recovery activities between the organisation and its business-critical suppliers.
- **Define Roles and Responsibilities**
  Roles, responsibilities, and authority for incident response should be documented for both internal teams and third-party participants, including those supporting OT systems and infrastructure.
- **Promote Joint Learning**
  Collaborative lessons-learned sessions should be conducted with critical suppliers and third parties following major incidents to improve future coordination and resilience.

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-01.2** The inventory of enterprise assets associated with information and information processing facilities shall reflect changes in the organisation's context and include all information necessary for effective accountability.

Implementation guidance

The goal of this control is to ensure that asset inventories support operational transparency, enable responsible ownership, and adapt to changes in the organisation's structure, technology, and risk landscape.

To achieve this goal:
- **Include Essential Asset Details**
  Inventories should capture key specifications such as manufacturer, device type, model, serial number, machine name, network address, and physical location. OT assets should be included where applicable.
- **Support Accountability**
  Asset records should enable traceability of actions and decisions, ensuring that responsible parties can be identified and held answerable for outcomes.
- **Reflect Organisational Changes**
  Inventories should be updated to reflect changes such as asset relocation, upgrades, or decommissioning, including those affecting OT environments.

> **ID.AM-01.3** When unauthorised hardware is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.

Implementation guidance

The goal of this control is to reduce security risks by ensuring that Unauthorised hardware is promptly identified, isolated, and addressed, while maintaining an accurate and accountable asset inventory.

To make this happen:
- **Define Unauthorised hardware**
  Any hardware not approved or lacking documented exceptions should be designated as Unauthorised.
- **Respond to Detection**
  Unauthorised hardware should be quarantined for review, removed, or replaced as appropriate. The asset inventory should be updated accordingly.
- **Include OT Considerations**
  Unauthorised devices in OT environments should be treated with heightened caution due to potential safety and operational impacts.

Examples of unauthorised hardware may include:
- **Unapproved Endpoints**
  Personal or unregistered laptops, desktops, or mobile devices connected to the network without Authorisation.
- **External Storage Devices**
  USB drives or external hard disks not approved for use, which may introduce malware or data leakage risks.
- **Unvetted IoT and OT Devices**
  Smart devices, sensors, or industrial components connected without proper vetting, posing risks to both IT and OT environments.
- **Unauthorised Network Equipment**
  Wireless access points or switches installed without approval, potentially bypassing network security controls.

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-02.2 The inventory reflecting which software, services and systems are used in the organisation shall reflect changes in the organisation's context and include all information necessary for effective accountability.

Implementation guidance

The goal of this control is to ensure that inventories of software, services, and systems remain current and complete, enabling traceability, responsible ownership, and alignment with changes in the organisation's operational and risk context.

To achieve this goal:
- **Include Key Inventory Details**
  Inventories should capture relevant attributes such as software title, publisher, initial install or use date, business purpose, version, deployment method, and decommission date. URLs or app store sources should be included where applicable.
- **Support Accountability**
  Inventory records should enable traceability of actions and decisions, ensuring that responsible roles can be identified and held answerable for the use and management of software and services.
- **Reflect Organisational Changes**
  Inventories should be updated to reflect changes such as new deployments, upgrades, or removals, including those affecting OT systems and embedded software components.

ID.AM-02.3 The people responsible and accountable for managing software platforms and applications within the organisation shall be formally identified.

Implementation guidance

The goal of this control is to ensure that software platforms and applications are properly managed, by clearly identifying who is responsible for day-to-day operations and who is accountable for overall oversight and outcomes.

To achieve this goal:
- **Define Roles Clearly**
  Individuals responsible for managing software should be formally designated. These are the people who perform the work, make technical decisions, and carry out operational tasks (e.g. developers, system administrators, testers).
- **Assign Accountability**
  A separate role should be formally assigned to oversee and approve the successful completion of software-related tasks. This may include project managers, product owners, or team leads.
- **Apply to All Environments**
  These roles should be defined for both IT and OT environments, ensuring that software used in industrial systems is also properly governed.

ID.AM-02.4 When unauthorised software is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.

Implementation guidance

The goal of this control is to minimise security, operational, and compliance risks by ensuring that unauthorised software is promptly identified, handled appropriately, and reflected in the organisation's software inventory.

To make this happen:
- **Define Unauthorised Software**
  Software installed or used without proper licensing, approval, or documented exceptions should be classified as unauthorised.
- **Understand the Risks**
  Unauthorised software may introduce:
  - **Security vulnerabilities** (e.g. malware or backdoors)
  - **Data protection risks** (e.g. unapproved data handling)
  - **Operational inefficiencies** (e.g. compatibility issues)
  - **Loss of control** over software usage and updates
- **Establish Response Procedures**
  Unauthorised software should be quarantined for possible exception handling, removed, or replaced. The software inventory should be updated accordingly.
- **Support with Centralised Management**
  A centralised software management process should be in place to oversee vendor selection, legacy software, and security controls.
- **Use SBOMs Where Applicable**
  Software Bills of Materials (SBOMs) should be used to track components, libraries, and modules, supporting licence compliance and vulnerability management, especially in OT and embedded systems.

ID.AM-03 **Representations of the organisation's authorised network communication and internal and external network data flows are maintained**

ID.AM-03-2 The organisation's network communication and internal data flows shall be mapped, documented, authorised, and updated when changes occur.

Implementation guidance

The goal of this control is to ensure that internal network communications and data flows are clearly understood, properly documented, and kept up to date to support secure operations and informed decision-making across ICT and OT environments.

To achieve this goal:
- **Establish Network Baselines**
  Communication and data flows across wired, wireless, and cloud-based infrastructure (e.g. IaaS) should be mapped, documented, and authorised. Updates should be made when changes occur.
- **Document Technical Details**
  Expected network ports, protocols, and services used between authorised systems should be recorded to support monitoring and troubleshooting.
- **Integrate with Configuration Management**
  Configuration management processes should support the maintenance and validation of network flow documentation.
- **Ensure Resilient Documentation**
  Network flow documentation should be stored securely and not solely on the network it describes. A protected offline copy (e.g. encrypted external drive or hardcopy) should be maintained to ensure availability during outages or incidents.

ID.AM-04 Inventories of services provided by suppliers are maintained

ID.AM-04.1 Organisations shall keep a clear and up-to-date list of all external services it uses, including how they connect to their systems. These services shall be reviewed and approved before use, and the list shall be updated whenever changes happen.

Implementation guidance

The goal of this control is to ensure that all external services used by the organisation are clearly identified, reviewed, and kept up to date to reduce the risk of unauthorised access, unmanaged third-party dependencies, or service disruption across ICT and OT environments.

To achieve this goal:
- **Maintain an Inventory of External Services**
  All external services relied upon by the organisation should be identified and documented. This includes services used in both IT and OT environments. The inventory should be updated whenever services are added, changed, or removed.
- **Describe and Map Service Connections**
  The way each external service connects to internal systems should be clearly described and recorded. This includes remote access tools, cloud-based SCADA platforms, and vendor-managed OT systems.
- **Review and Approve Services Before Use**
  External services should be reviewed and approved before being used. This process should verify that the service aligns with internal security, compliance, and operational requirements.
- **Categorise and Classify Services**
  External services should be categorised by type (e.g. IaaS, SaaS, APIs) and classified based on their criticality and data sensitivity. This helps prioritise oversight and risk management efforts.
- **Integrate with Risk and Change Management**
  The inventory should be integrated into broader risk and change management processes. Any changes to external services should trigger a review of associated risks and required controls.

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-07.2 Inventories of data and associated metadata shall be maintained for designated data types.

Implementation guidance

The goal of this control is to ensure that inventories of data and their associated metadata are maintained for all data types explicitly selected or designated by policy or guidelines (for example, customer data, financial information, or production data). This supports secure data management, regulatory compliance, and operational integrity across ICT and OT environments.

To achieve this goal:
- **Define a Data Classification Scheme**
  A classification scheme should be established to categorise data types based on sensitivity and usage. This scheme should guide how data is handled, protected, and retained.
- **Apply Security Measures by Classification Level**
  Appropriate security controls should be implemented for each classification level. These may include encryption, role-based access controls, and tailored data retention policies.
- **Identify and Protect Sensitive Data Types**
  Inventories should include sensitive data such as:
  - Personally identifiable information (PII)
  - Financial and health information
  - Confidential business data
  - Intellectual property
  - Government and personnel records
    OT environments should also include operational data critical to safety and reliability.
- **Track Metadata for Each Data Instance**
  Metadata should be maintained to support data governance. This includes:
  - Descriptive metadata (e.g. title, author, keywords)
  - Structural metadata (e.g. format, schema)
  - Administrative metadata (e.g. access rights, retention policy)
  - Technical metadata (e.g. encoding, checksum)
- **Monitor Data Provenance and Location**
  The origin, ownership, and geolocation of each data instance should be documented. This helps to understand where and how data is stored and processed, especially in distributed or OT systems.
- **Continuously Discover and Analyse Ad Hoc Data**
  Processes should be in place to identify new instances of sensitive data not captured by initial inventories. This helps address gaps in data flow mapping and supports ongoing data protection.
- **Consider Using the Traffic Light Protocol (TLP)**
  TLP should be considered as a method to classify and share cybersecurity-related data, especially in incident response and threat intelligence contexts.

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.

ID.AM-08.3 The organisation shall enforce accountability for all its business-critical assets throughout the system lifecycle, including removal, transfers, and disposition.

Implementation guidance

The goal of this control is to ensure accountability for all business-critical assets throughout their lifecycle, including deployment, movement, and disposal, to reduce the risk of unauthorised access, data leakage, or operational disruption across ICT and OT environments.

To achieve this goal:
- **Secure Assets Before Deployment**
  Systems, hardware, software, and services should be properly configured and secured before being introduced into production environments.
- **Identify and Remove Redundant Assets**
  Redundant or unused systems, software, and services that increase the attack surface should be periodically identified and removed.
- **Monitor and Document Asset Movements**
  Movements of business-critical assets should be tracked, and documentation should be maintained to ensure traceability and accountability.
- **Authorise Asset Transfers**
  Business-critical assets should only be allowed to enter or leave facilities with proper Authorisation, especially in OT environments where physical asset control is critical.
- **Dispose of Assets Securely**
  Disposal of business-critical assets should be conducted in a secure, responsible, and auditable manner to prevent data leakage or unauthorised reuse.
- **Update Inventories Promptly**
  Asset inventories should be updated whenever systems, hardware, software, or services are moved, transferred, removed, or decommissioned.

ID.AM-08.4 The organisation shall ensure that the necessary measures are taken to deal with loss, misuse, damage, or theft of assets.

Implementation guidance

The goal of this control is to ensure that appropriate measures are in place to prevent and respond to the loss, misuse, damage, or theft of assets, in order to protect business operations and reduce security risks across ICT and OT environments.

To achieve this goal:
- **Apply Physical Security Measures**
  Physical protections such as locks, surveillance cameras, and alarms should be used to secure facilities and critical assets, including those in OT environments.
- **Implement Technical Safeguards**
  Technical controls such as encryption, secure data erasure, and regular backups should be applied to protect data and systems from unauthorised access or loss.
- **Establish Organisational Controls**
  Policies, procedures, and user agreements should be in place to define responsibilities and expectations. Mobile Device Management (MDM) and other administrative tools should be used to manage asset usage.

- Conduct Regular Audits and Inventory Checks
  Periodic audits and asset inventories should be performed to verify that all assets are accounted for and properly managed.
- Restrict Access to Sensitive Assets
  Access to critical systems, data, and physical areas should be limited to authorised personnel only, especially in environments where operational continuity is essential.
- Provide Employee Awareness and Training
  Staff should be trained on asset protection practices and encouraged to report suspicious activity or incidents involving asset misuse or loss.
- Maintain Appropriate Insurance Coverage
  Insurance policies should be in place to help mitigate financial losses resulting from asset theft, damage, or other incidents.

> **ID.AM-08.6** **The organisation shall plan, perform and document preventive maintenance and repairs on its critical system components according to approved processes and tools.**

Implementation guidance

The goal of this control is to ensure that preventive maintenance and repairs on critical system components are planned, performed, and documented in a secure and consistent manner to maintain system reliability and reduce operational risks across ICT and OT environments.

To achieve this goal:
- Document Maintenance Procedures
  Maintenance policies and procedures should be clearly defined and included in the organisation's cybersecurity and operational plans. Oversight of these procedures should be part of management responsibilities.
- Authorise Maintenance Personnel
  A process should be established to authorise individuals or external providers who perform maintenance. A list of approved personnel or organisations should be maintained and reviewed regularly.
- Schedule and Record Maintenance Activities
  Preventive maintenance and repairs should be scheduled, performed, and documented according to organisational requirements and vendor specifications. Records should be reviewed to ensure completeness and accuracy.
- Monitor All Maintenance Activities
  All maintenance, whether performed on-site or remotely, should be approved in advance and monitored during execution. This includes servicing of components removed from the facility.
- Ensure Safe and Reliable OT Maintenance
  Maintenance of OT systems should be planned and carried out in a way that keeps operations safe, avoids unnecessary downtime, and follows any specific instructions or requirements from equipment vendors.

ID.AM-08.8   **The organisation shall pre-approve, monitor and enforce maintenance tools for use on its critical systems.**

Implementation guidance

The goal of this control is to ensure that maintenance tools used on critical systems are pre-approved, monitored, and enforced to protect system integrity, safety, and operational continuity. In OT environments, improper tool use can interfere with physical processes, making control over tool approval and usage essential for operational safety and reliability.

To achieve this goal, the organisation should:
- **Identify Critical Systems**
  Systems that impact safety, quality, regulatory compliance, or operational throughput should be classified as critical. Metrics such as Mean Time to Repair (MTTR) and Mean Time Between Failures (MTBF) should support this classification.
- **Pre-Approve Tools**
  Only maintenance tools that have been reviewed and approved should be allowed for use on critical systems. This includes both hardware and software tools such as diagnostic devices, packet sniffers, and laptops.
- **Monitor Usage**
  The use of maintenance tools on critical systems should be actively monitored to detect unauthorised or unsafe activity.
- **Enforce Controls**
  Policies and technical controls should be in place to prevent the use of unapproved tools and to ensure conformance with internal procedures and compliance with applicable laws and regulations.

ID.AM-08.11   **Remote maintenance and diagnostic activities of organisational assets shall be pre-approved and the performance logged.**

Implementation guidance

The goal of this control is to ensure that remote maintenance and diagnostic activities are authorised, traceable, and secure. In OT environments, remote maintenance must be tightly controlled, as unauthorised changes can directly affect the safety and stability of physical systems.

To achieve this goal, the organisation should:
- **Pre-Approve Activities**
  All remote maintenance and diagnostic activities should be reviewed and approved before execution.
- **Log Performance**
  Each remote session should be logged in detail, including time, duration, personnel involved, and actions taken.
- **Establish Logging Procedures**
  Logging and monitoring procedures should be documented, approved, communicated, applied, and regularly reviewed, ideally on an annual basis.
- **Prevent Unauthorised Changes**
  Technical and procedural measures should be implemented to detect or prevent unauthorised changes to systems, configurations, applications, or infrastructure during remote access.
- **Ensure Conformance and Compliance**
  All activities should conform to internal policies and comply with applicable laws, regulations, and industry standards.

ID.AM-08.12 Setting up non-local maintenance and diagnostic sessions over remote network connections shall require strong authenticators and such connections shall be terminated when non-local maintenance is completed.

Implementation guidance

The goal of this control is to ensure that non-local maintenance and diagnostic sessions are securely established and properly terminated to prevent unauthorised access or lingering connections. In OT environments, secure session setup and termination are essential to prevent persistent access paths that could be exploited to disrupt physical operations.

To achieve this goal, the organisation should:
- **Use Strong Authentication**
  Remote sessions should be protected by strong authenticators that resist replay attacks. Multi-factor authentication should be used where possible.
- **Protect Communications**
  Cryptographic mechanisms should be implemented to ensure the confidentiality and integrity of remote maintenance communications.
- **Terminate Sessions**
  Remote connections should be terminated immediately after maintenance is completed to reduce exposure to potential threats.
- **Verify Disconnection**
  Remote disconnect verification should be used to confirm that sessions have been fully closed and are no longer accessible.
- **Ensure Conformance and Compliance**
  All remote access activities should conform to internal security procedures and comply with applicable laws, regulations, and industry standards.

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

ID.RA-01.2   A process shall be established to continuously monitor, identify, and document vulnerabilities of the organisation's business critical systems.

Implementation guidance

The goal of this control is to ensure that vulnerabilities in business-critical systems are continuously identified, monitored, and documented to support timely risk mitigation and maintain operational resilience.

To achieve this goal, the organisation should:
- **Use Vulnerability Scanning Where Safe**
  Vulnerability scanning should be applied to IT and OT systems where it does not disrupt operations or compromise safety. Passive or non-intrusive methods should be preferred in OT environments.
- **Deploy Vulnerability Management Tools**
  Tools should be used to detect unpatched software, misconfigurations, and outdated firmware across both IT and OT assets.
- **Assess Architectures for Weaknesses**
  Network and system architectures, including segmentation, remote access paths, and legacy components, should be reviewed for design flaws that could expose OT systems to cyber threats.
- **Monitor Threat Intelligence Sources**
  Public and private sources of cyber threat intelligence should be monitored for vulnerabilities affecting OT products, industrial control systems (ICS), and vendor-specific technologies.
- **Review Organisation-Developed Software**
  Custom applications, including those used in OT environments (e.g. HMIs, PLC logic), should be analysed and tested for insecure coding practices and default configurations.
- **Evaluate Operational Procedures**
  Processes and procedures, especially those involving remote access, maintenance, and emergency operations, should be reviewed for exploitable weaknesses that could impact OT system integrity.

> **ID.RA-01.3** **The organisation shall establish and maintain a documented process that enables continuous review, analysis and remediation of vulnerabilities and provides for information sharing where applicable.**

Implementation guidance

The goal of this control is to ensure that vulnerabilities are continuously reviewed, analysed, and remediated through a documented process that also supports information sharing where applicable.

To achieve this goal, the organisation should:
- **Incorporate Lessons Learned and Emerging Threats**
  The process should be updated based on incidents, changes in technology, and evolving threats, including those targeting OT systems and industrial protocols.
- **Use Internal Feedback and Metrics**
  Audit results, performance indicators, and operator feedback should be used to refine the vulnerability management process, especially where manual processes are common.
- **Leverage Software Bills of Materials (SBOMs)**
  SBOMs should be used to identify vulnerable components in both IT and OT software stacks, including embedded systems and firmware.
- **Monitor Threat Intelligence Sources**
  Trusted sources such as vendor advisories, ICS-CERT, and ENISA should be monitored for vulnerabilities affecting OT products, control systems, and field devices.
- **Review Processes and Procedures**
  Operational procedures, especially those involving remote access, maintenance, and safety-critical functions, should be reviewed for exploitable weaknesses.
- **Coordinate with Engineering and Operations**
  Remediation efforts should be planned in coordination with OT and engineering teams to avoid unplanned downtime or safety risks.

ID.RA-01.5   Vulnerability scanning shall not adversely impact system functions.

Implementation guidance

The goal of this control is to ensure that vulnerability scanning does not disrupt or degrade the performance of business-critical systems, particularly in Operational Technology (OT) environments where system stability and availability are critical.

To achieve this goal, the organisation should:
- **Schedule Scans During Low-Usage Periods**
  Scans should be performed during off-peak hours or planned maintenance windows to minimise operational impact.
- **Use Non-Intrusive Scanning Tools**
  Tools should be selected based on their ability to scan without overloading system resources or interfering with real-time operations.
- **Test in Staging Environments First**
  Scans should be trialled in non-production environments to identify potential issues before deployment in live systems.
- **Apply Incremental Scanning**
  Scanning should be broken down into smaller, manageable segments to reduce system load and avoid overwhelming critical components.
- **Monitor System Performance During Scans**
  System behaviour should be actively monitored during scanning to detect and respond to any performance degradation or anomalies.

Distinction from ID.RA-01.4 (CyFun® Essential)

While ID.RA-01.4 focuses on testing activities such as penetration and load testing, which are typically planned, infrequent, and often conducted in controlled environments, ID.RA-01.5 addresses the safe execution of vulnerability scanning, which is more frequent, often automated, and must be carefully managed to avoid unintended disruptions in live OT systems.

ID.RA-01.6   Vulnerabilities shall be identified and managed in all relevant assets, including software, network and system architectures, and facilities.

Implementation guidance

The goal of this control is to ensure that vulnerabilities are systematically identified and managed across all relevant assets, including software, network and system architectures, and physical facilities. This builds on control ID.RA-01.1, which focuses on identifying both threats and vulnerabilities to support risk reduction.

To achieve this goal, the organisation should:
- **Extend the Scope of Vulnerability Management**
  Vulnerability identification and remediation should cover all relevant assets, including IT and OT systems, applications, network designs, and facilities that support critical operations.
- **Maintain a Dedicated Vulnerability Management Process**
  A structured process should be in place to continuously track, assess, and mitigate vulnerabilities, distinct from threat intelligence activities.

- Differentiate Between Threat Intelligence and Vulnerability Management
  Separate processes or evidence should be maintained to distinguish between identifying external threats (e.g. threat actors, campaigns) and managing internal weaknesses (e.g. unpatched systems, misconfigurations).
- Integrate with Broader Risk Management
  The vulnerability management process should align with the organisation's overall risk management framework and support timely decision-making.
- Ensure OT-Specific Considerations
  In OT environments, vulnerability management should account for legacy systems, vendor dependencies, and operational constraints that may limit patching or scanning options.

ID.RA-02   Cyber threat intelligence is received from information sharing forums and sources

ID.RA-02.1	**A threat and vulnerability awareness program that includes a cross-organisation information-sharing capability shall be implemented.**

Implementation guidance

The goal of this control is to strengthen the organisation's ability to anticipate and respond to cyber threats by implementing a threat and vulnerability awareness program that includes cross-organisational information sharing.

To achieve this goal, the organisation should:
- Monitor Threat Actor Tactics and Emerging Vulnerabilities
  Cyber threat intelligence should include up-to-date information on threat actors, their tactics, techniques, and procedures (TTPs), as well as vulnerabilities in emerging technologies (e.g. AI-enabled attacks, data poisoning in machine learning).
- Establish Ongoing External Engagement
  The organisation should maintain active participation in security groups, forums, and professional associations to receive alerts, advisories, and peer insights relevant to both IT and OT environments.
- Enable Information Sharing
  The program should support the sharing of unclassified and, where appropriate, classified information about vulnerabilities and incidents across departments and with trusted external partners.
- Support OT-Specific Awareness
  Threat intelligence should include OT-specific sources (e.g. ICS-CERT, vendor advisories) to address vulnerabilities in industrial control systems, legacy devices, and sector-specific technologies.
- Differentiate Threat Intelligence from Vulnerability Management
  The awareness program should complement, but remain distinct from, vulnerability management processes by focusing on external threat developments and strategic insights.

ID.RA-03 — Internal and external threats to the organisation are identified and recorded

ID.RA-03.1 Threats shall be identified and assessed in relation to all relevant assets, including software, network and system architectures, and facilities.

Implementation guidance

The goal of this control is to ensure that threats are systematically identified and assessed in relation to all relevant assets, including software, network and system architectures, and facilities. This builds on ID.RA-01.1, which establishes the foundation for identifying both threats and vulnerabilities across critical assets.

To achieve this goal, the organisation should:

- **Extend Threat Identification Across All Assets**
  Threats should be assessed in relation to all relevant assets, including IT and OT systems, applications, network designs, and physical facilities that support critical operations.
- **Maintain a Dedicated Threat Intelligence Process**
  A structured process should be in place to gather, analyse, and assess threat intelligence from internal and external sources, including sector-specific advisories and OT-focused threat feeds.
- **Differentiate Threat Intelligence from Vulnerability Management**
  Threat intelligence should be managed separately from vulnerability management, with distinct processes and evidence to ensure clarity and focus. Threats refer to potential actors or events, while vulnerabilities refer to weaknesses that could be exploited.
- **Integrate with Risk Analysis**
  Identified threats should be linked to known vulnerabilities and recorded in a central risk register to support prioritisation and mitigation planning, as outlined in ID.RA-01.1.
- **Include OT-Specific Threats**
  Threat assessments should consider OT-specific risks such as supply chain compromise, unauthorised remote access, and exploitation of legacy systems or proprietary protocols.

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.

ID.RA-05.2   The organisation shall conduct and document risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and likelihood of their occurrence.

Implementation guidance

The goal of this control is to ensure that risk assessments are conducted and documented using a structured approach that considers threats, vulnerabilities, business impact, and likelihood. This supports informed decision-making and prioritisation of cybersecurity efforts across both IT and OT environments.

To achieve this goal, the organisation should:
- **Include Internal and External Threats**
  Risk assessments should consider threats originating from within the organisation as well as from external actors.
- **Apply Recognised Risk Analysis Methods**
  Qualitative and/or quantitative methods — such as the MAPGOOD model, ISO/IEC 27005, or the CIS Risk Assessment Method — should be used. These methods may be supported by risk management software tools.
- **Prioritise Based on Likelihood and Impact**
  Cybersecurity resources and investments should be allocated based on the estimated likelihood of threats and the potential impact on business processes and critical assets.
- **Ensure OT-Specific Risk Considerations**
  Risk assessments should account for OT-specific factors such as safety implications, system availability, legacy technologies, and operational constraints.

ID.RA-06   Risk responses are chosen, prioritised, planned, tracked, and communicated

ID.RA-06.1   Risk responses shall be identified, prioritised, planned, tracked and communicated.

Implementation guidance

The goal of this control is to ensure that risk responses are clearly identified, prioritised, planned, tracked, and communicated to support effective risk mitigation and informed decision-making across the organisation.

To achieve this goal, the organisation should:

- **Apply Risk Response Criteria**
  Decisions to accept, transfer, mitigate, or avoid risk should follow the organisation's vulnerability management criteria, as referenced in ID.RA-08.1.
- **Select Compensating Controls Thoughtfully**
  Where direct mitigation is not feasible, compensating controls should be selected based on the same criteria to ensure consistent risk reduction.
- **Base Actions on Risk Assessment Findings**
  All risk response decisions should be grounded in the results of documented risk assessments, ensuring alignment with actual threats, vulnerabilities, and business impact.
- **Track Implementation Progress**
  Risk response actions should be tracked using structured tools such as a risk register, plan of action and milestones, or risk detail reports.
- **Communicate in Priority Order**
  Planned risk responses should be communicated to affected stakeholders in order of priority, ensuring timely awareness and coordination.
- **Include OT-Specific Considerations**
  Risk responses in OT environments should account for operational constraints, safety requirements, and system availability, especially when planning mitigation or compensating controls.

ID.RA-08   Processes for receiving, analysing, and responding to vulnerability disclosures are established

ID.RA-08.1   The organisation shall establish and implement a vulnerability management plan to identify, analyse, assess, mitigate and communicate all types of vulnerabilities including in the form of a Coordinated Vulnerability Disclosure (CVD) according to applicable legal modalities.

Implementation guidance

The goal of this control is to ensure that all types of vulnerabilities are systematically identified, analysed, assessed, mitigated, and communicated through a documented vulnerability management plan. This includes handling disclosures in line with Coordinated Vulnerability Disclosure (CVD) practices and applicable legal requirements.

To achieve this goal, the organisation should:
- **Establish a Comprehensive Vulnerability Management Plan**
  The plan should cover vulnerabilities from internal testing, external sources such as security bulletins, and disclosures from researchers, vendors, partners, or government cybersecurity bodies.
- **Assign Responsibilities and Monitor Implementation**
  Clear roles should be defined for processing, analysing, and responding to disclosed vulnerabilities. Implementation of procedures should be monitored to ensure timely and effective handling.
- **Support Coordinated Vulnerability Disclosure (CVD)**
  The plan should include procedures for receiving and responding to vulnerability reports from external parties. CVD practices should align with guidance provided by ENISA's CVD framework, which outlines legal, technical, and communication considerations.
- **Ensure OT-Specific Coverage**
  The plan should address vulnerabilities in OT environments, including legacy systems, vendor-managed components, and embedded firmware, where patching or mitigation may require coordination with engineering teams.

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

ID.IM-02 **Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties**

ID.IM-02.1 Security tests and exercises, including those conducted with suppliers and relevant third parties, shall be used to identify areas for improvement.

Implementation guidance

The goal of this control is to identify opportunities for improving security, incident response, and resilience by conducting security tests and exercises — internally and in collaboration with suppliers and third parties. In Operational Technology (OT) environments, these activities are essential to ensure preparedness for incidents that could impact physical operations, safety, or service continuity.

To achieve this goal, the organisation should:
· **Assess Incident Response Readiness**
   Security tests such as tabletop exercises, simulations, internal reviews, and audits should be used to identify improvements in incident response procedures.
· **Coordinate with External Parties**
   Exercises involving critical service providers and product suppliers should be conducted to strengthen business continuity, disaster recovery, and incident response capabilities.
· **Engage Internal Stakeholders**
   Relevant internal roles, including senior executives, legal, and HR, should be involved in exercises to ensure broad organisational awareness and alignment.
· **Conduct Penetration Testing**
   High-risk systems should undergo penetration testing to identify vulnerabilities. These tests should be pre-approved by leadership.
· **Test Contingency Plans**
   Plans for responding to unauthorised or tampered products or services should be tested and refined to ensure effective recovery.
· **Ensure Conformance and Compliance**
   All testing activities should conform to internal procedures and comply with applicable laws, regulations, and industry standards.

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.

ID.IM-03.2 The organisation shall incorporate lessons learned from incident handling activities into updated or new incident handling processes and/or procedures that are framed by appropriate training after review, approval and testing.

Implementation guidance

The goal of this control is to improve the organisation's incident handling capabilities by incorporating lessons learned from past incidents into updated or new processes and procedures. In Operational Technology (OT) environments, where incidents can directly affect physical systems and operational continuity, applying real-world insights helps strengthen response effectiveness and reduce the likelihood of repeated failures.

To achieve this goal, the organisation should:
- **Cover the Full Incident Lifecycle**
  Lessons should be drawn from all phases of incident handling, including identification, categorisation, prioritisation, investigation, resolution, recovery, closure, and post-incident review.
- **Demonstrate Process Optimisation**
  Updates to incident handling procedures should reflect insights gained from previous incidents and be clearly documented.
- **Collaborate with Suppliers**
  Lessons learned sessions should be conducted jointly with key suppliers to improve coordination and response across the supply chain.
- **Use Performance Metrics**
  Metrics should be used to track and assess the effectiveness of incident handling over time and guide improvements.
- **Ensure Conformance and Compliance**
  All updates to processes and procedures should conform to internal governance requirements and comply with applicable laws, regulations, and industry standards.

ID.IM-03.3 The organisation shall identify improvements derived from the monitoring, measurements, assessments, and lessons learned and consequently translate this into improved processes / procedures / technologies to enhance its cyber resilience (continuous improvement).

Implementation guidance

The goal of this control is to enhance the organisation's cyber resilience by identifying improvements from monitoring, measurements, assessments, and lessons learned, and translating them into updated processes, procedures, or technologies. In Operational Technology (OT) environments, where system reliability and safety are tightly linked to cyber performance, continuous improvement helps maintain operational integrity and adapt to evolving threats.

To achieve this goal, the organisation should:
- **Use Cyber Resilience Metrics**
  Metrics should be used to assess the organisation's ability to withstand and recover from cyber incidents, supporting informed risk management and decision-making.
- **Apply Measures of Effectiveness (MOEs)**
  MOEs should be used to evaluate and compare the effectiveness of different cyber resilience strategies and guide investment or design decisions.

- Implement Objective-Driven Metrics
  Metrics should cover preparedness, operational continuity during attacks, damage limitation, and recovery and restoration capabilities.
- Conduct Independent Assessments
  Independent teams should be engaged to perform assessments and provide objective insights into areas for improvement.
- Use Structured Scoring Systems
  Scoring methodologies such as MITRE's SSM-CR (Situated Scoring Methodology for Cyber Resiliency) should be considered to support structured evaluation and prioritisation of improvements.
- Ensure Conformance and Compliance
  All improvements should align with internal governance requirements and comply with applicable laws, regulations, and industry standards.

ID.IM-03.4 **The organisation shall collaborate and share information about its critical system's related security incidents and mitigation measures with designated partners.**

Implementation guidance

The goal of this control is to strengthen cyber resilience by sharing information about security incidents and mitigation measures related to critical systems with designated partners. In Operational Technology (OT) environments, timely and coordinated information exchange helps prevent the spread of threats, supports faster recovery, and enhances collective defence across interconnected systems.

To achieve this goal, the organisation should:
- Define Roles and Authorities
  The incident response plan should clearly outline roles, responsibilities, and authorisation for sharing incident-related information with designated partners.
- Train the Response Team
  Incident response personnel should be regularly trained on procedures for communicating with external partners during and after incidents.
- Coordinate with Partners
  Information sharing should include details on incidents, mitigation actions, and lessons learned, especially with suppliers and service providers involved in critical system operations.
- Reference Trusted Guidance
  Relevant practices should be informed by trusted sources such as *ENISA/CERT-EU Security Guidance 22-001*, which provides recommended mitigation measures against critical threats.
- Ensure Conformance and Compliance
  All collaboration and sharing activities should conform to internal policies and comply with applicable laws, regulations, and industry standards.

ID.IM-03.5 Communication of effectiveness of protection technologies shall be shared with relevant stakeholders.

Implementation guidance

The goal of this control is to ensure that the effectiveness of protection technologies is clearly communicated to relevant stakeholders. In Operational Technology (OT) environments, where protection tools safeguard critical physical systems, meaningful communication supports informed decisions, risk awareness, and alignment across technical and non-technical teams.

To achieve this goal, the organisation should:
- **Tailor Communication to Stakeholders**
  Information should be adapted to the needs of different audiences; Technical teams may require detailed logs, while executives may need high-level summaries linked to business risk.
- **Go Beyond Technical Metrics**
  Communication should include not only data (e.g. threats blocked, incidents detected) but also insights into risk posture, emerging trends, and recommended actions.
- **Include All Relevant Roles**
  Stakeholders such as CISOs, IT security teams, compliance officers, internal auditors, and executive leadership should receive the information necessary to support their responsibilities.
- **Monitor and Report Performance**
  The performance of protection technologies (e.g. antivirus, firewalls, intrusion prevention, endpoint detection, data loss prevention) should be continuously monitored and reported.
- **Support Continuous Improvement**
  Communication should help identify gaps, inform strategic decisions, and promote a culture of transparency and resilience.
- **Ensure Conformance and Compliance**
  All communication practices should align with internal policies and comply with applicable laws, regulations, and industry standards.

ID.IM-03.6 The organisation shall implement, where feasible, automated mechanisms to facilitate the process of information sharing and collaboration.

Implementation guidance

The goal of this control is to improve the efficiency, accuracy, and security of information sharing and collaboration by implementing automated mechanisms where feasible. In Operational Technology (OT) environments, automation helps reduce manual errors, enforce access controls, and support timely decision-making across interconnected systems.

To achieve this goal, the organisation should:
- **Match Access Authorisations**
  Automated tools should verify that the access rights of information-sharing partners align with the sensitivity of the information. Mismatches should be flagged before sharing occurs.
- **Automate Policy Enforcement**
  Systems should automatically evaluate whether information can be shared based on its classification and the recipient's access rights. These checks should be integrated with identity and access management (IAM) systems to ensure up-to-date authorisation data.
- **Control Search and Retrieval**
  Search and retrieval tools should enforce access restrictions using metadata tagging and classification, ensuring users can only access authorised information.

- **Monitor and Audit Activities**
  Automated logging and monitoring should track all information-sharing actions. Logs should be reviewed regularly to detect unauthorised access or policy violations.
- **Promote Usability and Training**
  Automated tools should be user-friendly to encourage correct usage. Training should be provided to ensure users understand how to use these tools effectively and responsibly.
- **Ensure Conformance and Compliance**
  All automated mechanisms should align with internal policies and comply with applicable laws, regulations, and industry standards.

ID.IM-04 Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved

ID.IM-04.1 Contingency and continuity plans shall be established, communicated, maintained, tested, validated, and improved.

Implementation guidance

The goal of this control is to ensure organisational resilience by establishing, maintaining, and improving contingency and continuity plans that enable effective response and recovery from disruptions.

To achieve this goal, the organisation should:
- **Establish Comprehensive Plans**
  Plans should include:
  - **Incident Response Plan (IRP)**
  - **Business Continuity Plan (BCP)**
  - **Disaster Recovery Plan (DRP)**
    These should address operational disruptions, data breaches, and mission-critical failures.
- **Define Clear Plan Content**
  Plans should include:
  - Contact and communication details
  - Roles, responsibilities, and authorities (aligned with GV.RR-02.1)
  - Procedures for common scenarios
  - Criteria for prioritisation, escalation, and decision-making
    IRPs should cover detection, containment, response, and recovery from cyber incidents.
- **Communicate and Train**
  Plans should be communicated to all relevant personnel. A Crisis Management Team should be established with representatives from key departments (e.g. IT, legal, HR, PR) and trained to act during crises.
- **Maintain and Review Plans**
  Plans should be reviewed at least annually or after major changes or incidents. Updates should reflect lessons learned and evolving risks.
- **Test and Validate Regularly**
  Plans should be tested through realistic scenarios. Validation should confirm that procedures work as intended and meet operational needs. Results should be documented.
- **Continuously Improve**
  Feedback from tests, incidents, and reviews should drive improvements. Enhancements should be prioritised based on risk and impact to ensure continuity of essential functions.
- See also: Policy templates available on www.cyfun.eu

PROTECT

Protect

IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL [PR.AA]

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-01.2 Identities and credentials for authorised users, services and hardware shall be managed through automated mechanisms whenever feasible.

Implementation guidance

The goal of this control is to reduce the risk of credential misuse and unauthorised access by automating identity and credential management processes, ensuring consistency, scalability, and security across IT and OT environments.

To achieve this goal, the organisation should:
- **Automate Credential Management**
  Automated systems should be used to issue, verify, revoke, and audit credentials for users, services, and hardware. This reduces manual errors and improves operational efficiency.
- **Implement Strong Authentication Mechanisms**
  In alignment with control PR.AA-03.2, MFA shall be required for all remote access to the organisation's networks. Multifactor authentication (MFA) should use at least two independent factors:
  - *Knowledge* (e.g. password or PIN)
  - *Possession* (e.g. token or smartphone)
  - *Inherence* (e.g. fingerprint or facial recognition)
  These factors should be independent to ensure that compromise of one does not affect the others.
- **Use Cryptographic and Token-Based Solutions**
  Digital certificates and identity tokens should be used to authenticate users, devices, and services, especially in OT environments where manual credential handling may be impractical.
- **Ensure OT-Specific Integration**
  Identity and access management solutions should support OT systems, including legacy devices and vendor-managed components, with minimal disruption to operations.
  Where individual user accounts are not feasible (e.g. shared access to PLCs or HMIs), access should be routed through secure jump servers with logging and additional authentication layers. Remote access to OT systems should use secure protocols (e.g. VPN, SSH, TLS), be time-limited (Just-In-Time), and be fully monitored.

PR.AA-02 · Identities are proofed and bound to credentials based on the context of interactions

PR.AA-02.1 The organisation shall implement documented procedures for verifying the identity of individuals before issuing credentials that provide access to the organisation's systems.

Implementation guidance

The goal of this control, which builds further on GV.RR-04.1, is to ensure that only verified individuals are granted access credentials, thereby reducing the risk of identity fraud, unauthorised access, and insider threats.

To achieve this goal, the organisation should:
- **Establish Documented Identity Verification Procedures**
  A formal process should be developed and approved to verify identities before issuing credentials. This process should ensure accountability, traceability, and auditability.
- **Verify Identity Using Trusted Sources**
  Identity verification should rely on official documents such as government-issued ID cards, passports, or driver's licences. For remote or digital onboarding, practices should align with ENISA's Remote Identity Proofing Good Practices.
- **Prevent Identity Fraud and Misuse**
  Procedures should include controls to detect and prevent identity theft or impersonation. This helps reduce the risk of financial loss, reputational damage, and unauthorised access.
- **Ensure OT-Relevant Adaptation**
  Identity verification processes should be adapted for OT environments, especially where third-party technicians or vendor personnel require access to critical systems.

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-03.3 The organisation shall define, document, and implement usage restrictions, connection requirements, and authorisation procedures for remote access to its critical systems. These controls shall ensure that only approved users can connect, using secure methods, with access limited to what is necessary for their role.

Implementation guidance

The goal of this control is to ensure that remote access to critical systems is tightly controlled through defined usage restrictions, secure connection methods, and formal authorisation procedures. This helps prevent unauthorised access and limits exposure to cyber threats.

To achieve this goal, the organisation should:
- **Define Usage Restrictions**
  Identify which systems are critical (e.g. OT systems, production servers, financial databases). Define who may access them remotely (e.g. specific roles, third-party vendors). Limit access to approved timeframes and restrict it to only the systems and functions necessary for the user's role.
- **Set Secure Connection Requirements**
  Remote access should be established using secure methods such as VPNs with strong encryption, TLS/SSH, or jump servers for OT environments. All remote access should be protected by Multi-Factor Authentication (MFA), in line with PR.AA-03.2. Devices used for remote access should meet endpoint security requirements (e.g. antivirus, patching).
- **Document and Approve Access**
  A remote access policy should define request and approval procedures, roles, and technical requirements. A register of remote users should be maintained, including access scope, approval dates, and review timelines.
- **Monitor and Review Access**
  All remote sessions should be logged, capturing user identity, time, duration, and systems accessed. Logs should be reviewed regularly for anomalies. Remote access permissions and configurations should be audited periodically.
- **Apply OT-Specific Controls**
  For OT systems, access should be routed through secure front-end interfaces or jump servers. If shared accounts are required (e.g. for PLCs or HMIs), access should be logged, time-limited, protected by MFA at the jump server level, and follow the principle of least privilege.
- **Align with ENISA Guidance**
  These practices align with ENISA's NIS2 Technical Implementation Guidance, which recommends secure remote access policies, strong authentication, and continuous monitoring as part of cybersecurity risk management for critical systems.

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-05.5** Where technically, operationally, and economically feasible — without compromising system integrity, safety, or compliance — automated mechanisms shall be implemented to manage user accounts on critical ICT and OT systems. Feasibility shall be determined based on system capabilities, integration potential, risk assessment, and business impact.

Implementation guidance

The goal of this control is to ensure that user accounts on critical ICT and OT systems are managed securely, efficiently, and consistently through automated mechanisms — where technically, operationally, and economically feasible — without compromising system integrity, safety, or compliance.

To achieve this goal, the organisation should:
- **Assess Feasibility of Automation**
  Feasibility should be based on system capabilities, integration potential, risk assessment, and business impact.
  - For **ICT systems**, feasibility depends on the availability of automation tools, APIs, or integration options, and the absence of major technical or financial barriers.
  - For **OT systems**, feasibility depends on system age, vendor limitations, safety requirements, and the risk of disrupting critical operations.
  - General feasibility should consider technical capability, operational safety, cost-effectiveness, and compliance with security and regulatory standards.
- **Automate Account Lifecycle Management**
  Automated mechanisms should manage account creation, modification, and deletion based on predefined rules. This ensures that only authorised users have access and that accounts are promptly removed when no longer needed.
- **Disable Inactive or Unauthorised Accounts**
  Accounts should be automatically disabled when users leave the organisation or no longer require access. This reduces the risk of unauthorised access to critical systems.
- **Monitor and Report Account Activity**
  Automated tools should continuously monitor account usage and generate reports to detect unusual or unauthorised activity. Alerts should be triggered for suspicious behaviour.
- **Send Notifications for Key Events**
  Automated notifications should inform administrators of important events such as account creation, modification, or deletion, enabling timely oversight.
- **Maintain Audit Trails for Compliance**
  All account-related activities should be logged automatically to support compliance with internal policies and external regulations.
- **Ensure OT-Specific Feasibility**
  In OT environments, automation should be implemented only where it does not compromise safety or operational continuity. Where direct automation is not feasible, account management should be handled through secure interface layers or jump servers.
- **Align with ENISA Guidance**
  These practices are supported by ENISA's NIS2 Technical Implementation Guidance and its work on secure access management in critical infrastructure environments.

PR.AA-05.6   Separation of duties (SoD) shall be ensured in the management of access rights.

Implementation guidance

The goal of this control is to ensure that no single individual has full control over critical systems or processes by enforcing Separation of Duties (SoD). This should reduce the risk of errors, fraud, and misuse of access rights.

To achieve this goal, the organisation should:
- **Define Separation of Duties**
  - Responsibilities should be divided so that key tasks are performed by different individuals.
  - SoD should include:
    - Operational and system support roles should be assigned to different individuals.
    - System support tasks should require oversight or dual control.
    - A single person should not initiate and approve the same transaction.
    - Access control and audit functions should be handled by separate roles.
- **Manage Access Rights Appropriately**
  - Role-Based Access Control (RBAC) should be used to assign permissions based on job roles.
  - The principle of least privilege should be applied to limit access to what is strictly necessary.
  - Access rights should be reviewed regularly, especially for critical systems and high-risk roles.
  - Separate tools or accounts should be used for administrative and audit functions where feasible.
- **Apply Controls for System Administrators**
  - Administrative responsibilities should be split to prevent full control by a single individual.
  - Administrators should use separate accounts for regular and privileged tasks.
  - All administrative actions should be logged and reviewed by an independent party.
  - Administrators managing access should not be responsible for auditing that access.
- **Ensure Feasibility in OT Environments**
  - In OT systems, SoD should be adapted to operational and safety constraints.
  - Where full separation is not feasible, compensating controls such as dual approval, logging, and external review should be implemented.
- **Align with ENISA Guidance**
  These practices align with ENISA's Security Measures for Operators of Essential Services, which highlight the importance of Separation of Duties (SoD) and Role-Based Access Control (RBAC) in reducing access-related risks across ICT and OT environments.

PR.AA-05.7   Privileged users shall be managed and monitored.

Implementation guidance

The goal of this control is to reduce the risk of unauthorised access, data breaches, and operational disruption by ensuring that privileged users, who have elevated access to critical systems, are subject to strict management and continuous oversight.

To achieve this goal, the organisation should:
- **Monitor Privileged Activities**
  Activities of privileged users should be logged and reviewed routinely or continuously, even if performed by individuals not independent of the process.
- **Protect Sensitive Data**
  Monitoring should help prevent privileged users from exposing or misusing sensitive information and system configurations.
- **Prevent Abuse of Privileges**
  Privileged accounts should be managed to avoid unauthorised changes, privilege escalation, or bypassing of security controls.
- **Detect Suspicious Behaviour**
  Behavioural anomalies and unauthorised actions should be identified through automated logging and alerting mechanisms.
- **Support Incident Response**
  Monitoring data should be used to investigate and respond to security incidents involving privileged accounts.
- **Manage Access Rights Proactively**
  Access rights should be clearly defined, regularly reviewed, and adjusted based on role changes, operational needs, or risk assessments.
- **Ensure OT-Specific Feasibility**
  In OT environments, privileged access should be managed with consideration for system stability and safety. Where full monitoring is not feasible, compensating controls such as interface-level logging[1] or external review should be implemented.
- **Align with ENISA Guidance**
  These practices align with ENISA's NIS2 Technical Implementation Guidance, which emphasises the importance of privileged access control and monitoring in securing essential services and critical infrastructure.

---

1   Interface-level logging means recording what users do at the point where they connect to a system, such as through a remote access tool, jump server, or secure gateway, without needing to log directly inside the system itself (e.g. using Splunk®). This helps monitor privileged activity in environments where direct system logging is not possible, such as in OT systems.

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, should 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.

PR.AA-06.2 Physical access controls shall include specific procedures for emergency situations, ensuring continued protection of critical and non-critical assets during such events.

Implementation guidance

The goal of this control is to ensure that physical access controls remain effective and adaptable during emergency situations. This includes maintaining security over critical and non-critical assets while enabling safe, authorised, and traceable access for emergency response, recovery, or containment actions — especially in environments where physical and operational safety are tightly linked, such as Operational Technology (OT) and Internet of Things (IoT) systems.

To achieve this goal, the organisation should:
- **Define Emergency Scenarios**
  Emergency procedures should cover a range of events, including:
  - Environmental and safety incidents (e.g. fire, flood, medical emergencies, evacuations)
  - Infrastructure failures (e.g. power outages, system malfunctions)
  - Security incidents (e.g. intrusions, access control failures)
  - Cybersecurity events (e.g. ransomware, data breaches, insider threats)
- **Maintain Emergency Access Procedures**
  Emergency access should be:
  - Logged: Record who accessed what, when, and why.
  - Monitored: Use surveillance or access control systems to track activity.
  - Reviewed: Conduct post-event reviews to verify appropriate use and detect misuse.
- **Support Emergency Readiness with Physical Controls**
  - Up-to-date lists of authorised individuals with emergency access rights should be maintained.
  - Identity credentials (e.g. access badges) should be used and security zones defined.
  - Escort requirements should be applied for visitors or temporary personnel.
  - Physical barriers should be implemented such as fences, locks, turnstiles, and staffed checkpoints.
  - Surveillance systems should be used to monitor entry and exit points.
- **Apply Additional Safeguards**
  - Badge systems with differentiated access levels for various zones should be considered.
  - Physical access to servers and network components should be restricted to authorised personnel only.
  - All access to critical infrastructure should be logged and reviewed regularly.
  - Maintain and review — Visitor access records should be maintained and reviewed. Corrective action should be taken when necessary.
- **Ensure OT-Specific Feasibility**
  In OT environments, physical access procedures should be adapted to avoid disrupting safety or operational continuity. Emergency access should be designed to support both rapid response and asset protection.
- **Align with ENISA Guidance**
  These practices align with ENISA's NIS2 Technical Implementation Guidance, which highlights the importance of physical and logical access controls in maintaining resilience during emergencies.
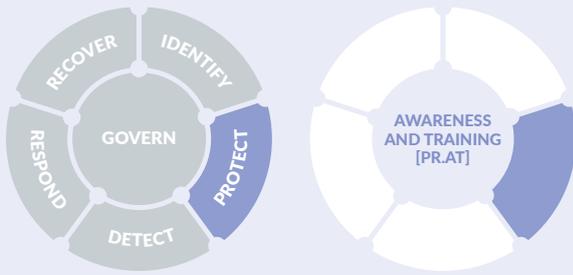
The organisation's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks

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.

PR.AT-01.2 The organisation shall include insider threat awareness and reporting in its cyber-security training to help personnel recognise and respond to potential internal risks.

Implementation guidance

The goal of this control is to ensure that all personnel are trained to recognise and report potential insider threats, thereby reducing the risk of internal cybersecurity incidents.
This control builds on the general awareness from PR.AT-01.1 by introducing specific threat scenarios and response actions.

The implementation should consider:
- Training should include how to recognise behavioural signs of insider threats, such as unusual access patterns, data hoarding, or sudden changes in behaviour.
- The organisation should define insider threats clearly (e.g. malicious, negligent, or compromised insiders, including employees and contractors).
- Staff should be trained on how and where to report suspicious activity, and why timely reporting matters.
- Real-life case studies or simulations should be used to show the impact of insider threats and reinforce learning.
- Insider threat awareness should be part of regular security training and onboarding for all staff.
- Specialised training should be provided to staff with access to sensitive data or systems, focusing on their specific responsibilities.
- Cross-functional teams-training should be developed with both IT security and OT operational expertise (Cross-Training).
- Annual refresher training should be used to reinforce key messages and introduce updates.
- The organisation should promote a culture of security where employees feel safe to report concerns without fear of retaliation.

PR.AT-01.3 Personnel shall receive training to understand their specific roles, responsibilities, and priorities during a cybersecurity or information security incident, including the steps they need to follow to respond effectively.

Implementation guidance

The goal of this control is to ensure that all personnel understand their specific roles, responsibilities, and priorities during a cybersecurity or information security incident, enabling them to respond effectively and in coordination with the organisation's incident response and contingency plans. This control builds on the threat-specific awareness from PR.AT-01.2 by introducing role-based training and incident response readiness.

The implementation should consider the following:
- Training should be tailored to different roles (e.g., IT, HR, executives) so that each group understands its specific responsibilities during an incident.
- Personnel should be familiar with their objectives, recovery priorities, and the correct order of actions to take during an incident.
- Tabletop exercises or simulated drills should be used to practice incident response in a realistic but controlled environment.
- Clear documentation should be provided outlining each role's tasks and responsibilities during an incident.
- Training should explain how incident response connects to contingency planning, ensuring that staff understand when and how to activate contingency measures (see also ID.IM-04.1).
- Regular refresher sessions should be held to keep knowledge up to date and reinforce readiness.

PR.AT-02 **Individuals in specialised roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind**

PR.AT-02.1 Members of management bodies shall be able to demonstrate that they have completed training that gives them a solid understanding of information and cybersecurity and risk management so that they can assess information and cybersecurity risks and their consequences and propose the necessary risk mitigation, considering their roles, responsibilities and authorities.

Implementation guidance

The goal of this control is to ensure that members of management bodies are equipped to make informed decisions on cybersecurity risks and mitigation strategies by developing a foundational understanding of information security, cyber threats, and risk management principles relevant to their leadership roles.

To achieve this goal, the following practices should be considered:
· Training should provide management with the ability to assess cybersecurity risks, understand their potential impact, and propose appropriate mitigation measures aligned with their responsibilities and authority.
· Training content should consider:
  · Core concepts of information and cybersecurity
  · Risk identification, assessment, and mitigation
  · Strategic decision-making in the context of cyber threats
  · Recognition of potential security gaps and governance responsibilities
· Training should be tailored to leadership roles, using guidance from the European Union Agency for Cybersecurity (ENISA) on role profiles, including titles, missions, tasks, skills, and competencies (Ref. European Cybersecurity Skills Framework Role Profiles).
· Annual refresher sessions should be considered to reinforce existing practices and introduce new developments in cybersecurity and risk management.

PR.AT-02.2 Individuals in specialised roles shall be provided with awareness and training before privileges are granted, so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind.

Implementation guidance

The goal of this control is to ensure that individuals in specialised roles receive cybersecurity awareness and training before privileged access is granted, enabling them to perform their tasks with a strong understanding of cybersecurity risks.

To achieve this goal, the organisation should:
· The specialised roles within the organisation that require additional cybersecurity training (e.g. physical and cybersecurity personnel, finance personnel, people in management roles, and anyone with access to business-critical data) should be formally identified.
· Role-based cybersecurity awareness and training should be provided to all those in specialised roles, including contractors, partners, suppliers, and other third parties.
· It should be ensured that the training is delivered before access is granted, and that it is tailored to the specific risks and responsibilities of each role.

- Individuals should be periodically assessed and tested on their understanding of cybersecurity practices through tests, simulations, or practical evaluations relevant to their role.
- Consider annual refreshers to reinforce existing practices and introduce new practices.
- Both Information Technology (IT) and Operational Technology (OT) contexts should be included, particularly for roles that interact with industrial systems or critical infrastructure.

PR.AT-02.3	Privileged users shall be qualified before privileges are granted, and these users shall be able to demonstrate the understanding of their roles, responsibilities, and authorities.

Implementation guidance

The goal of this control is to ensure that individuals granted privileged access, whether in IT or OT environments, are demonstrably competent and fully aware of the cybersecurity responsibilities, risks, and authority boundaries tied to their role. This reduces the likelihood of accidental misuse or exploitation of elevated privileges, especially in critical systems where operational continuity and safety are at stake.

To ensure this goal is met, the organisation should consider the following:
- Privileged users should be trained in various aspects to ensure that they use their elevated access rights in a safe and responsible manner. The following training topics could be considered:
  - Security awareness: It is crucial that privileged users are aware of the security risks associated with their elevated access rights. This includes knowledge about phishing, malware, and other cyber threats.
  - Access management: Users should understand how to properly manage their access rights, including using strong passwords, multi-factor authentication, and restricting access only to what is necessary for their role.
  - Compliance and regulation: It is important that privileged users are aware of relevant laws and regulations, such as GDPR, NIS2, DORA…, and how they affect their work.
  - Incident response: Training on how to respond to security incidents is essential. This includes recognising suspicious activity and knowing how and to whom to report it.
  - Data management best practices: Users should be trained on how to store, process and transfer sensitive data securely.
  - Ethics and responsibility: It is important that privileged users are aware of their ethical responsibilities and the possible consequences of misusing their access rights.
- Privileged users should be periodically assessed and tested on their understanding of cybersecurity practices for their specialised roles.
- Consider annual refreshers to reinforce existing practices and introduce new practices.
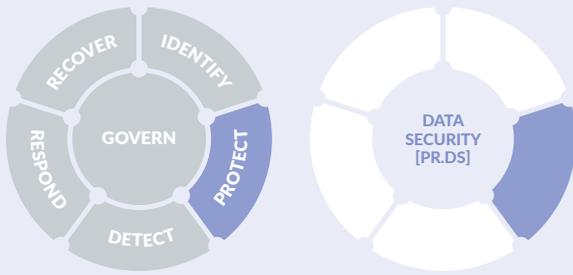
Data are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information

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

PR.DS-01.1 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 when determined necessary.

Implementation guidance

The goal of this control is to ensure the integrity and trustworthiness of critical system components, such as software, firmware, and configuration data, by detecting unauthorised modifications that could compromise operational safety, reliability, or security across all lifecycle stages, including storage, transport, and start-up.

To effectively protect the integrity of data-at-rest, the organisation should implement a layered set of controls designed to detect and prevent unauthorised changes to stored data, software, and system components.

The following practices should be considered:
- Apply Cryptographic Integrity Mechanisms
  - Use cryptographic hashes (e.g., SHA-256), digital signatures, or other cryptographic mechanisms (e.g. message authentication codes (MACs)) to verify the integrity of stored data and critical files.
  - Integrity values should be generated at the time of storage and verified before access or execution.
- Implement Automated Integrity Monitoring
  - Deploy file integrity monitoring (FIM) tools to continuously track changes to critical system files, configurations, and applications.
  - Alerts should be generated for any unauthorised or unexpected modifications, and logs should be retained for audit and investigation.
- Validate Software and Firmware Integrity
  - Ensure that software and firmware stored on systems are validated using signature verification or secure boot mechanisms before execution.
  - Integrity validation should be part of the system start-up process and enforced through technical controls.
- Enforce Change Control and Access Restrictions
  - Limit write access to critical data and system components through role-based access controls (RBAC) and least privilege principles.
  - All changes to data-at-rest should be subject to formal change management procedures and logged for traceability.
- Protect Integrity of Backups
  - Backups should include integrity verification mechanisms (e.g. checksums or digital signatures) to ensure they have not been tampered with.
  - Regular test restorations should be performed to confirm the integrity and usability of backup data.

PR.DS-01.4 The organisation shall define and enforce clear policies and practical safeguards to manage and restrict the use of portable storage media, in order to reduce the risk of data leakage, unauthorised access, and malware introduction.

Implementation guidance

The goal of this control is to reduce the risk of data leakage, unauthorised access, and malware introduction by defining and enforcing clear policies and safeguards for the use of portable storage media.

To achieve this goal, the organisation should:
- **Define and Communicate Policy**
  - A documented policy on acceptable use of portable storage devices (e.g. USB drives, SD cards, external hard disks) should be established.
  - The policy should be communicated during onboarding and reinforced through regular security awareness training.
- **Control Device Usage**
  - Only organisation-approved portable storage devices should be permitted.
  - An inventory of approved devices should be maintained and linked to specific users or departments.
- **Apply Practical Safeguards**
  - **Access Control**: Devices should require user authentication (e.g. password protection).
  - **Encryption**: Data on portable devices should be encrypted using hardware-encrypted drives or software tools such as BitLocker To Go or VeraCrypt.
  - **Read-Only Mode**: Devices used for distribution (e.g. software updates) should be configured as read-only.
  - **Malware Scanning**: Devices should be scanned for malware before and after use.
  - **Physical Security**: Devices should be stored securely (e.g. in locked drawers or cabinets) when not in use.
- **Monitor and Log Usage**
  - On managed systems, USB device connections and file transfers should be logged using endpoint management tools.
  - Logs should be reviewed periodically to detect unauthorised use or anomalies.
- **Examples**
  - A field technician should use a company-issued, encrypted USB drive to collect data from remote sensors. The drive should be scanned before and after use, and data should be uploaded to a secure server upon return.
  - A marketing team should use a read-only USB stick to distribute promotional materials at a trade show, thereby preventing any data from being copied back onto the device.

PR.DS-01.5 The organisation shall only allow the use of removable media when absolutely necessary and shall put technical measures in place to block automatic execution of files from these devices.

Implementation guidance

The goal of this control is to minimise the attack surface in operational and IT environments by strictly limiting the use of removable media and preventing automatic execution of potentially harmful files.

To reduce the risk of malware infections and data leaks from removable media (e.g. USB sticks, external drives), the organisation should:
- Allow Use Only When Necessary
  - The organisation should state in its policy that removable media should only be used when no safer alternative is available (e.g., secure file transfer).
  - Technical tools should be used to limit access to USB ports or require approval before use.
- Disable Autorun and Auto-Execution
  - All systems should be configured to disable autorun and autoplay features so that files on removable media do not run automatically.
  - This should help prevent malware from executing without user action.
- Use Security Tools to Control Access
  - The organisation should use endpoint protection tools to:
    - Block or limit USB access.
    - Allow only approved devices.
    - Require administrator approval for new devices.
- Monitor and Review Usage
  - The organisation should monitor removable media use by logging device connections through endpoint protection tools or operating system logs. In OT environments, manual logging or controlled access procedures should be used. Logs should be reviewed regularly to detect unauthorised activity.
- Example: A finance team should use encrypted, company-approved USB drives to transfer sensitive reports. These drives should be scanned before use, autorun should be disabled on all systems, and access should be logged and reviewed.

Clarification of the difference with PR.DS-01.4
- PR.DS-01.4 focuses on setting rules and procedures for how removable media should be used (e.g., who can use them, encryption, physical protection).
- PR.DS-01.5 focuses on the technical enforcement of those rules — how systems should be configured to reduce risk.

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.

PR.DS-11.2 The reliability and integrity of backups shall be verified and tested regularly.

Implementation guidance

The goal of this control is to ensure that backup data can be trusted and successfully restored when needed, supporting operational continuity and resilience.

To achieve this goal, the organisation should:
- **Test Recovery Procedures**
  Backup recovery procedures should be tested regularly to confirm that data can be restored accurately and completely.
- **Verify Backup Integrity**
  - Backups should be checked for signs of compromise, corruption, or tampering before use.
  - Integrity checks should focus on indicators of security breaches or data loss.
- **Schedule Testing**
  - All types of data sources should be included in backup and restore tests.
  - Testing should occur at least annually, or more frequently on a sample basis.
- **Align with Related Controls**
  This control should be implemented in coordination with RC.RP-05.1 (Recovery Planning), ensuring consistency in recovery strategies.

> **PR.DS-11.3** The organisation shall maintain secure backups of business-critical data in a separate storage location to ensure data availability in case of system failure or data loss. Backup storage shall apply equivalent security controls as the primary environment.

Implementation guidance

The goal of this control is to ensure that the organisation can reliably recover its business-critical data in two key scenarios:
- **Natural disasters or physical damage** to the primary site (requiring offsite or cloud-based backups).
- **Advanced cyberattacks**, including ransomware or insider threats, where attackers may attempt to corrupt or delete backups (requiring isolated or tamper-proof backups).

This control helps ensure that an organisation can recover its critical data if something goes wrong. It focuses on keeping backups separate and just as secure as the original data, making it especially useful for organisations that are still building up their cybersecurity capabilities (organisations with less mature security posture).

- **Backup Strategy to be considered**
  - To meet these objectives, the organisation should implement a diversified and resilient backup approach, such as the **3-2-1 backup rule**:
    - Maintain three copies of business-critical data.
    - Store these copies on at least two different types of storage media (e.g. local disk and cloud).
    - Ensure at least one copy is stored offsite or off-premises, in a physically separate location.
- To protect against both physical and cyber threats, the organisation should consider the following backup types:
  - **Offsite or Cloud Backups**
    These backups are stored in a geographically separate location and help ensure recoverability in case of natural disasters or physical damage to the primary site.
  - **Immutable Backups**
    These are backups that cannot be altered or deleted for a defined period. They are especially effective against ransomware and insider threats, and can be automated to reduce manual effort.
  - **Offline or Air-Gapped Backups**
    These are backups stored on devices that are completely disconnected from any network, including the internet. This isolation ensures that even if the organisation's network is compromised, the backup remains untouched.
- Additional Considerations
  - **Geographic Separation**: Backup locations should be in different physical regions to reduce the risk of simultaneous impact from regional disasters.
  - **Security Parity**: All backup locations should implement the same level of security controls as the primary environment (e.g. encryption, access control, monitoring).
  - **Regular Testing**: Backup and recovery procedures should be tested regularly to ensure data integrity and operational readiness.
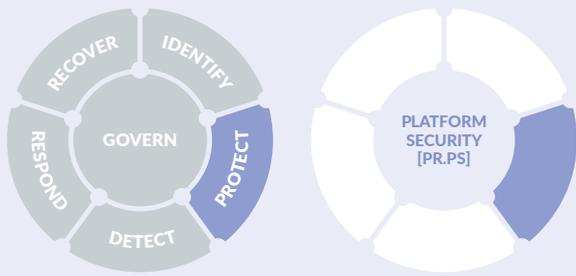
The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organisation's risk strategy to protect their confidentiality, integrity, and availability

PLATFORM SECURITY [PR.PS]

PR.PS-01 Configuration management practices are established and applied

PR.PS-01.1 The organisation shall develop, document, and maintain a baseline configuration for its business critical systems.

Implementation guidance

This control ensures that all business-critical systems operate in a known, secure, and approved state. A baseline configuration defines the standard setup for these systems, helping to detect unauthorised changes, enforce security policies, and support consistent operations.

To implement this control the following should be considered:
· **Definition of what is Business-Critical**
  Business-critical systems may include IT, OT (Operational Technology), and potentially IoT (Internet of Things) components — if they support essential business functions:
  · IT systems are typically managed internally.
  · OT systems may include industrial control systems.
  · IoT systems (e.g. sensors, smart devices) can be business-critical if their failure disrupts operations or introduces security risks.
· **Establish and Maintain Baseline Configurations**
  For each business-critical system, the baseline should include:
  · System components (e.g. approved software, hardware)
  · Operating system and application versions, including patch levels
  · Configuration settings and parameters
  · Network topology, showing how components are connected, including:
    · External connections
    · Servers hosting sensitive data or functions
    · DNS and security services
  · Logical placement of components within the system architecture
· **Apply Security Principles**
  · Baselines should enforce the principle of least functionality — only necessary features and services should be enabled.
  · Default settings should be reviewed and adjusted to reduce security risks during installation or upgrades.
· **Monitor and Update**
  · Continuously monitor systems for deviations from the approved baseline.
  · Update baselines when systems are patched, upgraded, or reconfigured.
· **Cloud and Supplier-Managed Systems**
  For systems managed by third parties (e.g. cloud services), ensure that baseline expectations are defined contractually and that suppliers provide visibility into configuration and change management.

PR.PS-02   Software is maintained, replaced, and removed commensurate with risk

PR.PS-02.1   The organisation shall enforce restrictions on software usage and installation, and ensure that software is maintained, replaced, or removed based on its associated risk.

Implementation guidance

The goal of this control is to reduce security and operational risks by controlling which software is used, ensuring it is properly maintained, and removing it when no longer needed or supported.

To achieve this goal, the organisation should consider to:
- Allow only approved software and restrict access based on user roles and responsibilities.
- Replace unsupported or end-of-life software to avoid unpatched vulnerabilities.
- Uninstall unused or unnecessary software, including outdated OS utilities, to reduce the attack surface.
- Apply patches based on risk:
  - Critical vulnerabilities should be patched within hours.
  - Routine updates should follow a defined schedule (e.g. weekly or monthly).
- In container environments, only trusted and up-to-date images should be used; outdated containers should be replaced.
- Remove or disable software and services that pose unacceptable risk, such as FTP or peer-to-peer tools, unless explicitly required and secured.
- In ICS/OT environments, ensure PLC programming is pre-approved and scheduled; avoid ad-hoc changes to protect operational safety.
- Maintain a software inventory with version and support status.
- Define procedures for software approval, patching, replacement, and removal.

PR.PS-03   Hardware is maintained, replaced, and removed commensurate with risk

PR.PS-03.1   Hardware used in business-critical environments shall be maintained, replaced, or removed based on its associated security and operational risk.

Implementation guidance

The goal of this control is to ensure that hardware used in business-critical environments remains secure, reliable, and fit for purpose by managing it based on operational and security risks.

To achieve this goal, the organisation should consider to:
- Regularly assess whether hardware supports required security features (e.g. encryption, secure boot, firmware updates); replace hardware that cannot meet these needs.
- Phase out end-of-life or unsupported hardware in a controlled manner.
- Define and maintain a hardware lifecycle plan, including:
  - Inventory tracking
  - End-of-life timelines
  - Replacement schedules
  - Secure disposal procedures
- Perform preventive maintenance and timely replacements to avoid unexpected failures that could impact operations or security.
- Ensure hardware can support secure, up-to-date software; address any limitations that prevent this.

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-04.2   The organisation shall ensure that logbook records contain an authoritative time source or internal clock time stamp that is compared and synchronised with an authoritative time source.

Implementation guidance

The goal of this control is to ensure that logbook records across systems use a consistent and trusted time reference, so that events can be accurately tracked and correlated.

To achieve this goal, the organisation should consider to:
- Use a reliable time reference such as a GPS clock, internal time server, or other trusted source to synchronise system clocks.
- Configure systems to update their clocks regularly to avoid time drift.
- Set up multiple time sources to ensure redundancy and accuracy.
- Monitor synchronisation status and trigger alerts if systems fall out of sync.
- Document procedures for time synchronisation, including server settings, update intervals, and monitoring processes.

PR.PS-04.3   Audit data from the organisation's critical systems shall be moved to an alternative system.

Implementation guidance

The goal of this control is to protect the integrity of audit records by transferring them from critical systems to a separate, secure location where they cannot be changed or tampered with.

To achieve this goal, the organisation should consider to:
· Transfer audit data to a separate system where records cannot be modified by users or services from the original system.
· Ensure the destination system keeps audit records unchanged once stored.
· Monitor the impact of log transfers to avoid performance issues on the source systems.
· Put measures in place that protect the data without slowing down or disrupting system operations.

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.

PR.PS-05.2   Installation and execution of unauthorised software shall be prevented.

Implementation guidance

The goal of this control is to reduce the risk of compromise by ensuring only trusted and approved software is installed and executed on systems.

To achieve this goal:
- Software installation and execution should be limited to pre-approved applications and environments.
- Platforms should be configured to block unauthorised software and restrict execution where the risk justifies it.
- The source and integrity of all new software should be verified before installation.
- Access to harmful websites should be blocked using trusted and approved internet filtering services that are designed to detect and stop known online threats.
- Where possible, systems should be configured to allow installation of organisation-approved software only.

PR.PS-06   **Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle**

PR.PS-06.1   Security shall be considered throughout the lifecycle of systems and applications, whether developed internally or acquired externally.

Implementation guidance

The goal of this control is to make sure that security is built into systems and applications from the beginning and maintained throughout their entire life — from design to retirement — whether they are developed in-house or purchased.

To achieve this goal:
- **Initiation Phase**
  Security requirements should be defined early, risks identified, and relevant stakeholders, including security experts, engaged from the start.
- **Acquisition or Development Phase**
  - For acquired solutions: vendors should follow secure development practices, provide evidence of testing, and meet contractual security requirements.
  - For in-house development: secure coding practices should be applied, changes managed, and security testing conducted.
- **Implementation Phase**
  Systems should be securely configured before deployment, with access controls and encryption applied to protect sensitive data.
- **Operations and Maintenance Phase**
  Systems should be monitored for incidents, regularly updated, and security controls reviewed and improved as needed.
- **Disposition Phase**
  Systems should be decommissioned securely, sensitive data removed, and lessons learned documented to strengthen future processes.

PR.PS-06.2 Changes and exceptions shall be tested and validated before being implemented into operational systems.

Implementation guidance

The goal of this control is to reduce the risk of disruptions or vulnerabilities by ensuring that all changes and exceptions are properly tested and validated before being applied to operational systems.

To achieve this goal:
- All proposed changes and exceptions should follow a formal process that includes documentation, review, testing, and approval.
- The potential risks of applying, or not applying, a change should be assessed and recorded.
- Exceptions, defined as approved deviations from standard policies or procedures, should be evaluated with a clear understanding of the risks and a defined plan to reduce or manage them.
- Accepted risks should be periodically reviewed to confirm that the original decision to accept them remains valid, especially if conditions change or if the acceptance was based on future actions or milestones.
- These practices should be adapted to the operational environment to avoid unplanned downtime or safety issues, especially in OT systems.
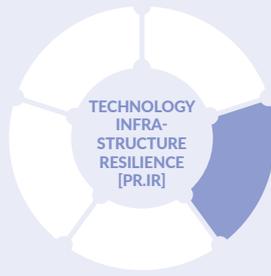
Security architectures are managed with the organisation's risk strategy to protect asset confidentiality, integrity, and availability, and organisational resilience

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.

PR.IR-01.3 To ensure operational stability and security, the organisation shall, without exception, identify, document, and control connections between components of its critical systems.

Implementation guidance

The goal of this control is to maintain operational stability and security by ensuring that all connections between components of critical systems are known, documented, and actively managed.

In OT environments, undocumented or uncontrolled connections — whether physical, wireless, or logical — can introduce vulnerabilities, disrupt processes, or bypass safety mechanisms.

To effectively manage and secure network connections between system components, the following practices should be considered:
- **Configuration Management**
  Organisations should implement configuration management processes to ensure that all changes to network connections are documented, reviewed, and approved. Configuration files and logs should be kept current and securely maintained.

- **Access Controls**
  Strict access controls should be enforced to ensure that only authorised personnel can modify network configurations. Role-Based Access Control (RBAC) should be used to restrict access based on job responsibilities and operational needs.
- **Regular Audits**
  Regular audits should be conducted to verify that all documented connections remain accurate and that no unauthorised changes have occurred. Audit results should be used to update documentation and strengthen controls.
- **Link to Asset Management (ID.AM)**
  Connections between system components should be documented under ID.AM (Asset Management) and controlled under this requirement (PR.IR-01.3) to ensure consistency, traceability, and enforceability across the organisation's cybersecurity architecture.

PR.IR-01.4 **The organisation shall implement appropriate boundary protection measures to monitor and control communications at external and key internal boundaries of its critical systems, across both IT and OT environments, to ensure secure and reliable operations.**

Implementation guidance

The goal of this control is to ensure secure and reliable operations by actively monitoring and controlling communications at key network boundaries — especially where critical systems interface with external networks or less trusted internal zones.

In OT environments, where legacy systems often lack built-in security, boundary protection is essential to prevent unauthorised access, contain potential threats, and maintain process integrity across IT and OT domains.

To achieve this goal, the following should be considered:
- **Boundary Protection Devices**
  Firewalls, security gateways, and routers should be deployed at external and internal boundaries to enforce traffic filtering and routing policies. These devices should operate under a "deny by default, allow by exception" model.
- **Zoning and Isolation in OT Environments**
  In OT environments, boundary protection should include strict separation between control systems and external networks. Zones should be defined based on criticality and trust, and communications between zones should be tightly controlled and monitored.
- **Unidirectional Gateways (Data Diodes)**
  Where data must flow from secure OT systems to external destinations (e.g. cloud services or regulators), unidirectional gateways should be used to prevent inbound threats while allowing outbound data transfer.
- **Encrypted Communications**
  Communications across boundaries should be encrypted using secure protocols (e.g. VPNs, TLS) to protect data in transit and ensure confidentiality and integrity.
- **Intrusion Detection and Prevention**
  Intrusion Detection and Prevention Systems (IDPS) should be deployed at key boundaries to monitor traffic for anomalies, detect unauthorised access attempts, and block malicious activity.
- **Access Control Enforcement**
  Access to boundary devices and communication channels should be restricted to authorised personnel. Network Access Control (NAC) solutions should be considered to enforce device and user authentication at entry points.
- **Continuous Monitoring and Patching**
  Boundary devices and communication channels should be continuously monitored for suspicious activity. All systems exposed to external or inter-zone communication should be regularly updated and patched to address known vulnerabilities.

PR.IR-02   **The organisation's technology assets are protected from environmental threats**

> **PR.IR-02.1**   The organisation shall define, implement and maintain policies and procedures related to emergency and safety systems, fire protection systems and environmental controls for its critical systems.

Implementation guidance

The goal of this control is to protect critical systems from environmental hazards and emergencies that could disrupt operations, damage equipment, or endanger safety — especially in OT environments where physical conditions directly impact system availability and human safety.

To achieve this goal, the organisation should:

- **Conduct risk assessments** of all locations housing critical systems to identify environmental and emergency risks.
- **Define policies and procedures** for fire protection, emergency response, and environmental controls.
- **Install monitoring systems** such as temperature, humidity, smoke, and water leak sensors, with alerts for abnormal conditions.
- **Implement fire protection measures** including appropriate suppression systems (e.g. gas-based for data centres), alarms, detectors, and extinguishers.
- **Inspect and maintain** fire safety and environmental systems regularly, including HVAC and emergency lighting.
- **Include environmental protection requirements** in third-party contracts, and request evidence of compliance and maintenance.
- **Train staff** on emergency procedures and conduct evacuation and fire response drills at least annually.

PR.IR-04   Adequate resource capacity to ensure availability is maintained

> **PR.IR-04.1**   Adequate resource capacity planning shall ensure that availability of organisation's critical system information processing, networking, telecommunications, and data storage is maintained.

Implementation guidance

The goal of this control is to ensure that critical systems have enough computing, storage, and network resources available at all times by planning ahead for current and future capacity needs.

To achieve this goal, the organisation should:

- **Forecast and Plan**
  Resource needs should be regularly forecasted based on business growth, seasonal patterns, and usage trends. Future demand for compute, storage, and network capacity should be anticipated to prevent performance issues or outages.
- **Account for Procurement Lead Times**
  Capacity planning should consider potential delays in hardware or service delivery due to supply chain or geopolitical disruptions. Buffer capacity should be maintained to absorb unexpected demand or expansion delays.
- **Monitor and Set Thresholds**
  Systems should be continuously monitored to track usage. Thresholds and alerts should be configured to trigger timely scaling actions before performance is impacted.
- **Use High-Availability Components**
  Redundant components (e.g. RAID arrays, dual network interfaces, backup power) should be deployed to reduce downtime from hardware failures. These should complement, not replace, capacity planning.
- **Review and Adjust Regularly**
  Capacity plans should be reviewed periodically and updated based on changes in business strategy, technology, or external risk factors.

DETECT

Detect

CONTINUOUS MONITORING [DE.CM]

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 work-stations, 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 sched-uled 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-01.3 The organisation shall monitor and identify unauthorised use of its business critical systems through the detection of unauthorised local connections, network connections and remote connections.

Implementation guidance

The goal of this control is to ensure that the organisation can detect and respond to unauthorised access or misuse of its business-critical systems. This includes identifying suspicious local, network, or remote connections that could indicate a security breach or misuse of sensitive systems.

To achieve this goal, consider the following:
- Monitoring of network communications should happen at the external boundary of the organisation's business critical systems and at key internal boundaries within those systems.
- Facilities should be monitored for unauthorised or rogue wireless networks that could allow attackers to bypass normal controls.
- Critical network services such as Domain Name System (DNS – which translates website names to IP addresses), Border Gateway Protocol (BGP – which helps route internet traffic), and other network services should be monitored for signs of tampering or misuse.
- When hosting applications that are accessible from the internet, a Web Application Firewall (WAF) should be considered to protect against attacks. If the application is not web-based, it should be protected using other appropriate methods, such as an Identity Provider (IdP) to control access.

DE.CM-02 **The physical environment is monitored to find potentially adverse events**

DE.CM-02.1 The physical environment shall be monitored to find potentially adverse events.

Implementation guidance

The purpose of this control is to ensure that the physical spaces where critical systems and data are located are monitored for signs of suspicious or harmful activity. This helps detect potential threats such as unauthorised access, tampering, or other unusual events in the physical environment.

To achieve this purpose, consider the following:
- Logs from physical access systems (such as badge readers) should be reviewed to detect unusual patterns, like someone trying to enter at odd hours or repeated failed attempts to access a restricted area.
- Records of visitor access (such as sign-in sheets or digital check-ins) should be regularly reviewed to ensure that only authorised individuals have entered secure areas.
- Physical security equipment (such as locks, door latches, hinge pins, and alarms) should be checked for signs of tampering or damage that could indicate an attempted breach.

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.

Implementation guidance

This control builds on DE.CM-03.1 by shifting the focus from implementation to ongoing management of mon-
itoring tools. The goal of this control is to ensure that tools used to monitor user behaviour and detect harmful
activity on devices and networks are properly maintained and actively managed. This supports the continued
effectiveness of the tools as threats evolve, and ensures that the alerts they produce are accurate, relevant,
and helpful for identifying real security risks.

To achieve this goal, consider the following:
- Tools that monitor devices such as laptops, mobile phones, and servers should be regularly checked to confirm
  they are working properly, updated with the latest threat information, and able to detect new types of attacks.
- A central system should be used to collect and analyse logs from different sources. These logs should be
  complete, up to date, and useful for identifying suspicious activity.
- Logs related to system access, such as login attempts or access outside normal hours, should be reviewed
  regularly. Alerts should be set up to notify security teams of unusual patterns.
- Tools that analyse user behaviour should be fine-tuned over time. Security teams should review alerts, adjust
  detection rules to reduce false alarms, and improve accuracy.
- Deception tools, such as fake systems or files designed to attract attackers, should be monitored closely.
  Alerts from these tools are often early signs of a real attack and should be treated as high priority.
- Security teams should regularly assess how well all monitoring tools are performing, update detection rules,
  and ensure the tools are integrated with incident response processes.
- Roles and responsibilities for monitoring and responding to alerts should be clearly defined. Staff should be
  trained to use the tools effectively and respond appropriately to incidents.

DE.CM-06   External service provider activities and services are monitored to find potentially adverse events

Implementation guidance

The goal of this control is to ensure that activities performed by external service providers, whether remote
or onsite, are securely managed and continuously monitored. This helps detect any unusual or harmful actions
that could affect the organisation's systems, data, or services.

The achieve this goal, the following should be considered:
- External providers may include contractors, cloud service vendors, IT support teams, software developers, and
  other third parties involved in system maintenance, development, or security.
- Monitoring should focus on:
  - Access and login activity, including how and when external users connect to systems.
  - Data transfers and network traffic, to detect unusual or unauthorised movement of information.
  - System changes, such as software updates or configuration adjustments made by external parties.
- All remote and onsite activities by external providers should be logged and reviewed to identify unauthorised
  actions or risky behaviour.
- Cloud services and internet providers should be monitored for unexpected behaviour or performance issues
  that could indicate a security problem.
- A centralised logging system should be used to collect and analyse data from all external services.
- Any security incidents involving external providers — such as malware infections, phishing attempts, or unau-
  thorised access — should be detected early, reported quickly, and addressed effectively.

Implementation guidance

The goal of this control is to ensure that external service providers follow the organisation's personnel security policies and contract requirements, especially when they have access to sensitive systems or data. This helps reduce the risk of security incidents caused by third-party staff and ensures that providers are held to the same standards as internal personnel.

To achieve this goal, consider the following:
- External providers should have clearly defined security responsibilities, which are documented in contracts or service-level agreements.
- Contracts should include requirements such as:
  - Background checks for provider personnel
  - Signing of confidentiality agreements
  - Adherence to acceptable use policies
- Compliance with these requirements should be monitored regularly, including checks for completed security training and signed agreements.
- Providers should be required to notify the organisation immediately when staff with system access are transferred or leave their role, so access rights can be revoked without delay.
- Periodic audits should be conducted to confirm that providers are following security policies. These may include:
  - Reviewing access logs and permissions
  - Verifying onboarding and offboarding procedures
  - Ensuring only authorised individuals have access to critical systems
- Any issues or non-compliance should be documented, reported, and addressed through corrective actions and follow-up reviews.

DE.CM-09 Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events

Implementation guidance

This control aims to ensure that organisations continuously monitor their computing systems and data to detect potentially harmful events early. This helps maintain visibility, support timely responses, and reduce the risk of security incidents.

To achieve the goal of this control, the organisation should consider the following:
- Turn on system logging on computers and servers to record important events.
- Use built-in antivirus or endpoint protection to detect threats and generate alerts.
- Regularly review logs and alerts to spot unusual activity or errors.
- Store logs in a shared folder or simple log viewer to make them easier to access and review.
- Set a routine (e.g. weekly or monthly) to check logs and update monitoring tools.
- Assign someone responsible for monitoring, even if it is a part-time role.

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

DE.AE-02 Potentially adverse events are analysed to better understand associated activities

DE.AE-02.1 Cybersecurity and information security events shall be reviewed and analysed to identify potential attack targets and methods, in accordance with applicable laws, regulations, standards, and policies.

Implementation guidance

The goal of this control is to ensure that cybersecurity and information security events are reviewed and analysed to detect attack targets and methods. This enables organisations to respond effectively to threats while maintaining compliance with legal, regulatory, and policy requirements.

To achieve this goal, consider the following:
- Organisations should follow relevant federal and regional laws, industry regulations, standards, and internal policies when reviewing security events.
- Log analysis tools should be used to generate reports and identify suspicious activity.
- System and application logs should be regularly reviewed to detect signs of security threats, such as repeated failed login attempts or unusual data transfers.
- Logs should be analysed for patterns that indicate attempted or ongoing attacks.
- Threat intelligence should be used to stay informed about emerging threats and attack techniques, and security measures should be adjusted accordingly.
- Regular audits and assessments should be conducted to evaluate the organisation's security posture.
- The results of these audits should be used to improve monitoring and analysis processes.

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.

DE.AE-03.2   The organisation shall ensure that event data from critical systems is collected and correlated using information from multiple relevant sources.

Implementation guidance

The goal of this control is to enable the organisation to detect complex or distributed threats by combining and analysing event data from different systems and sources. Correlating this data helps identify patterns that may not be visible when systems are monitored in isolation.

The achieve this goal, the following should be considered:
- Relevant sources of event data can include system logs, audit logs, network monitoring tools, physical access records, and reports from users or administrators.
- Log data should be sent continuously, ideally in real-time or near real-time, to a centralised system for storage and analysis. This improves the ability to detect patterns and respond quickly to potential issues.
- Centralising logs on a small number of dedicated servers or platforms, such as a SIEM, lightweight log management tools, cloud-based logging services, or managed detection services (often part of Managed Detection and Response, or MDR), can support efficient analysis and correlation of events across systems.
- Cyber threat intelligence can be used to enhance event correlation by providing context about known threats, attack methods, and indicators of compromise.
- Threat intelligence should be securely integrated into detection tools and processes to support more accurate and timely identification of threats.

DE.AE-06 Information on adverse events is provided to authorised staff and tools

DE.AE-06.1 Information about adverse events shall be promptly delivered to authorised personnel and systems to enable timely detection, investigation, and response.

implementation guidance

The goal of this control is to ensure that information about adverse events is delivered promptly to the right people and systems, so that appropriate action can be taken without delay. This supports faster detection, investigation, and response to potential threats or disruptions.

To achieve the goal of this control, consider the following:
- **Types of Adverse Events**
  Include indicators such as unusual account activity, unauthorised access, system configuration changes, physical security breaches, or malware alerts.
- **Detection and Alerting**
  Use cybersecurity tools to detect such events and automatically alert authorised personnel (e.g. SOC analysts, incident responders).
- **Integration with Ticketing Systems**
  Alerts should be integrated with the organisation's ticketing system. Tickets should be:
  - Automatically generated for predefined alert types.
  - Manually created when technical staff identify suspicious activity.
- **Access to Logs and Analysis**
  Authorised staff must have continuous access to log data and analysis results to support investigations.
- **Maturity and Effectiveness Assessment**
  Evaluate the control's implementation by checking:
  - Documentation of procedures for alert generation, review, and escalation. This documentation should be regularly reviewed and updated.
  - Use of automation for standard alerts, with manual processes as a backup.
  - Access controls for alerts and logs, with periodic reviews of permissions (Access to alerts and logs should be limited to authorised personnel).
  - Monitoring and reporting should for example track the number of alerts, response times, and whether procedures are followed.
  - Training should be provided regularly to staff responsible for handling alerts, ensuring they understand how to interpret and act on them.

DE.AE-08   Incidents are declared when adverse events meet the defined incident criteria

DE.AE-08.1   Incidents shall be reported when adverse events meet defined and documented incident criteria.

Implementation guidance

This control ensures that adverse events are identified and reported when they meet clearly defined and documented incident criteria. It emphasises the importance of having consistent thresholds and guidelines in place to determine when an event qualifies as an incident, supporting timely awareness and appropriate escalation or response.

To achieve this goal, the following should be considered:
- Incident criteria (rules for what qualifies as an incident) should be clearly defined, documented, and regularly reviewed.
- These criteria should help determine when an adverse event becomes an incident that must be reported.
- The criteria should be based on known patterns of normal and abnormal activity, including lessons learned from past incidents.
- Known false positives should be considered when setting the criteria, to avoid unnecessary reporting.
- When an event meets the defined criteria, it should be treated as an incident and reported according to the organisation's procedures.
- Where appropriate and feasible, systems should be configured to support this process by generating alerts when incident criteria are met. This can help detect incidents more quickly, especially in larger or more complex environments.

RESPOND

Respond

INCIDENT MANAGEMENT [RS.MA]

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.

| RS.MA-01.2 | The organisation shall coordinate information/cybersecurity incident response actions with all predefined stakeholders. |

Implementation guidance

The goal of this control is to ensure that all relevant internal and external stakeholders work together effectively during a cybersecurity or information incident.

To achieve this goal:
- Incident response actions should be coordinated with predefined stakeholders, including business leaders, IT and OT system owners, cybersecurity teams, vendors, HR, legal, physical security, operations, and procurement.
- Coordination should follow the organisation's documented incident response plans.
- A lead person should be assigned to each incident to manage the response and ensure clear communication.
- If needed, additional plans, such as business continuity or disaster recovery, should be activated to support the response.
- Information should be shared with the right people at the right time, following established communication procedures.
- Different types of incidents should be recognised and handled accordingly:
  - Information incidents (e.g. accidental data exposure)
  - Cybersecurity incidents (e.g. malware, hacking)
  - OT incidents (e.g. disruptions to industrial control systems)
- OT incidents should involve specialised OT personnel and may require different response procedures to protect safety and operations.

RS.MA-02   Incident reports are triaged and validated

RS.MA-02.1   Information/cybersecurity incident reports shall be triaged and validated in accordance with the organisation's incident response procedures.

Implementation guidance

The goal of this control is to ensure that all reported incidents are systematically reviewed and assessed before any further action is taken. This control is a foundational step in the incident response process and the following should be considered:

- **Filter out irrelevant or false reports**
  Not every report received is a real incident. This control ensures that only legitimate, cybersecurity-relevant incidents are acted upon.
- **Ensure timely and appropriate response**
  By triaging and validating reports early, organisations can prioritise real threats and avoid wasting resources on non-issues.
- **Support consistent decision-making**
  Applying structured triage and validation criteria helps ensure that incident response is consistent, repeatable, and aligned with organisational policies.
- **Enable effective escalation and categorisation**
  Validation is a prerequisite for categorising and escalating incidents (as required in RS.MA-03.1). Without it, the response process could be misdirected or delayed.
- **Improve situational awareness**
  Early validation helps build a clearer picture of the threat landscape and supports better coordination across teams.

## RS.MA-03   Incidents are categorised and prioritised

RS.MA-03.1   Information/cybersecurity incidents shall be categorised, prioritised and escalated as determined in the incident response plan.

Implementation guidance

This control is an evolution of RS.MA-02.1 and is to ensure that once an incident is validated, it is systematically classified and managed based on its nature, urgency, and potential impact, so that the organisation can respond efficiently, consistently, and appropriately.

Therefore the following should be considered:

- Incidents should be reviewed and classified based on their type (e.g. data breach, ransomware, DDoS, account compromise) and the validated magnitude of their impact.
- The estimation and validation of an incident's magnitude — further developed in RS.AN-08.1 (Essential), should inform how incidents are categorised and prioritised.
- Indicators such as scope, severity, and time sensitivity should guide prioritisation decisions.
- Software Bills of Materials (SBOM) can support impact assessment by identifying affected components and dependencies.
- Criteria for categorisation, prioritisation, and escalation should be documented in the incident response plan and applied consistently.
- Incident response strategies should balance the need for rapid recovery with the potential benefits of observing attacker behaviour or conducting deeper investigation.
- Escalation procedures should be coordinated with designated internal and external stakeholders to ensure timely and appropriate response.
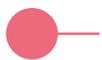
RS.MA-05   **The criteria for initiating incident recovery are applied**

> **RS.MA-05.1**   Clear criteria shall be defined and applied to determine when incident recovery processes need to be initiated.

Implementation guidance

The goal of this control is to ensure that organisations have a clear, consistent, and risk-informed decision-making process for determining when to begin recovery actions following a cybersecurity incident.

Therefore the following should be considered:
- Criteria for initiating incident recovery should be based on the known or assumed characteristics of the incident, such as its severity, scope, and potential impact on operations, data, or systems.
- The decision to begin recovery should also consider the potential disruption that recovery activities may cause to ongoing operations.
- Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) should be included in the criteria to ensure that recovery actions align with business continuity requirements and acceptable downtime or data loss thresholds.

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.

RS.CO-02.2 **Cybersecurity incidents shall be shared with relevant external stakeholders within the timeframes defined in the Incident Response Plan, including reporting significant incidents to authorities as required by law.**

Implementation guidance

The goal of this control is to ensure that all relevant external parties are informed about cybersecurity incidents in a timely, secure, and appropriate manner, helping to maintain trust and meet legal and contractual obligations.

To achieve this:
- Information should be shared securely and in line with the organisation's Incident Response Plan and any information-sharing agreements.
- Relevant stakeholders may include designated internal roles, affected customers, suppliers, third-party service providers, and business partners.
- Customers and partners should be notified if they are affected by an incident, with clear instructions on any actions they need to take.
- Communication with external parties should follow any contractual requirements or agreements in place.
- Crisis communication should be coordinated with critical suppliers to ensure consistent messaging.
- When sharing information about attackers' tactics or techniques, any sensitive or identifying data should be removed.
- The Human Resources department should be informed if the incident involves malicious activity by an insider.
- Senior leadership should receive regular updates on the status of major incidents.
- National authorities, such as the CSIRT, law enforcement, or regulators, should be notified based on the criteria defined in the IRP and with approval from senior management.
- All reporting should comply with relevant national and EU legislation, such as the EU Implementing Regulation.
- Public updates about incidents are addressed under a separate control (RC.CO-04.1).

Activities are performed to prevent expansion of an event and mitigate its effects

RS.MI-01 Incidents are contained

RS.MI-01.1 **Cybersecurity incidents shall be contained and eliminated. Any decision to accept and retain certain cybersecurity risks shall be formally documented.**

Implementation guidance

The goal of this control is to stop cybersecurity incidents from spreading, remove their cause, and ensure that any accepted risks are clearly recorded and approved.

To achieve this:
- A formal risk acceptance process should be in place for cybersecurity risks that are considered low-impact and do not threaten critical business systems. These risks should be reviewed and approved by the responsible person or team, based on the organisation's risk tolerance.
- Cybersecurity tools, such as antivirus software or built-in security features in operating systems and network devices, should be allowed to automatically take action to contain or remove threats when appropriate.
- Incident response teams should be able to manually choose and carry out actions to stop and remove incidents when needed.
- Trusted third parties, such as internet service providers or managed security service providers, should be allowed to help with containment and elimination actions if this is part of the organisation's response plan.

RS.MI-01.2 The organisation shall detect unauthorised access or data leakage and take appropriate mitigation actions, including monitoring of critical systems at external boundaries and key internal points.

Implementation guidance

The goal of this control is to detect unauthorised access and data leakage in a timely manner and to take appropriate mitigation actions. This should help protect the confidentiality, integrity, availability, and safety of data, whether it is stored, being transmitted, or actively used, across both Information Technology (IT) and Operational Technology (OT) environments.

To achieve this goal, the organisation should:
- **Monitor Critical Systems**
  Monitoring should be implemented at external network boundaries and key internal points to detect anomalies or unauthorised access attempts.
- **Protect Data in All States**
  Data should be protected using encryption, digital signatures, and cryptographic hashes to ensure confidentiality and integrity during storage, transmission, and use.
- **Control Outgoing Communications**
  Outbound communications containing sensitive data should be automatically blocked or encrypted based on data classification.
- **Restrict Use of Personal Services**
  Access to personal communication platforms (e.g. personal email, file-sharing services) from organisational systems should be restricted to reduce the risk of data leakage.
- **Prevent Data Reuse in Non-Production Environments**
  Sensitive production data should not be reused in development or testing environments unless properly anonymised or masked.
- **Clear Temporary Data**
  Sensitive data should be cleared from memory or temporary storage once it is no longer needed.
- **Audit Identity and Access Management**
  Systems such as Microsoft Active Directory should be regularly audited, with a focus on privileged accounts and access control consistency.
- **Ensure OT-Specific Feasibility**
  In OT environments, detection and mitigation measures should be adapted to avoid disrupting safety or operational continuity. Passive monitoring and interface-level logging may be used where direct integration is not feasible.
- **Align with ENISA Guidance**
  These practices align with ENISA's Threat Landscape Reports and Information Leakage Guidance, which provide recommendations for detecting and mitigating data breaches and unauthorised access.

RECOVER

Recover

INCIDENT RECOVERY PLAN EXECUTION [RC.RP]
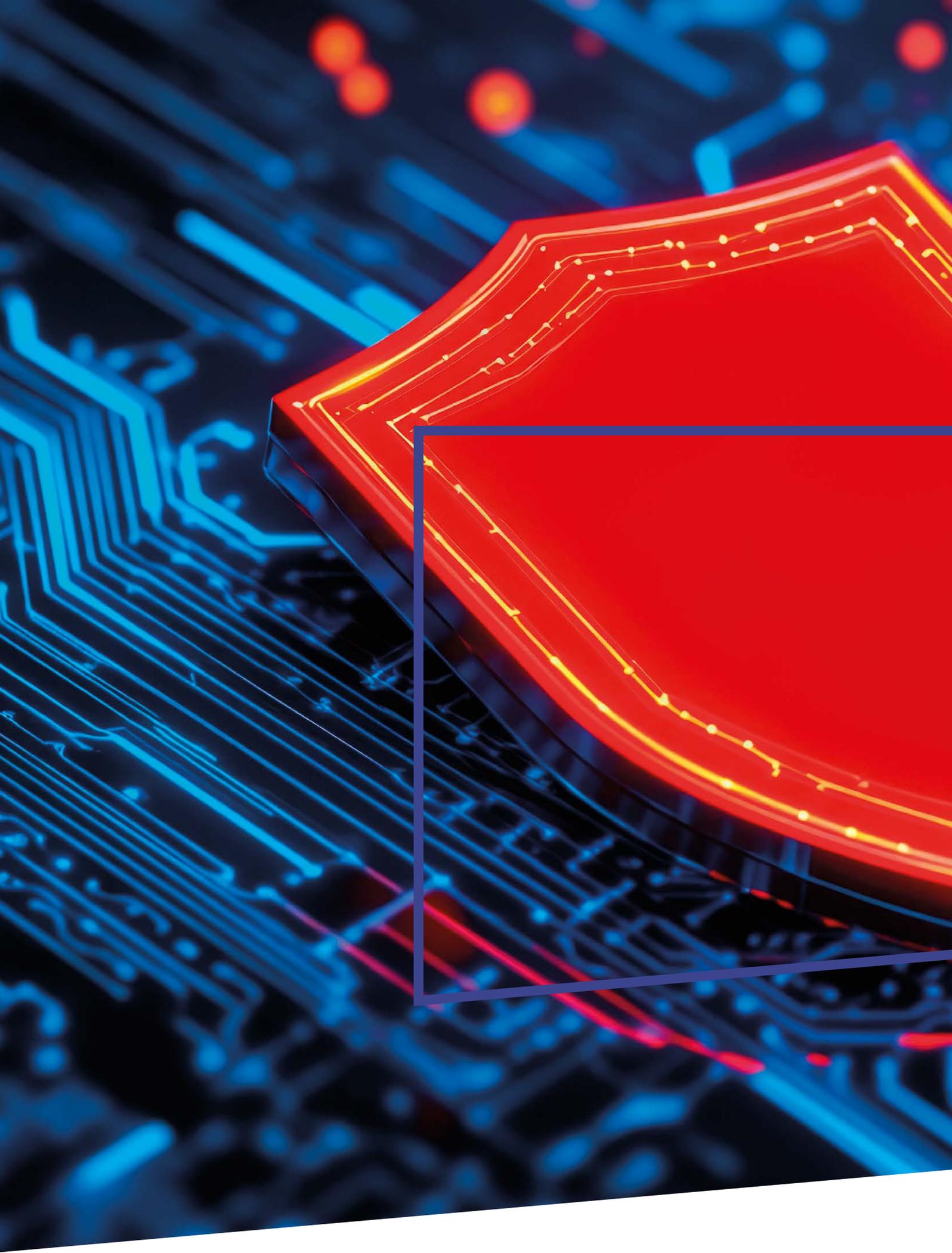
Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents

---

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.

RC.RP-05 The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed

RC.RP-05.1   The integrity of restored systems and assets shall be verified before they are returned to service. Systems and services shall be fully restored, and normal operations shall be confirmed.

Implementation guidance

The goal of this control is to ensure that systems and services are not only restored after an incident, but also verified to be safe, uncompromised, and fully functional before being returned to normal operations.

To achieve this goal the following should be considered:
- Restored systems should be checked for signs of compromise, such as malware or unauthorised access, before being brought back online.
- The root cause of the incident should be identified and addressed to prevent recurrence.
- All recovery actions should be reviewed to ensure they were completed correctly and that no security gaps remain.
- A final check should confirm that the system is safe, complete, and ready for normal use.

RC.RP-06 The end of incident recovery is declared based on criteria, and incident-related documentation is completed

RC.RP-06.1   The end of incident recovery shall be formally declared based on predefined criteria, and all incident-related documentation shall be completed and reviewed.

Implementation guidance

The goal of this control is to ensure that the incident recovery process is formally and responsibly concluded, and that comprehensive documentation is completed to support accountability, learning, and future preparedness.

To achieve this goal the following should be considered:
- An After-Action Report should be prepared that includes:
  - A summary of the incident and its impact.
  - The steps taken to respond and recover.
  - Lessons learned and recommendations for improvement.
- Before declaring the recovery phase complete, the following criteria should be met:
  - All affected systems and services are fully operational.
  - No known threats or vulnerabilities remain in the environment.
  - Data has been restored and verified for integrity.
  - Necessary security patches or updates have been applied.
  - Monitoring is in place to detect any recurring or related issues.
  - The After-Action Report is finalised and reviewed by relevant stakeholders.
  - All stakeholders are informed that the incident has been resolved.

Restoration activities are coordinated with internal and external parties

RC.CO-03 **Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders**

RC.CO-03.1 Recovery activities and progress in restoring operational capabilities shall be communicated to designated internal and external stakeholders in accordance with established communication procedures.

Implementation guidance

The goal of this control is to ensure that recovery efforts and the progress of restoring operational capabilities are clearly and consistently communicated to all relevant internal and external stakeholders. This supports transparency, coordination, and informed decision-making during the recovery phase of an incident.

To achieve this goal the following should be considered:
- Recovery updates, including progress on restoring systems and services, should be shared securely and consistently with internal and external stakeholders, in line with the organisation's response plans and information-sharing agreements.
- Senior leadership should receive regular updates on the status of recovery efforts, especially during major incidents.
- Communication protocols defined in contracts with suppliers and partners should be followed to ensure timely and accurate information exchange.
- Crisis communication with critical suppliers should be coordinated to support aligned recovery actions.
- If no actual incidents have occurred, tabletop exercises should be conducted to test and validate recovery communication procedures and stakeholder coordination.

RC.CO-04 Public updates on incident recovery are shared using approved methods and messaging

RC.CO-04.1 Public updates on incident recovery shall be shared using approved communication methods and messaging, in accordance with established procedures.

Implementation guidance

The goal of this control is to ensure that public communication during the recovery phase of an incident is accurate, timely, and delivered through approved channels, in order to maintain trust, manage reputational risk, and meet legal or regulatory obligations.

To achieve this goal the following should be considered:
- Approved methods for public communication, such as press releases, official websites, or designated spokespersons, should be defined in advance and used consistently.
- Contact information for relevant parties (e.g. internal staff, third-party vendors, law enforcement, cyber insurance providers, government agencies) should be established and maintained.
- Contact lists should be reviewed and verified regularly (e.g. annually) to ensure accuracy.
- Primary and secondary communication mechanisms (e.g. phone calls, emails, letters) should be identified, considering that some methods may be unavailable during an incident.
- Communication protocols and mechanisms should be reviewed periodically or when significant organisational changes occur.
- If no actual incidents have occurred, tabletop exercises or simulations should be conducted to test public communication procedures and ensure readiness.

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 life cycles**

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.

ANNEX B: LIST OF ADDITIONAL KEY MEASURES FOR THE ASSURANCE LEVEL 'IMPORTANT'

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

🛡 Govern

GV.RR-02 **Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced**

GV.RR-02.1 Information security and cybersecurity roles, responsibilities and authorities for employees, suppliers, customers, and partners shall be documented, reviewed, authorised, kept up-to-date, communicated, and coordinated internally and externally.

🛡 Identify

ID.RA-08 **Processes for receiving, analysing, and responding to vulnerability disclosures are established**

ID.RA-08.1 The organisation shall establish and implement a vulnerability management plan to identify, analyse, assess, mitigate and communicate all types of vulnerabilities including in the form of a Coordinated Vulnerability Disclosure (CVD) according to applicable legal modalities.

🛡 Protect

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

PR.AA-03.3 The organisation shall define, document, and implement usage restrictions, connection requirements, and authorisation procedures for remote access to its critical systems. These controls shall ensure that only approved users can connect, using secure methods, with access limited to what is necessary for their role.

PR.PS-01 **Configuration management practices are established and applied**

PR.PS-01.1 The organisation shall develop, document, and maintain a baseline configuration for its business-critical systems.

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

PR.IR-01.3   To ensure operational stability and security, the organisation shall, without exception, identify, document, and control connections between components of its critical systems.

PR.IR-01.4   The organisation shall implement appropriate boundary protection measures to monitor and control communications at external and key internal boundaries of its critical systems, across both IT and OT environments, to ensure secure and reliable operations.

Detect

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

DE.CM-01.3   The organisation shall monitor and identify unauthorised use of its business-critical systems through the detection of unauthorised local connections, network connections and remote connections.

Respond

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

RS.CO-02.2   Cybersecurity incidents shall be shared with relevant external stakeholders within the timeframes defined in the Incident Response Plan, including reporting significant incidents to authorities as required by law.

RS.MI-01   **Incidents are contained**

RS.MI-01.2   The organisation shall detect unauthorised access or data leakage and take appropriate mitigation actions, including monitoring of critical systems at external boundaries and key internal points.

ANNEX C: LIST OF CONTROLS LINKED TO THE MANAGEMENT ASPECTS FOR THE ASSURANCE LEVEL 'IMPORTANT'

GV.RM-01 **Risk management objectives are established and agreed to by organisational stakeholders**

GV.RM-01.1 Information/cybersecurity objectives shall be identified, agreed to by organisational stakeholders and approved by senior management

GV.RM-02 **Risk management objectives are established and agreed to by organisational stakeholders**

GV.RM-02.1 Risk appetite and risk tolerance statements shall be defined, documented, approved by senior management, communicated, and maintained.

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

GV.RM-03.2 Information and Cybersecurity risks shall be documented, as part of the enterprise risk management processes, formally approved by senior management, and updated when changes occur.

GV.RR-02 **Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.**

GV.RR-02.1 Information security and cyber security roles, responsibilities and authorities for employees, suppliers, customers, and partners shall be documented, reviewed, authorised, kept up-to-date, communicated, and coordinated internally and externally.

Identify

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

ID.RA-05.2   The organisation shall conduct and document risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and likelihood of their occurrence.

ID.RA-06   **Risk responses are chosen, prioritised, planned, tracked, and communicated.**

ID.RA-06.1   Risk responses shall be identified, prioritised, planned, tracked and communicated.

ID.IM-04   **Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved**

ID.IM-04.1   Contingency and continuity plans shall be established, communicated, maintained, tested, validated, and improved.

Protect

PR.IR-04   **Adequate resource capacity to ensure availability is maintained.**

PR.IR-04.1   Adequate resource capacity planning shall ensure that availability of organisation's critical system information processing, networking, telecommunications, and data storage is maintained.

Recover

RC.CO-03   **Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders**

RC.CO-03.1   Recovery activities and progress in restoring operational capabilities shall be communicated to designated internal and external stakeholders in accordance with established communication procedures.

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.

All texts, layouts, designs and other elements of any nature in this document are subject to **copyright law**. The reproduction of extracts from this document is authorised for non-commercial purposes only and provided that the source is acknowledged.

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.
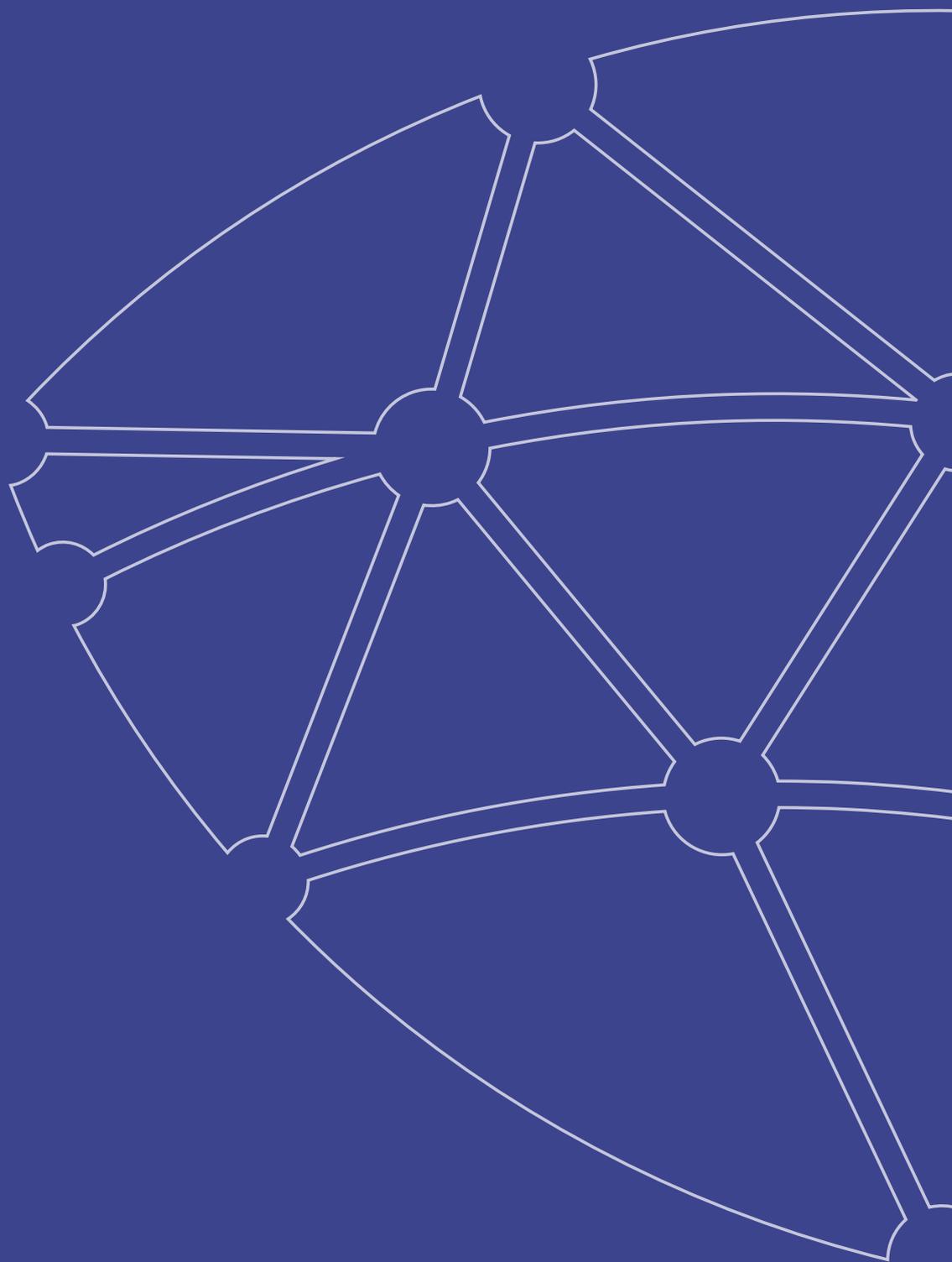· is not necessarily exhaustive, precise, or up to date on all points.