CyFun®

CyberFundamentals 2025

Version 2025-10-01

TABLE OF CONTENTS

INTRODUCTION

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

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

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

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

- **Govern**: Ensures that cybersecurity is treated as a strategic priority, not just a technical issue. It sets clear expectations, policies, responsibilities and authorities, and makes sure these are communicated and reviewed across the organisation.
- **Identify**: Helps build a clear understanding of what matters most to the organisation, such as systems, people, assets, data, and the processes and tools that support operations. This function helps recognise potential cyber threats and lays the foundation for informed decisions about managing cybersecurity risks.
- **Protect**: Involves putting safeguards in place to reduce the chance of a cyber incident or limit its impact. This includes technical measures, processes, and awareness efforts.
- **Detect**: Supports the ability to notice cybersecurity events quickly. Early detection helps reduce harm and allows for faster response.
- **Respond**: Covers the actions taken when a cybersecurity incident occurs. It helps contain the issue, coordinate communication, and reduce disruption.
- **Recover**: Focuses on restoring affected services and operations after an incident. It also includes learning from the event to improve future resilience.

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

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

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

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

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.

At the assurance level **Essential**, the security measures from the assurance level Important are further strengthened to meet the highest cybersecurity requirements. These measures include advanced security features and are designed to withstand sophisticated cyber-attacks carried out by threat actors with significant resources and expertise.

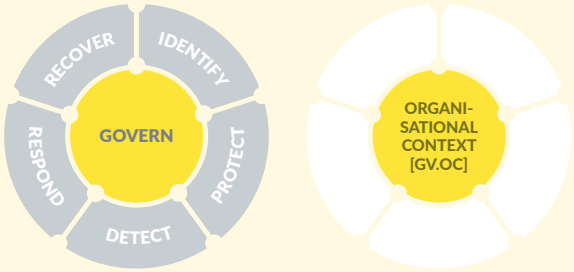
Controls related to **management aspects** have to be reviewed during every certification audit – whether it is an initial audit, a surveillance audit, or a recertification audit – when auditing the CyFun® "Essential" assurance level. These controls correspond to the management system principles that 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 measures**". These shall be addressed at this assurance level, in addition to the key measures already required at the assurance level Basic and the assurance level Important.


POLICIES

GOVERN

Govern



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

GV.OC-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-02 Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered

GV.OC-02.1 **The organisation shall demonstrate it understands and considers the needs and expectations of both internal and external stakeholders regarding information and cybersecurity risk management.**

Implementation guidance

The goal of this control is to ensure that the organisation understands and takes into account the needs and expectations of both internal and external stakeholders when managing information and cybersecurity risks. This helps to align cybersecurity efforts with business priorities, legal obligations, and stakeholder trust.

To achieve this goal, the following should be considered:

- The organisation should identify key internal stakeholders such as employees, senior management, board members, and internal auditors. Their roles, responsibilities, and expectations related to cybersecurity should be understood and documented.
- Key external stakeholders, including customers, suppliers, partners, regulators, shareholders, service providers, and external auditors, should be identified, and their compliance, contractual, and data protection expectations should be considered.
- Stakeholder needs and expectations should be gathered through methods such as interviews, surveys, contract reviews, or regulatory analysis.
- These insights should be integrated into the organisation's cybersecurity risk management strategy to ensure alignment with business and regulatory priorities.
- Regular communication channels should be established to keep stakeholders informed and engaged in cybersecurity matters.
- Stakeholder expectations should be reviewed and updated periodically, especially when there are changes in business operations, legal requirements, or risk exposure.

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-04.3 Redundancy shall be implemented to meet availability requirements as defined by the organisation, legislation and/or regulations

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.

To achieve this goal, the following should be considered:

- The focus of this control is on ensuring that essential services continue to operate even if part of the system fails.
- Redundancy should be built into key components such as data storage, network infrastructure, and critical systems. Examples include:
  - Backup servers, load balancers, RAID arrays, and multiple data centres
  - Failover internet connections and multiple internet service providers (ISPs)
- Critical equipment and services should be protected against power failures and utility disruptions using:
  - Uninterruptible Power Supplies (UPS), backup generators, and redundant power cabling, 2 different power service providers…
  - Regular testing and maintenance contracts to ensure reliability

GV.OC-04.4 Recovery time and recovery point objectives for the resumption of essential ICT/OT system processes shall be defined and monitored.

Implementation guidance

The goal of this control is to ensure that the organisation defines and monitors clear Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for restoring essential ICT and OT system processes after a disruption.

Consider the following elements for defining and monitoring RTO's and RPO's for critical ICT/OT systems:

- Governance & Policy Definition
  - Establish formal policies and accountability for defining and monitoring RTO/RPO.
  - Align recovery objectives with business continuity and disaster recovery frameworks (e.g., ISO 22301, ISO/IEC 27031).
  - Ensure leadership buy-in and regulatory compliance.
- Business Impact Analysis (BIA)
  - Identify interdependencies between ICT and OT systems and their cascading effects on business operations.
  - Determine acceptable downtime thresholds for different system categories.
- Risk & Threat Assessment
  - Perform real-world threat simulations (e.g., ransomware drills, DDoS stress testing).
  - Integrate threat intelligence into recovery planning to anticipate evolving risks.
- Classification & Prioritisation of Systems
  - Define tiered recovery strategies based on business impact (e.g., Tier 1 = immediate restoration, Tier 2 = delayed recovery).
  - Establish failover mechanisms for critical OT processes that must operate continuously.
- Backup & Recovery Strategies
  - Implement immutable backups to protect against ransomware.
  - Ensure offsite and cloud-based recovery options for geographic resilience.
  - Conduct regular validation and integrity checks on backups to prevent failures during recovery.

- Testing & Validation of Recovery Objectives
  - Perform disaster recovery testing (tabletop exercises, full restoration drills).
  - Measure RTO/RPO effectiveness through real-time monitoring and incident response simulations.
  - Establish automated recovery orchestration to speed up resumption of services.
- Continuous Monitoring & Improvement
  - Use real-time analytics to assess deviations from expected RTO/RPO values.
  - Adapt recovery objectives based on lessons learned from incidents and audits.

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.**

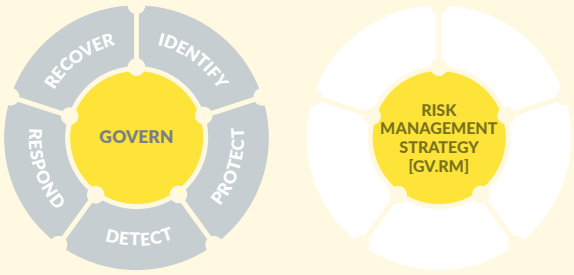
Implementation guidance

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

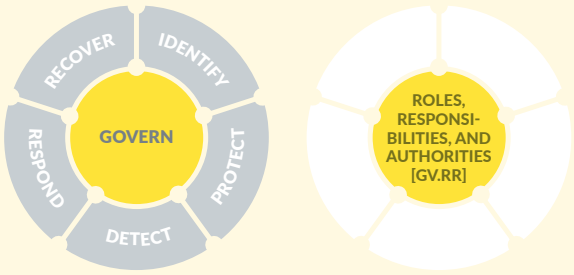
The aim of this control is to ensure that cybersecurity and information security risk information is shared effectively across the organisation and with external parties.

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-01 Organisational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving

GV.RR-01.1 Organisation's top management shall be responsible and accountable for cyber-security risk and shall foster a culture that is risk-aware, ethical, and continually improving.

Implementation guidance

The goal of this control is to ensure top management is accountable for cybersecurity risk and promotes a risk-aware and continuously-improving culture.

To make this happen, the following should be considered:

- Organisations' top management should agree on their roles and responsibilities in developing, implementing, and assessing the organisation's cybersecurity strategy.
- The expectations of organisations top management regarding a secure culture, including highlighting positive or negative examples of cybersecurity risk management, should be shared with the entire organisation.
- Organisations top management should direct the senior-level executive (information) security officer (e.g. CSO, CISO) to maintain a comprehensive cybersecurity risk strategy and review and update it at least annually and after major events (see also GV.RR-02.2).
- Reviews should be conducted to ensure adequate authority and coordination among those responsible for managing cybersecurity risk.

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-02.2 The organisation shall appoint a senior-level executive information security officer.

Implementation guidance

The goal of this control is to establish clear executive accountability for cybersecurity by appointing a senior leader to drive strategy, oversight, and alignment with business objectives.

To achieve this goal, the following should be considered:

- A senior executive is defined as a high-ranking member of the organisation involved in major decision-making processes.
- The senior-level executive information security officer, which could be the Chief Information Security Officer (CISO), should have the authority, responsibility and resources to coordinate, develop, implement, monitor, and maintain an organisation-wide vision, strategy, and program to ensure that information assets and technologies are adequately protected.

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 cyber security 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.

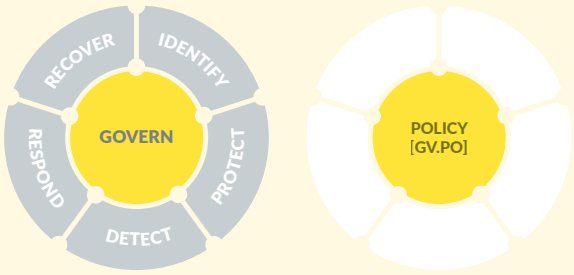
GV.RR-04.2 A cybersecurity process for human resources shall be developed and maintained applicable at recruitment, during employment and at termination of employment.

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

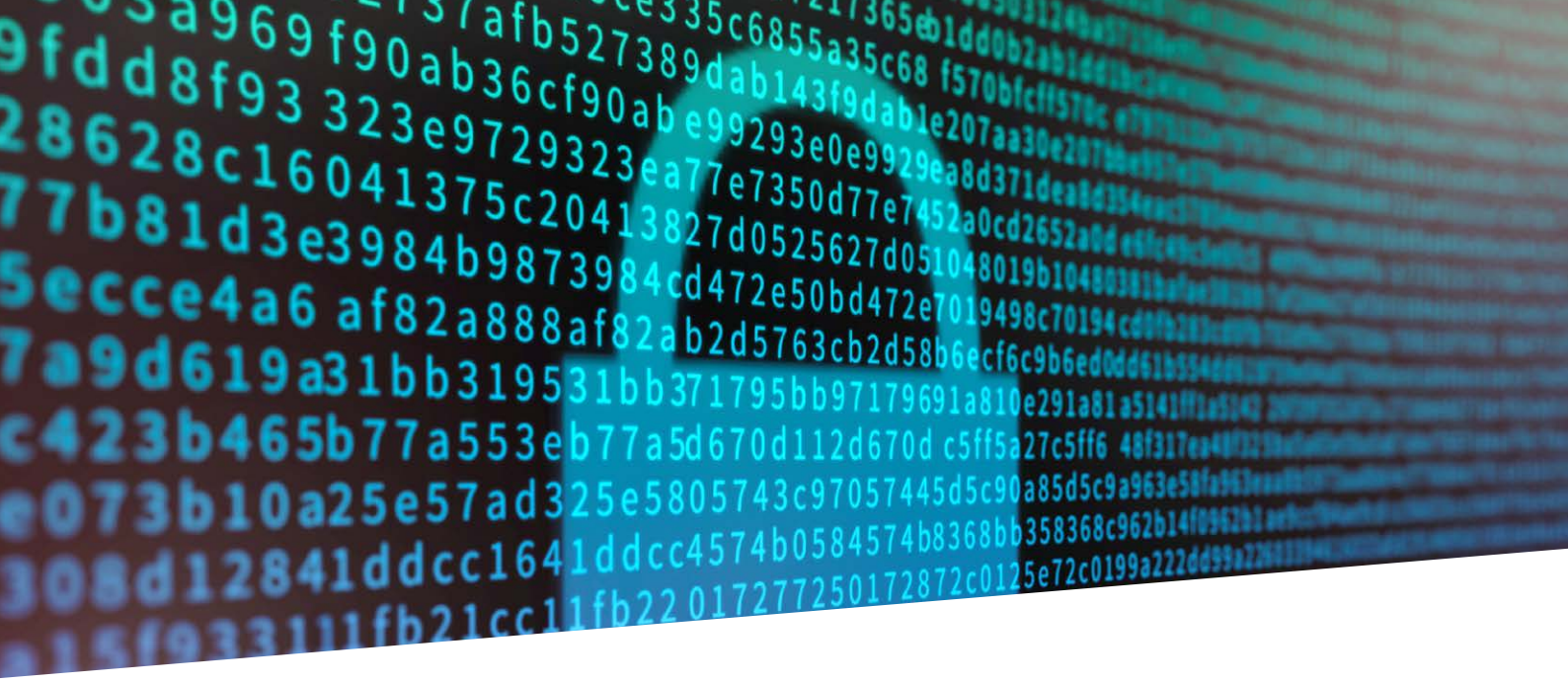
GV.PO-01.1 Policies and procedures for managing information and cybersecurity shall be established, documented, reviewed, approved, updated when changes occur, communicated and enforced.

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.

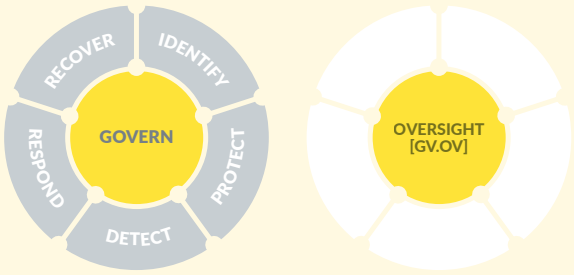


GV.PO-01.2 **Organisational-wide information and cybersecurity policies and procedures shall include the use of cryptography and, where appropriate, encryption, reflect changes in requirements, threats, technology and organisational roles, and be approved by senior management, who oversee its implementation.**

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.



Results of organisation-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy

GV.OV-02 The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organisational requirements and risks

GV.OV-02.1 The information and cybersecurity risk management strategy shall be reviewed and adjusted to ensure coverage of organisational requirements and risks.

Implementation guidance

The goal of this control is to ensure that the information and cybersecurity risk management strategy is regularly reviewed and updated to reflect organisational needs, evolving risks, and compliance requirements.

To achieve this goal, the following should be considered:

- The strategy should define the overall direction and goals for managing information and cybersecurity risks.
- Supporting policies and procedures should guide how the strategy is implemented in practice.
- The strategy should address risks to organisational operations, assets, individuals, and other entities, including potential privacy impacts.
- Reviews should be conducted at planned intervals, including through internal audits, based on a documented audit program that defines frequency, methods, responsibilities, and reporting.
- Audits should be carried out by competent and impartial personnel.
- Audit results should be reviewed to assess whether the strategy meets internal expectations and complies with legal and regulatory requirements.
- The strategy should be updated when necessary, especially after incidents or audit findings.
- Evidence of audit activities and outcomes should be documented and reported to relevant management.

GV.OV-03 Organisational cybersecurity risk management performance is evaluated and reviewed for adjustments needed

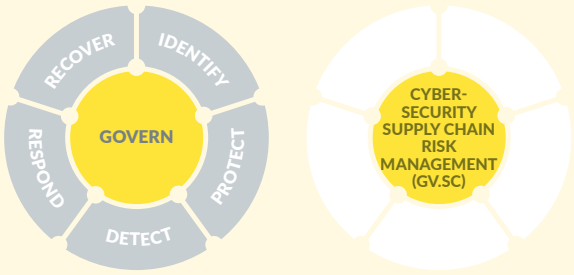
GV.OV-03.1 The organisation's cybersecurity risk management performance shall be evaluated, reviewed and adjusted when necessary

Implementation guidance

The goal of this control is to ensure that an organisation's cybersecurity risk management performance is continuously evaluated, reviewed, and adjusted as necessary.

To achieve this goal, the following should be considered:

- Key Performance Indicators (KPIs) should be identified, implemented and regularly reviewed to ensure that organisation-wide policies and procedures achieve the information- and cybersecurity objectives.
- Key information and cybersecurity-related risk indicators should be regularly assessed to identify risks to the organisation, including likelihood and potential impact. Information and cybersecurity-related risk indicators are for example:
  - Number of cyber-attacks detected
  - Number of data leaks detected
  - Time to detection
  - Time to recovery
  - Number of devices not managed by the organisation
  - Level of access different users have to sensitive data
  - Number of not-up-to-date software and systems
  - Number of unmanaged network connections
- Metrics on information- and cybersecurity risk management should be collected and shared with senior leadership.



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

GV.SC-01 A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organisational stakeholders

GV.SC-01.1 A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes shall be documented, reviewed, updated when changes occur, and approved by organisational stakeholders.

Implementation guidance

The goal of this control is to ensure supply chain cybersecurity risks are proactively managed through a documented, stakeholder-approved, and regularly updated risk management program.

The steps below should be considered for organisations to establish a cybersecurity supply chain risk management (C-SCRM) program that is aligned with their strategic objectives and supported by all relevant stakeholders:

Define the Program and Strategy

- **Identify Objectives**: Clearly define what the organisation aims to achieve with its C-SCRM program. Objectives might include protecting against supply chain attacks, ensuring compliance with regulations, and maintaining business continuity.
- **Develop a Strategy**: Outline a high-level strategy that aligns with the organisation's overall cybersecurity and business strategies. This should include risk assessment, risk mitigation, and continuous monitoring plans.

Engage Stakeholders

- **Identify Stakeholders**: Determine who the key stakeholders are, including executives, IT, procurement, legal, and compliance teams.
- **Stakeholder Involvement**: Engage stakeholders early in the process to ensure their input and buy-in. This can be done through workshops, meetings, and regular updates.

Establish Policies and Processes

- **Develop Policies**: Create comprehensive documented policies that cover all aspects of C-SCRM, including vendor risk management, incident response, and compliance requirements.
- **Implement Processes**: Define and document processes for risk assessment, vendor evaluation, contract management, and incident response. Ensure these processes are integrated into existing business workflows.

Risk Assessment and Management
- **Conduct Risk Assessments**: Regularly assess risks associated with the supply chain, including potential vulnerabilities and threats.
- **Mitigate Risks**: Develop and implement risk mitigation strategies based on the assessment results. This might include diversifying suppliers, enhancing security controls, and establishing contingency plans.

Continuous Monitoring and Improvement
- **Monitor Continuously**: Implement continuous monitoring of the supply chain to detect and respond to new risks promptly. This includes monitoring supplier performance and compliance.
- **Review and Improve**: Regularly review the effectiveness of the C-SCRM program and make improvements as needed. This should include feedback from stakeholders and lessons learned from incidents.

Training and Awareness
Educate Employees: Provide training and awareness programs for employees to understand their roles in C-SCRM. This includes recognising supply chain risks and following established policies and procedures.

Documentation and Communication
- **Document Everything**: Ensure all policies, processes, risk assessments, and mitigation plans are well-documented, kept up to date, approved by relevant management and accessible to relevant stakeholders.
- **Communicate Effectively**: Maintain open lines of communication with stakeholders to keep them informed about the program's progress, changes, and any incidents that occur.

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-03 Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes

GV.SC-03.1 **Information- and Cybersecurity supply chain risk management shall be integrated into information/cybersecurity and enterprise risk management, risk assessment, and improvement processes.**

Implementation guidance

The goal of this control is to ensure supply chain cybersecurity risks are consistently identified, assessed, and mitigated by embedding them into enterprise risk assessments, control reviews, and continuous improvement cycles.

To effectively integrate supply chain risk management into broader cybersecurity and enterprise risk frameworks, organisations should consider to:

Identify Alignment and Overlap

- Map existing information/cybersecurity risk management and enterprise risk management (ERM) processes.
- Identify touchpoints where supply chain risks intersect with:
  - Vendor management
  - Procurement
  - Business continuity
  - Legal and compliance
- Document areas of overlap, duplication, or gaps to streamline integration.

Establish Integrated Control Sets

- Develop a unified control framework that includes:
  - Controls specific to supply chain cybersecurity (e.g., third-party access, data handling, software integrity).
  - Controls from existing cybersecurity standards (e.g., ISO/IEC 27036).
- Ensure controls are risk-based, scalable, and aligned with both IT and OT environments.

Embed in Risk Assessment Processes

- Include supply chain-specific threat scenarios in risk assessments (e.g., supplier compromise, counterfeit hardware, software vulnerabilities).
- Evaluate supplier criticality and risk exposure as part of the enterprise risk register.
- Use tiered risk assessments based on supplier impact and sensitivity of services/data.

Integrate into Continuous Improvement

- Incorporate supply chain risk insights into:
  - Lessons learned from incidents and audits
  - Post-mortem reviews of supplier-related disruptions
  - Process improvement cycles (e.g., PDCA)
- Update policies, procedures, and controls based on evolving threats and supplier performance.

Escalate Material Risks to Senior Management

- Define criteria for materiality (e.g., financial impact, regulatory exposure, operational disruption).
- Establish a formal escalation path to senior leadership and risk committees.
- Ensure material supply chain risks are:
  - Reflected in the enterprise risk register
  - Addressed in strategic risk discussions
  - Considered in business continuity and crisis management planning

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-05.2 Contractual information/cybersecurity requirements for suppliers and external partners shall be implemented to ensure a verifiable flaw resolution process and to ensure that deficiencies identified during information/cybersecurity testing and evaluation are remedied.

Implementation guidance

The goal of this control, which is related to GV.SC-09.1, is to embed enforceable requirements in supplier contracts to guarantee timely flaw remediation and resolution of cybersecurity issues identified through testing and evaluation.

To achieve this goal, the following should be considered:

- Information systems containing software (or firmware) affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) should be identified.
- Newly released security relevant patches, service packs, and hot fixes should be installed, and these patches, service packs, and hot fixes are tested for effectiveness and potential side effects on the organisation's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation should be incorporated into configuration management as an emergency change.
- Consider to contractually require suppliers to disclose information/cybersecurity features, functions, and vulnerabilities of their products and services for the life of the product or the term of service.
- Consider to contractually require suppliers to provide and maintain a current component inventory (e.g. software or hardware bill of materials) for critical products.

GV.SC-05.3 The organisation shall establish contractual requirements permitting the organisation to review the information/cybersecurity programs implemented by suppliers and third-party partners.

Implementation guidance

The goal of this control is to ensure that the organisation can assess and verify the information/cybersecurity practices of suppliers and third-party partners through contractual agreements.

To achieve this goal:

- Information/Cybersecurity Requirements
  Contracts should define clear information/cybersecurity expectations, including OT-specific controls where relevant.
- Audit and Review Rights
  Agreements should grant the organisation the right to audit, assess, or review the information/cybersecurity programs of suppliers and partners.
- Verification Methods
  Conformance should be verified through self-assessments, third-party certifications, or scheduled security evaluations.
- Information Sharing Protocols
  Contracts should specify what information/cybersecurity-related information must be shared, how often, and through which channels.
- Continuous Monitoring
  Suppliers should regularly report on their information/cybersecurity posture and disclose incidents that could impact operations, especially in OT environments.
- Non-Compliance Consequences
  Contracts should outline consequences for failing to meet information/cybersecurity requirements, such as penalties or contract termination.

GV.SC-06 Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

GV.SC-06.1 Planning and due diligence shall be carried out to reduce risks before entering into formal relationships with suppliers or other third parties.

Implementation guidance

The goal of this control is to reduce cybersecurity and operational risks by ensuring that appropriate planning and due diligence are conducted before entering into formal relationships with suppliers or third parties.

To achieve this goal:

- Risk-Based Due Diligence
  Due diligence should be performed on prospective suppliers in line with the organisation's procurement policy and scaled to the level of risk, criticality, and complexity of the relationship.
- Cybersecurity and Risk Capability Assessment
  The cybersecurity maturity, risk management practices, and OT-specific capabilities of suppliers should be evaluated for suitability.
- Supplier Risk Assessments
  Risk assessments should be conducted to ensure alignment with business needs and applicable cybersecurity requirements, including those relevant to OT environments.
- Product Integrity and Security
  The authenticity, integrity, and security of critical products and components should be verified before acquisition and deployment, especially in OT systems where vulnerabilities can impact safety and operations.

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-07.2 A documented list of all critical suppliers, vendors and partners of the organisation that may be involved in a major incident shall be established, kept up-to-date and made available online and off-line with due regard to confidentiality and security.

Implementation guidance

The goal of this control is to ensure that a reliable, up-to-date list of critical suppliers, vendors, and partners is maintained and accessible, both online and offline, to support rapid response during major incidents, while safeguarding confidentiality and security.

To achieve this goal:

- **Maintain a Comprehensive Record**
  A complete list of suppliers, vendors, and partners should be maintained as a foundation for identifying those critical to operations, including OT environments.
- **Define Criticality Criteria**
  Clear criteria should be established to classify supplier criticality based on factors such as:
  - Sensitivity of data handled
  - Access to systems or networks
  - Importance to core business or OT functions
- **Document Key Information**
  For each critical supplier, the list should include:
  - Primary and secondary contact details
  - Description of services provided
  - Escalation paths and support availability
- **Ensure Online and Offline Availability**
  The list should be:
  - Regularly updated and securely stored
  - Accessible both online and offline (e.g. printed copies, encrypted USBs) to ensure availability during cyber incidents or outages

GV.SC-07.3 The organisation shall audit business-critical third-party service providers for security compliance.

Implementation guidance

The goal of this control is to ensure that business-critical third-party service providers are regularly audited to confirm conformance with agreed-upon security requirements, helping to manage risks to operations and critical systems.

To achieve this goal:

- **Identify Critical Providers**
  The criticality of third-party service providers should be assessed based on their impact on operations, including OT systems, and the level of risk they introduce.
- **Acceptable Audit Evidence**
  Third-party audit results, such as certifications, independent assessments, or security attestations, should be accepted as valid evidence of conformance where appropriate.
- **Conduct Security Audits**
  Regular audits should be performed on critical providers to verify that they meet contractual and policy-based security obligations.

GV.SC-07.4 The organisation shall ensure conformity with information/cybersecurity contractual obligations by suppliers and third-party partners through regular reviews of independent audits, assessments, and third-party evaluations.

Implementation guidance

The goal of this control is to ensure that suppliers and third-party partners conform to contractual information and cybersecurity obligations through regular reviews of independent audits, assessments, and third-party evaluations.

To achieve this goal:

- **Build on Related Controls**
  This control should be implemented in alignment with GV.SC-05.3 and GV.SC-07.1 to strengthen supplier oversight.
- **Integrate Risk Assessments**
  Independent audits and third-party assessments should include evaluations of corporate and applicable cybersecurity requirements, including supply chain and OT-specific risks.
- **Pre-Engagement Verification**
  Before engaging with critical suppliers, independent evaluations should be reviewed to confirm conformance with agreed cybersecurity standards and obligations.
- **Risk-Based Review Depth**
  The depth and frequency of reviews should be adapted based on the criticality of the supplier's products or services. More critical suppliers should undergo more thorough evaluations.

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.

GV.SC-09 Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle

GV.SC-09.1 Supply chain security practices shall be integrated into information/cybersecurity and enterprise risk management programs, and their performance shall be monitored throughout the product and service life cycle.

Implementation guidance

The goal of this control is to ensure that supply chain security practices are embedded into the organisation's information security, cybersecurity, and enterprise risk management programs, with performance monitored and improved throughout the lifecycle of products and services.

To achieve this goal:

- **Align with Related Controls**
  This control builds on GV.SC-05.2 by ensuring that contractual information and cybersecurity requirements, such as flaw resolution and remediation of identified deficiencies, are actively managed within broader risk programs.
- **Establish Governance Foundations**
  Supply chain security policies should be documented, covering both information and cybersecurity expectations for suppliers and third parties.
- **Integrate into Risk Frameworks**
  Supply chain risks should be embedded in enterprise and information security risk management frameworks, including OT-specific risks and dependencies.
- **Formalise Security Expectations**
  Contracts and SLAs should include clear clauses on information and cybersecurity, audit rights, and performance metrics.
- **Monitor and Evaluate Performance**
  Risk assessments, audit reports, and incident records should be reviewed regularly to assess supplier posture and identify areas for improvement.
- **Enable Continuous Monitoring**
  Monitoring tools and KPIs should be used to track supplier security performance across the lifecycle, including incident response times and conformance rates.
- **Support Awareness and Training**
  Training and awareness programs should address supply chain-related information and cybersecurity risks for both internal teams and suppliers.
- **Ensure Lifecycle Coverage**
  Documentation should demonstrate that supply chain security is considered from procurement through to decommissioning, especially for OT systems and components.

GV.SC-010 Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

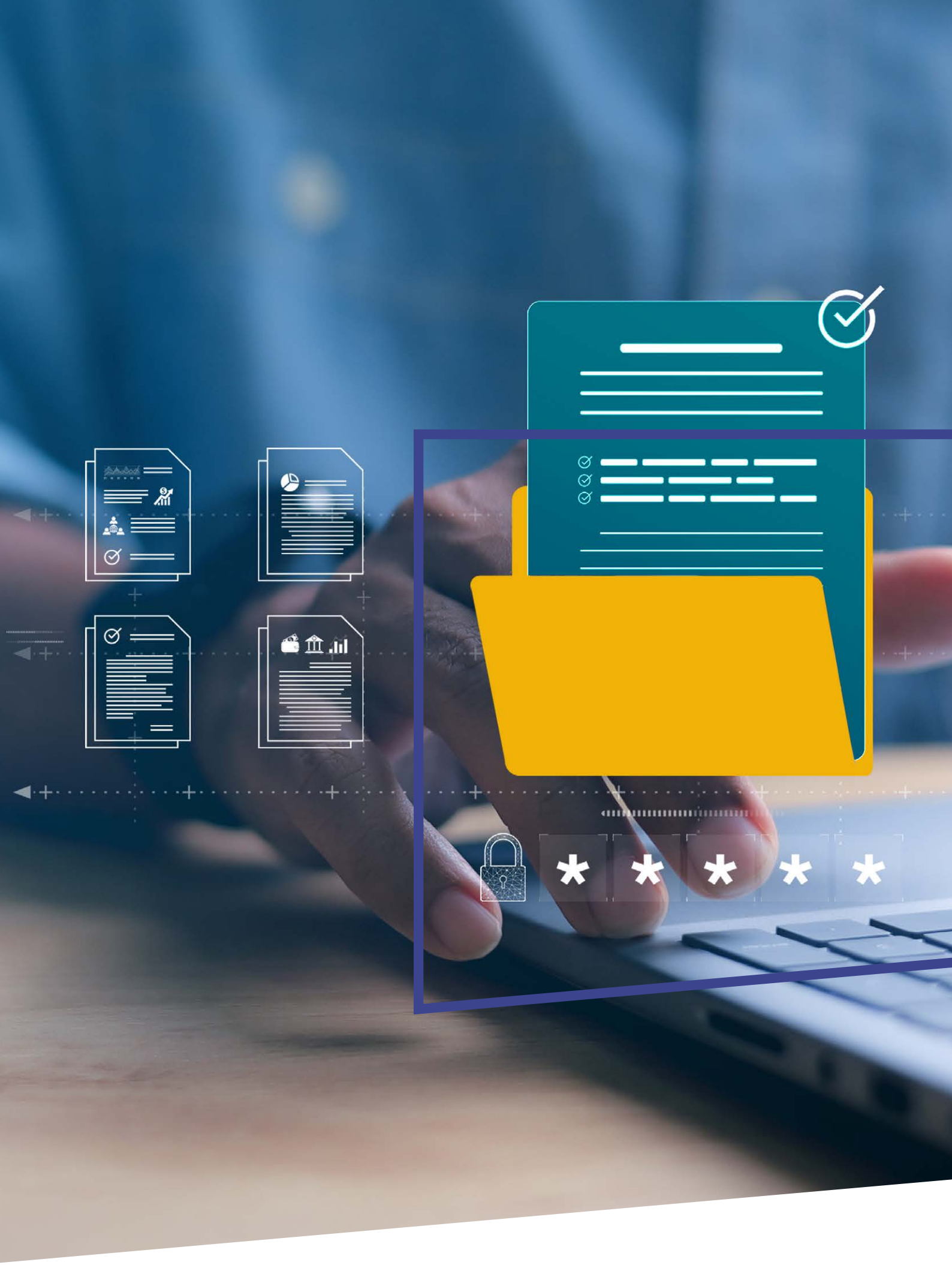
GV.SC-10.1 **Cybersecurity supply chain risk management plans shall include actions and responsibilities for managing risks that may arise after a supplier relationship or service agreement has ended.**

Implementation guidance

The goal of this control is to ensure that residual cybersecurity and information security risks are effectively addressed after supplier relationships end, thereby preventing disruptions, data exposure, and vulnerabilities in operational and OT environments.

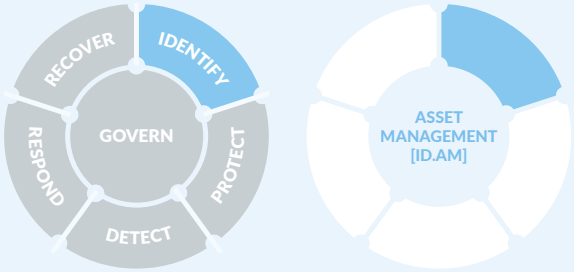
To achieve this goal:

- **Plan for Termination of the Relationship**
  Formal offboarding procedures should be defined for ending supplier relationships under both normal and adverse conditions, including breach, insolvency, or security incidents.
- **Ensure Secure Transition or Exit**
  Transition plans should be developed for critical services, to maintain continuity and address supply chain resilience, including fallback suppliers or internal alternatives.
- **Revoke Access and Secure Data**
  Supplier access to systems, networks, and data should be promptly revoked. All credentials and remote access tools should be deactivated or removed.
- **Protect Organisational Assets**
  Devices, storage media, and documents containing organisational data should be securely returned or sanitised. Controls should prevent unauthorised retention or leakage of sensitive information.
- **Address Component Obsolescence**
  Plans should be in place to manage end-of-life components or services, ensuring continued support or secure replacements, especially for OT systems.
- **Monitor Residual Risks**
  Post-termination risks should be identified, assessed, and escalated to senior management when necessary. These risks should be tracked within the enterprise risk management process.



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-01.4 **Mechanisms for detecting the presence of unauthorised hardware and firmware components within the organisation's ICT/OT environment shall be identified.**

Implementation guidance

The goal of this control is to proactively identify unauthorised hardware and firmware components within ICT and OT environments, thereby enabling timely response and reducing the risk of compromise or operational disruption.

To achieve this goal:

- **Automate Where Feasible**
  Detection mechanisms should be automated where safe and technically possible, especially in complex or high-risk environments.
- **Continuously Monitor Networks**
  Networks should be continuously monitored to detect new or unauthorised hardware and firmware components. Detected changes should trigger automatic updates to the asset inventory.
- **Establish a Response Process**
  A defined process should exist to regularly review and address unauthorised components.
  - For unauthorised hardware, refer to **ID.AM-01.3**
  - For unauthorised firmware, refer to **ID.AM-02.4**
- **Include OT-Specific Considerations**
  Detection methods in OT environments should account for safety, availability, and vendor-specific constraints when identifying unauthorised components.

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-02.5 Mechanisms for detecting the presence of unauthorised software within the organisation's ICT/OT environment shall be identified.

Implementation guidance

The goal of this control is to ensure that mechanisms are in place to detect unauthorised software across ICT and OT environments, thereby enabling timely response and maintaining an accurate software inventory.

To achieve this goal:

- **Automate Where Feasible**
  Detection mechanisms should be automated where safe and technically appropriate, especially in complex or high-risk environments.
- **Monitor All Platforms**
  All platforms, including physical systems, virtual machines, containers, and embedded OT systems, should be continuously monitored for new or unauthorised software. Detected changes should trigger automatic updates to the software inventory.
- **Establish a Review Process**
  A process should be in place to regularly investigate and address unauthorised software. When unauthorised software is detected, **ID.AM-02.4** should be applied.
- **Adapt Detection to OT Environments**
  In OT environments, detection mechanisms should be tailored to avoid operational disruption. Passive monitoring, vendor-approved tools, and scheduled scans should be considered to ensure safety and system availability.

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-03-3 The organisation's network communication and external data flows shall be mapped, documented, authorised, and updated when changes occur.

Implementation guidance

The goal of this control is to ensure that external network communications are clearly understood, controlled, and monitored to reduce the risk of unauthorised access, data leakage, or service disruption across ICT and OT environments.

To achieve this goal:

- Map and Document External Flows
  Communication and data flows between the organisation and external parties should be mapped, documented, and authorised. These records should be updated when changes occur.
- Enforce Access Controls
  Network connections should be restricted to explicitly authorised interfaces to reduce the attack surface and prevent unauthorised data transfers.
- Enhance Monitoring When Needed
  Monitoring should be intensified in response to elevated risk levels. This may include real-time alerts, enhanced logging, or more frequent audits of external network activity.
- Prevent Information Leakage
  The risk of data leakage through electromagnetic emissions or side-channel attacks should be assessed. Where appropriate, mitigation measures such as EMSEC or TEMPEST controls should be applied, especially for systems handling sensitive or classified information.

The two controls — ID.AM-03-3 and ID.AM-04.2 — are closely related but focus on different scopes of information flow and network activity. This control, ID.AM-03-3, covers network-layer interactions with external entities, including:

- Internet traffic (e.g., outbound web access, DNS queries, email traffic).
- VPN connections, remote access, and cloud service communications.
- Any communication that traverses the organisational perimeter, regardless of whether it involves a specific external system.

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-04.2 **The organisation shall map, document and authorise the flow of information to/from external systems and update the flow when changes occur.**

Implementation guidance

The goal of this control is to ensure that the flow of information to and from external systems is clearly understood, securely managed, and kept up to date to reduce the risk of data leakage, unauthorised access, or disruption across ICT and OT environments.

To achieve this goal:

- **Identify and Map Data Pathways**
  All pathways through which data enters or exits the organisation's systems should be identified and documented. This includes functions, ports, protocols, and services used in both IT and OT environments.
- **Document Data Flows in Detail**
  Records should describe the types of data being transferred, the systems involved, and the security measures applied (e.g. encryption, authentication, access controls). This supports transparency and secure data handling.
- **Authorise and Control Access**
  Only designated and authorised personnel should be allowed to approve and manage data transfers. This helps prevent unauthorised access and ensures accountability.
- **Review and Update Regularly**
  Information flow documentation should be reviewed and updated whenever systems, processes, or external connections change. This ensures that controls remain effective and aligned with the current environment.

The two controls — ID.AM-03-3 and ID.AM-04.2 — are closely related but focus on different scopes of information flow and network activity. This control focuses on granular, content-specific data flows between the organisation and specific external systems. It includes:

- Data transfers to/from third-party platforms such as CRM systems, cloud storage providers, and external APIs.
- File transfers, API calls, and database synchronisation with external systems.

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-08.5 The organisation shall ensure that disposal actions are approved, tracked, documented, and verified.

Implementation guidance

The goal of this control is to ensure that all disposal actions involving information systems, data, or physical assets are properly authorised, traceable, and verifiable to reduce risks, maintain compliance, and protect sensitive information, especially in operational technology (OT) environments.

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

- **Approval**: Disposal actions should be reviewed and approved by authorised personnel before execution. This ensures alignment with internal policies and external regulations.
- **Tracking**: Each disposal action should be logged with key details, including the asset or media type, disposal method, date, and individuals involved.
- **Documentation**: All steps, from approval to verification, should be clearly documented. This includes approval records, tracking logs, and any supporting evidence.
- **Verification**: Disposal should be verified to confirm it was completed correctly. This may involve checking that data was securely wiped or that physical destruction was effective.

This structured approach helps maintain accountability and security, particularly in OT environments where improper disposal can lead to operational disruptions or safety risks.

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-08.7 **The organisation shall prevent unauthorised removal of maintenance equipment containing critical system information of the organisation.**

Implementation guidance

The goal of this control is to prevent unauthorised removal of maintenance equipment that may contain critical system information, reducing the risk of data leakage or theft, especially in operational technology (OT) environments.

To achieve this goal, the following measures should be applied:

- **Verify**: Maintenance equipment should be checked to confirm it does not contain organisational information before removal
- **Sanitise or Destroy**: If sensitive data is present, the equipment should be sanitised or securely destroyed according to approved procedures.
- **Retain Within Facility**: Equipment should remain within the facility unless removal is strictly necessary.
- **Obtain Exemption**: If removal is required, explicit authorisation should be obtained from designated personnel or roles.

Maintenance equipment in this context refers to hardware temporarily used for servicing or diagnostics, such as external drives, temporary servers, or specialised OT/ICS tools, not regular maintenance tools covered under control ID.AM-08.9.

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-08.9 **Maintenance tools and portable storage devices shall be inspected as they enter the facility and shall be protected by anti-malware solutions that scan them for malicious code before they are used on the organisation's systems.**

Implementation guidance

The goal of this control is to prevent the introduction of malicious code into organisational systems, by ensuring that all maintenance tools and portable storage devices are inspected and scanned before use. In OT environments, introducing unverified tools or storage devices can compromise system integrity and disrupt critical physical operations.

To achieve this goal, the organisation should:

- **Inspect on Entry**: Maintenance tools and portable storage devices should be inspected when entering the facility, to detect unauthorised or suspicious items.
- **Scan for Malware**: All devices should be scanned using up-to-date anti-malware solutions before being connected to organisational systems.
- **Apply to All Tool Types**: This includes software tools (e.g. diagnostic software, firmware updaters, configuration tools, remote access tools), portable storage (e.g. USB drives, external hard drives, SD cards), and hardware tools (e.g. laptops, tablets, portable diagnostic devices).
- **Use Non-Destructive Clean-Up**: When devices are newly acquired or lack a trusted chain of custody, non-destructive sanitisation techniques should be applied before first use.
- **Ensure Conformance and Compliance**: All actions should conform to internal procedures and comply with applicable cybersecurity regulations and industry standards.

ID.AM-08.10 The organisation shall verify security controls following maintenance or repairs/ patching, and take action as appropriate.

Implementation guidance

The goal of this control is to ensure that security controls remain effective after maintenance, repairs, or patching activities. In OT environments, even small configuration changes can have significant safety or operational consequences, making post-maintenance verification critical.

To achieve this goal, the organisation should:

- **Verify Security Controls**: After maintenance, systems should be assessed to confirm that no changes have weakened security. This includes checking configurations, access permissions, and other security-relevant settings.
- **Update Records**: Any changes made during maintenance should be documented, including updates to security controls or the implementation of new measures.
- **Report Issues**: If security concerns are identified during verification, findings should be communicated to relevant stakeholders, to ensure awareness and coordinated response.
- **Take Corrective Action**: If controls are found to be inadequate or compromised, corrective actions should be taken. This may include reconfiguring settings, applying additional patches, or strengthening existing controls.
- **Ensure Conformance and Compliance**: All verification and corrective actions should conform to internal procedures and comply with applicable laws, regulations, and industry standards.

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.

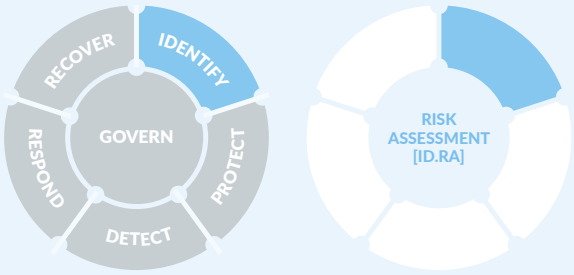
ID.AM-08.13 **The organisation shall require remote maintenance diagnostic services to be performed from a system that implements security features similar to the security features implemented on the equivalent organisation's critical system.**

Implementation guidance

The goal of this control is to ensure that remote maintenance and diagnostic services are performed from systems that implement security features equivalent to those of the organisation's critical systems. In Operational Technology (OT) environments, this alignment is essential to maintain a consistent security posture, prevent the introduction of vulnerabilities, and protect the safety, reliability, and continuity of physical operations.

To achieve this goal, the organisation should:

- **Use Strong Authentication**: Remote systems should implement multi-factor authentication to ensure access is restricted to authorised personnel.
- **Maintain Activity Records**: Detailed logs of all remote maintenance activities should be maintained and reviewed regularly to detect anomalies or unauthorised actions.
- **Align Tools and Procedures**: All tools and procedures used during remote maintenance should align with organisational policies and be documented in the relevant cybersecurity or information security plans.
- **Terminate Sessions**: Remote sessions should be properly terminated once maintenance is complete, to prevent lingering access.
- **Ensure Conformance and Compliance**: Remote systems and activities should conform to internal security requirements 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-01.4 **To ensure that organisation's operations are not adversely affected by the testing process, performance/load testing and penetration testing on the organisation's systems shall be carried out with care.**

Implementation guidance

The goal of this control is to ensure that performance/load testing and penetration testing are conducted carefully to avoid disrupting operations or compromising system stability, especially in environments with business-critical or safety-critical systems.

To achieve this goal, the organisation should:

- **Establish and Maintain Test Programs**
  Test programs for performance/load testing and penetration testing should be tailored to the organisation's size, complexity, and maturity, including OT-specific constraints.
- **Use Controlled Testing Environments**
  Penetration testing should be conducted in isolated or controlled environments where possible to prevent unintended impacts on live OT systems.
- **Engage Qualified Ethical Hackers**
  Experienced ethical hackers should be used to perform penetration testing, particularly in complex or sensitive OT environments.
- **Validate Security Measures Post-Test**
  After testing, security controls should be revalidated to confirm that defences remain effective and no unintended changes have occurred.

Distinction from ID.RA-01.5 (CyFun® Important)

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-01.5 **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-02.2 Automated mechanisms shall be implemented to disseminate security alerts and advisories to relevant organisation stakeholders.

Implementation guidance

The goal of this control is to ensure that security alerts and advisories are delivered promptly and reliably to relevant stakeholders through automated mechanisms, enabling timely awareness and response across the organisation.

To achieve this goal, the organisation should:

- Implement Centralised Security Platforms
  Solutions such as SIEM (Security Information and Event Management), XDR (Extended Detection and Response), SOAR (Security Orchestration, Automation, and Response), or UEBA (User and Entity Behaviour Analytics) should be used to collect, analyse, and correlate alerts from multiple sources, including OT and IT systems.
- Automate Alert Distribution
  Alerts should be configured to automatically notify stakeholders via email, messaging platforms, or other channels to ensure rapid dissemination of critical information.
- Use Real-Time Dashboards
  Dashboards should be implemented to provide continuous visibility into security alerts and advisories, supporting situational awareness and decision-making.

- **Integrate with Incident Response Platforms**
  Automated mechanisms should support the distribution of alerts to incident response teams, ensuring they have the latest information to act effectively.
- **Pull from External Threat Intelligence Sources**
  Automated tools should retrieve data from trusted external sources to enrich internal alerts with broader threat context, including OT-specific advisories.

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-05.3 Risk assessment results shall be disseminated to relevant stakeholders.

Implementation guidance

The goal of this control is to ensure that risk assessment results are communicated effectively to relevant stakeholders, enabling informed decisions and coordinated responses across the organisation.

To achieve this goal, the organisation should:

- **Define a Communication Plan or Procedure**
  A documented process should specify how, when, and to whom risk-related information is communicated. This should include both internal and external stakeholders.
- **Ensure Timely and Clear Communication**
  Risk information should be shared promptly and in a format that is easy to understand, especially for non-technical stakeholders involved in operational or strategic decision-making.
- **Verify Stakeholder Contact Information**
  Stakeholder contact details should be reviewed at least annually to ensure accuracy and reliability of communications.
- **Support OT-Specific Communication Needs**
  Communication procedures should account for OT-specific roles, such as engineering, maintenance, and operations teams, ensuring they receive relevant risk information tied to system availability, safety, and continuity.

ID.RA-06 Risk responses are selected, 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 important

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.

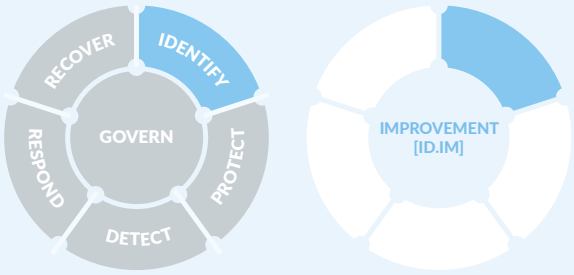
ID.RA-08.2 **The organisation shall implement automated mechanisms for disseminating and tracking remedial measures related to vulnerability information that automatically handles vulnerability data collection, disseminates information, tracks remedial measures, includes reporting and accountability, and enables continuous monitoring.**

Implementation guidance

The goal of this control is to ensure that vulnerability-related information is automatically collected, disseminated, tracked, and acted upon through a documented and automated vulnerability management process. This includes enabling continuous monitoring, reporting, and accountability to support timely and effective remediation.

To achieve this goal, the organisation should:

- Automate Vulnerability Data Collection and Distribution
  Vulnerability information should be gathered from internal sources (e.g. audits, OT/IT scans) and external sources (e.g. ENISA advisories, threat intelligence feeds, vendor bulletins). This information should be automatically distributed to relevant stakeholders using dashboards, alerts, or integrated communication tools.
- Track Remediation Actions and Monitor Progress
  Automated systems should track the implementation of remediation measures such as patching, configuration changes, or compensating controls. Progress should be monitored to ensure timely resolution.
- Generate Reports and Ensure Accountability
  Regular reports should be generated to provide visibility into vulnerability status, assigned responsibilities, and remediation progress. These reports should support transparency and management oversight.
- Enable Continuous Monitoring Through Automation
  Automated mechanisms should be in place to continuously monitor for new vulnerabilities and ensure that remediation workflows are updated accordingly.
- Evaluate Automation Effectiveness
  The effectiveness of automation should be assessed regularly to determine improvements in response time, efficiency, and stakeholder awareness. Adjustments should be made if objectives are not met.
- Ensure OT-Specific Coverage
  The automation process should include OT environments, addressing legacy systems, vendor-managed components, and embedded firmware. Coordination with engineering teams may be required for remediation in these environments.



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-03.7 The organisation shall implement independent teams to assess its processes, best practices, and technology solutions to safeguard critical systems and assets.

Implementation guidance

The goal of this control is to strengthen the protection of critical systems and assets by ensuring objective assessments of organisational processes, practices, and technologies. In Operational Technology (OT) environments, independent evaluations help identify vulnerabilities, reduce bias, and support continuous improvement in system resilience and safety.

To achieve this goal, the organisation should:

- **Engage Independent Teams**
  Independent assessors should include internal personnel not involved in the system's development or operation, and external experts with no financial or operational ties to the system.
- **Ensure Impartiality**
  Assessors should be free from conflicts of interest. Assessment roles should be rotated to avoid familiarity bias. Independence and qualifications should be documented.
- **Define Scope and Criteria Clearly**
  Assessment objectives, scope, and evaluation criteria should be agreed upon in advance to prevent undue influence from stakeholders.
- **Establish Independent Reporting Lines**
  Assessment results should be reported directly to senior management or an oversight body, bypassing the teams responsible for the systems under review.
- **Review Assessment Effectiveness Regularly**
  The independence and performance of assessment teams should be periodically reviewed to maintain objectivity and relevance.

ID.IM-03.8 **The organisation shall ensure that the security plan for its critical systems facilitates the review, testing, and continual improvement of the security protection processes.**

Implementation guidance

The goal of this control is to ensure that the organisation's security plan for critical systems supports regular review, testing, and continuous improvement of protection measures. In Operational Technology (OT) environments, this helps maintain system integrity, adapt to evolving threats, and align with broader risk management efforts.

To achieve this goal, the organisation should:

- **Develop and Maintain a Security Plan**
  A documented plan should describe how critical systems are protected from security threats. It should be distinct from, but aligned with, the Risk Treatment Plan.
- **Focus on Operational and Technical Controls**
  The plan should include defined security objectives, assigned responsibilities, security architecture, control measures, and procedures for monitoring, testing, and reviewing controls.
- **Enable Regular Review and Testing**
  The plan should support scheduled reviews, vulnerability assessments, and penetration testing to evaluate the effectiveness of security measures.
- **Support Continuous Improvement**
  Updates should be based on lessons learned, threat intelligence, audit results, and changes in the threat landscape.
- **Integrate with Risk Management**
  The plan should align with the organisation's risk treatment and governance processes to ensure consistency and accountability.
- **Keep the Plan Up to Date**
  The plan should be reviewed and updated regularly to reflect system changes, new threats, and evolving operational needs.

ID.IM-03.9 **The organisation shall conduct specialised assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the organisation's critical systems.**

Implementation guidance

The goal of this control is to strengthen the security posture of critical systems by conducting specialised assessments that uncover vulnerabilities, evaluate performance, and test defences against insider and external threats. In Operational Technology (OT) environments, these assessments help validate protections and support continuous improvement.

To achieve this goal, the organisation should:

- **Conduct Specialised Assessments**
  Assessments should include in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessments, performance/load testing, and verification and validation testing.
- **Outsource to Accredited Providers**
  Specialised assessments may be outsourced, preferably to accredited organisations. Accreditation should follow recognised standards such as:
  - CREST for penetration testing and vulnerability assessments
  - ISO/IEC 17025 for testing laboratories
    Accreditation should be granted by recognised bodies such as CREST, national accreditation authorities (e.g. BELAC), or industry-specific bodies (e.g. PCI Security Standards Council). This ensures assessments are conducted with technical competence, impartiality, and in line with best practices.
- **Integrate Findings into Remediation**
  Vulnerabilities identified during assessments should be addressed through established remediation processes, as outlined in control ID.IM-03.3.
- **Support Readiness and Maturity Evaluation**
  Assessment results should inform organisational readiness and performance levels (e.g. CyFun® maturity), guiding targeted improvements.

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

ID.IM-04.2 The organisation shall coordinate the development and the testing of Incident Response Plans and other cybersecurity plans that affect operations with stakeholders to ensure that these plans align with overall organisational goals and enhance resilience.

Implementation guidance

The goal of this control is to ensure that Incident Response Plans and other cybersecurity plans affecting operations are aligned with organisational goals and enhance resilience through coordinated development and testing with relevant stakeholders.

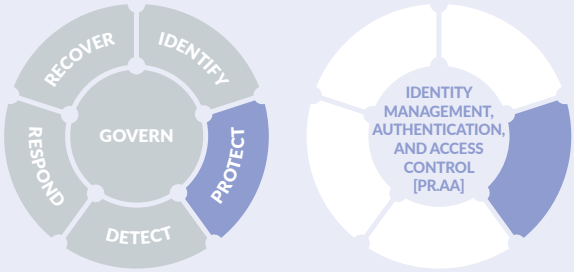
To achieve this goal, the organisation should:

- **Review and Update Plans Regularly**
  Plans should be reviewed and updated to reflect evolving threats, organisational changes, and operational needs.
- **Engage Stakeholders Early**
  Stakeholders, including internal teams, suppliers, and relevant third parties, should be involved early in the planning process to ensure alignment and relevance.
- **Maintain Ongoing Communication**
  Stakeholders should be kept informed of plan progress, updates, and changes to maintain shared understanding and readiness.
- **Coordinate Testing Activities**
  Testing of plans should be coordinated with stakeholders to validate effectiveness, clarify roles, and strengthen collaborative response capabilities.


Username
Password
Remember me
Protected
Balance:
5,367.50 $

PROTECT

Protect



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

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

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

Implementation guidance

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

To achieve this goal, the following should be considered:

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

- Shared Access to PLCs/HMIs (OT-Specific Measures)
  - If individual accounts are not feasible, the principle of least privilege should still apply.
  - A secure jump server or HMI front-end should be used to control access, log activity, and add authentication layers.
- Secure Remote Access
  - Technical requirements for remote access should be clearly defined and documented.
  - Secure methods such as VPNs, encrypted protocols (e.g. SSH, TLS), and multi-factor authentication (MFA – see also PR.AA-03.2) should be used.
  - Remote access should be monitored and logged.

PR.AA-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-01.3 **System credentials shall be deactivated after a specified period of inactivity unless it would compromise the safe operation of (critical) processes.**

Implementation guidance

The goal of this control is to ensure that system credentials are deactivated after a defined period of inactivity, unless doing so would compromise the safe operation of critical processes. This helps reduce the risk of unauthorised access while maintaining operational continuity.

To achieve this goal, the organisation should:

- Use Service Accounts for Automated Operations
  Service accounts should be used to run applications, services, or automated tasks. These accounts should be configured with minimal permissions, isolated from user accounts, and monitored separately to support auditability and secure automation.
- Apply the Principle of Least Privilege
  Service accounts should only have the permissions necessary for their function. This limits potential misuse and supports secure operations in both IT and OT environments.
- Monitor and Audit Service Account Activity
  Actions performed by service accounts should be logged and reviewed regularly. This improves traceability and helps detect anomalies or misuse.
- Implement Credential Inactivity Policies
  System credentials, including those of service and user accounts, should be automatically deactivated after a defined period of inactivity. Exceptions should be documented and justified, especially in OT environments where continuous operation is critical.
- Establish Formal Access Procedures for External Parties
  External access should follow a defined process, including role-based access levels, authorisation steps, identity verification, and awareness training. Monitoring and revocation mechanisms should be in place to manage access violations.
- Ensure OT-Specific Considerations
  In OT environments, credential deactivation policies should account for system uptime requirements, vendor-managed components, and legacy systems. Coordination with engineering teams may be necessary to avoid operational disruptions.

PR.AA-01.4 **For transactions within the organisation's critical systems, the organisation shall implement Multi Factor Authentication (MFA), cryptographic certificates, identity tokens, cryptographic keys and other credentials as appropriate and where feasible.**

Implementation guidance

The goal of this control is to ensure that strong authentication mechanisms are applied to transactions within critical systems. This includes using Multi-Factor Authentication (MFA – PR.AA-03.2), cryptographic credentials, and other secure methods to protect sensitive operations and data exchanges.

To achieve this goal, the organisation should:

- Apply Strong Authentication to Critical Transactions
  Transactions involving access to sensitive data, system configuration changes, command execution, user/device authentication, or data transmission between systems should be protected using MFA, identity tokens, cryptographic keys, or certificates, where feasible.

- **Use Context-Aware and Behaviour-Based Authentication**
  Strong authentication should include context-based checks (e.g. location, time, device) and behavioural biometrics (e.g. typing patterns) to detect anomalies and enhance security.
- **Combine MFA with Single Sign-On (SSO)**
  MFA should be integrated with SSO solutions to streamline access while maintaining robust protection for internal and external critical systems.
- **Manage Cryptographic Credentials Securely**
  Cryptographic certificates, identity tokens, and keys should be issued, stored, rotated, and revoked securely. This supports the secure implementation of strong authentication mechanisms required by this control and complements PR.AA-03.2, which mandates MFA for remote access.
- **Ensure OT-Specific Feasibility**
  In OT environments, authentication methods should be adapted to system constraints, legacy equipment, and operational continuity requirements. Coordination with engineering teams may be necessary to implement feasible solutions.

PR.AA-01.5 The organisation's critical systems shall be monitored for atypical use of system credentials. Credentials associated with significant risk shall be disabled.

Implementation guidance

The goal of this control is to detect and respond to abnormal or high-risk use of system credentials in critical systems, helping to prevent unauthorised access, insider threats, and credential-based attacks.

To achieve this goal, the organisation should:

- **Detect Atypical Credential Use**
  Systems should be monitored for deviations from normal credential usage patterns, such as unusual login times, access from unfamiliar locations, use of unfamiliar systems, simultaneous logins from distant locations, or sudden access to sensitive data.
- **Limit and Respond to Failed Login Attempts**
  A threshold for failed login attempts should be enforced. Accounts should be locked automatically after repeated failures and remain inaccessible until a defined lockout period expires or an authorised administrator resets them.
- **Manage Credential Lifecycles**
  Credential issuance, usage, and revocation should be automated where possible. An up-to-date inventory of active credentials should be maintained, and unused or orphaned accounts should be regularly reviewed and disabled.
- **Monitor and Correlate Events**
  Security Information and Event Management (SIEM) tools or equivalent solutions should be considered to detect anomalies and correlate events across systems. Behavioural baselining should be implemented to identify deviations from typical usage.
- **Disable High-Risk Credentials Automatically**
  Credentials associated with confirmed or high-risk anomalous activity should be disabled immediately. Security teams should be notified for investigation and response. All actions should be logged for audit and forensic purposes.
- **Raise User Awareness**
  Users should be trained on secure credential practices and encouraged to report suspicious activity or anomalies in access behaviour.

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-02.2 The organisation shall ensure that unique credentials are used for each authenticated user, device, and process interacting with the organisation's critical systems. These credentials shall be verified, and the unique identifiers shall be captured during system interactions. Exceptions may be made for emergency access ("break-glass" procedures), provided such access is strictly controlled, logged, and reviewed.

Implementation guidance

The goal of this control is to ensure that each user, device, and process interacting with critical systems is uniquely identifiable and authenticated. This supports accountability, traceability, and secure access, while allowing for controlled exceptions in emergencies.

To achieve this goal, the organisation should:

- Assign Unique Credentials
  Each user, device, and automated process should have its own unique credentials. Shared accounts should be avoided. All credentials should be verified before access is granted.
- Implement Strong Authentication
  Multi-Factor Authentication (MFA – PR.AA-03.2) has to be used wherever feasible. Authentication mechanisms should be resistant to replay attacks and credential reuse. These practices align with ENISA's Secure User Authentication Guidelines, which recommend layered and context-aware authentication for critical systems.

- **Enforce Credential Management Practices**
  Password policies and credential rotation should be enforced. Credentials should be reviewed and updated regularly, especially after role changes or offboarding. This supports the principles outlined in ENISA's NIS2 Technical Implementation Guidance, which emphasise secure identity lifecycle management.
- **Apply Access Control and Monitoring**
  Access should follow the Principle of Least Privilege. Logs and audit trails should be continuously monitored to detect anomalies. Suspicious activity should be investigated promptly.
- **Control Emergency Access ("Break-Glass")**
  Emergency access should be granted only through designated break-glass accounts. These accounts should be tightly controlled, time-limited, fully logged, and reviewed after use. Justification and approval should be required for each instance.
- **Promote User Awareness and Training**
  Personnel should be trained on the importance of using individual credentials and reporting suspicious access. Awareness should include the risks of credential sharing and misuse.
- **Ensure OT-Specific Feasibility**
  In OT environments, unique credentials should be implemented in a way that respects operational constraints and system limitations. Coordination with engineering teams may be required.

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-03.4 Remote access to the organisation's critical systems shall be monitored and cryptographic mechanisms shall be implemented where determined necessary.

Implementation guidance

The goal of this control is to ensure that remote access to critical systems is not only restricted and approved (as defined in PR.AA-03.3), but also actively monitored and protected using cryptographic mechanisms to prevent unauthorised access and data compromise.

To achieve this goal, the organisation should:

- **Monitor Remote Access Activities**
  All remote access sessions should be logged, capturing user identity, time, duration, and systems accessed. Monitoring tools should detect unusual or unauthorised access patterns and alert security teams in real time. Logs should be reviewed regularly and retained according to policy.
- **Apply Cryptographic Protections**
  Remote connections should use strong encryption protocols such as TLS (Transport Layer Security), SSH (Secure Shell), or IPsec. Data transmitted during remote sessions should be encrypted in transit. Where sensitive data is accessed, end-to-end encryption should be considered.
- **Enforce Access Rules from PR.AA-03.3**
  Monitoring and encryption settings should reflect the access restrictions defined in PR.AA-03.3. For example, alerts should trigger on out-of-hours access or attempts to reach unauthorised systems. All access should be verified against documented approvals.
- **Support Continuous Improvement**
  Monitoring data should be used to refine access policies, identify enforcement gaps, and support incident response. Cryptographic standards should be reviewed periodically to ensure alignment with current best practices.
- **Ensure OT-Specific Feasibility**
  In OT environments, monitoring and encryption should be implemented in a way that respects system constraints and operational continuity. Jump servers or secure gateways should be used to centralise control and logging.
- **Align with ENISA Guidance**
  These practices align with ENISA's NIS2 Technical Implementation Guidance, which recommends secure remote access, encryption of communications, and continuous monitoring as part of effective cybersecurity risk management for critical systems.

PR.AA-03.5 The security for connections with external systems shall be verified and framed by documented agreements.

Implementation guidance

The goal of this control is to ensure that all connections with external systems are secured through verified security controls and governed by documented agreements. This reduces the risk of unauthorised access, data leakage, and supply chain compromise.

To achieve this goal, the organisation should:

- **Control and Document All External Interactions**
  All interactions between internal systems and external parties (e.g. vendors, partners, cloud services) should be identified, controlled, and documented to ensure traceability and accountability.
- **Verify Security Controls of External Parties**
  Before establishing any connection, the external party's security posture should be verified through third-party assessments, audits, certifications (e.g. CyFun®), or technical documentation such as M154. These documents should describe security architecture, access controls, encryption, and monitoring.
- **Establish Documented Agreements**
  Formal agreements (e.g. contracts, SLAs, DPAs) should define security requirements, roles and responsibilities, data exchange protocols, incident response procedures, and termination conditions.

- **Specify Access Control Requirements**
  Agreements should include technical restrictions such as IP whitelisting, role-based access control, data handling rules, and encryption requirements for data in transit and at rest.
- **Monitor and Review External Connections**
  All external connections should be continuously monitored for anomalies or policy violations. Agreements and technical documentation (e.g. M154) should be reviewed periodically and updated as needed. Any changes in the external system's security posture should trigger a reassessment.
- **Ensure OT-Specific Considerations**
  In OT environments, external access should be routed through secure gateways or jump servers. Shared access (e.g. for vendor-managed PLCs) should be logged, time-limited, and protected by strong authentication.
- **Align with ENISA Guidance**
  These practices align with ENISA's Technical Implementation Guidance on Cybersecurity Risk Management Measures, which recommends verifying third-party security, formalising responsibilities through contracts, and continuously monitoring external dependencies.

PR.AA-04 Identity assertions are protected, conveyed, and verified

PR.AA-04.1 Identity assertions shall be protected, conveyed, and verified

Implementation guidance

The goal of this control is to ensure that identity assertions — claims about the identity of a user, device, or process — are protected against tampering, securely transmitted, and reliably verified before granting access to critical systems or data.

Definition: An identity assertion is a digital statement used during authentication that confirms the identity of a user, device, or process. It typically includes information such as the identity provider, authentication method, and validity period, and is used to grant access to systems or services.

To achieve this goal, the organisation should:

- **Protect Identity Assertions**
  Identity assertions should be protected from tampering, theft, or misuse. Strong encryption (e.g. TLS 1.2 or higher) and digital signatures should be applied. Identity providers should comply with the eIDAS Regulation (e.g. itsme®, SPID, FranceConnect). These practices align with ENISA's Digital Identity and Trust Services guidance.
- **Convey Identity Assertions Securely**
  Identity data should be transmitted using secure protocols such as SAML 2.0 or OpenID Connect. Token exposure in URLs should be avoided; HTTP headers or POST methods should be used. For cross-border identity federation, eIDAS nodes should be used to ensure secure interoperability between EU member states.
- **Verify Identity Assertions**
  All assertions should be validated before access is granted. This includes verifying digital signatures using trusted certificate authorities listed in the EU Trusted List (EUTL), checking token claims (issuer, audience, expiration), and validating against eIDAS metadata. Qualified Trust Service Providers (QTSPs) should be used for issuing and verifying identity credentials.
- **Ensure OT-Specific Feasibility**
  In OT environments, identity assertions should be integrated into secure access gateways or jump servers. Where direct integration is not feasible, identity verification should occur at the interface layer, with logging and monitoring in place.
- **Align with ENISA Guidance**
  These practices are supported by ENISA's NIS2 Technical Implementation Guidance and its work on secure digital identity frameworks under the eIDAS and European Digital Identity regulations.

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-05.8 **Account usage restrictions for specific time periods and locations shall be taken into account in the organisation's security access policy and applied accordingly.**

Implementation guidance

The goal of this control is to reduce the risk of unauthorised access by ensuring that account usage is restricted based on time, location, device, and user context. These restrictions should be defined in the organisation's security access policy and applied consistently across ICT and OT environments.

To achieve this goal, the organisation should:

- Apply Time-Based Restrictions
  - Access to systems should be limited to defined working hours to reduce exposure during off-hours.
  - Usage durations for certain accounts should be capped to prevent excessive or unattended sessions.
- Apply Location-Based Restrictions
  - Geofencing should be used to allow access only from trusted geographic locations.
  - IP address filtering should restrict access to known and approved network ranges.
- Apply Device-Based Restrictions
  - Access should be allowed only from managed devices that comply with the organisation's security policies.
  - Unmanaged devices should be restricted or granted limited access (e.g. read-only or no access to sensitive data).
- Apply User-Based Restrictions
  - Role-Based Access Control (RBAC) should ensure users only access systems and data relevant to their job.
  - Conditional access policies should require additional verification (e.g. Multi-Factor Authentication) in high-risk scenarios.
  - Continuous Adaptive Risk and Trust Assessment (CARTA) should be considered to evaluate user and device trust dynamically. This approach aligns with the Zero Trust principle, which assumes no implicit trust for any user or device, even inside the network.
- Ensure OT-Specific Feasibility
  In OT environments, restrictions should be adapted to operational and safety requirements. Where technical limitations exist, compensating controls such as physical access restrictions or monitored jump servers should be implemented.
- Align with ENISA Guidance
  These practices align with ENISA's NIS2 Technical Implementation Guidance, which supports contextual access control as part of effective cybersecurity risk management.

PR.AA-05.9 Privileged users shall be managed, monitored and audited.

Implementation guidance

The goal of this control is to ensure that privileged user accounts, those with elevated access to critical systems, are tightly controlled, continuously monitored, and independently audited. This should reduce the risk of misuse, ensure accountability, and protect critical Information Technology (IT), Operational Technology (OT), and Internet of Things (IoT) environments.

To achieve this goal, the organisation should:

- **Enforce Strong Privileged Access Management**
  Privileged accounts should have clearly defined roles, limited access scopes, and be subject to regular access reviews.
- **Implement Continuous Monitoring**
  All privileged user activities should be logged and monitored continuously, using automated tools where possible, to support traceability and incident response.
- **Conduct Independent Audits**
  - Audits should be performed periodically by individuals who are independent of the access management process.
  - Audits should:
    - Verify that privileged access is granted in line with policy.
    - Confirm that monitoring and logging mechanisms function correctly.
    - Identify misuse, policy violations, or deviations.
    - Produce documented outcomes such as audit reports or corrective action plans.
- **Apply the Four-Eyes Principle**
  No single individual should be able to grant, modify, or revoke privileged access without oversight or approval from another authorised person.
- **Differentiate Between Monitoring and Auditing**
  - Daily compliance monitoring should focus on operational issues (e.g. alerts, anomalies).
  - Periodic audits should assess the overall effectiveness and integrity of the privileged access management process.
- **Ensure OT-Specific Feasibility**
  In OT environments, privileged access controls should be adapted to operational and safety constraints. Where full auditing is not feasible, compensating controls such as interface-level logging or external review should be implemented.
- **Align with ENISA Guidance**
  These practices should align with ENISA's NIS2 Technical Implementation Guidance, which highlights the importance of privileged access control, monitoring, and auditing in securing essential services and critical infrastructure.

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

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

Implementation guidance

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

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

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

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.

PR.AA-06.3 **Critical zones shall have additional physical access controls beyond those applied to general facilities.**

Implementation guidance

The goal of this control is to reduce the risk of unauthorised physical access to areas essential for operational continuity, data integrity, and personnel and equipment safety by applying stricter access measures than those used in general facility areas.

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

- **Critical zones should be identified during asset classification. These typically include:**
  - Production and Operational Technology (OT) environments
  - Server rooms and data centres
  - Finance and Human Resources offices
  - Control rooms
  - Locations storing sensitive or classified information
- **The following enhanced physical access controls should be considered:**
  - Dual-factor authentication (e.g. badge + biometrics)
  - Continuous surveillance (e.g. CCTV, motion sensors)
  - Access logging with regular review
  - On-site or patrolling security personnel
  - Alarm systems with real-time alerts
  - Visitor management procedures:
    - Pre-approval and escorting
    - Time-limited access
    - Visitor logs
- **Ensure consistency with broader physical access policies, including:**
  - PR.AA-06.1 – Risk-based access control
  - PR.AA-06.2 – Emergency access procedures
  - PR.AA-06.4 – Physical protection of assets
- **Adapt controls to the criticality of each zone and integrate them into the overall physical security strategy.**

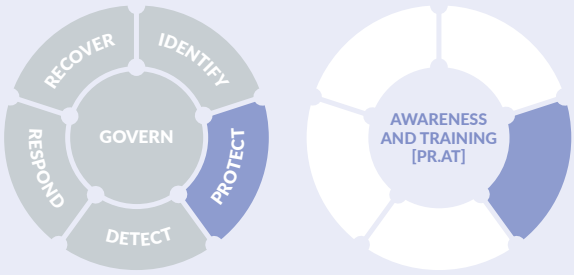
PR.AA-06.4 **Assets located within critical zones shall be physically protected against unauthorised access, damage, or interference.**

Implementation guidance

The goal of this control is to safeguard essential assets located in critical zones from unauthorised access, damage, or interference, whether intentional or accidental, by applying tailored physical protection measures.

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

- Assets within critical zones should be physically protected based on their criticality and risk profile. These assets may include:
  - Servers and control systems
  - Power infrastructure and cabling
  - Sensitive data repositories
  - Operational Technology (OT) components
- Protection measures should include:
  - Physical barriers and containment:
    - Locked enclosures, secure cabinets, or cages for sensitive equipment
    - Tamper-evident seals to detect unauthorised access
    - Environmental safeguards (e.g. fire suppression, temperature control)
  - Infrastructure protection:
    - Securing power and network cabling, access interfaces, and equipment
    - Redundant and physically separated power systems for critical operations
  - Access control and supervision:
    - Escorting guests, vendors, and third parties at all times
    - Maintaining and regularly reviewing access logs
- Controls should be aligned with related requirements, including:
  - PR.AA-06.1 – Risk-based access control
  - PR.AA-06.2 – Emergency access procedures
  - PR.AA-06.3 – Enhanced access controls for critical zones
- Protection should be proactive, initiated during asset classification and facility design, and integrated into the broader physical security strategy.



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 cybersecurity 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-01.4 **The organisation shall evaluate whether its cybersecurity awareness training is effective in improving knowledge, behaviour, and readiness across the organisation.**

Implementation guidance

The goal of this control is to ensure that cybersecurity awareness training leads to measurable improvements in personnel knowledge, secure behaviour, and readiness to respond to cyber threats across all levels of the organisation. This control builds on the threat-specific awareness from PR.AT-01.2 and the role-based training from PR.AT-01.3 by introducing a structured approach to measure the impact of awareness efforts.

The implementation should consider the following:

- The organisation should assess whether awareness training is accessible to all relevant personnel and whether it effectively influences their cybersecurity behaviour, awareness, and attitudes.
- If the organisation lacks experience in evaluation, it should consider using existing evaluated frameworks or tools, such as ENISA's AR-in-a-Box, which includes guidance on setting goals, selecting KPIs, and measuring impact.
- If developing an evaluation method internally, the organisation should look into good practices and evidence-based approaches for evaluating awareness programmes.
- Evaluation methods should include a mix of:
  - Pre- and post-training assessments or quizzes.
  - Simulated phishing or social engineering tests.
  - Surveys to measure changes in awareness, confidence, and behaviour.
  - Feedback from participants and trainers.
- The organisation should document lessons learned and use the results to improve future training efforts.

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.

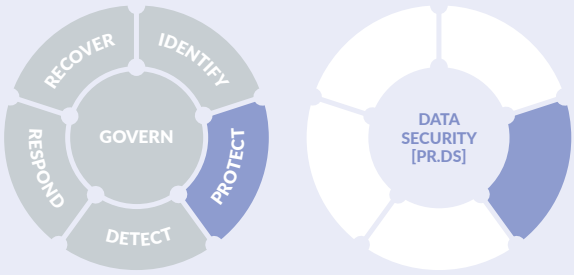
PR.AT-02.3 **Privileged users shall be qualified before privileges are granted, and these users shall be able to demonstrate the understanding of their roles, responsibilities, and authorities.**

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-01.2 The organisation shall implement automated tools where feasible to provide notification upon discovering discrepancies during integrity verification.

Implementation guidance

The goal of this control is to ensure that discrepancies in system or data integrity are detected and reported automatically, enabling timely response and reducing the risk of undetected tampering, especially in environments where operational continuity and safety are critical.

To achieve this goal, the organisation should:

- Implement automated tools where feasible to continuously verify the integrity of critical data and systems.
- Ensure these tools promptly report integrity violations when discrepancies are detected.
- Configure alerts to notify relevant personnel, such as system administrators, business owners, and information security officers, to enable swift investigation and response.
- Use centrally managed integrity verification solutions to streamline monitoring and reporting across both IT (Information Technology) and OT (Operational Technology) environments.
- Follow guidance from ENISA, such as the NIS2 Technical Implementation Guidance (ENISA, 2025), which outlines best practices for automated integrity monitoring and incident response.

PR.DS-01.3 The organisation shall define and implement automated responses to detected integrity violations, using predefined safeguards that are proportionate to the severity and impact of the violation.

Implementation guidance

The goal of this control is to minimise the impact of integrity violations by enabling timely, proportionate, and automated responses that help contain threats, preserve system stability, and support forensic analysis, especially in environments where manual intervention may be delayed or impractical.

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

- Severity levels and response actions should be defined, with integrity violations being categorised (e.g. low, medium, high impact) and linked to appropriate automated safeguards.
- Alerts and notifications should be triggered automatically when integrity violations are detected, and integrated with Security Orchestration, Automation, and Response (SOAR) platforms to streamline incident handling.
- Affected components should be quarantined or isolated, such as compromised files, applications, or systems, to prevent further damage.
- All events should be logged and auditable, including detected violations and automated actions, to support forensic investigations and compliance reporting.
- Lightweight automation should be used where possible, such as:
  - Blocking specific processes or users
  - Reverting to a known-good configuration
  - Temporarily disabling affected services
- Response mechanisms should be tested and tuned regularly in controlled environments to ensure effectiveness and avoid unnecessary disruption.
- The European Union Agency for Cybersecurity (ENISA) guidance in the *"Implementation Guidance on Security Measures"* (*For Public Consultation*, Document No. ENISA/2024/IGSM) should be consulted.

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-01.6 The organisation shall protect the confidentiality of its critical assets while at rest.

Implementation guidance

The goal of this control is to ensure that sensitive operational and business data stored on systems, servers, or devices remains protected from unauthorised access, even if physical or logical security is compromised.

In OT environments, where legacy systems and shared infrastructure are common, protecting data-at-rest is critical to prevent exposure of configuration files, process data, or credentials that could be exploited to disrupt operations or gain lateral access.

This control builds further on PR.DS-01.1.

To enable the protection of the organisation' s critical assets at-rest, the following techniques should be considered:

- Encryption: Encrypt data-at-rest, on hard drives, on external media, in stored files, in configuration files and stored in the cloud, using strong encryption algorithms to prevent unauthorised access and protect the data against tampering.
- Access Controls: Implement strict access controls to ensure only authorised personnel can access sensitive information.
- Regular Audits: Conduct regular security audits to identify and address vulnerabilities.
- Data Masking: Use data masking techniques to obscure sensitive information in non-production environments (For example, GDPR-sensitive data from the production environment may not be copied to a test environment without randomisation to prevent unauthorised access to data).

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-02 The confidentiality, integrity, and availability of data-in-transit are protected

PR.DS-02.1 Portable storage devices containing system data shall be controlled and protected while in transit and in storage.

Implementation guidance

The goal of this control is to prevent unauthorised access, tampering, or loss of critical system data when portable storage devices are moved between locations or stored outside secure environments.

In OT environments, where data may be transferred between isolated systems or remote sites using physical media, protecting these devices is essential to maintain system integrity and confidentiality.

To achieve this goal, the organisation should:

- Scan all portable storage devices for malicious code before use on organisational systems.
- Encrypt data to ensure confidentiality if a device is lost or stolen.
- Use tamper-evident seals and locked containers during transport.
- Rely on trusted couriers or secure transport services, and avoid leaving devices unattended.
- Limit access to stored devices to authorised personnel, supported by documented access control policies.
- Store devices in secure, climate-controlled environments to prevent physical damage.
- Conduct regular audits and inventory checks to ensure devices are accounted for and properly secured.

PR.DS-02.2 The organisation shall protect its critical and sensitive information while in transit.

Implementation guidance

The goal of this control is to ensure that critical and sensitive information remains confidential and unaltered while being transmitted across networks or between systems, especially in environments where data flows between IT and OT layers or across remote sites.

In OT contexts, where data may traverse less secure or legacy communication channels (e.g. between control systems, field devices, or remote monitoring stations), protection in transit is essential to prevent interception, manipulation, or leakage. This control builds further on PR.DS-01.1.

To enable the protection of the organisation's critical and sensitive information while in transit, the following techniques should be considered:

- Encryption: Use strong encryption protocols like Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt data during transmission. This ensures that even if data is intercepted, it remains unreadable to unauthorised parties.
- End-to-End Encryption (E2EE): Implement E2EE, which encrypts data on the sender's device and only decrypts it on the recipient's device.
- Multi-Factor Authentication (MFA): Require MFA for accessing sensitive information.
- Strong Password Policies: Enforce strong password policies, including the use of complex passwords and regular updates.
- Virtual Private Networks (VPNs): Use VPNs — either site-to-site or remote access — to establish secure tunnels for data transmission, in particular when connecting over untrusted networks such as public Wi-Fi.
- Regular Security Audits: Conduct regular security audits to identify and address vulnerabilities in your data transmission processes.

PR.DS-10 The confidentiality, integrity, and availability of data-in-use are protected

PR.DS-10.1 The organisation's critical systems shall be protected against denial-of-service attacks or at least the effect of such attacks shall be limited.

Implementation guidance

The goal of this control is to ensure that critical systems remain available and operational even when targeted by denial-of-service (DoS) attacks, which aim to overload or disrupt services.

To achieve this goal, the organisation should:

- Limit the impact of DoS attacks by:
  - Deploying boundary protection devices or services that filter malicious traffic.
  - Ensuring sufficient network capacity and redundancy to absorb traffic spikes.
- Restrict the ability to launch DoS attacks by:
  - Limiting connectivity options to prevent unauthorised transmission over wired, wireless, or satellite links.
  - Enforcing resource usage limits to prevent system overload.
  - Applying strong authentication and authorisation to control access to critical functions.
- Strengthen system resilience by:
  - Conducting regular security testing and audits to identify and address vulnerabilities.
  - Monitoring network traffic for anomalies that may indicate early signs of a DoS attempt.
- OT-Specific Considerations
  In OT environments, where availability directly affects safety and production, even short disruptions can have severe consequences. DoS protections should be tailored to industrial protocols and legacy systems, ensuring that defences do not interfere with real-time operations.

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.

PR.DS-11.4 **The organisation shall regularly verify the integrity and recoverability of backups through coordinated testing with all relevant continuity and incident response functions. Backup testing shall be integrated into broader resilience planning, including business continuity, disaster recovery, and cyber incident response.**

Implementation guidance

This control is an evolution of PR.DS-11.3 and ensures that backup systems are not only in place but are regularly tested and aligned with the organisation's broader recovery and continuity plans. It highlights the importance of coordination across teams and proactive planning, helping the organisation stay prepared to recover quickly and effectively from serious incidents.

To ensure that backup and recovery capabilities are effective and integrated into the organisation's overall resilience strategy, the following practices should be implemented:

- **Coordinate Backup Testing Across Plans**
  Backup verification should be planned and executed in coordination with the teams responsible for the organisation's key continuity and response plans. These include:
  - Business Continuity Plans (BCP)
  - Disaster Recovery Plans (DRP)
  - Contingency Plans
  - Continuity of Operations Plans (COOP)
  - Crisis Communications Plans
  - Critical Infrastructure Protection Plans
  - Cyber Incident Response Plans
- **Include Backup Recovery in Scenario Testing**
  During exercises or simulations of incidents (e.g. cyberattacks, system failures, or natural disasters), the recovery of backup data should be explicitly tested. This ensures that backups are not only available but also usable and aligned with recovery time and recovery point objectives (RTO/RPO).
- **Document and Review Results**
  The outcomes of backup verification and recovery tests should be documented and reviewed with relevant stakeholders to identify gaps and improve procedures.

PR.DS-11.5 **Backups of critical systems (such as operating systems, configurations, and applications) shall be kept separate from backups of critical information (such as business data, documents, and databases) to support faster and more reliable recovery.**

Implementation guidance

The goal of this control is to support faster and more reliable recovery by separating backups of critical systems (e.g. operating systems, configurations, applications) from backups of critical information (e.g. business data, documents, databases).

To achieve this goal, the organisation should:

- **Separate backup scopes**
  - System backups should include operating systems, configurations, installed software, and system-level settings.
  - Information backups should include business-critical data such as databases, documents, and application data.
- **Use tailored backup methods**
  - System backups should use full images or snapshots to capture the complete system state.
  - Information backups should use incremental or differential methods to efficiently capture data changes.
- **Encrypt sensitive data**
  Both system and information backups should be encrypted during storage and transmission, especially when containing sensitive or regulated data.
- **Align with recovery objectives**
  Backup separation should reflect different Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). For example, system recovery may require faster restoration than business data.
- **Document and automate**
  - Backup scopes and procedures should be clearly documented.
  - Backup processes should be automated where possible to reduce human error and ensure consistency.

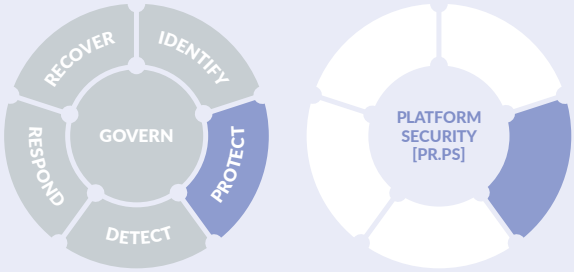
OT-Specific Considerations

In OT environments, separating system and data backups helps restore control systems quickly without waiting for large data sets to be recovered. This supports operational continuity and reduces downtime in critical industrial processes.

Relation with PR.DS-11.3 and PR.DS-11.4

PR.DS-11.5 is an evolution — not a repetition — of PR.DS-11.3 and PR.DS-11.4. While the earlier controls focus on where and how backups are stored and verified, PR.DS-11.5 focuses on what is being backed up and how it is logically separated to optimise recovery:

- PR.DS-11.3 ensures backups are secure and stored separately.
- PR.DS-11.4 ensures backups are tested and integrated into recovery planning.
- PR.DS-11.5 ensures functional separation between system and data backups to enable faster, more targeted recovery.



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

PR.PS-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-01.2 **The organisation shall configure its business-critical systems to operate with only the essential functions needed for their intended purpose. This includes reviewing and updating baseline configurations to disable any non-essential capabilities.**

Implementation guidance

The goal of this control is to reduce security risks and system complexity by ensuring that business-critical systems are configured to run only the functions necessary for their intended purpose.

To achieve this goal, the organisation should:

- Apply the principle of least functionality by disabling non-essential features, services, and components.
- Regularly review and update baseline configurations to reflect operational needs and evolving threats.
- Assess and limit the following elements to what is strictly required:
  - Installed software
  - Enabled services
  - Open ports
  - Allowed protocols
  - System features
- Align configurations with security policies to minimise exposure to vulnerabilities and improve system performance.

PR.PS-01.3 **The organisation shall identify and disable specific functions, ports, protocols, and services within its critical systems that are not required for business operations.**

Implementation guidance

The goal of this control is to reduce the attack surface of critical systems by disabling functions, ports, protocols, and services that are not essential for business operations.

To achieve this goal, the organisation should:

- Identify system features that are not required based on the system's role and associated risks.
- Disable unnecessary elements to limit potential entry points and reduce lateral movement within the network.
- Regularly assess and update configurations to reflect operational needs and evolving threats.
- Elements to consider disabling include:
  - Bluetooth
  - File Transfer Protocol (FTP)
  - Peer-to-peer networking
  - Other unused or legacy services

PR.PS-01.4 **The organisation shall implement technical safeguards to enforce a policy of 'deny-all' and 'permit-by-exception' so that only authorised software programmes are executed.**

Implementation guidance

The goal of this control is to ensure that only explicitly authorised software is allowed to run, reducing the risk of unauthorised or malicious programs affecting critical systems.

To achieve this goal, the organisation should consider the following:

- Implement application whitelisting to allow only approved software to execute.
- Use group policies to enforce application control rules across systems.
- Apply Software Restriction Policies (SRP) or similar mechanisms to block unauthorised software based on file path, hash, or digital signature.
- Enforce role-based access control (RBAC) to ensure only authorised users can run specific applications.
- Configure Java Security Manager to restrict which classes and methods can execute in Java-based environments.
- Use configuration management tools to maintain consistent enforcement of authorised software across all systems.

PR.PS-01.5 **Unauthorised configuration changes to organisation's systems shall be monitored and addressed with the appropriate mitigation actions.**

Implementation guidance

The goal of this control is to detect and respond to unauthorised configuration changes that could compromise system integrity or availability.

To achieve this goal, the organisation should consider to:

- Monitor configuration changes in line with defined policies and procedures.
- Detect and log unauthorised modifications to system settings.
- Alert designated personnel when unauthorised changes occur.
- Restore approved configurations promptly to maintain operational stability.
- Halt, in critical cases, affected system processes to prevent further impact.
- Consult the guidance in ENISA NIS2 Technical Implementation Guidance (latest version), which recommends continuous monitoring and prompt mitigation of unauthorised changes to preserve system resilience and compliance.

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-04.4 **The organisation shall ensure that audit processing failures on the organisation's systems generate alerts and trigger defined responses.**

Implementation guidance

The goal of this control is to ensure that any failure in audit logging, such as errors in log collection, processing, or storage, triggers alerts and predefined responses to maintain system integrity and traceability.

To achieve this goal:

- Audit failures should include software or hardware issues, broken logging mechanisms, or full storage.
- Alerts should be automatically generated when such failures occur, and predefined actions should be triggered to address them.
- Each audit log repository, whether on a server, firewall, or application, should be monitored individually and collectively.
- System Logging Protocol (Syslog) servers or similar centralised logging solutions should be used to support reliable log collection and alerting.
- Systems generating logs should be configured to capture detailed activity, access, and behaviour data to support zero-trust principles.
- Audit logs should be continuously monitored to ensure availability, integrity, and sufficient storage capacity.

PR.PS-04.5 **The organisation shall ensure that authorised personnel can extend or enhance audit logging and monitoring capabilities when needed to support investigations or incident response.**

Implementation guidance

The goal of this control is to ensure that audit logging can be quickly adapted to provide deeper visibility during security incidents or investigations, without disrupting normal operations.

To achieve this goal:

- Audit logging systems should allow on-demand adjustments, such as increasing log detail, extending retention, or expanding coverage.
- Authorised personnel and conditions for enabling extended logging should be clearly defined.
- Activation procedures should include approvals, documentation, and change tracking.
- Logbook records should be reviewed regularly for accuracy and completeness across ICT and OT systems.
- Policies should ensure extended logging is used only when justified and is properly recorded.
- Technical capacity, escalation paths, and personnel availability should be pre-planned to support timely activation.

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.

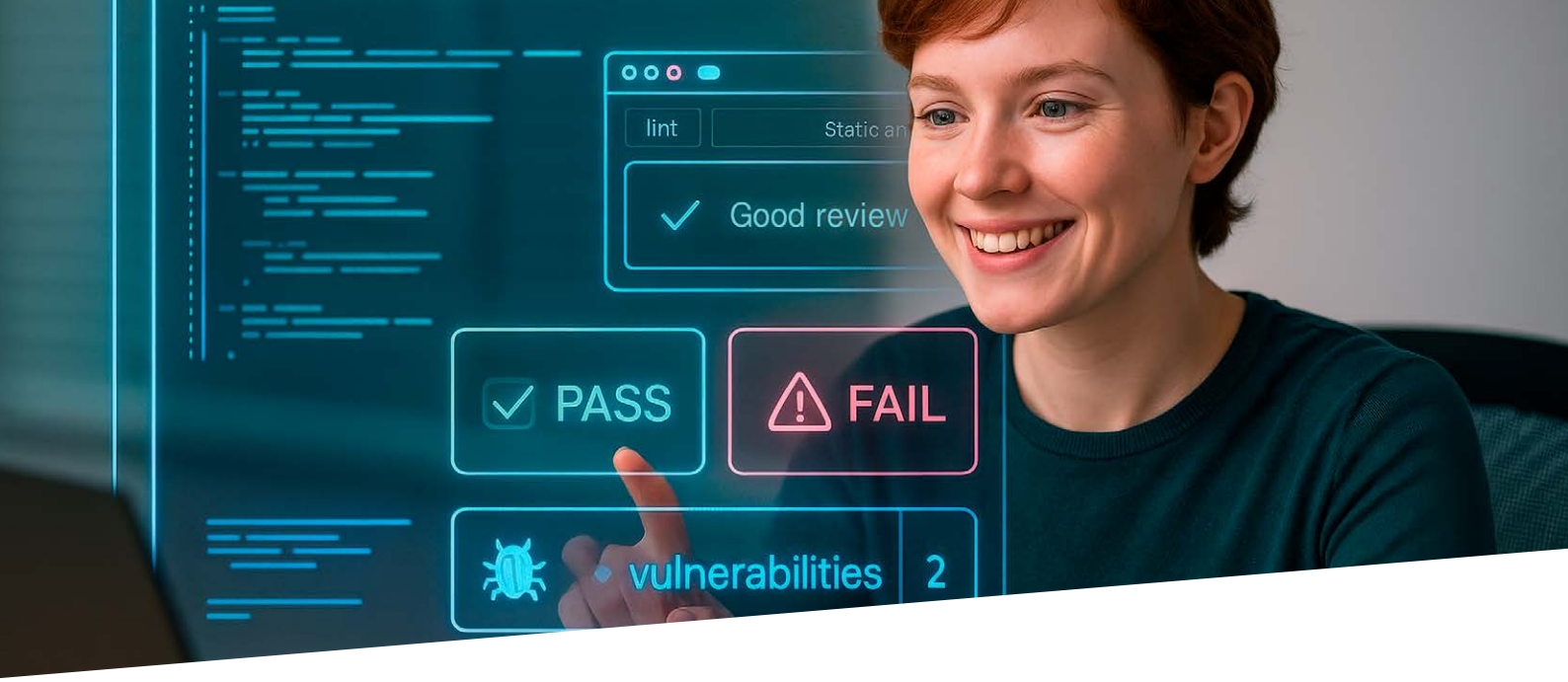
PR.PS-06.3 Secure software development practices shall be integrated into all phases of the software development lifecycle, and their effectiveness should be regularly monitored and improved.

Implementation guidance

The goal of this control is to reduce security risks in software by embedding protective measures throughout development and continuously improving them based on performance and evolving threats.

To achieve this goal, the organisation should:

- Integrate Security into the Development Lifecycle
  - Secure coding standards and trusted development frameworks should be applied.
  - Threat modelling should be conducted early to identify and reduce risks.
  - All software components should be protected from tampering and unauthorised access.
  - Access controls for databases and sensitive data should be enforced.
  - Software dependencies and libraries should be kept up to date.
  - Outdated or unused software should be securely removed.
- Monitor the Effectiveness of Security Practices
  - Metrics should be defined and tracked, such as:
    - Vulnerabilities found during development vs. in production.
    - Time taken to fix identified issues.
    - Percentage of code reviewed or tested for security.
    - Developer participation in secure coding training.
  - These metrics should be used to identify gaps and improve practices.
- Build Security Awareness
  Developers and technical teams should receive regular training on secure coding and design principles.
- Maintain and Improve
  Secure development practices should be reviewed and updated based on:
  - New threats or vulnerabilities.
  - Lessons learned from incidents or audits.
  - Industry standards and best practices.



PR.PS-06-4 **For planned changes to the organisation's critical systems, a security impact analysis shall be performed in a separate test environment before implementation in an operational environment.**

Implementation guidance

The goal of this control is to prevent unintended security risks by testing planned changes to critical systems in a controlled environment before deployment.

To achieve this goal, the organisation should:

- Plan the Test Scenario
  - Security threats to systems, assets, processes, and people should be identified.
  - Planned configuration changes or system modifications should be analysed for their potential impact on security.
- Prepare the Test Environment
  - Test data should reflect realistic operational scenarios.
  - Hardware, software, and network requirements should be clearly defined.
  - The test environment should closely mirror the production environment in setup and configuration.
  - Sufficient disk space should be allocated for testing activities.
  - Software versions in the test environment should match those in production.
- Ensure Security and Maintainability
  - Software in the test environment should be regularly updated to address known vulnerabilities.
  - Virtualisation or containerisation should be used to create consistent and replicable environments.
  - Isolated virtual machines (VMs) should be used to prevent interference with operational systems.
  - Security controls such as firewalls and access restrictions should be implemented in the test environment.

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-01.5 **The organisation shall implement, where feasible, authenticated proxy servers or firewalls with URL filtering and threat intelligence capabilities for defined communications traffic between its critical systems and external networks.**

Implementation guidance

The goal of this control is to reduce the risk of cyber threats entering critical systems, by filtering and inspecting outbound and inbound communications through authenticated proxies or firewalls.

To achieve this goal, the following should be considered:

- **Access Controls**
  Proxy servers and firewalls should enforce strict access controls, allowing only authorised users and systems. Strong authentication methods, such as multi-factor authentication (MFA), should be used to support zero-trust principles.
- **Encryption**
  Communications between clients and proxy servers should be encrypted using the most current and secure versions of SSL/TLS to protect against eavesdropping and man-in-the-middle attacks.
- **Threat Intelligence and URL Filtering**
  - To effectively monitor and control communications across IT and OT environments, proxy servers and firewalls should:
    - Integrate threat intelligence feeds to detect and block known malicious domains, IP addresses, and URLs.
    - Apply URL filtering to prevent access to harmful or unauthorised web content.
  - In OT environments, where systems often lack built-in security features, intelligent filtering at network boundaries should be used to:
    - Detect and block malicious traffic before it reaches critical systems.
    - Prevent data exfiltration and unauthorised external communication.
    - Enforce communication policies without disrupting operational processes.

  These measures should be part of a layered defence strategy that supports secure and reliable operations across both IT and OT domains.
- **Logging and Monitoring**
  Detailed logging and continuous monitoring should be enabled to track access, detect anomalies, and support incident response. Logs should be regularly reviewed for signs of compromise.
- **Firewall Configuration**
  Firewalls should be configured to allow only explicitly authorised traffic to and from proxy servers. A “deny by default” policy should be enforced.
- **Regular Updates and Patching**
  Proxy servers, firewalls, and their underlying systems should be regularly updated and patched to address known vulnerabilities and maintain security effectiveness.
- **Performance and Reliability**
  Load balancing should be used to distribute traffic across multiple proxy servers or firewalls, ensuring high availability and optimal performance. Resource usage should be monitored to prevent overload and degradation.

PR.IR-01.6 **The organisation shall ensure that its critical systems are designed to fail securely and remain protected in the event of an operational failure of a border protection device.**

Implementation guidance

The goal of this control is to ensure that critical systems remain protected and do not become exposed or vulnerable if a firewall, proxy, or other boundary protection device fails.

In OT environments, where availability and safety are paramount, systems should be designed to fail securely, for example, by defaulting to a deny-all state, isolating affected segments, or triggering alerts, so that a failure in one component does not compromise the entire system or allow unauthorised access.

To achieve this goal, the following should be considered:

- **Fail-Secure Configuration**
  Devices should be configured to default to a secure state (e.g. deny all traffic) in the event of failure, preventing unauthorised access or data leakage.
- **Redundancy and High Availability**
  Redundant systems or failover mechanisms should be in place to ensure continuous protection. Avoid single points of failure, especially in OT environments where uptime is critical.
- **Regular Testing and Maintenance**
  Failover mechanisms and secure failure configurations should be tested regularly. Maintenance should ensure devices remain in a secure and functional state.
- **Access Control Integrity**
  Access Control Lists (ACLs) and security policies should remain protected and unaltered during failures to preserve the system's security posture.
- **Monitoring and Alerts**
  Real-time monitoring and alerting should be implemented to detect failures promptly and initiate corrective actions.
- **Segmentation and Isolation**
  Network design should include segmentation and isolation to limit the impact of a failure and prevent cascading effects across systems.

These practices align with recognised standards, including NIST SP 800-53 Rev. 5, NIST SP 800-53A, and IEC 62443-3-3 SR 5.2 RE 3 – Fail Close, which emphasise secure failure and resilience in critical infrastructure systems.

PR.IR-01.7 **The organisation shall ensure that development and test environments are strictly separated from the production environment, particularly in ICS/OT systems where any crossover could compromise safety, endanger health, or disrupt essential operations.**

Implementation guidance

The goal of this control is to prevent unintended disruptions, safety risks, or security breaches by ensuring that development and testing activities do not interfere with live operational systems.

In OT environments, such as Industrial Control Systems (ICS), even minor crossovers between test and production can lead to unsafe conditions, process interruptions, or exposure of sensitive configurations. Strict separation helps maintain system integrity, supports change control, and reduces the risk of accidental or malicious actions affecting critical operations.

To achieve this goal, the following should be considered:

- Strict Environment Separation
  Development and testing activities should be conducted in environments that are physically or logically separated from the production environment. This is especially critical in ICS/OT settings, where operational safety and reliability must not be compromised.
- Pre-Deployment Testing
  Any change intended for the ICT or OT environment should first be tested in a non-production environment. This allows for the evaluation of potential impacts and necessary adjustments before deployment.
- Realistic Test Environments
  Test environments should closely replicate the production environment in terms of configuration, architecture, and data flow, to ensure accurate testing outcomes.
- Secure Development Practices
  Cybersecurity features should be integrated and tested as early as possible in the development lifecycle, following secure development lifecycle (SDLC) principles.

PR.IR-01.8 **The organisation shall define, monitor, and control the flow of information and data within and between its critical systems to ensure that only authorised and secure exchanges occur, regardless of network boundaries or system architecture.**

Implementation guidance

This requirement builds on PR.IR-01.3 (control of system connections) and PR.IR-01.4 (boundary protection), but goes further by focusing on what data is allowed to move, where, and under what conditions — not just how systems are connected or segmented.

It also complements ID.AM-03.2, which requires that network communication and internal data flows be mapped, documented, authorised, and updated. PR.IR-01.8 ensures that these documented flows are also actively enforced and monitored.

Controlling information and data flows is especially critical in ICS/OT environments, where any unauthorised or unintended exchange of data can compromise health, safety, and environmental protection, and must therefore be strictly governed.

To implement this requirement effectively, the organisation should:

- **Define and Enforce Flow Control Policies**
  Tools and policies should be used to control how data moves between systems and within different parts of the network, ensuring only authorised flows occur.
- **Encrypt Data-in-Transit and at-Rest**
  Use secure encryption protocols such as TLS/SSL for data in transit and AES-256 for data at rest to protect confidentiality and integrity.
- **Use Multi-Factor Authentication (MFA)**
  MFA should be implemented to verify the identity of users accessing systems that handle or transmit sensitive data.
- **Secure APIs**
  APIs used for inter-system communication should follow secure development practices and be regularly reviewed for vulnerabilities.
- **Implement Continuous Monitoring**
  Real-time monitoring tools should detect unauthorised data flows or anomalies, with alerts for immediate response.
- **Conduct Periodic Audits**
  Regular audits should verify compliance with data flow policies and identify potential weaknesses or unauthorised changes.
- **Apply Network Segmentation**
  Segment the network to restrict unnecessary data flows and limit the impact of potential breaches.
- **Secure Remote Access**
  VPNs should be used to securely connect remote systems and users to the organisation's network.
- **Deploy Data Loss Prevention (DLP)**
  DLP solutions should monitor and control the transfer of sensitive information, especially when leaving the organisation.
- **Train Staff and Raise Awareness**
  Employees should be trained on data handling policies and the importance of controlling information flows.
- **Simulate Phishing Attacks**
  Regular phishing simulations should be conducted to reduce the risk of social engineering attacks.

PR.IR-01.9 **The organisation shall manage interfaces with external telecommunications services as part of its broader network security policy, by defining how traffic is controlled, ensuring the confidentiality and integrity of transmitted information, and reviewing and documenting any exceptions to established rules.**

Implementation guidance

This control builds on PR.IR-01.8 by focusing specifically on how external communications are governed within the organisation's network security policy. While firewall configurations and baseline security settings provide technical enforcement, this requirement emphasises the policy and oversight layer.

To implement this effectively, the organisation should:

- Integrate Traffic Flow Management into the Network Security Policy
  The network security policy should include clear rules for how data and voice traffic is allowed to flow between internal systems and external telecommunications services.
- Define Security Objectives and Scope
  The policy should outline the goals for protecting external communications and specify which systems and services are covered.
- Control and Monitor Traffic
  Network traffic should be continuously monitored to ensure it complies with defined rules. Suspicious or unauthorised flows should trigger alerts and be investigated.
- Protect Data in Transit
  Confidentiality and integrity of transmitted data should be protected using encryption protocols such as TLS/SSL.
- Document and Review Exceptions
  Any exceptions to the traffic flow rules (e.g., temporary access for a third party) should be formally documented, justified, and regularly reviewed.
- Respond to Incidents
  The organisation should be prepared to isolate and respond to abnormal or malicious traffic patterns quickly.
- Maintain Policy Alignment
  The traffic flow component should align with other elements of the network security policy, including access control, VPN usage, patch management, and incident response.

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-02.2 The organisation shall implement fire detection devices that activate and notify key personnel automatically in the event of a fire.

Implementation guidance

The goal of this control is to ensure that fire incidents are detected early and that key personnel are automatically alerted, to enable a rapid and coordinated response — especially in environments where critical systems support safety or essential operations.

To achieve this goal, the organisation should:

- Deploy automated fire detection systems using smoke and heat detectors that activate without manual intervention.
- Integrate fire detection with automatic suppression systems where appropriate (e.g. sprinklers or gas-based systems).
- Configure systems to automatically notify designated personnel or emergency responders upon activation.
- Define and maintain a notification list with clearly assigned roles, ensuring that individuals have the necessary access and clearance — particularly in sensitive or classified environments.

PR.IR-03 Mechanisms are implemented to achieve resilience requirements in normal and adverse situations

PR.IR-03.1 The organisation shall implement mechanisms to ensure that critical systems and services remain operational or can be quickly restored during both normal operations and adverse conditions.

Implementation guidance

The goal of this control is to ensure that critical systems and services remain operational, or can be quickly restored, during both normal operations and adverse conditions such as cyber-attacks, hardware failures, or natural disasters.

This control supports the broader objective of operational resilience. While redundancy (as addressed in GV.OC-04.3) helps prevent outages by duplicating components, resilience ensures that operations can continue or recover quickly even when failures do occur. Both are essential for maintaining availability in complex IT and OT environments.

To achieve this goal, the organisation should:

- Define Resilience Objectives
  - Identify critical systems and define acceptable Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
  - Align resilience goals with business continuity and disaster recovery plans.
- Design for Resilience
  - Implement fault-tolerant architectures (e.g. clustering, load balancing, geo-redundancy).
  - Use diverse technologies and suppliers to reduce dependency on single points of failure.
- Ensure Operational Readiness
  - Test failover systems regularly through simulations and switchovers.
  - Keep operational procedures and recovery instructions current and accurate.
- Enhance Cyber Resilience
  - Integrate resilience strategies into incident response plans (e.g. ransomware containment, data restoration).
  - Use immutable backups and network segmentation to limit the impact of cyber incidents.
- Assess Third-Party Resilience
  - Evaluate the resilience of critical service providers and document findings.
  - Include resilience and recovery requirements in service-level agreements (SLAs).
- Promote Continuous Improvement
  - Review and update resilience mechanisms after incidents or major changes.
  - Incorporate lessons learned into future planning and testing.

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.

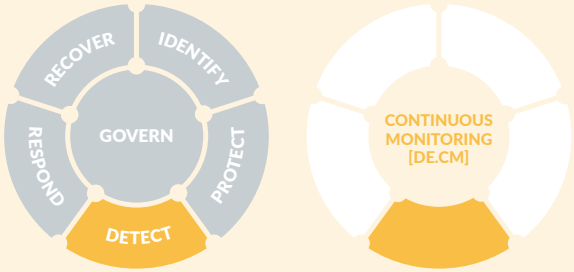
To achieve this goal, the organisation should:

- 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.


WARNING!
SYSTEM WARNING

DETECT

Detect



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

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

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

Implementation guidance

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

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

To achieve this goal, the following should be considered:

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

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

Implementation guidance

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

To achieve this goal, consider the following:

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

DE.CM-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-01.4 **The organisation shall continuously monitor its network to spot signs of cyber threats or unusual activity, using clearly defined rules for what counts as a potential security incident.**

Implementation guidance

The aim of this control is to ensure that the organisation continuously monitors its network and systems to detect signs of cyber threats or unusual activity. This is done using clearly defined rules that help identify what qualifies as a potential security incident.

To achieve this, consider the following:

- This control builds on DE.AE-08.1, which requires that incidents have to be reported based on predefined criteria.
- The organisation should decide which types of cybersecurity events and warning signs need to be monitored, and define what information must be recorded in audit logs.
- Automated tools should be used to detect suspicious activity, such as unexpected network traffic, failed login attempts, or incorrect system settings.
- Monitoring should be flexible and increase during high-risk periods, such as when threat alerts are received during geopolitical tensions, or after internal issues.
- Monitoring should include not only digital systems but also physical spaces, staff behaviour, and interactions with service providers, where relevant.
- Network activity should be continuously analysed to detect changes that might indicate weakened security, following zero-trust principles.
- Alerts should be triggered automatically when certain thresholds are met, and known false alarms should be filtered out to avoid overwhelming staff.

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-02.2 Physical access to the organisation's critical systems and devices, in addition to physical access monitoring to the facility, shall be supplemented by physical intrusion alarms, surveillance equipment, and independent monitoring teams.

Implementation guidance

The purpose of this control is to strengthen the protection of critical systems and devices by supplementing basic physical access monitoring with active intrusion detection, surveillance technologies, and independent monitoring capabilities. This helps ensure timely detection and response to physical security threats.

To achieve this purpose, consider the following:

- Intrusion detection systems should be deployed to identify unauthorised physical entry attempts. These systems may include motion sensors, door/window contact sensors, and glass break detectors, which trigger alerts when unusual activity is detected.
- Surveillance technologies such as CCTV cameras, video recording systems, and access control systems should be used to continuously monitor and record activity in sensitive areas. These systems help verify incidents and support investigations.
- Visitor tracking should be enhanced by logging all entries, including contractors and temporary personnel, using digital systems or manual logs.
- Independent monitoring teams, typically external security professionals, should be engaged to oversee surveillance systems and respond to incidents. These teams bring specialised expertise and operate separately from internal staff, making it important to apply third-party cybersecurity requirements to their operations.
- Surveillance and intrusion detection should be integrated with broader security operations, allowing alerts to be correlated with other physical and digital indicators of compromise.

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.

DE.CM-03.2 **End point and network protection tools that monitor end-user behaviour for dangerous activity shall be managed.**

Implementation guidance

This control builds on DE.CM-03.1 by shifting the focus from implementation to ongoing management of monitoring 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

DE.CM-06.1 **External service provider activities and services shall be secured and 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 unauthorised access — should be detected early, reported quickly, and addressed effectively.

DE.CM-06.2 **External service providers' conformance with personnel security policies and procedures and contract security requirements shall be monitored relative to their cybersecurity risks.**

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

DE.CM-09.1 **The organisation shall monitor computing hardware, software, runtime environments, and their data to detect 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.

DE.CM-09.2 **The organisation shall implement hardware integrity checks to detect unauthorised tampering of critical system hardware. Controls shall be proportionate to the organisation's risk profile and operational capacity.**

Implementation guidance

The goal of this control is to ensure that critical hardware components are protected against unauthorised tampering. By implementing integrity checks that match the organisation's risk level and operational capacity, it becomes possible to detect physical or firmware-level changes that could compromise security.

Consider the following elements to achieve this goal:

- **Define What Needs Protection**
  Identify which systems are most critical, such as servers handling sensitive data, industrial control systems (ICS/SCADA), or cryptographic devices, and prioritise them based on business impact, legal requirements, and exposure to threats.
- **Choose the Right Level of Protection**
  Select controls based on how critical the system is and what the organisation can support:
  - **Basic controls**: Locked server rooms, tamper-evident seals, secure boot, and regular hardware audits.
  - **Intermediate controls**: Alerts when hardware is opened, use of Trusted Platform Modules (TPMs), and firmware validation tools.
  - **Advanced controls**: Remote validation of hardware state, tamper-resistant cryptographic hardware (HSMs), and monitoring for hardware-level anomalies using security tools.
- **Connect to Security Operations**
  Feed alerts from hardware integrity tools into central monitoring systems (like a SIEM or SOC) for real-time visibility. Define how to respond if tampering is suspected.
- **Assign Clear Responsibilities**
  Designate roles for designing, implementing, and responding to hardware integrity issues. Use role profiles (e.g. from ENISA ECSF) to guide responsibilities:
  - Security architects design the controls.
  - System administrators implement and monitor them.
  - Incident responders investigate alerts.
- **Document and Review**
  Include hardware integrity checks in security policies, risk assessments, and audit logs. Review their effectiveness at least once a year or after major changes or incidents.
- **Train Staff and Raise Awareness**
  Train relevant personnel to recognise signs of tampering, use integrity tools correctly, and follow reporting procedures.

DE.CM-09.3 **The organisation's incident response plan shall include measures to detect unauthorised tampering with the hardware of critical systems.**

Implementation guidance

The goal of this control is to ensure that the organisation's incident response plan includes steps to detect and respond to unauthorised tampering of critical hardware. This helps the organisation react quickly and effectively if someone tries to physically or digitally compromise important systems. This control can be implemented in a practical and scalable manner.

By considering the below measures, also small organisations can effectively include hardware tampering detection in their incident response capabilities, without requiring extensive resources:

- **Incident Response Plan**
  The incident response plan should include clear instructions for what steps to take if hardware tampering is suspected.
- **Regular Inspections**
  Have IT and OT staff or designated personnel regularly inspect critical hardware for signs of tampering, such as broken seals, loose cables, or unexpected changes.
- **Monitoring Tools**
  Simple tools can be used to send alerts when something unusual happens to a device, such as the case being opened, a new USB device being connected, or the system restarting unexpectedly. Many of these tools are designed to be affordable and easy to use, especially for small organisations.
- **Training and Awareness**
  Train employees to recognise signs of hardware tampering and report any suspicious activity. Awareness is key to early detection.
- **Vendor Support**
  Use tools or services offered by hardware vendors to help detect tampering, often included with support contracts.

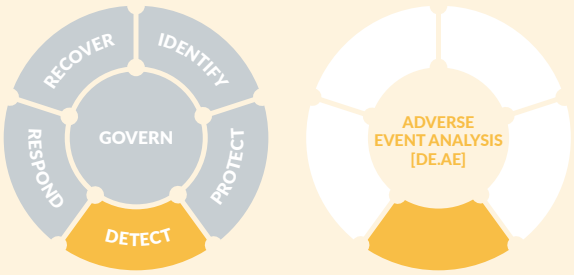
DE.CM-09.4 The organisation shall establish a system to accurately distinguish between legitimate alerts and false positives, ensuring effective detection and removal of malicious code.

Implementation guidance

The goal of this control is to ensure that the organisation can accurately identify real threats while avoiding unnecessary alerts caused by false positives. This helps improve the effectiveness of detecting and removing malicious code, while reducing wasted time and resources responding to harmless activity.

To help detect and remove malicious code effectively while avoiding false alarms, the following practices should be considered:

- **Automatic Updates**
  Malicious code protection tools should be configured to update automatically where possible, or manually according to a defined schedule, in line with organisational policies and operational constraints.
- **Secure Development Practices**
  Software used in IT and OT systems should follow secure development practices, including code reviews and vulnerability checks, to reduce the risk of introducing malicious code.
- **Layered Protection**
  Both signature-based protection (which detects known threats) and behaviour-based protection (which looks for unusual or suspicious activity) should be used in places where networks connect to the internet, where staff access control systems, and where files or data are shared between systems.
- **Scanning for Threats**
  Protection tools should be set to perform regular scans and, where feasible, real-time checks of files and data transfers, especially those coming from external sources or removable media.
- **Blocking and Quarantine**
  Detected malicious code should be blocked and isolated to prevent it from affecting other systems. In OT environments, this should be done in a way that does not disrupt critical operations.
- **Alerts and Notifications**
  Alerts should be sent to designated personnel when malicious code is detected, with clear procedures for responding in both IT and OT contexts.



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.

DE.AE-02.2 The organisation shall implement automated mechanisms where feasible to review and analyse detected events.

Implementation guidance

The goal of this control is to ensure that the organisation uses automation, where practical, to support the efficient and consistent review and analysis of detected cybersecurity events. This helps reduce the risk of human error, speeds up threat detection and response, and allows limited security resources (especially in smaller organisations) to focus on higher-value tasks like investigating complex incidents or improving defences.

To achieve this goal, the following should be considered:

- **Use Built-in Capabilities**
  Enable and configure logging and alerting features in existing platforms (e.g. Microsoft 365, Google Workspace, firewalls) to automatically detect suspicious activity.
- **Deploy Lightweight Detection Tools**
  Use affordable endpoint detection and response (EDR) solutions that offer automated alerts and basic analysis, such as detecting malware or unusual login behaviour.
- **Consider Managed Detection Services**
  For organisations with limited internal resources, a Managed Detection and Response (MDR) service can provide outsourced monitoring, threat detection, and incident response.
- **Automate High-Impact Areas**
  Focus automation on common threat indicators, such as:
  - Multiple failed login attempts
  - Unusual access to sensitive files
  - Unexpected outbound traffic
- **Integrate Threat Intelligence**
  Use free or low-cost threat intelligence feeds to enhance detection tools with known indicators of compromise and attacker behaviours.
- **Maintain Manual Review Practices**
  Schedule regular manual reviews of logs and alerts to identify threats that automated tools may miss, especially those involving new or subtle attack techniques.

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-03.3 **The organisation shall combine event analysis with information from vulnerability scans, system performance data, monitoring of critical systems, and facility monitoring, where feasible.**

Implementation guidance

The goal of this control is to strengthen the organisation's ability to detect complex or hidden threats by combining event analysis with other relevant data sources.

This broader view supports more accurate and timely identification of suspicious activity, and the following should be considered to achieve the goal of this control:

- Tools that collect and link data from different systems (such as SIEM, XDR, or SOAR) should be used to support this integration.
- Security issues reported by suppliers or trusted sources should be collected quickly and reviewed for possible risks.
- Data from different monitoring systems should be brought together to make it easier to detect patterns or problems.
- The setup should allow fast detection and response when something unusual is found.

DE.AE-04 The estimated impact and scope of adverse events are understood

DE.AE-04.1 **The organisation shall assess the negative impacts of detected events on its operations, assets, and individuals, and shall link these impacts to the results of its risk assessments.**

Implementation guidance

The goal of this control is to ensure that the organisation understands how detected events could cause harm, and uses this understanding to guide risk-based decisions and responses.

To achieve the goal of this control, the following should be considered:

- Tools that help estimate the scope and impact of events should be used to support this assessment.
- The assessment should consider how problems in one part of a system could affect other connected parts.
- Negative impacts can include financial loss, service disruption, damage to equipment, or harm to people.
- Detected events can include cyber incidents, system failures, or natural disasters.
- The severity and likelihood of these impacts should be evaluated and compared with existing risk assessments.
- This comparison should help prioritise actions, allocate resources, and improve response planning.

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

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-02.2 **Automated tools shall be used to support the investigation and impact assessment of validated cybersecurity incidents.**

Implementation guidance

The goal of this control is to ensure that organisations are equipped with the technical capabilities to efficiently and accurately handle cybersecurity incidents once they have been validated.

To implement this control, the following should be considered:

- Automated tools should help collect, analyse, and correlate incident data to support timely and accurate investigation.
- These tools should assist in identifying the scope, severity, and potential impact of incidents that have been validated through triage. A validated incident is one that has been confirmed to be cybersecurity-related (not a false alarm or unrelated technical issue, meets predefined severity criteria (such as indicators of compromise, threat intelligence, or known attack patterns), and requires response actions (meaning it meets the threshold for further investigation, categorisation, and escalation).
- The following types of tools can be considered to support these activities:
  - Security Information and Event Management (SIEM) systems for centralised log collection and analysis.
  - Extended Detection and Response (XDR) platforms for integrated threat detection across endpoints, networks, and servers.
  - Security Orchestration, Automation and Response (SOAR) platforms to automate workflows and coordinate response actions.
  - Threat Intelligence Platforms to enrich incident data with external threat context.
  - Network Intrusion Detection Systems (NIDS) to monitor and alert on suspicious network activity.
  - Computer Incident Response Centres (CIRCs) for centralised coordination and expert analysis.
- Automated mechanisms should be integrated with the incident response process to ensure that validated incidents are investigated efficiently and prioritised appropriately, in line with the organisation's incident response plan.

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

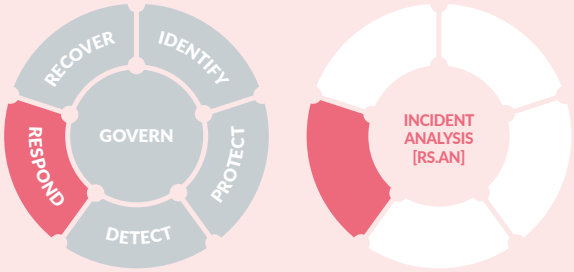
RS.MA-05.1 **Clear criteria shall be defined and applied to determine when incident recovery processes need to be initiated.**

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.



Investigations are conducted to ensure effective response and support forensics and recovery activities

RS.AN-03 Analysis is performed to establish what has taken place during an incident and the root cause of the incident

RS.AN-03.1 Each incident shall be analysed to determine what occurred and to identify its root cause.

Implementation guidance

The goal of this control is to understand the full scope of a cybersecurity incident and identify its root cause, enabling effective response and prevention of similar future events.

To achieve this goal, the organisation should consider the following:

- The sequence of events during the incident should be reconstructed, identifying which systems, assets, and resources were involved.
- Vulnerabilities, threats, and threat actors linked to the incident should be identified, whether directly or indirectly involved.
- Forensic analysis should be used when necessary to examine collected data and determine the root cause.
- The analysis should focus on identifying underlying, systemic causes, not just immediate triggers.
- Cyber deception technologies should be reviewed for additional insights into attacker behaviour.

RS.AN-06 Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved

RS.AN-06.1 Actions performed during an investigation shall be recorded, and the records' integrity and provenance shall be preserved.

Implementation guidance

The goal of this control is to ensure that all actions taken during an incident investigation are properly recorded, and that the integrity and origin of those records are protected.

To achieve this goal, the organisation should:

- Require all personnel involved in incident response (e.g., responders, system administrators, engineers) to log their actions in a way that prevents tampering or deletion.
- Assign responsibility to the incident lead for documenting the full investigation, including timelines, decisions, and sources of information.
- Ensure that all records are stored securely and remain traceable to their original source.

RS.AN-07 Incident data and metadata are collected, and their integrity and provenance are preserved

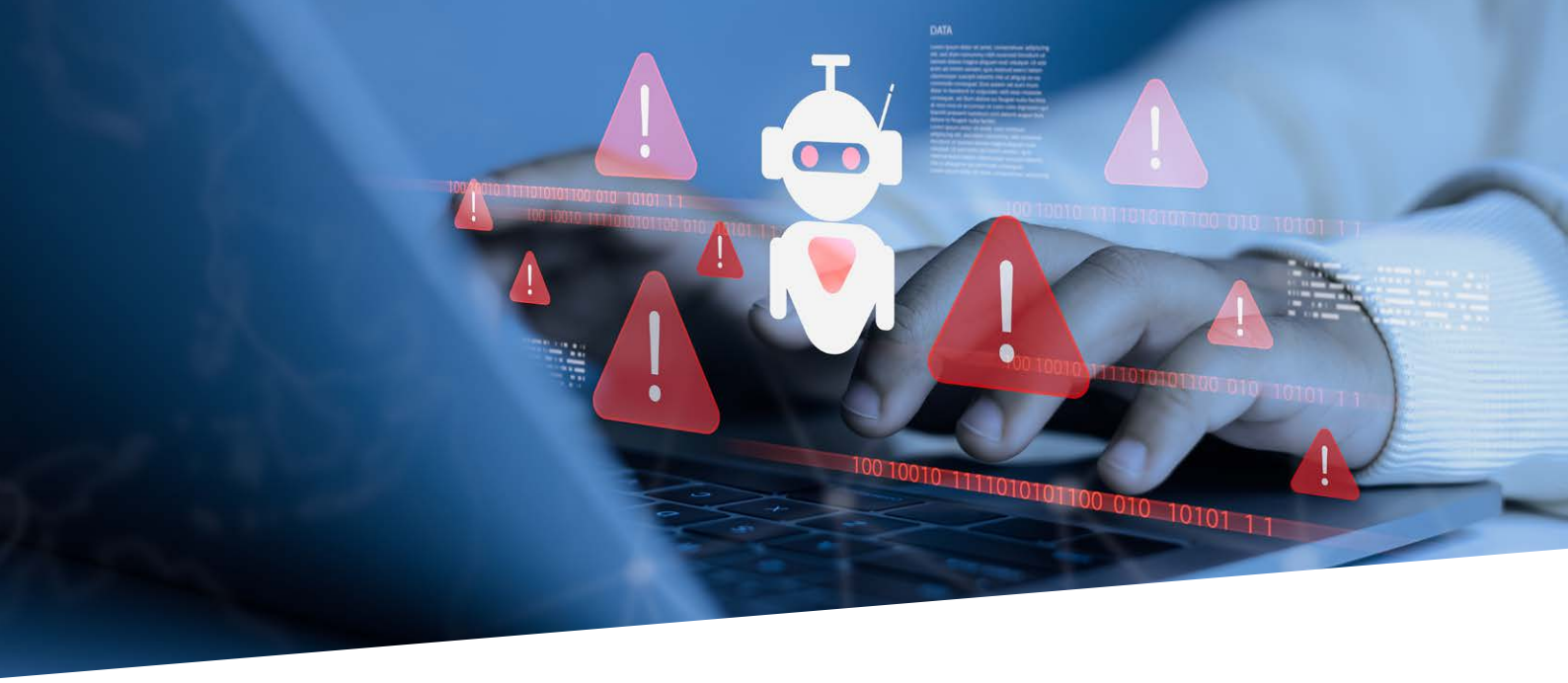
RS.AN-07.1 Incident data and metadata shall be collected and protected to ensure their accuracy, authenticity, and traceability.

Implementation guidance

The goal of this control is to ensure that all relevant information about a cybersecurity incident is accurately captured, securely stored, and reliably traceable, so it can be used effectively for response, investigation, and legal or compliance purposes.

Therefore the following should be considered:

- Incident data and metadata (such as the source of the data and the time it was collected) should be gathered and stored in a way that protects them from tampering or loss.
- The integrity and origin of this information should be preserved using methods such as:
  - **Chain of custody documentation** to track how the data is handled from collection to analysis.
  - **Digital signatures and encryption** to prevent unauthorised access and confirm authenticity.
  - **Audit logs** to record who accessed or changed the data and when.
- Collecting and protecting this information should support:
  - **Timely response** by helping to understand when and how the incident occurred.
  - **Investigation and analysis** by providing reliable details about the incident's cause, scope, and impact.
  - **Legal and compliance needs** by ensuring the data can be used as evidence if required.



RS.AN-08 An incident's magnitude is estimated and validated

RS.AN-08.1 An incident's magnitude shall be estimated and validated.

Implementation guidance

The goal of this control is to ensure that organisations have a clear understanding of the full scope and impact of a cybersecurity incident, so that response actions can be appropriately scaled, prioritised, and coordinated.

Therefore the following should be considered:

- The scope and impact of an incident should be assessed by examining not only the initially affected system but also other systems or devices that may be compromised.
- Indicators of Compromise (IoCs), such as unusual network activity, unauthorised access attempts, or unexpected software changes, should be identified to understand how far the incident has spread.
- Signs of persistence, including backdoors or malware that allow continued access, should be investigated to determine whether the attacker remains active in the environment.
- Automated tools should be used to scan for IoCs and persistence mechanisms across potentially affected assets to support timely and thorough analysis.
- The validated magnitude of the incident should inform how the incident is categorised, prioritised, and escalated, as described in RS.MA-03.1 (Important), ensuring that response actions are aligned with the actual risk and business impact.

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.

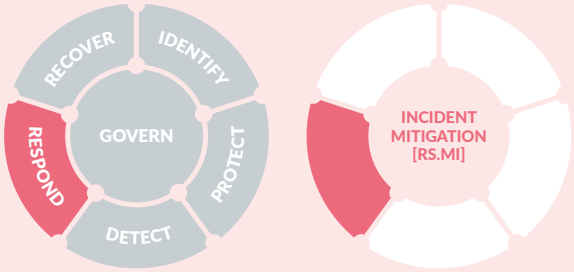
RS.CO-02.2 **Cybersecurity incidents shall be shared with relevant external stakeholders within the timeframes defined in the Incident Response Plan, including reporting significant incidents to authorities as required by law.**

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.

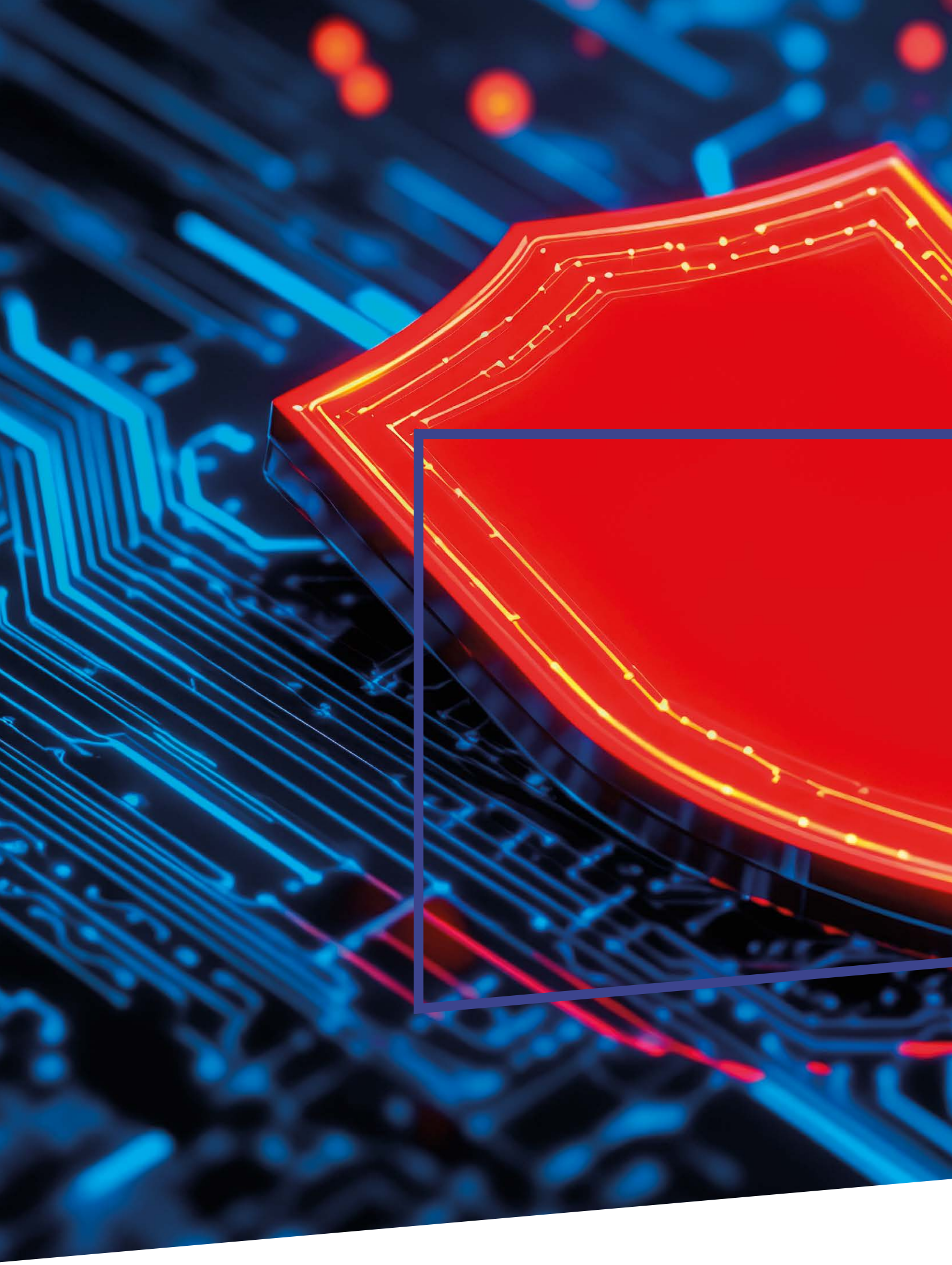
RS.MI-01.2 **The organisation shall detect unauthorised access or data leakage and take appropriate mitigation actions, including monitoring of critical systems at external boundaries and key internal points.**

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

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-02 Recovery actions are selected, scoped, prioritised, and performed

RC.RP-02.1 **The organisation's essential functions and services shall be continued with little or no loss of operational continuity, and continuity shall be maintained until full system recovery.**

Implementation guidance

The goal of this control is to minimise disruption to critical operations during incidents and ensure they remain functional until systems are fully restored.

To achieve this goal, the organisation should:

- Plan for Continuity
  - A business continuity plan should be maintained to identify essential functions and define procedures for uninterrupted operation during incidents.
  - An incident response plan should be included, detailing steps for containment, damage assessment, and staged recovery.
- Sustain Operations Until Recovery
  - Continuity measures should support essential functions until full restoration is achieved.
  - Temporary workarounds, redundant systems, or manual procedures should be used where necessary to maintain operations.
- Prioritise Recovery
  - Business impact analysis and system categorisation should be used to define recovery priorities.
  - Systems should be categorised based on the impact of losing availability, integrity, or confidentiality, with special attention to safety-critical OT environments.
- Ensure Data Resilience
  - Robust backup solutions should be implemented to enable fast and reliable data restoration.
  - Backups should be secured and tested regularly.
- Monitor and Respond
  - Systems should be continuously monitored to detect disruptions early.
  - Quick response actions should be taken to minimise operational impact.
- Test and Improve
  - Recovery procedures should be tested regularly to ensure effectiveness.
  - Recovery actions should be documented and reviewed to improve readiness over time.

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

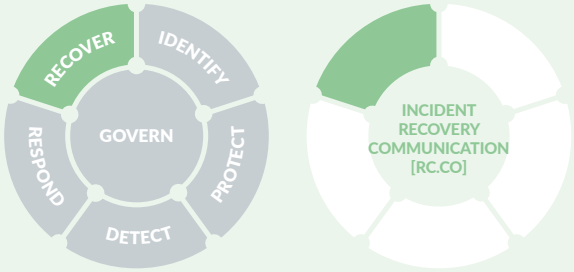
RC.RP-06.1 The end of incident recovery shall be formally declared based on predefined criteria, and all incident-related documentation shall be completed and reviewed.

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.

RC.CO-04.2 **The organisation shall assign a Public Relations Officer (PRO) to manage public communications during information/cybersecurity incident recovery, ensuring that public updates are shared while maintaining the confidentiality, integrity, and accuracy of the information.**

Implementation guidance

The goal of this control is to ensure that public communication during cybersecurity or information security incident recovery is professionally managed, accurate, and aligned with the organisation's confidentiality and integrity standards. By assigning a dedicated Public Relations Officer (PRO), the organisation ensures that public messaging is handled by a trained individual who can maintain trust, protect the organisation's reputation, and comply with legal and regulatory requirements.

To achieve this goal, the following should be considered:

- **Assign a Public Relations Officer (PRO)**: Designate a qualified individual to handle public communications during incident recovery. The job description of the PRO may include the following:
  - Developing Communication Strategies
  - Writing and Distributing Press Releases
  - Building and maintaining relationships with journalists and media outlets to ensure positive coverage (media relations).
  - Handling communication during crises to maintain the organisation's reputation (crisis management).
  - Keeping track of media coverage and conducting media analysis to gauge public perception (monitoring media coverage).
- **Develop Communication Protocols**: Establish clear protocols for the PRO to follow when sharing public updates, ensuring all information maintains confidentiality, integrity, and accuracy.
- **Training and Preparedness**: Provide the PRO with training on incident communication strategies and ensure they are prepared to act swiftly during an incident.
- **Regular Reviews**: Periodically review and update communication protocols to adapt to new challenges and ensure effectiveness.

RC.CO-04.3 **The organisation shall implement a crisis communication strategy to mitigate negative impacts during a crisis and help restore its reputation afterward.**

Implementation guidance

The goal of this control is to ensure that the organisation is prepared to manage communications effectively during and after a crisis, in order to minimise reputational damage, maintain stakeholder trust, and support recovery efforts.

To achieve this goal, the following should be considered:

- **Develop the Strategy**: Create a comprehensive crisis communication plan that outlines procedures for managing communications during and after a crisis to employees, customers, partners, regulators, and the media. Ensure that all communications comply with legal requirements and industry regulations.
- **Assign Roles and Responsibilities**: Designate a crisis communication team, including a spokesperson, to handle public and internal communications. The participation of PR professionals, legal advisers and senior management should be considered.
- **Establish Communication Channels**: Identify and set up reliable channels for disseminating information, such as social media, press releases, and internal communications platforms. Media coverage and social media should be continuously monitored for misinformation or negative sentiment. Inaccuracies should be responded to and corrected immediately.
- **Training and Drills**: Conduct regular training sessions and crisis simulations to ensure the team is prepared to respond effectively.
- **Monitor and Adapt**: Continuously monitor the situation and adapt the communication strategy as needed to address evolving circumstances.
- **Post-Crisis Review**: After the crisis, review the communication efforts to identify lessons learned and improve future responses.

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 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-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 ADDITIONAL KEY MEASURES FOR THE ASSURANCE LEVEL 'ESSENTIAL'

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

Govern

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-05.2 Contractual information/cybersecurity requirements for suppliers and external partners shall be implemented to ensure a verifiable flaw resolution process and to ensure that deficiencies identified during information/cybersecurity testing and evaluation are remedied.

GV.SC-05.3 The organisation shall establish contractual requirements permitting the organisation to review the information/cybersecurity programs implemented by suppliers and third-party partners.

Identify

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

ID.AM-03-3 The organisation's network communication and external data flows shall be mapped, documented, authorised, and updated when changes occur.

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

ID.AM-08.7 The organisation shall prevent unauthorised removal of maintenance equipment containing critical system information of the organisation.

ID.AM-08.9 Maintenance tools and portable storage devices shall be inspected as they enter the facility and shall be protected by anti-malware solutions that scan them for malicious code before they are used on the organisation's systems.

ID.AM-08.10 The organisation shall verify security controls following maintenance or repairs/patching, and take action as appropriate.

Protect

PR.DS-02 The confidentiality, integrity, and availability of data-in-transit are protected

PR.DS-02.1 Portable storage devices containing system data shall be controlled and protected while in transit and in storage.

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

Govern

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.

ANNEX E: LIST OF CONTROLS LINKED TO THE MANAGEMENT ASPECTS FOR THE ASSURANCE LEVEL 'ESSENTIAL'

Govern

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

GV.RR-02.2 The organisation shall appoint a senior-level executive information security officer.

GV.SC-01 A cybersecurity supply chain risk management programme, strategy, objectives, policies, and processes are established and agreed to by organisational stakeholders.

GV.SC-01.1 A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes shall be documented, reviewed, updated when changes occur, and approved by organisational stakeholders.

Identify

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

ID.RA-05.3 Risk assessment results shall be disseminated to relevant stakeholders.

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

ID.IM-03.9 The organisation shall conduct specialised assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the organisation's critical systems.

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

ID.IM-04.2 The organisation shall coordinate the development and testing of Incident Response Plans and other cybersecurity plans that affect operations with stakeholders to ensure that these plans align with overall organisational goals and enhance resilience.

Detect

DE.AE-04 The estimated impact and scope of adverse events are understood

DE.AE-04.1 Negative impacts to the organisation's operations, assets, and individuals resulting from detected events shall be determined and correlated with risk assessment outcomes.

Disclaimer

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

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

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

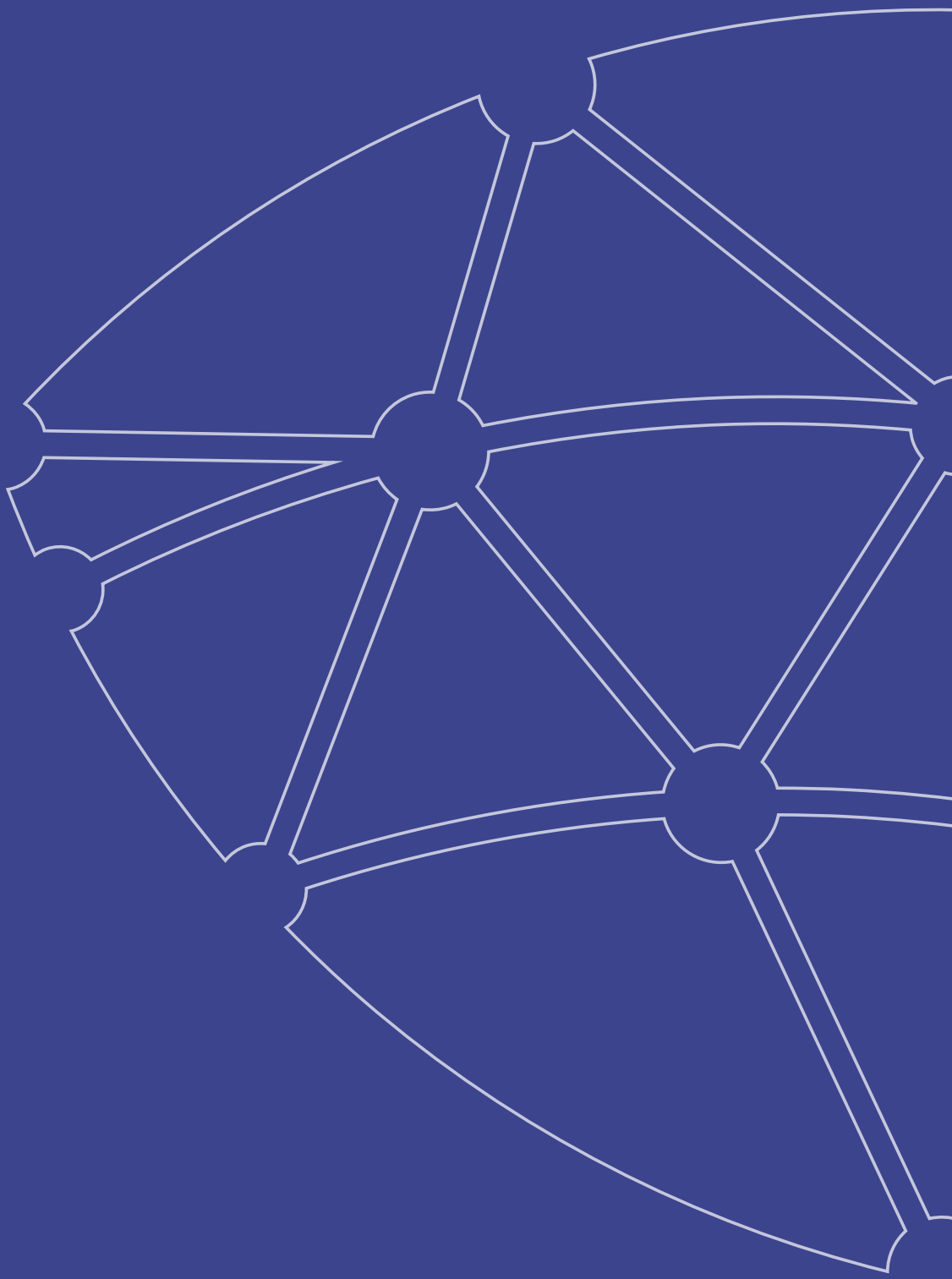
- is exclusively of a general nature and is not intended to take into consideration all particular situations.
- is not necessarily exhaustive, precise, or up to date on all points.

Responsible editor

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

Legal depot

D/2025/14828/002



Centre for Cybersecurity Belgium

Rue de la Loi, 18

1000 Brussels