Guidance

RIIO-2 Cyber Resilience Guidelines

Publication date: 5 February 2020

Contact: Stuart Okin, Head of Security, Privacy & Resilience

Team: Ofgem Competent Authority

Tel: 020 7901 1810

Email: RIIO2Cyber@ofgem.gov.uk

Ofgem has developed a detailed set of Cyber Resilience Guidelines for gas and electricity network companies and their stakeholders, associated with Network price controls: Revenue Incentives Innovation Outputs (RIIO-2).

This document acts as an operational guide to support security professionals within network companies to mature the cyber security and resilience of their network and information systems.

Version	Date	Change Log
1.0	11 September 2019	Release version of individual Cyber Resilience Guidelines and supplemental documents
1.1	20 January 2020	Consultation feedback incorporated and Ofgem internal review
1.2	03 February 2020	Editorial review
2.0	05 February 2020	Formal publication of Cyber Resilience Guidelines

Any enquiries related to the text of this publication should be sent to Ofgem at:
10 South Colonnade, Canary Wharf, London, E14 4PU. Alternatively, please call Ofgem on 0207 901 7000.

This publication is available at **www.ofgem.gov.uk**. Any enquiries regarding the use and re-use of this information resource should be sent to: psi@nationalarchives.gsi.gov.uk

Contents

Foreword

The RIIO (Revenue=Incentives+Innovation+Outputs) framework is a price control mechanism set by Ofgem, through which energy operators can seek approval for funding, including cyber security and resilience.

Each network company recently performed a short-to-medium term cyber-security improvement plan, aiming to be completed under the RIIO-1 timeframes. These plans referenced the Network and Information Systems ("NIS") Regulations 2018 requirements and the associated National Cyber Security Centre ("NCSC") sector-agnostic Cyber Assessment Framework ("CAF").

For December 2019, network companies were invited to submit Business Plans for Transmission, Gas Distribution and the Electricity System Operator, covering the RIIO-2 period. Ofgem published Business Plan Guidance for RIIO-2 (https://www.ofgem.gov.uk/publications-and-updates/riio-2-sector-specific-methodology-decision), which states, under paragraph 6.96, that; "…network companies must demonstrate how companies will take appropriate and proportionate technical and organisational cyber security measures to manage risks posed to the security of the network and information systems on which their essential services depend, and to prevent and minimise the impact of incidents on these essential services.".

To assist in developing Cyber Resilience Operational Technology ("OT") plans, Ofgem published draft guidance in September 2019. Ofgem received feedback and incorporated these into a new single document – and we would like to thank all those who contributed. It is important to note that this guidance is not a compliance benchmark, and that overall management of risks and associated mitigation planning are the sole responsibility of the network companies.

This document is based on NCSC guidance, International Organizational for Standardization ("ISO") 27019, International Electro Technical Commission ("IEC") 62443, Industrial Automation and Control Systems Security ("ISA") 99, National Institute of Standards and Technology ("NIST") 800-82, NIST 800-53 and the Health and Safety Executive - Cyber Security for Industrial Automation and Control Systems ("IACS") Edition 2 Operational Guidance 86 ("OG86").

Stuart Okin, Head of Security, Privacy & Resilience

Introduction

The following RIIO-2 guidance applies to the Cyber Resilience Scope (please see Supplemental sections of this document) and is not a compliance benchmark. The guidance found within this document is presented as a minimum set for RIIO-2 network companies to consider.

However, companies may decide to use alternative approaches and solutions, including compensating controls, depending on their risk tolerability and exposure.

This document is structured into three key sections:

1. Guidelines associated with the National Cyber Security Centre's Cyber Assessment Framework ("CAF");
2. Supplemental guidance pertaining to the OT replacement business case development, and;
3. Supplemental guidance pertaining to the scope of Operational Technology when considering the development of Cyber Resilience Plans.

RIIO-2 Cyber Resilience Guidelines A1.a Board Direction

RIIO-2 Cyber Resilience Outcome Description for A1.a Board Direction:

You have effective organisational security management led at board level and articulated clearly in corresponding policies.

RIIO-2 Cyber Resilience Guidance:

1. **Comprehensive Management System** – There is a comprehensive management system relating to the security of networks and information systems supporting the delivery of your essential service.
   a) A management system exists which clearly defines the company's approach to managing the security of networks and information systems supporting your essential service.
   b) The management system clearly defines the governance roles and responsibilities including risk ownership.
   c) The management system is reviewed in accordance with company policy and updated, if necessary, to ensure it is in line with the latest threats and the approved risk appetite.
   d) The management system consists of appropriate policies, standards, processes, procedures and/or practices which translate and embed the board's direction into business as usual activities.
   e) The management system is integrated into the company's corporate management system.
   f) The management system is communicated to relevant personnel.

2. **Board Level Ownership** – There is a board-level individual[1] who has overall accountability for the security of networks and information systems supporting your essential service and drives regular discussion at board-level.
   a) A member of the board should be the owner of risks, with accountability for ensuring that risks are identified, assessed and managed to the required standard.
   b) The risk owner is also accountable for ensuring that security issues are regularly discussed by the board, in accordance with company policy.

[1] or a suitably accountable delegate.

c) The board member may delegate the responsibility but retains the accountability for managing risk.

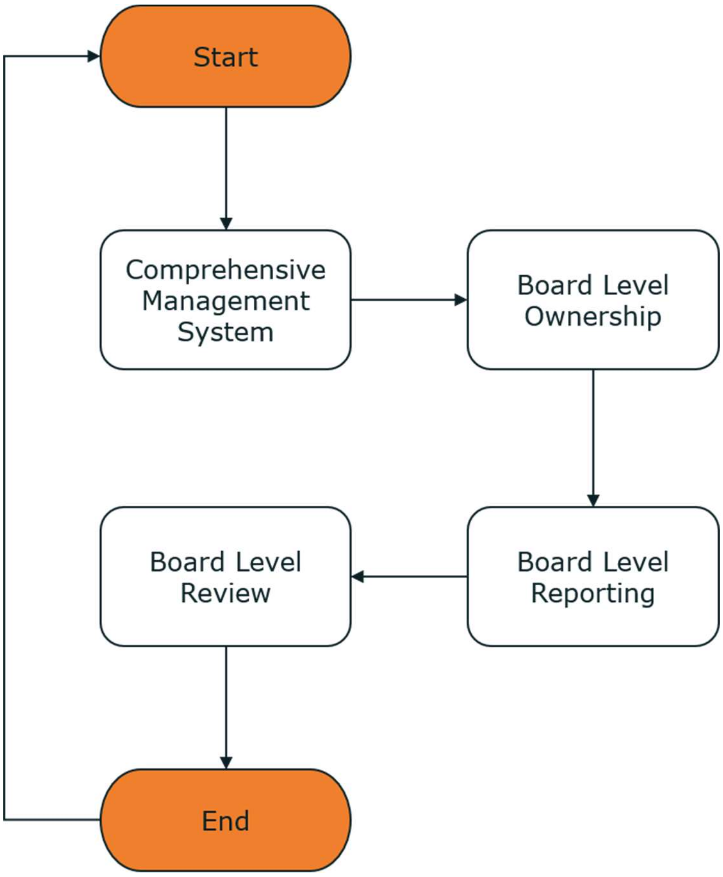
3. **Board Level Reporting** – Reports are issued to the board containing timely and accurate information informed by expert guidance.
   a) Senior management supply the board, in accordance with company policy, with regular reports on the security of networks and information systems supporting the delivery of your essential service.
   b) These reports should be prepared by suitably qualified and experienced personnel from within the organisation or third parties.
   c) Reports could include, but not be limited to:
      - Cyber security risk status and trajectory;
      - Cyber security risks in relationship to the company position within the supply chain;
      - Cyber security performance (supported by key performance indicators);
      - Incidents experienced within the organisation;
      - Incidents experienced in the industry or similar industries;
      - Progress against Cyber improvement plans;
      - Any changes to relevant cyber security threats.

4. **Board Level Review** – Board to review regularly security of networks and information systems supporting the delivery of essential services.
   a) The security of networks and information systems supporting the delivery of essential services should be a standing item on the board agenda and monitored as part of the organisation’s enterprise risk management system.

References and Further Guidance:

- NIST 800-53 R4 – Appendix D: CA-1 Security Assessment and Authorisation Policies and Procedures, PL-1 Security Planning Policy and Procedures
- OG86 – Appendix 2 A1 Governance

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines A1.b Roles and Responsibilities

RIIO-2 Cyber Resilience Outcome Description for A1.b Roles and Responsibilities:

Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.

RIIO-2 Cyber Resilience Guidance:

1. **Define Roles and Responsibilities** – Roles and responsibilities for the security of networks and information systems supporting your essential service are clearly defined.
   a) The company should ensure that roles and responsibilities are defined with sufficient detail for employees and third-party personnel to understand their roles and responsibilities.
   b) Key roles and assigned personnel are published internally and kept-up to-date.
   c) Definitions may be in the form of job descriptions.
   d) Roles can include, but is not limited to:
      - Operational Technology (OT) personnel who may be implementing and supporting OT devices;
      - Operations personnel responsible for delivery of the service and meeting demand;
      - Process safety management personnel whose job it is to ensure that no Health, Safety and Environment (HSE) incidents occur;
      - Information Technology (IT) personnel who may be responsible for corporately managed IT networks and systems;
      - Security personnel associated with physical and IT security at the site;
      - Additional resources who may be in the legal, human resources and customer support.

2. **Communicate Roles and Responsibilities** – Communicate roles and responsibilities for the security of networks and information systems supporting your essential service ensuring clarity and understanding across the organisation.
   a) A responsible, accountable, consulted and informed (RACI) matrix should be used to highlight role interdependencies to provide clarity, alignment, and set expectations of people, their roles and their responsibilities within the organisation (e.g. system operator and system owner).

3. **Suitable Skills and Experience** – Roles are assigned to personnel with the appropriate knowledge and capabilities.
   a) The knowledge and the capabilities of personnel to whom roles are to be assigned should be assessed and, if necessary, additional training and/or support is provided.
   b) Those assigning roles should have sufficient understanding of the role and responsibilities to assess the suitability of the intended role holder.

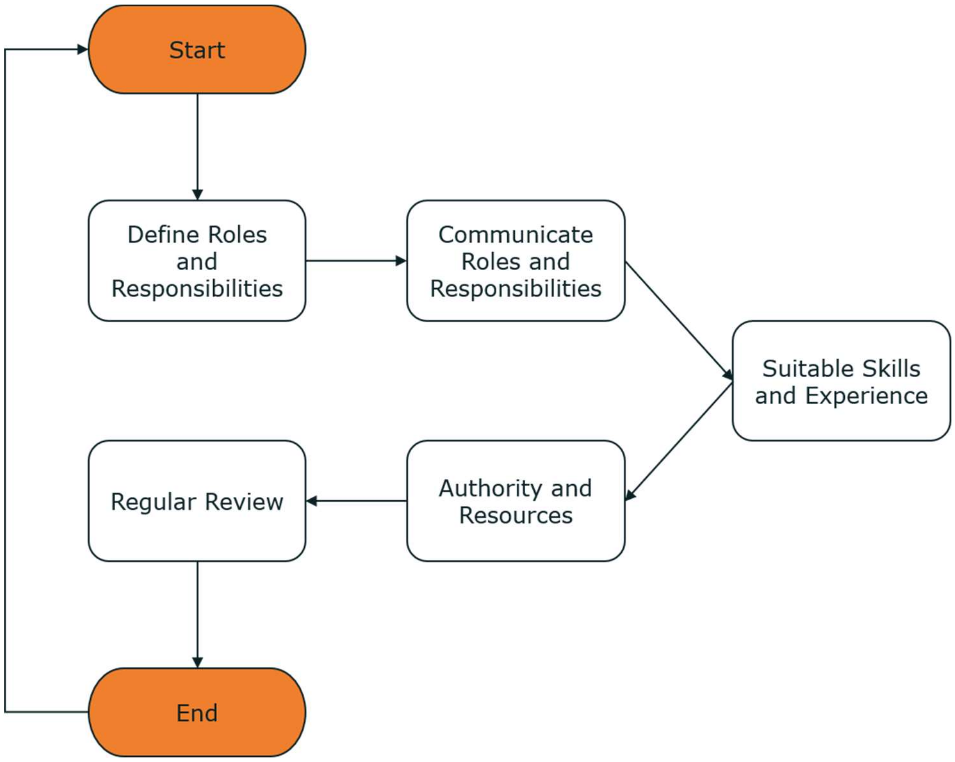
4. **Authority and Resources** – Personnel to whom roles have been assigned will be given the appropriate authority and resources to carry out their duties.
   a) Personnel should be provided with sufficient information, financial, physical and human resources to carry out their duties.

5. **Regular Review** – Roles and responsibilities for the security of networks and systems supporting your essential service are to be regularly reviewed.
   a) Definitions of roles and responsibilities should periodically be reviewed, in accordance with company policy, with employees and third parties to ensure they remain relevant and understood.

References and Further Guidance:

- NIST SP800-82 R2 – Section 4.2
- OG86 – Appendix 2 - A1 Governance
- IEC 62443/ISA99 2-1 – Sections A.3.2.2.2, A.3.2.3.4.2
- ISO 27019 – Sections 6.1.1, 6.1.2

Guidance Flow:


Start
Define Roles and Responsibilities
Communicate Roles and Responsibilities
Suitable Skills and Experience
Authority and Resources
Regular Review
End

RIIO-2 Cyber Resilience Guidelines A1.c Decision Making

RIIO-2 Cyber Resilience Outcome Description for A1.c Decision Making:

You have senior-level accountability for the security of networks and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the delivery of essential services are considered in the context of other organisational risks.

RIIO-2 Cyber Resilience Guidance:

1. **Appropriately Skilled Risk Management Team** – Risk management decisions are assigned to personnel with the appropriate skills, knowledge, tools and authority.
   a) The personnel responsible for risk management and treatment should be:
      - Suitably experienced in the design, use and operation of OT;
      - Understand the operational business model of the company;
      - Knowledgeable in the assets and dependencies on third parties used to deliver and support the essential services.

2. **Define Risk Appetite** – Senior management's risk appetite regarding the essential service is defined and agreed.
   a) The risk appetite should be agreed by the board.
   b) The risk appetite should be reviewed periodically, in accordance with company policy, or due to any significant change in threat level.
   c) The risk appetite, which has been agreed at board level, should be communicated to all relevant personnel, who are updated promptly if there are any changes in the risk appetite or associated guidance as a result of any review.

3. **Effective Risk Decisions** – Risk management decision makers understand their responsibilities for making effective and timely decisions regarding the security of networks and information systems supporting your essential service in the context of the risk appetite.
   a) Risk management decision-makers should be properly briefed and trained.
   b) Those involved should be given the necessary authority to make decisions and drive risk management activities in line with the guidance from the board.
   c) The risk management function should be part of their formal job description and they are given the necessary time and resources to do the work effectively.

4. **Delegation and Escalation** – Suitable structures are in place to support the delegation and escalation of risk management decision making to the appropriate level.
    a) Risk management decision-makers should be given the necessary authority to make decisions and drive risk management activities in line with the guidance from the board.
    b) The decision makers should be given appropriate support by senior management and their authority is promulgated to those with a need to know in order to facilitate their work to meet objectives.

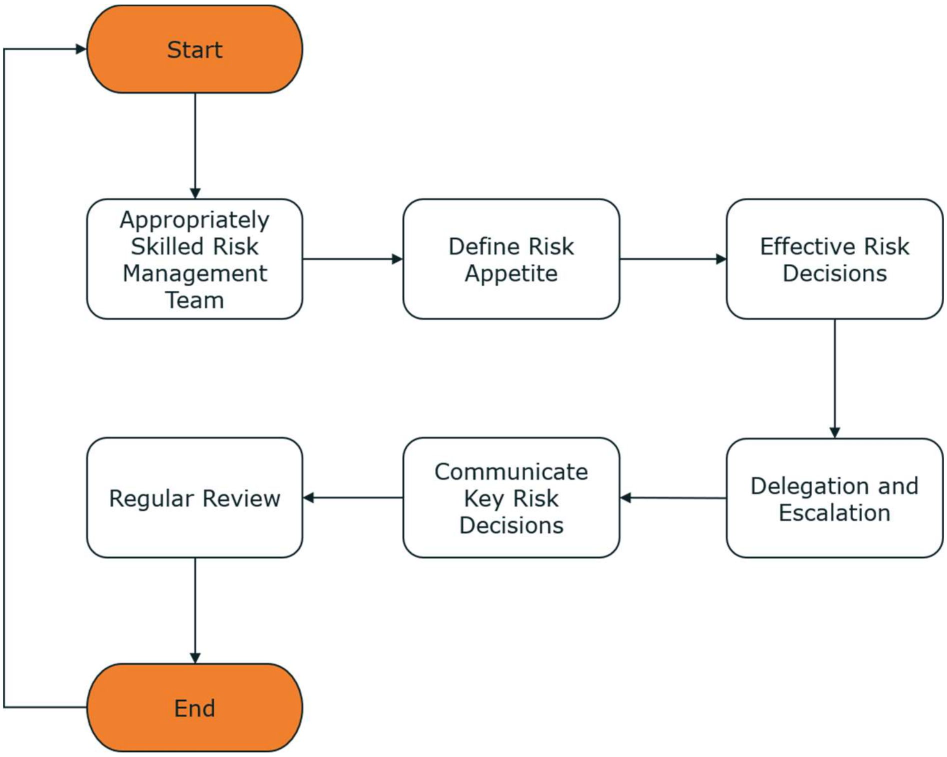
5. **Communicate Key Risk Decisions** – Key risk decisions concerning security of networks and information systems supporting your essential service are communicated to senior management.
    a) The policy and direction surrounding risk should be:
        - Drafted by a subject matter expert, and reviewed and approved by the board;
        - Documented and disseminated directly to those who need it as part of their role;
        - Published in the company's cyber security management system where it can be accessed by anyone with a need to know.

6. **Regular Review** – Risk management decisions are reviewed periodically to ensure their continued relevance and validity.
    a) The decisions and treatment plans made concerning risk management should be subject to periodic review by a subject matter expert in risk and OT who is not part of the risk management team. This may be a third-party assessor, conducting a fully independent review.
    b) The review should consider the continued relevance and validity of the methodology for the selection of the approach (e.g. treat, tolerate, terminate & transfer), control type and associated countermeasures used for risk treatment

References and Further Guidance:

- NIST 800-53 R4 – Appendix D: RA-1 Risk Assessment Policy and Procedures, RA-2 Security Categorization, RA-3 Risk Assessment
- OG86 – Appendix 2 - A1 Governance

Guidance Flow:


Start
Appropriately Skilled Risk Management Team
Define Risk Appetite
Effective Risk Decisions
Delegation and Escalation
Communicate Key Risk Decisions
Regular Review
End

RIIO-2 Cyber Resilience Guidelines A2.a Risk Management Process

RIIO-2 Cyber Resilience Outcome Description for A2.a Risk Management Process:

Your company should have effective internal processes for managing risks to the security of network and information systems related to the delivery of essential services and should communicate risk associated activities.

RIIO-2 Cyber Resilience Guidance:

1. **Security risks to networks and information systems supporting your essential service should be identified, analysed, prioritised and managed.**
   a) Risks should be identified, analysed, prioritised and managed for all assets in scope that are supporting your essential services.
   b) The organisation should use a documented risk assessment methodology.
   c) There are a number of recognised risk assessment methodologies and taxonomies (e.g. ISO27005, Information Risk Assessment Methodology 2 (IRAM2), Factor Analysis Information Risk (FAIR), Value at Risk (VAR), BowTie,) that could be adopted. The company could use its own methodology provided it covers the appropriate elements of risk assessment. The company should also use an appropriate OT control framework.
   d) Risk management should have a first line, second line and third line of defence.
   e) Inherent risks identified should be qualified with the required stakeholders.
   f) Residual risks should be based on an OT cyber security control set and determined based on expert judgement. Where OT cyber security control sets cannot be applied in certain circumstances, the determination of residual risk may be undertaken with due consideration from other experts on respective compensating controls.
   g) Residual risks identified in the assessment should be categorised according to the risk appetite agreed by the company.
   h) Risks should be prioritised into time-bound risk treatment plans, including an owner responsible for the mitigation of that risk.
   i) It might not be practicable to implement some of the required risk mitigation countermeasures, especially for existing systems due to their proprietary nature or asset age. In such cases countermeasures and mitigating controls to address the risks should be considered.
   j) Where a risk cannot be reduced below tolerance, the residual risk should be recorded, approved by management and reviewed regularly according to policy.

k) Where likelihood forms a major component of quantitative risk assessment, it should be based on empirical data and a continuum be set up to ensure the currency of related case studies and intelligence.

l) The company should carry out threat analysis using available threat intelligence communities considering the capabilities and intent of potential threat sources, reviewing possible attack patterns, current vulnerabilities and overall exposure.

2. Risk assessments should be conducted when appropriate for events potentially affecting the security of networks and systems supporting your essential service.

a) Risk assessments should be reviewed, according to policy, to take into account changes in the cyber security landscape or scope.

b) Triggers to conduct a risk assessment should include but not be limited to:

- Change in threat levels;
- Change in system configuration;
- System upgrade and change in asset scope;
- Introduction of new suppliers and third parties;
- Change in risk profiles of assets and network zones;
- Change in system criticality;
- Following a major cyber security incident;
- Changes to the risk landscape such as knowledge of new vulnerabilities;
- Change in scope.

c) Examples of threats to assess risk against could include, but should not be limited to:

- Physical tampering;
- Local and remote denial of service (DoS);
- Loss of integrity of control/safety data;
- Third parties and system integrator risks;
- System availability and business continuity;
- Unauthorised control/operation (via local and remote access);
- Insider threats;
- Malware infection;
- Unauthorised access to critical/confidential system or network data (e.g. diagrams, IP addresses, passwords);
- Loss of view and control of operations.

3. **Threats that are applicable to your company should be communicated and understood by the relevant personnel.**
   a) Carry out suitable and effective risk assessments would typically require a range of personal competencies relating to understanding the specific threats to OT assets. Examples of risk assessment team members could include, but should not be limited to:
   - System and asset owners;
   - Vendors, system integrators or third-party representatives;
   - System Operators and Engineers;
   - Members of IT;
   - Any other risk or cyber security specialists required.

   b) Relevant personnel should understand and be informed of the risk assessment results.

4. **Vulnerabilities in the security of networks and systems supporting your essential service should be understood.**
   a) Vulnerabilities should be identified by, but not be limited to, the use of:
   - Penetration testing (e.g. as part of a secure development lifecycle). Penetration testing on OT systems must be done with extreme caution;
   - Continuous security monitoring tools specifically tailored for OT systems supporting your essential service (e.g. passively scanning vulnerabilities of OT assets, tools customised for proprietary OT vendors, detecting OT specific issues and protocol anomalies,);
   - Subscription to intelligence services or forums or information exchanges (e.g. CiSP, ICS-CERT);
   - OEMs (Original Equipment Manufacturer), vendors or third-party information;
   - Vulnerability or change records that could form part of an asset register (e.g. a roll back change in a system causes a previously treated vulnerability to resurface).

   b) Vulnerabilities in the security of networks and systems supporting your essential service should inform your risk assessments.

   c) Identified vulnerabilities should be used in risk assessments to ensure appropriate risk and threat scenarios are considered, to enable appropriate mitigations or compensating controls to be identified and applied.

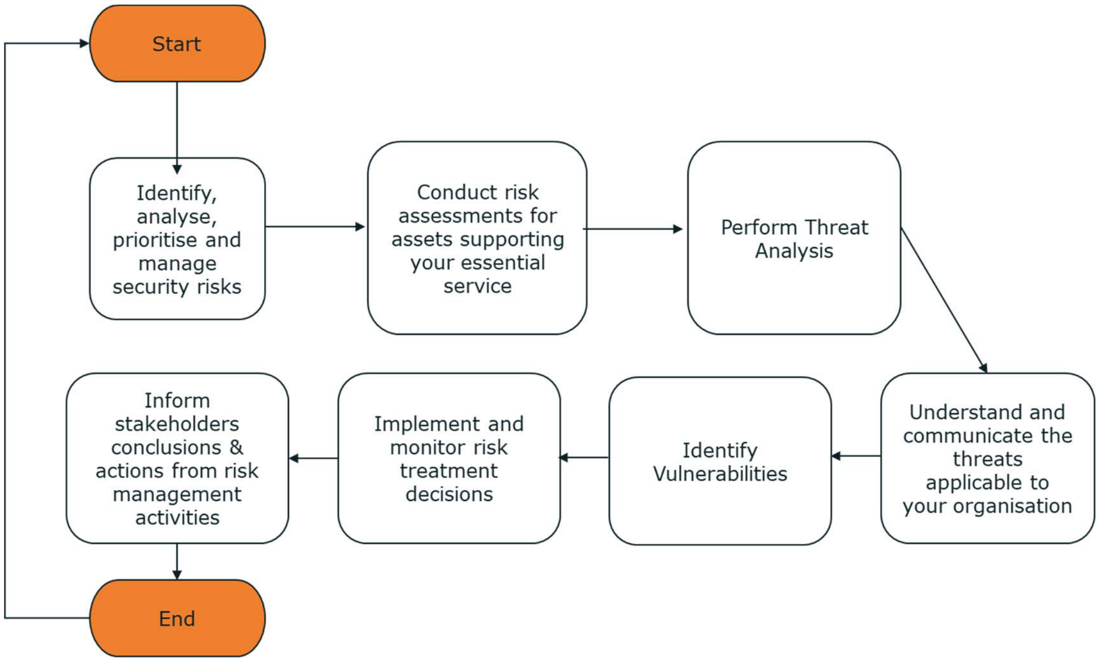
5. **There should be a clear set of security requirements resulting from your risk management process.**
   a) The risk management and assessment process should provide a clear set of actions with appropriate ownership, prioritisation, target implementation dates and regular monitoring to ensure all required actions or risk treatment options are addressed.

6. **Key security decision-makers and accountable personnel should be informed and understand significant conclusions from the risk management process.**
   a) All decisions are based on the risk tolerance levels set by the company. Any new risk above tolerance and deemed as accepted should be presented to the highest steering committee.
   b) Risk statements and guidance should be developed and communicated appropriately throughout the organisation to guide decision makers based on the current risk tolerance.

References and Further Guidance:

- NIST 800-82 R2 – Appendix D: RA-1 Risk Assessment Policy and Procedures, RA-2 Security Categorization, RA-3 Risk Assessment, RA-5 Vulnerability Scanning
- OG86 – Appendix 2 – A2 Risk Management, A4 Supply Chain
- IEC 62443-2-1 – 4.2.3 Risk identification, classification and assessment, 4.3.4.2 Risk management and implementation
- IEC 62443-3-3 – SR 5.2 Zone boundary protection
- NIST 800-53 R4 – Appendix F: RA-1 Risk Assessment Policy and Procedures, RA-2 Security Categorization, RA-3 Risk Assessment, RA-5 Vulnerability Scanning
- ISO/IEC 27001 – 4.2.x Risk Assessment Approach

Guidance Flow:


Start
Identify, analyse, prioritise and manage security risks
Conduct risk assessments for assets supporting your essential service
Perform Threat Analysis
Understand and communicate the threats applicable to your organisation
Identify Vulnerabilities
Implement and monitor risk treatment decisions
Inform stakeholders conclusions & actions from risk management activities
End

RIIO-2 Cyber Resilience Guidelines A2.b Assurance

RIIO-2 Cyber Resilience Outcome Description for A2.b Assurance:

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.

RIIO-2 Cyber Resilience Guidance:

1. **Identify and Select Assurance Methods** – The company has identified and selected appropriate assurance methods to gain confidence in the level of security of networks and information systems supporting your essential service.
   a) Assurance methods to gain confidence in the effectiveness of security controls of technologies, processes and people can include, but are not limited to:
      - Blackbox/Whitebox penetration testing;
      - Vulnerability assessments;
      - Independent information or physical security reviews, compliance assessments and auditing;
      - Configuration reviews/gap analysis against standards/best practices;
      - Human behavioural tests (e.g. simulated phishing email).

   b) Assurance methods should be chosen based on what is appropriate and safe for what is to be assessed. For example, tools that are used for testing corporately managed IT systems may be unsuitable for testing embedded control devices such as Programmable Logic Controllers (PLC) due to the sensitivity of these technologies to intrusive testing with potential safety implications.

2. **Validate Security Controls** – Validation is conducted throughout the system lifecycle to ensure that the security measures in place to secure the networks and information systems supporting your essential service are effective.
   a) Validating security controls after implementation can determine if the control has been implemented correctly, is operating as intended, and producing the desired outcome to meet the desired security requirements.
   b) Security controls should be monitored on an ongoing basis to ensure they remain effective over the time they are required.
   c) Monitoring activities could include, but are not limited to:
      - Configuration management and control of information system components;
      - Security impact analysis of changes to the system;

- Ongoing assessment of security controls;
- Status reporting.

d) Validation results should be expressed in the form of performance against a set of predefined and appropriate metrics to display security performance and security trends.

e) Security performance metrics should be sent to appropriate stakeholders, along with a view of security performance trends.

3. **Assure Security Measures** – Activities are conducted to assure the security measures in place to secure the networks and information systems supporting your essential service, as it relates to technology, people and processes can be justified to, and verified by, a third party.

   a) Validation assurance techniques could include, but are not limited to:

   - **People** – It is necessary to determine that security behaviours are being adopted and exhibited throughout the company. This could be achieved by interviewing personnel, security culture surveys and testing that personnel can identify malicious emails received (e.g. simulated phishing email scenario), keeping auditable records and conducting trend analysis;
   - **Process** – It is necessary to determine that processes designed to reduce risk are being followed. This could be achieved by validating that processes are being followed with an audit trail (e.g. the management of change program is being rigorously followed with an audit trail of reviews and approvals for all changes);
   - **Technology** – It is necessary to determine that systems are performing as intended, which could be achieved by:
     - Validating that the security controls present during system testing (e.g., factory acceptance testing and site acceptance testing) are still installed and operating correctly in the production system;
     - Validating that the production system is free from security compromises and provides information on the nature and extent of compromises as feasible, should they occur.

4. **Mitigate Deficiencies** – The company assesses, prioritises and remedies, if required, deficiencies in the security of networks and information systems supporting your essential service identified by assurance activities in a timely and effective manner.

   a) Identifying and assessing the risk presented by deficiencies should drive the prioritisation of remediation activities and selection of appropriate security controls.

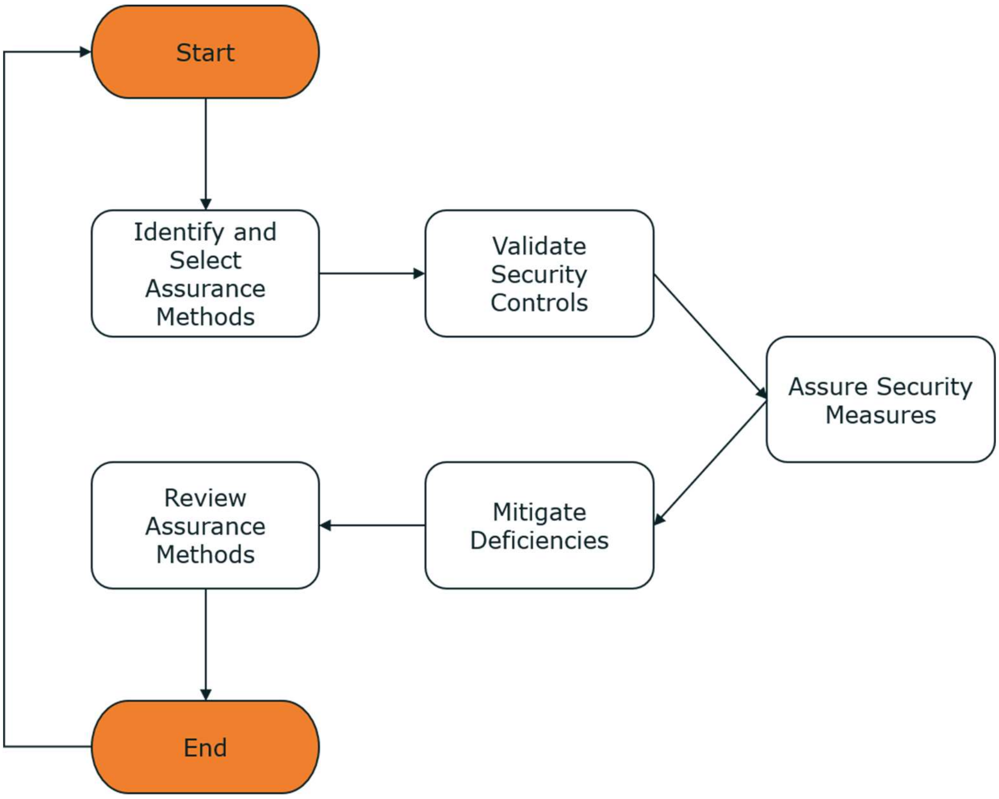
5. **Review Assurance Methods** – There is a regular review of the assurance methods used to confirm they remain fit for purpose.

a) Cyber security assurance can evolve over time as new threats are encountered, new technologies are released, or processes change to suit business needs. Assurance methods should be reviewed in accordance with company policy, to ensure that they are aligned to industry benchmarks, best practices and remain effective and fit for purpose.

References and Further Guidance:

- NIST SP800-82 R2 – Section 6.2.3
- OG86: Appendix 2 - A2 Risk Management
- ISO 27019: Sections 12.7, 14.2.8, 18.2

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines A3.a Asset Management

RIIO-2 Cyber Resilience Outcome Description for A3.a Asset Management:

You have identified and documented the assets that support the delivery of essential services and assets are tracked across their lifecycle.

RIIO-2 Cyber Resilience Guidance:

1. **Create and maintain a register of all assets** – The register of assets should be with an appropriate level of detail and format for all components that support the delivery of the essential service.
   a) The asset register does not have to be a formal database. Asset lists in the form of a spreadsheet and appropriate network diagrams are sufficient.
   b) The asset register should be protected with an appropriate level of security controls as this information could be valuable to an attacker.
   c) Procedures should be in place to ensure that the register is kept up to date following any changes, within a defined company policy schedule (for example within 24 hours of change, or the work permit cannot be closed until the asset register is updated).
   d) The asset register should be verified by periodic audits of location and condition, according to company policy.
   e) Incident and service records should be searchable by asset-ID/serial number so they can be cross-referenced with the asset register.
   f) Appropriate information that the asset register should contain could include sufficient information to support, for example, change management, maintenance, incident response, and obsolescence management.
   g) The asset register should also identify dependencies on supporting infrastructure (e.g. power, cooling).
   h) The asset register should include, but not be limited to:
      - Asset criticality (relating to their importance to the delivery of the essential services);
      - Unique identifier, location and zone reference;
      - Asset/conduit type, manufacturer, serial number, etc.;
      - Relevant risk profile and/or criticality information (e.g. risk-level, restore criticality, known vulnerabilities such as untreated Common Vulnerabilities and Exposures "CVEs");
      - Responsible person (where responsibilities are divided, e.g. between different departments or owners);

- Network connectivity arrangements (e.g. addresses, ports, connection types, network protocols, encryption algorithms & location of secure storage for encryption keys) for each network connection;
- For assets, each network connection type should be included, e.g. for multi-homed assets, or other (e.g. fieldbus) connections;
- For conduits (typically a firewall, router etc.), each connection to separate zones should be included;
- Any temporary connections such as portable assets (e.g. laptops) and assets where portable media connections are required / used;
- Firmware, operating system, and application software (including security software such as antivirus) types, versions (may be part of another system rather than the asset register, though should be recorded) and patch levels need to be recorded, including last update;
- Where appropriate, anticipated lifespan/due date for replacement may be required to assist in inventory planning;
- Where appropriate, planning details for managing aging or obsolete hardware and software assets.

2. **Prioritise assets** – The assets are prioritised according to their importance for delivering the essential service.

   a) A prioritisation scheme should exist to clearly identify the systems and assets that support the delivery of the essential services. There should be clear criteria for the priority levels.

   b) It is appropriate to differentiate between which assets are critical to the delivery of the essential services and which perform supporting functions and may be classed as non-critical.

3. **Define and assign asset ownership** – The assets should be assigned to a responsible person/owner as part of the asset lifecycle management.

   a) All systems and assets supporting the essential services should have a suitably qualified and experienced person or owner who is responsible for ensuring the security management of the asset at each stage of its lifecycle.

   c) The responsible person does not need to be the person that actually performs the day to day management activities, these duties could be delegated to appropriate personnel.

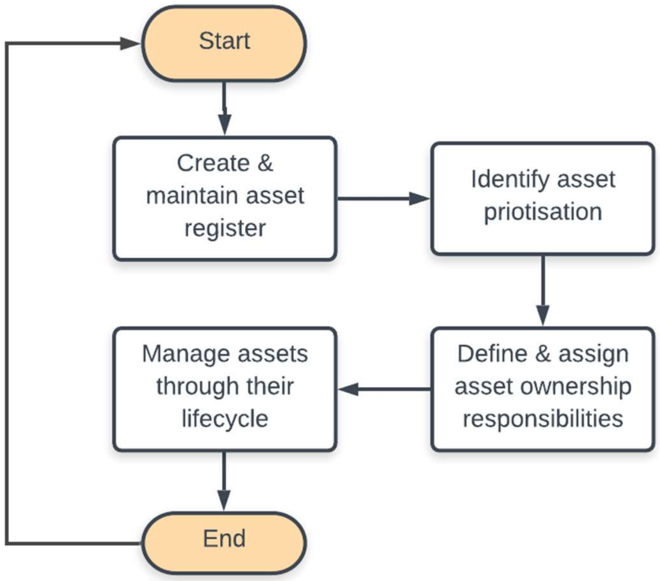
4. **Manage assets throughout their life-cycle –** With the execution of appropriate policies and procedures, security of assets from creation through to eventual decommissioning or disposal.

a) The cyber security management system or equivalent, should contain clear requirements for the life-cycle security management of assets, to include, but not limited to:
   - Specification of security requirements in the design and procurement processes;
   - Security by design to ensure the asset configuration is hardened as far as possible from day one;
   - Security testing as part of the acceptance and commissioning processes;
   - Operational security aspects such as patching, monitoring and obsolescence management, management of change, incident response and recovery, etc.;
   - Secure decommissioning and disposal, including media sanitisation, wiping configuration and performance data, where necessary.

References and Further Guidance:

- NIST 800-82 R2 – CM-8 Information System Component Inventory, PE-18 Location of Information System Components
- OG86 – Appendix 2 - A3 Asset Management
- IEC 62443 – SR 7.2 Resource Management, SR 3.3 Security Functionality Verification, SR 3.4 Software and Information Integrity, SR 3.7 Error Handling
- NIST 800-53 R4 – Appendix F: CM-8 Information System Component Inventory, PE-18 Location of Information System Components, PE-20 Asset Monitoring and Tracking
- ISO/IEC 27001 – A.7.1 Responsibility for Assets, A.7.2 Information Classification
- ISO/IEC 27019 – 8.1 Responsibility for Assets, 8.2 Information Classification

Guidance Flow:


Start
Create & maintain asset register
Identify asset priotisation
Define & assign asset ownership responsibilities
Manage assets through their lifecycle
End

RIIO-2 Cyber Resilience Guidelines A4.a Supply Chain

RIIO-2 Cyber Resilience Outcome Description for A4.a Supply Chain:

You understand the dependencies on third parties and the supply chain, have identified and managed the risks, and have appropriate security measures in place.

RIIO-2 Cyber Resilience Guidance:

1. **Identify all third-party connections** – Third-party connections and data flows to a networks and systems, supporting your essential service are identified and documented.
   a) Third party connections include, but are not limited to, vendor access for remote support and maintenance, customers, outsourced service providers, electricity companies (e.g. ESO, GSO, GT, ET, ENOs, DNOs).
   b) The type, purpose, boundaries and data flows for third party connections should be understood and documented, so all suppliers supporting your essential service can be easily identified.

2. **Identify supply chain dependences** – Supply chain dependencies for networks and systems supporting your essential services are identified and documented.
   a) The company should protect against supply chain threats to their information and OT systems, components, and essential services with a comprehensive and documented multi-layer cyber security strategy.
   b) Procedures should be in place for the following, but not limited to:
      - Identifying third parties (including sub-contractors) that provide, resources, equipment, OEMs, software, services (including any that use remote connections);
      - Identifying organisations dependent on you to supply information, or with whom you interact as part of the delivery, or support of essential services (i.e. remote access, telemetry, metering, pricing, emissions).

3. **Assess & manage supply chain risks** – Supply chain risks are assessed and managed, as part of the procurement process.
   a) The company should conduct an organisational, security review & assessment of risk prior to the acquisition, system update, contracting or outsourcing of third party services or systems.
   b) Special consideration should be given for highly sensitive components within the supply chain and according to your policy.

c) Risk assessments of the supply chain should include, but not be limited to, suppliers' partnerships, competitors, location, nationality, financial stability and other organisations with which they sub-contract.

d) The risk assessments should be embedded as part of the procurement process.

e) Reviews and assessments of suppliers should be periodically reviewed and maintained to ensure accuracy.

f) Consider risks to the essential services arising from supply chain subversion in your risk management and assessment approach.

g) The company should maintain a list of third and end parties that are preferred suppliers, and also suppliers that they are not allowed to procure from according to policy.

4. **Include security requirements in all contracts** – Security requirements and controls should be included in all contracts and managed according to policy. Cyber security requirements should be contractually defined, with a code of connection/conduct for suppliers. Special considerations should be given according to policy but not limited to:

a) Right to audit and monitor of their organisational processes and cyber security practices.

b) Define appropriate cyber security controls to manage the risk to defined levels based on industry best practice (Cyber Essentials, NIST 800-53, NIST 800-82, IEC/ISA 62443, ISO 27001, etc.).

c) Consideration about suppliers of auxiliary services such as Heating, Ventilation and Air Conditioning (HVAC), cleaning services, security guards, etc. should be included.

d) Employ organisation-defined security controls to validate that the information system or system component received is genuine and has not been altered.

e) Requires the same level of security and assurance from their sub-contractors when working on the supply of systems and services for the organisation.

f) The organisation should require providers of services to identify the functions, ports, protocols, access and other services required for the use of such services.

g) Personnel security requirements, including security roles and responsibilities, background checks and required security clearances for third-party providers.

h) Suppliers should notify of any transfers or employment terminations of third-party personnel who possess organisational access credentials and/or badges, to the organisation's systems and facilities.

i) Assurance that the third party access, identification and authentication of users, and security measures meet the contractual obligations.

5. **Detect, respond and manage supply chain incidents** – Consider the detection, response and management of incidents in your supply chain services and systems as part of your incident management processes.

a) The organisation should define management and reporting mechanisms for incidents which have the potential to impact essential services.

b) Assurance could be gained by audit / assessment, or through tested evidence.

c) In addition to the contractual requirement for collaboration on incident response the company should require suppliers to:

- Promptly report suspected security incidents to the company (e.g. Security Operation Centre, or information security team);
- Have their incident response teams work with the company to respond, recover and learn from the incident;
- Share diagnostic data that allows analysis of the incident to aid identification of the cause;
- Suppliers should inform the company of any vulnerabilities discovered.

d) Include mutual support, where appropriate, in the supply chain incident management approach to minimise the impact on the organisation's supply chain and on the essential services.

e) Define security safeguards to ensure an adequate supply of services of the supplier in case of an incident.

6. **Protect information lifecycle** – Information shared with suppliers, that is essential to the operation of your essential service, should be appropriately protected. Information about the essential services, OT assets, remote connections and their configuration is of particular interest to any potential attacker. This information should be suitably protected across its lifecycle, wherever is it stored or processed, including when created by or in the possession of suppliers.

a) The company should define the location and required controls of the supplier information processing, data in transit and data at rest, and systems based on company-defined requirements or conditions.

b) Conduct or commission periodic assessments, in accordance with the contractual agreement and company's policies to assure:

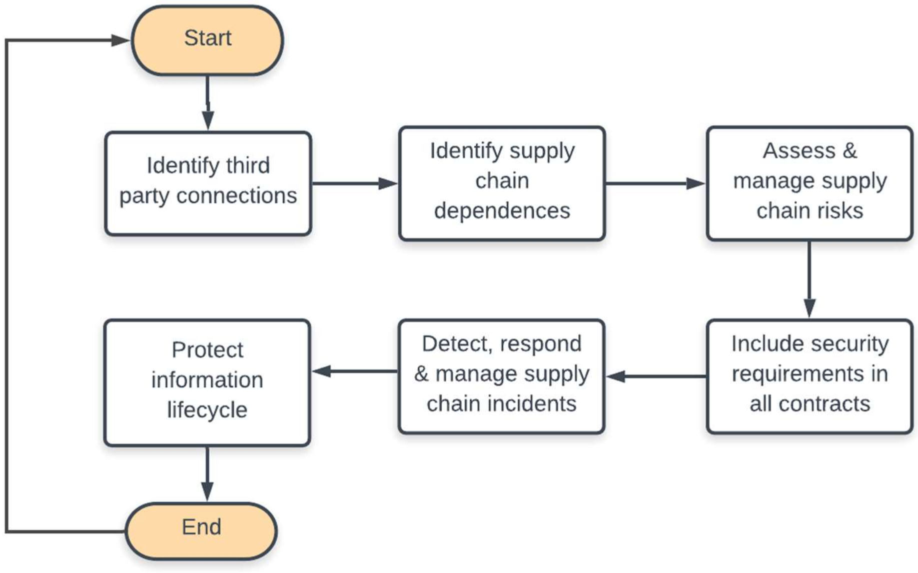
- That suppliers are complying with the contractual requirements to protect data;
- The security of any connections over which data is passed between the company and third parties.

c) Assurance can be gained by audit or assessment by the company, independent audit or assessment, or tested evidence provided by the supplier.

References and Further Guidance:

- NIST 800-82 R2 – SA-9 External Information System Services, PS-7 Third-Party Personnel Security, SA-12 Supply Chain Protection
- OG86 – Appendix 2 – A4 Supply Chain
- IEC 62443 – Sections 7.4.1, SR 3.3 Security Functionality Verification, SR 3.4 Software and Information Integrity, SR 3.7 Error Handling
- NIST 800-53 R4 – Appendix F: SA-9 External Information System Services, PS-7 Third-Party Personnel Security, SA-12 Supply Chain Protection
- ISO/IEC 27001 – A.15.2 Supplier service delivery management, A.15.2.1 Monitoring and review of supplier services, A.15.2.2 Managing changes to supplier services

Guidance Flow:


Start
Identify third party connections
Identify supply chain dependences
Assess & manage supply chain risks
Include security requirements in all contracts
Detect, respond & manage supply chain incidents
Protect information lifecycle
End

RIIO-2 Cyber Resilience Guidelines B1.a Policy and Process Development

RIIO-2 Cyber Resilience Outcome Description for B1.a Policy and Process Development:

You have developed and continue to improve a set of service protection policies and processes that manage and mitigate the risk of cyber security-related disruption to the essential service.

RIIO-2 Cyber Resilience Guidance:

1. **Policy and Process Documentation** – Your service protection policies, standards, processes and procedures document your overarching security governance and risk management approach, technical security practices and specific regulatory compliance.
   a) As part of the cyber security management system; service protection policies, standards, processes and procedures for the networks and information systems supporting your essential service should be developed.
   b) This management system should be aligned to NCSC NIS guidance, relevant industry standards and regulations.

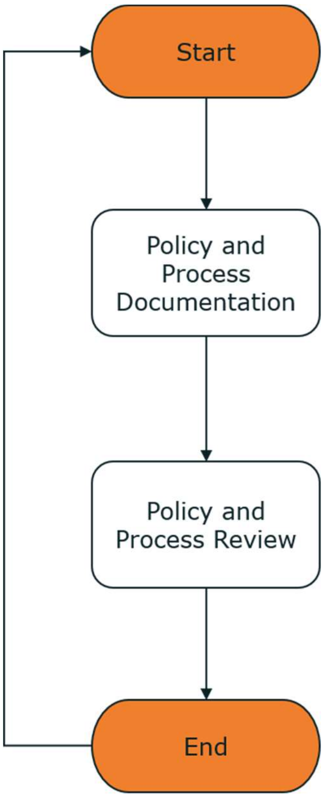
2. **Policy and Process Review** – The company reviews and updates, where required, service protection policies, standards, processes and procedures in response to relevant cyber security incidents relevant to your industry and all cyber security incidents identified in your company.
   a) The service protection policies, standards, processes and procedures should be reviewed and, if necessary, updated in accordance with company policy, or following relevant cyber security incidents, which could be other sectors or geographies.
   b) The results of these reviews should be documented and distributed to relevant personnel.

References and Further Guidance:

- NIST SP800-82 R2 – Section 4.4
- OG86: Appendix 2 - B1 Protection Policies and Processes

- IEC 62443/ISA99 2-1 - Section 4.3.2.6
- ISO 27019 – Section 12.1.1

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B1.b Policy and Process Implementation

RIIO-2 Cyber Resilience Outcome Description for B1.b Policy and Process Implementation:

You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved.

RIIO-2 Cyber Resilience Guidance:

1. **Policy and Process Implementation** – Your service protection policies, standards, processes and procedures, with respect to security of networks and information systems supporting your essential service, are integrated with other relevant organisational policies and processes.
   a) Where appropriate, service protection processes should be integrated or consistent with existing operational/management policies and procedures. e.g. HR policies and processes, physical security, health and safety.
   b) Where the requirements for OT justifiably deviate from standard processes and procedures, these should be developed and included in the management system.

2. **Personnel Security** – HR processes include assessment of individuals' suitability to perform their role.
   a) Specific requirements for HR processes could include but is not limited to:
      - Security screening of new and existing personnel within OT to a level commensurate with the risk (BS7858 – Security screening of individuals employed in a security environment. Code of Practice);
      - Joiners, Movers and Leavers (JML) process for granting or removing access.

3. **Staff Awareness** – All staff are aware of and understand their responsibilities under the service protection policies, standards, processes and procedures with respect to the security of networks and information systems supporting your essential service.
   a) Roles and responsibilities should be clearly defined in the management system and the supporting processes and procedures.
   b) All relevant personnel should be aware of their roles and responsibilities through appropriate training and awareness initiatives, such as, but not limited to:
      - Formal training courses, classroom or computer based;

- Awareness campaigns;
- Responsible, accountable, consulted and informed (RACI) matrices;
- Job descriptions;
- Toolbox talks.

4. **Policy and Process Monitoring** – The company monitors the application of all service protection policies and processes and confirms critical ones are being followed.
   a) Monitoring techniques can include, but are not limited to:
      - Use of checklists and other methods to generate an audit trail;
      - Surveys to confirm processes are followed;
      - Incidents reports, including near misses;
      - Conversations with personnel;
      - Authorisations and approvals;
      - Reviews of in-process quality checks and outcomes;
      - Regular ‘walk-downs’;
      - Viewing of recordings or video streams in real time (CCTV etc.).

   b) Monitoring evidence should be reviewed to ensure that critical service protection policies and processes are being followed.

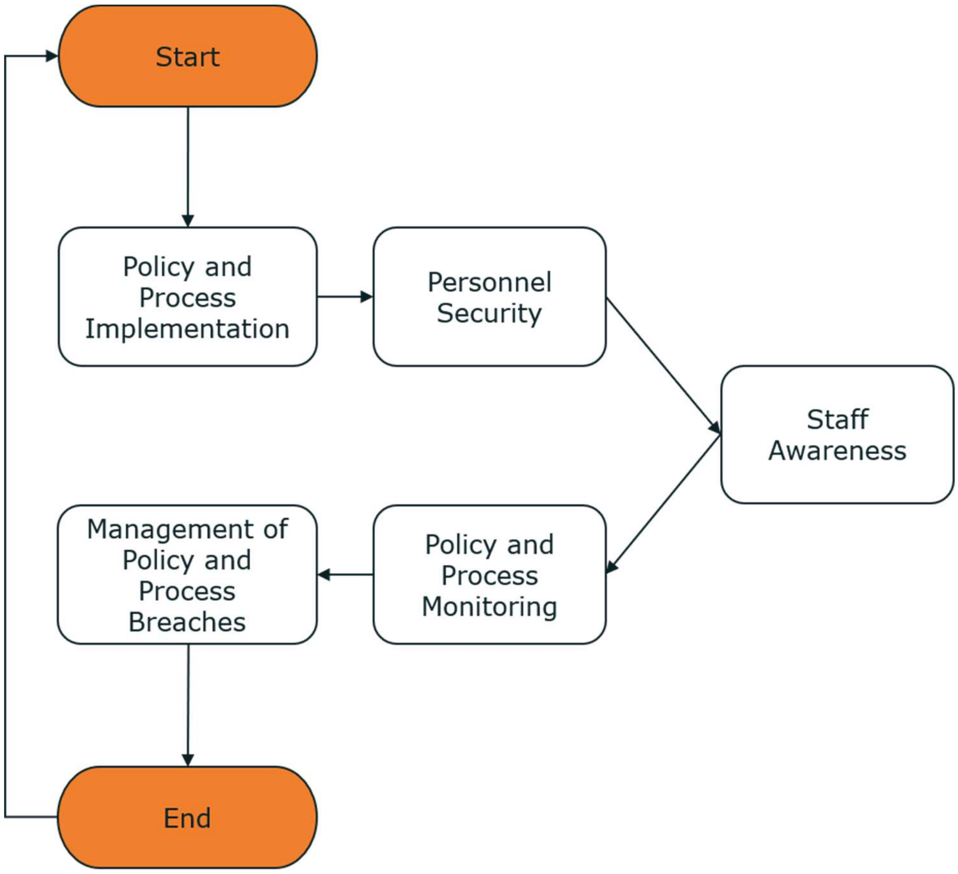
5. **Management of Policy and Process Breaches** – The company identifies, investigates and records all known breaches of service protection policies, standards, processes and procedures.
   a) Service protection process compliance monitoring evidence should be regularly reviewed at least quarterly or in accordance with company policy, to identify deviations from policy, standards, processes and procedures.
   b) Breaches should be investigated, lessons learned identified and escalated as appropriate.
   c) The investigation may require input from other stakeholders from across the business (HR, IT, etc.) and may require specialised external skills, which may be provided by third parties.
   d) Where identified breaches are assessed not to have the potential to impact the essential service, these should be recorded, assessed and appropriate action taken.

References and Further Guidance:

- NIST SP800-82 R2 – Section 4.4
- OG86: Appendix 2 - B1 Protection Policies and Processes

- IEC 62443/ISA99 2-1 – Section 4.3.2.6
- ISO 27019 – Section 12.1.1

Guidance Flow:


Start
Policy and Process Implementation
Personnel Security
Staff Awareness
Policy and Process Monitoring
Management of Policy and Process Breaches
End

RIIO-2 Cyber Resilience Guidelines B2.a Identity Verification, Authentication and Authorisation

RIIO-2 Cyber Resilience Outcome Description for B2.a Identity Verification, Authentication and Authorisation:

You robustly verify, authenticate and authorise access to the networks and information systems supporting your essential service.

RIIO-2 Cyber Resilience Guidance:

1. **Identify all authorised users** –There should be clear documentation that captures and identifies all authorised users and their access requirements, which should align with asset registers (A3a refers).
   a) Identify unique individuals who require access to a system and/or data, including the justification for that access and the parameters in which the access should be permitted.
   b) The documentation should include what physical and data assets are permitted to be accessed and what privileges are required to support that access.
   c) A record should be maintained of when networks and systems are accessed and the information recorded should contain sufficient information to support future fault finding, investigation or root cause analysis.

2. **Authenticate Authorised Users** –Unless restricted by system or operational limitations, that every authorised user is individually identified and authenticated.
   a) Enforce the use of named user accounts wherever possible.
   b) Where it is not possible to use individual named user accounts, alternative mechanisms may include proximity based log-in cards with a centralised authorisation and access system. Alternatively, this may include sign-in sheets, log sheets or shift rotas, with appropriate compensating physical controls such as CCTV directed at specific locations.

3. **Restrict logical access** – Appropriate controls should be in place to ensure that only authorised users can logically connect to networks and information systems.
   a) Logical access control restrictions should be enabled for applications, ancillary software, system services, operating systems, network and telecommunication infrastructure.
   b) The company should consider methods for control of logical access.
   c) The principle of least privilege should be applied and can minimise the accessibility to systems, networks, data or functionality that is based on:

- Roles and/or responsibilities;
- Assets requiring those privileges.

4. **Secondary Authentication Mechanisms** – Implement additional authentication mechanisms for privileged access to sensitive systems on which your essential service depends.
   a) Ensure that privileged user accounts are protected with authentication mechanisms, such as multi-factor authentication where appropriate and necessary.
   b) Existing primary authentication methods and management processes should also be considered to ensure that the secondary method utilises a diverse method to the primary and that the secondary method does introduce unnecessary overheads.
   c) Recognise that where technical strong authentication mechanisms cannot be implemented, alternative assurance processes should be implemented and could include, but are not limited to, identification checks or two-person rule procedures.
   d) The company should ensure that privileged users should have separate accounts for routine and for privileged functions[2].

5. **Remote Access** – Ensure that each instance of remote user access to all your networks and information systems that support your essential service is individually authorised, authenticated and protected with secondary authentication mechanisms as Para 4.
   a) The company should consider additional authentication mechanisms which could include multi-factor authentication such as, one-time passwords, individual personal identification.
   b) Where OEMs require remote access and the staff regularly change, or further assurances want to be gained by the company, a process could be developed, where the company's operational staff retain access to the physical secondary token and provide the information to the OEM on a case by case basis. Enabling temporary access methods (e.g. temporary firewall rules, temporary physical network connection) could further support the management of third party remote access.

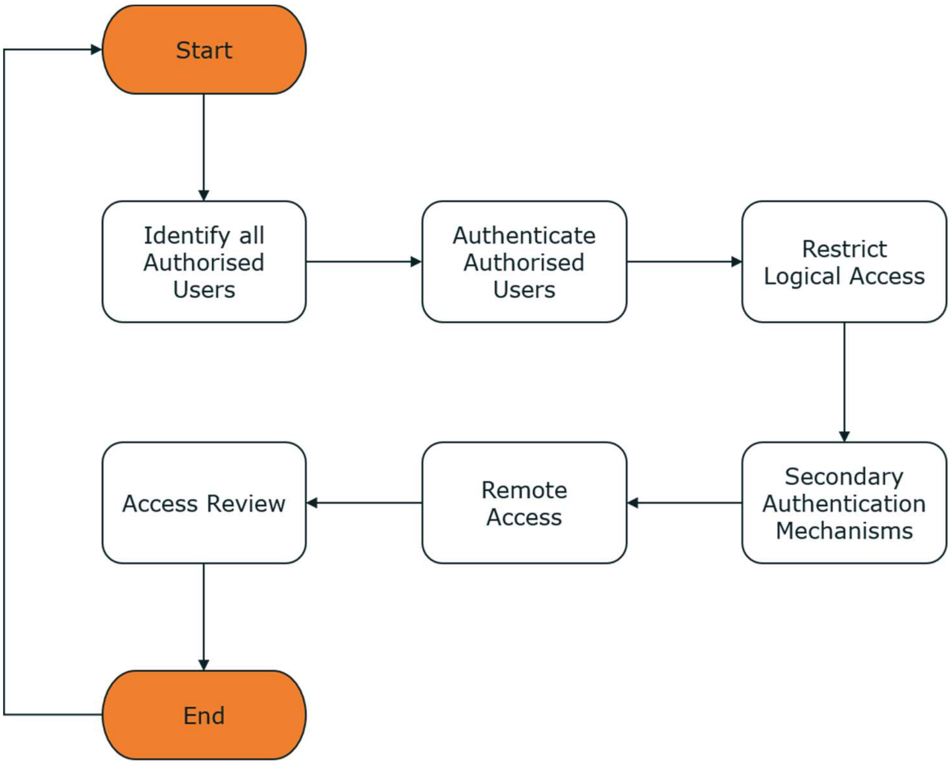
[2] https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management#section_6

6. **Access Review** – The list of users and systems with access to essential service networks and systems should be reviewed on a regular basis or when change occurs e.g. significant change in system configuration or personnel.
   a) The access should be recertified by the system owner or the line manager.

References and Further Guidance:

- NIST SP800-82 R2 – Sections 5.15 & 6.2.7, AC-3 Access Enforcement, AC-17 Remote Access, IA-2 Identification and Authentication (Organizational Users), IA-8 Identification and Authentication (Non-Organisational Users), PE-3 Physical Access Control
- OG86 Appendix 2 - B2 Identity and Access Control
- IEC 62443/ISA99 3-3 – SR 1.1 Human User Identification and Authentication, SR 1.2 Software Process and Device Identification and Authentication, SR 1.5 Authenticator Management, SR 1.7 Strength of Password-based Authentication
- ISA 99 (Part 4) - I&AM Requirement 10
- ISO 27002 Clause 9

Guidance Flow:


Start
Identify all Authorised Users
Authenticate Authorised Users
Restrict Logical Access
Secondary Authentication Mechanisms
Remote Access
Access Review
End

RIIO-2 Cyber Resilience Guidelines B2.b Device Management

RIIO-2 Cyber Resilience Outcome Description for B2.b Device Management:
You should fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential service.

RIIO-2 Cyber Resilience Guidance:

1. **Manage Devices** – The underpinning principle is that only devices owned and managed, or approved and authorised, by your company should be connected to the networks and systems supporting your essential service.
   a) The company should ensure that a process exists to approve and authorise connection of devices to the networks and systems supporting your essential service.
   b) By default, only your organisation’s owned and managed assets should be granted access (e.g. dedicated engineering devices or removable media).
   c) Where this is not possible, the company should have a documented risk assessment for the use of third-party assets, which may be granted with appropriate controls applied.

2. **Register Devices** – It should be known what devices are authorised to connect to networks and systems supporting your essential service.
   a) The company should have a register of all devices that are authorised to connect to the networks and systems supporting your essential service, and the use for which they are approved. This should include local and remote access by third parties or contractors.
   b) The company should have a process to ensure that this register is maintained and kept up-to-date.
   c) The company needs to ensure the process for identifying and authenticating portable and mobile devices is secure and the risk documented.

3. **Detect Unknown Devices** – It should possible to detect unknown devices connected to networks and systems supporting your essential service and to investigate such occurrences.
   a) The company should have automated mechanisms for the detection of unknown devices to generate an alert.
   b) Where automated mechanisms are not possible, the company should be operating regular, in accordance with the management system, manual checking processes to identify unknown devices.

4. **Privileged Access Management** – Privileged access, management and configuration functions on networks and systems supporting your essential service should only be performed with dedicated devices that are owned and managed by your organisation.
   a) Where this is not possible, the company should have a documented risk assessment of the use of third-party assets or non-dedicated devices for privileged access, which may be granted with appropriate controls applied (i.e. session monitoring and recording).

5. **Pre-Authorisation** – Third party devices and networks are identified before they are connected to networks and systems supporting your essential service.
   a) The company should have a process for identifying third party devices or networks prior to connection to the networks and systems supporting your essential service.
   b) The company should have processes to ensure appropriate risk assessments and application of additional security controls and checks (e.g. malware scan) are carried out prior to connection to the networks and systems supporting your essential service.
   c) Where possible, the company should ensure that these processes are integrated or consistent with existing operational or management processes. These can include but are not limited to:
      - Management of Change (MoC);
      - Ad-hoc or planned maintenance routine;
      - Granting local or remote access to the networks and systems supporting your essential service.

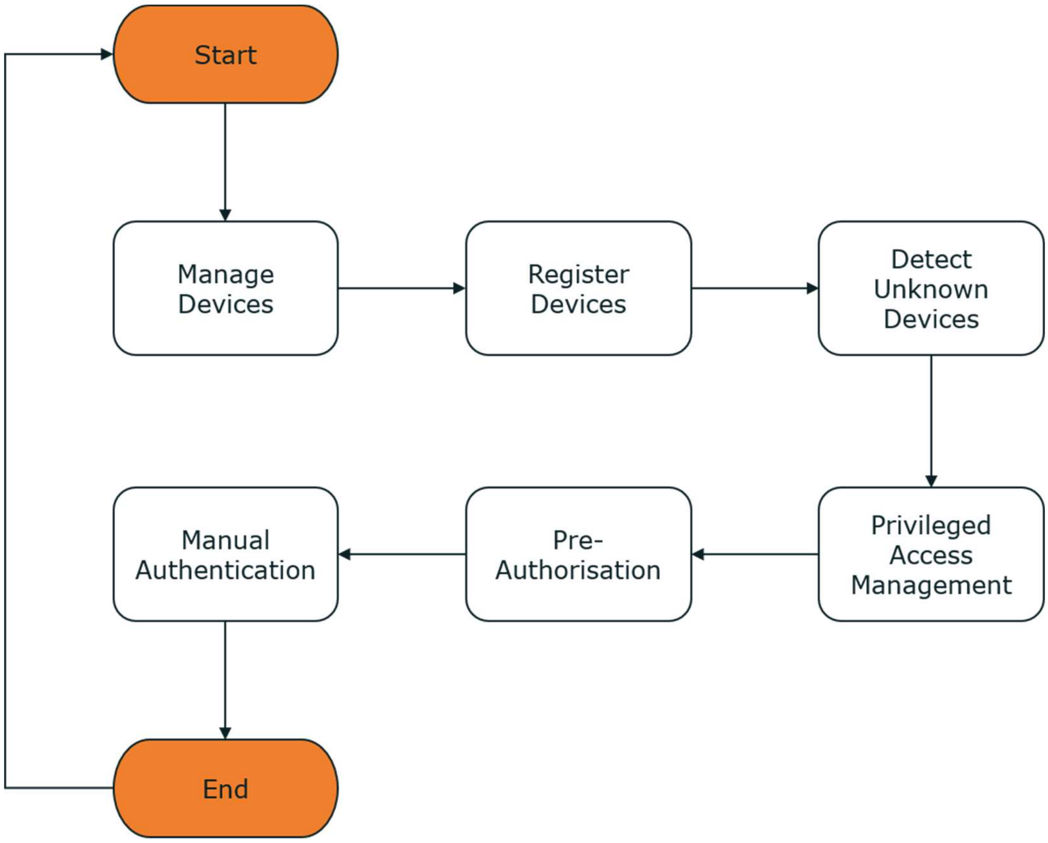
6. **Manual Authentication** – Connecting a device to a network, by cable or wirelessly, does not automatically grant access to networks and systems supporting your essential service.
   a) Where possible, the company should ensure that devices are authenticated and authorised prior to being granted access to system resources.
   b) Where this is not possible, the company should ensure that a documented risk assessment is completed, and additional compensating controls implemented.

References and Further Guidance:

- NIST SP800-82 R2 – IA-3 Device Identification and Authentication
- OG86 - Appendix 2 - B2 Identity and Access Control

- IEC 62443/ISA99 3-3 – SR 5.4 Application Partitioning, SR 1.2 Software Process and Device Identification and Authentication

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B2.c Privileged User Management

RIIO-2 Cyber Resilience Outcome Description for B2.c Privileged User Management:

You closely manage privileged user access to networks and information systems supporting the essential service.

RIIO-2 Cyber Resilience Guidance:

1. **Privileged User Access** – Individuals who require privileged levels of user access will require additional validation and authentication as per B2.a.
   a) The company should ensure that privileged user accounts are protected through the use of strong authentication mechanisms, including the implementation of secondary authentication mechanisms where appropriate.
   b) Where strong authentication mechanisms cannot be implemented, the company should consider implementing alternative assurance processes which could include, but are not limited to, identification checks or two-person rule procedures.
   c) The company should ensure that privileged users have separate accounts for day-to-day and for privileged functions.
   d) Privileged accounts should only be accessed from dedicated devices or workstations and should only be used to perform the tasks requiring that privileged access.

2. **User Management** – The identities of the individuals, whether within your organisation or third parties, with privileged access to networks and information systems to support your essential service systems are known and managed.
   a) The company should have a process to identify the individuals with privileged access verify their identify and need for access.
   b) The company should maintain a register to record all approved individuals with privileged access to the networks and information systems supporting your essential service.
   c) The company should consider integrating the process with existing operational / management and HR service protection policies and processes. This can include but is not limited to:
      - Security screening of new and existing personnel before granting privileged access;
      - Joiners, movers and leavers process for granting or removing logical or physical access.

3. **Role Based Access** – Privileged users are granted only specific privileged permissions which are essential to their business role or function.
   a) The company should ensure that user access privileges are granted and assigned to users based upon the principle of least privilege, i.e. only granting the permissions required and no more to those who need physical or logical access to carry out their role or a business function.
   b) The company should also ensure that any privileged access is:
   - Time bound and only valid for the minimum amount of time necessary;
   - Managed through a change control or permit to work style process;
   - Controlled on an individual basis;
   - Subject to appropriate considerations for internal and external users.

   c) The company should also consider implementing processes for exceptions and emergencies.

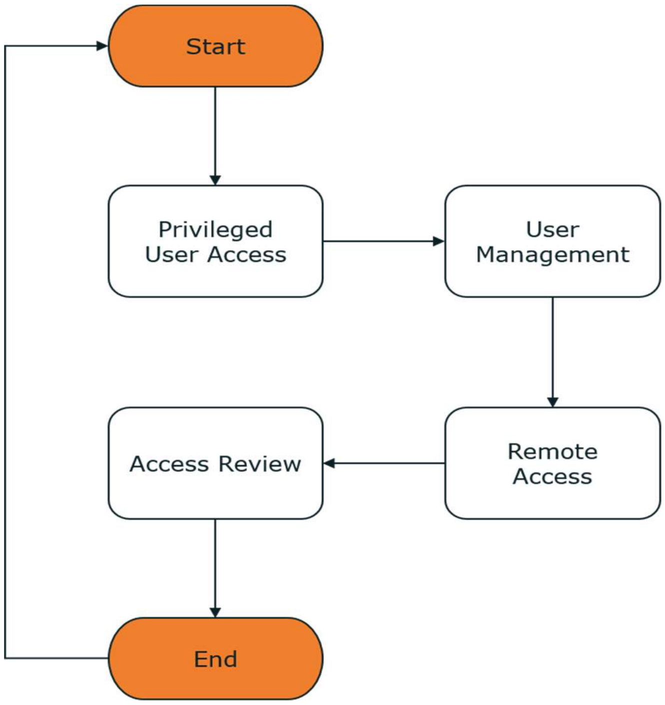
4. **Access Review** – There is regular review and validation of activity by privileged users to identify any unauthorised or unusual activities.
   a) The company should consider monitoring privileged users to validate activities, which can be achieved by but is not limited to:
   - Logging and analysing privileged user activity.
   - Validating any changes or deviations in process.
   - Tracking policy violations.
   - User behaviour monitoring.

   b) Reviews are conducted regularly in accordance with the management system.

References and Further Guidance:

- OG86 - Appendix 2 - B2 Identity and Access Control
- IEC 62443-2-1 – Section A.3.3.2.2
- IEC 62443/ISA99 3-3 – SR 1.4 Identifier Management, SR 2.1 Authorisation Enforcement, RE 2 Password Lifetime Enforcement for All Users
- ISO 27019 – Section 9.2.3

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B2.d Identity and Access Management

RIIO-2 Cyber Resilience Outcome Description for B2.d Identity and Access Management:

You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential service.

RIIO-2 Cyber Resilience Guidance:

1. **Identity Management** – There is a robust process to verify the identity of each user requesting access to networks and information systems supporting your essential service.
   a) The company should have processes which include, but not be limited to:
      - Confirmation of the individual's identity;
      - The purpose and need for access;
      - Granting the appropriate privileges to meet the approved purpose;
      - Recording this in an appropriate register which is kept up-to-date.

   b) Additional control(s), including, but not limited to call back procedures and fixed IP addresses may be required to authenticate access requests from third parties before they are processed.

   c) The company should have a means to assure the robustness and effectiveness of technical solutions.

2. **User Change Management** – The joiners, movers and leavers process ensures you grant only the minimum required access rights to each user.
   a) The company should ensure that the processes for granting appropriate access includes:
      - Joiners – confirmation of the level of access required to perform the approved role;
      - Movers – confirmation of the level of access required and prompt removal of access and privileges no longer required, and initiate changes of credentials, where required (e.g. shared accounts);
      - Leavers – the prompt removal of all access and return of, for example, keys and two-factor authentication tokens, and initiate changes of credentials, where required (e.g. shared accounts).

   b) The company should ensure that the above processes provide appropriate notifications to all relevant parties, both internal and external.

3. **User Access Review** – There is a regular review of user access rights and those which are no longer required are revoked, which should be aligned to a joiner, mover, leaver process.
   a) There should be a periodic review, in accordance with company policy, of third parties, specific users, user groups, and automated scripts (e.g. backups and peer-to-peer device communications) that have access to the networks and information systems supporting your essential service.
   b) Any periodic user review should be crossed checked against a system access review to confirm validity of access to individual systems.
   c) Consideration should be given to including the following checks:
      - User still employed by the organisation;
      - User still performing the same role for the same asset group(s) or OT zones;
      - Hardware or scripts still required and running.
   d) Where shared credentials are used, following termination of employment or change of role etc. by a user, checks should be made to see if any shared device credentials need to be changed for remaining/new users.

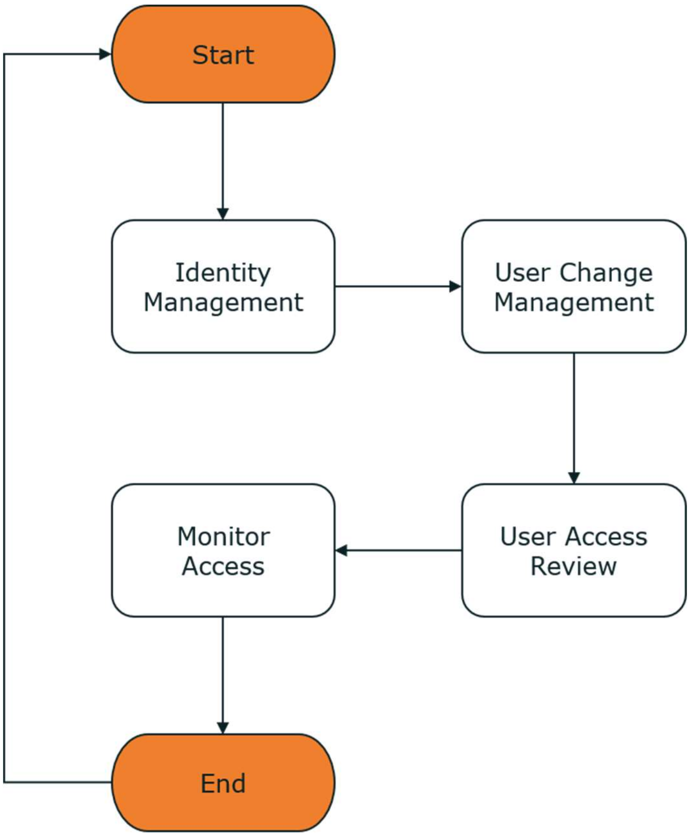
4. **Monitor Access** – The company should log and monitor all user access.
   a) The management system or security policy should include a clear statement that all user access will be logged and the purpose for this logging.
   b) Logging of all user access should be implemented and these logs monitored and reviewed on a regular basis, in accordance with company policy (Section C1 refers).
   c) Where automated logging is not possible, implementing manual processes, such as an offline log book, should be considered.
   d) The use of additional controls of other types of logging may be required where shared logins or hard-coded passwords are unavoidable.

References and Further Guidance:

- NIST 800-82 R2 – Section 6.2.1, Appendix G AC-1 Access Control Policy and Procedures, AC-2 Account Management, AC-3 Access Enforcement, AC-4 Information Flow Enforcement, AC-5 Separation of Duties, AC-6 Least Privilege, AC-7 Unsuccessful Logon Attempts, AC-8 System Use Notification, IA-1 Identification and Authentication Policy and Procedures, IA-2 Identification and Authentication (Organizational Users), IA-5 Authenticator Management, IA-6 Authenticator Feedback, IA-8 Identification and Authentication (Non-Organizational Users)

- OG86 – Appendix 2 - B2 Identity and Access Control
- IEC 62443-2-1 – Section A.3.3.2.2
- ISAO27001 – Sections 7.1.1, 7.1.2, 9.2, 12.4
- ISO 27019 – Sections 9.1, 9.2, 9.3, 9.4
- HMG GPG 44 – Authentication of claimed identity

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B3.a Understanding Data

RIIO-2 Cyber Resilience Outcome Description for B3.a Understanding Data:

You have a good understanding of data important to the delivery of the essential service, where it is stored, where it travels, and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to any third parties storing or accessing data important to the delivery of essential services.

RIIO-2 Cyber Resilience Guidance:

1. **Identify Critical Data** – Understand and maintain the location, type, quantity and quality of data important to the delivery of the essential service.
   a) The company should develop an inventory or data repository to include information within and about the data, networks and systems supporting your essential service, it could include, but not limited to:
      - Data and information held;
      - Volume;
      - Classification and/or sensitivity;
      - System(s) which use it, both organisational and third party;
      - Location where the data is stored (e.g. onsite, offsite, third party location);
      - Format data is stored in (e.g. physical (paper copies) or digital (server storage/tape drives));
      - Legal or regulatory requirements for data storage e.g. sensibility and hosting location;
      - Period data is stored for (e.g. in line with data retention practices);
      - Data owner;
      - Access permissions;
      - Method of disposal.

   b) The data inventory should be in an appropriate format (e.g. an automated service, database, spreadsheets) which is maintained and kept up-to-date.
   c) The information types could include, for example, network diagrams, design information and specifications, information held by third parties.
   d) Access to the data inventory and data should be permitted only to authorised personnel.
   e) The company should handle and retain information in accordance with applicable laws, directives, regulations, policies, standards, and operational requirements.
   f) Information handling and retention requirements should cover the full life cycle of information (including data in transit and at rest), and in some cases extending beyond the disposal of applicable systems.

2. **Understand Critical Data** – Understand the context, limitations and dependencies of your important data.
    a) The availability, integrity, confidentiality and safety requirements of the data which is important to the operation of your essential service should be understood and documented.

3. **Understand Data Links** – Maintain a current understanding of the data links used to transmit data that is important to your essential service.
    a) Methods could include but are not limited to:
        - Flow charts to map communication links and data flows (e.g. between systems, processes);
        - Network architecture diagrams;
        - Removable media usage logs.

    b) Documents should be reviewed and maintained on a regular basis, according to company policy.
    c) The process of maintaining documents should be integrated with other organisational/management service protection processes. This could include, but is not limited to:
        - Management of change;
        - Planned maintenance routines.

4. **Identify Mobile Devices and Portable Media** – Identify all mobile devices and media that may hold data important to the delivery of the essential service.
    a) A register should exist of mobile devices and/or media, which hold data that is important to the delivery of the essential service.
    b) This register should be maintained and kept up-to-date.

5. **Manage Data Holdings** – Remove or minimise unnecessary copies or unneeded historic data.
    a) A process should exist to delete unnecessary copies or unneeded historical data, and which may be integrated with other organisational/management service protection policies and processes. This can include, but should not be limited to:
        - Data retention policy;
        - Data deletion policy;
        - Data deletion process (includes method of deletion for data in line with data classification);

- Secure disposal and sanitisation process.

6. **Create Data Lifecycles** – Assess and document the impact on your essential service across all relevant data lifecycle scenarios including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data.

   a) Data should be securely handled throughout its lifecycle, in accordance with your media access, use, storage, transport and sanitisation polices and processes.
   b) Companies should undertake and document an impact assessment of a variety of relevant scenarios relating to the availability, integrity, confidentiality and safety of the data, important for the operation of the essential service.
   c) Companies should include the results of this in risk assessments of the networks and systems supporting the essential service according to their risk management process.

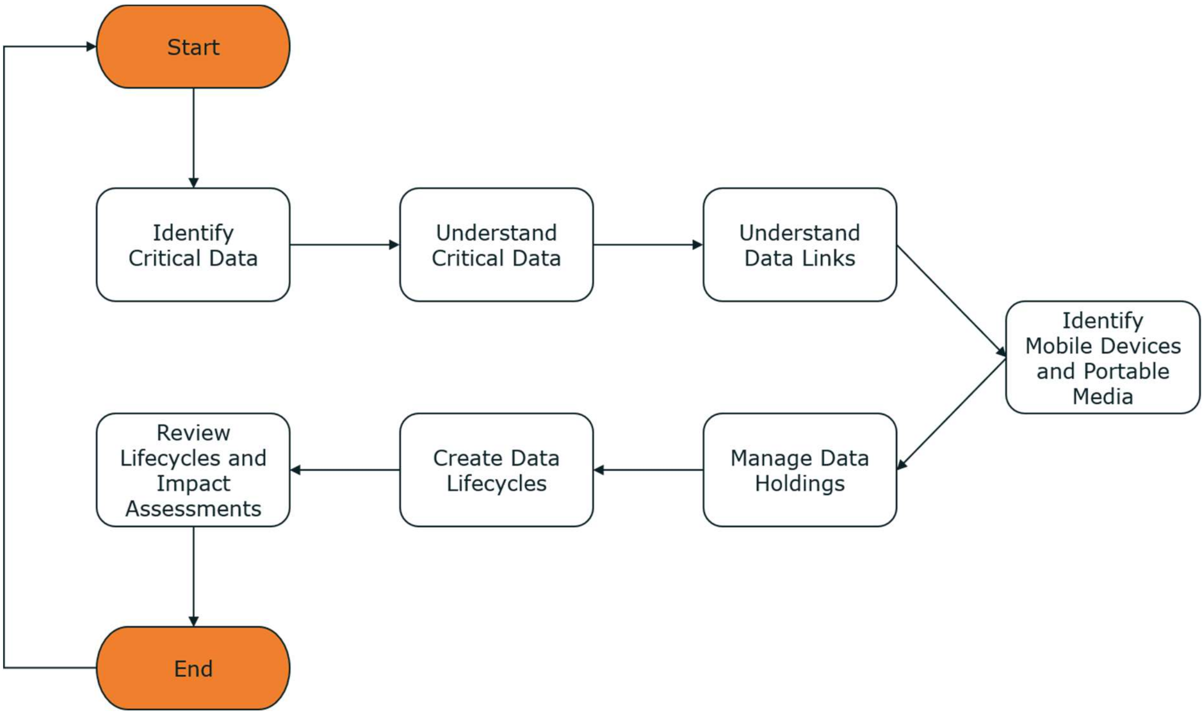
7. **Review Lifecycles and Impact Assessments** – Validate and review the impact assessments regularly.

   a) Impact assessments should be validated and reviewed regularly, according to company policy, to ensure they remain up-to-date and effective.

References and Further Guidance:

- NIST 800-82 R2 – SI-12 Information Handling and Retention, SI-10 Information Input Validation
- OG86 – Appendix 2 - B3 Data Security
- IEC 62443-2-1 – Sections 4.3.4.3 System Development and Maintenance, 4.3.4.4 Information and Document Management, 4.3.3.3 Physical and Environmental Security
- NIST 800-53 R4 – Appendix F: SI-12 Information Handling and Retention, AC-16 Security Attributes, ZI-10 Information Input Validation
- ISO/IEC 27001 – A.12.1 Security Requirements of Information Systems, A.12.2 Correct Processing in Applications, 4.3.1 General Document Requirements, 4.3.2 Control of Documents, 4.3.3 Control of Records
- ISO/IEC 27019 – 8.2 Information classification

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B3.b Data in Transit

RIIO-2 Cyber Resilience Outcome Description for B3.b Data in Transit:

You should protect the transit of data important to the delivery of the essential service. This includes the transfer of data to third parties.

RIIO-2 Cyber Resilience Guidance:

1. **Data Transfer** – Identify all conduits for data transfer.
   a) Conduits that transmit or carry data important to the delivery of your essential services should be identified. This includes, but should not be limited to:
      - Within the organisation;
      - To third parties and from third parties;
      - For storage and processing in services such as the cloud.

   b) Conduits include, but should not be limited to:
      - Continuously connected data links;
      - File transfers over data links;
      - Removable media;
      - Documents.

2. **Data Protection** – Implement appropriate protection for data in transit.
   a) Based on the impact assessment of the data conduits, appropriate protection against a loss of availability, integrity, confidentiality and safety should be implemented. Protective controls could include, but should not be limited to physical, segregation and cryptographic controls.

   b) Where cryptographic controls are implemented, there should be well-established cryptographic policy and supporting procedures that cover devices, protocols, algorithms, key generation and key management. Resource limitations should be identified through, for example, risk assessments and, architecture and design reviews. Resource limitations may be technical (e.g. power, networks, HVAC) or resources (e.g. skilled personnel).

   c) Appropriate mitigations or alternative compensating controls for the identified limitations should be identified and included in the design.

3. **Single Points of Failure** – Identify communication paths where, due to failure, there is a significant risk of impact on the delivery of the essential services.

a) Single points of failure in communication paths and data flows should be identified and catalogued.

b) The conduits should be classified according to the potential impact that loss of availability, integrity and/or confidentiality could have on the operation of the essential service.

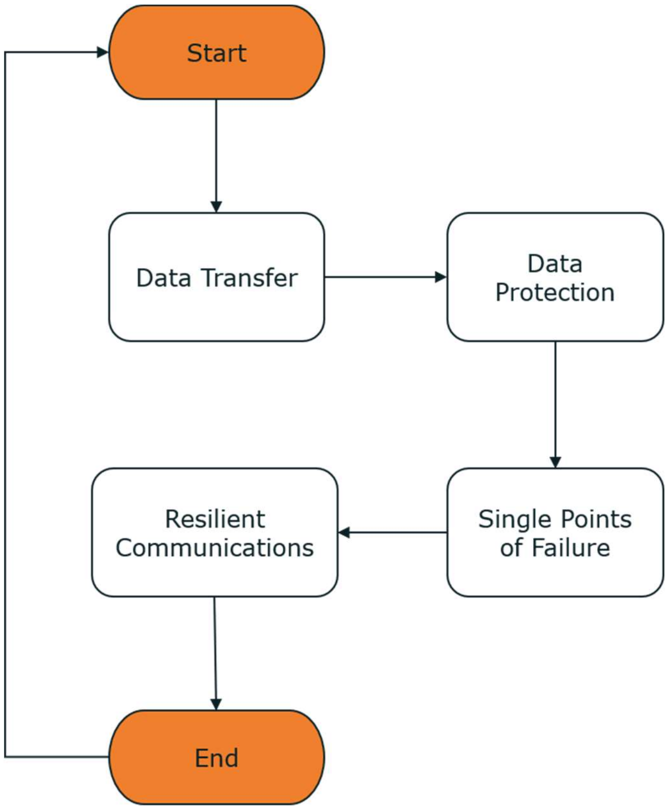
4. **Resilient Communications** – Provide alternative communication paths where there is a significant risk of impact on the delivery of your essential services.

   a) The company should consider utilising diverse routing and technologies to improve the resilience of communications paths where their failure could present a significant risk of impact on the delivery of your essential services aligned with company business continuity and disaster recovery policies.

References and Further Guidance:

- NIST SP800-82 R2 – Sections 5.14, 6.2.16, Appendix G MP-5 Media Transport
- OG86 - B3 Data Security
- IEC 62443-3-3 – SR 3.1 Communication Integrity
- ISO 27019 – Section 13.1.4
- NCSC NIS Guidance B5

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B3.c Stored Data

RIIO-2 Cyber Resilience Outcome Description for B3.c Stored Data:

You should protect stored data important to the delivery of the essential service.

RIIO-2 Cyber Resilience Guidance:

1. **Data Policy** – All copies of data important to the delivery of your essential services are necessary and approved.
   a) There should be policy and guidance to define:
      - The types and scope of data that need to be protected while stored and backed up for recovery.
      - How sensitive data about the OT domain and assets that might be useful to a potential attacker is minimised, stored, categorised, protected and shared only as required.

   b) Data types includes, but should not be limited to:
      - Process data (real-time and historical).
      - Physical and Network drawings.

- Risk assessments.
- System configuration records.
- Asset registers.
- Backups.
- Applications and other software.
- Staff and personal identifiable information.
- Business continuity (BC), Disaster Recovery (DR) and incident response plans.

2. **Sharing Data** – Only data which is required for an intended purpose should be copied to less secure or read-only storage.
   a) Where data is required to be copied to less secure systems, only the minimum data should be provided with limited details and/or as a read-only copy.
   b) These copies should be appropriately protected in line with Guidance 3 below.

3. **Data Protection** – Appropriate physical and technical means are in place to protect stored data from unauthorised access, modification or deletion.
   a) Policy and processes should be defined and implemented to ensure that data is protected against unauthorised physical and logical access or compromise across its lifecycle.
   b) Measures should ensure that:
      - Both operational and audit data are protected against loss or compromise.
      - Consideration has been given to having an alternative storage location for data and backups in case of loss of access to the main site for any reason that requires use of a backup location.
      - Data utilised or shared with third parties and contractors is protected.
      - Data is protected throughout its entire lifecycle, right up to the point of destruction or purging of the storage media for re-use.
      - Careful consideration is given to the risks of using cloud storage for OT data and appropriate security controls implemented.

4. **Encryption** – The cryptography in use should provide some degree of assurance in its ability to protect data at rest.
   a) Where cryptography is used to protect data at rest, organisations should implement cryptographic policy and procedures that cover devices, protocols, algorithms, key generation and key management.
   b) If encryption is readily available for any portable media, then it should be enabled.

c) Tools for the secure storage of data such as passwords (‘password vaults’) should be considered. These could be used to store system passwords for use by service engineers, third parties, contractors, etc.

5. **Backups** – The company has suitable, secured backups of the data required to allow the essential services to operate or to restore the essential services within an acceptable timeframe. Please follow the B5.c Backups guidance for additional information.

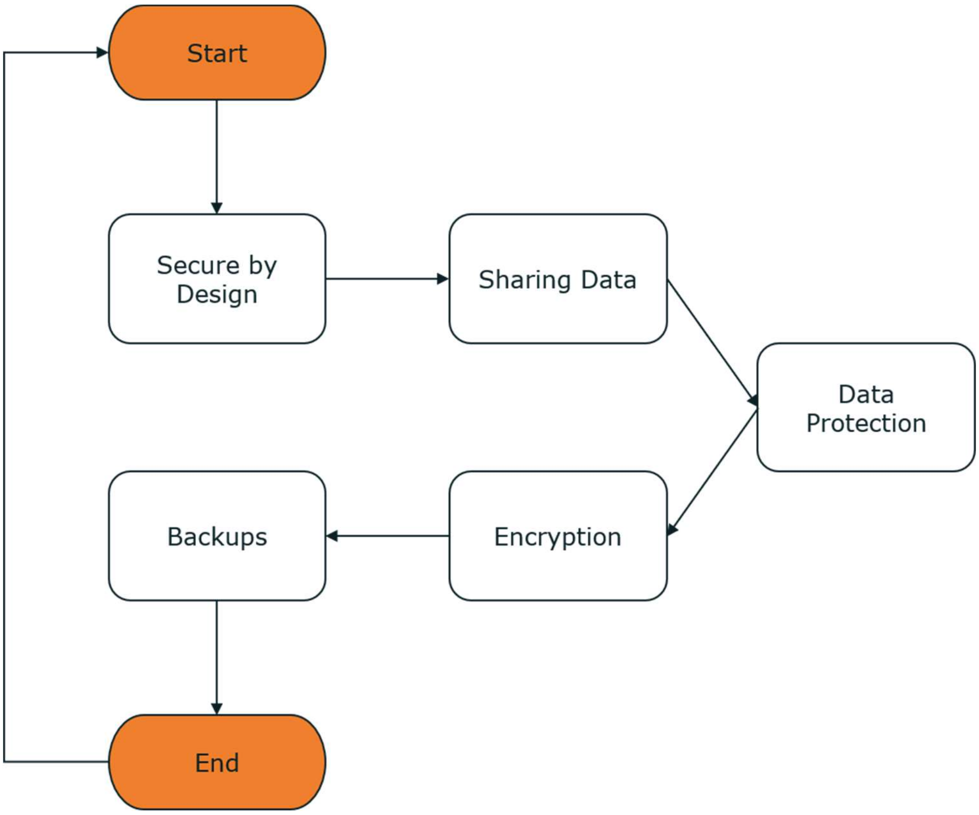
   a) The backups should be secured and protected against loss, and they should be:

   - Available at location(s) close enough to the data centres to allow prompt access and retrieval in the event that they are required.
   - Protected against loss or damage by physical or environmental incidents or tampering.
   - The data on the media can be recovered and restored to server/storage within the Recovery Time Objective (RTO), to the Recovery Point Objective (RPO), and to allow OT operations to resume delivery of the essential service without exceeding the Maximum Tolerable Period of Disruption (MTPD).

References and Further Guidance:

- NIST 800-82 R2 – Appendix G AC-4 Information Flow Enforcement, IA-1 Identification and Authentication Policy and Procedures, IA-5 Authenticator Management, IA-6 Authenticator Feedback, IA-7 Cryptographic Module Authentication, SC-28 Protection of Information at Rest
- OG86 – Appendix 2 - B3 Data Security
- IEC62443-3-3 – Sections 5.7.2 & 11.5, SR 4.1 Information Confidentiality
- NIST 800-53 R4 – Appendix D: AU-9 Protection of Audit Information, CP-9 Information System Backup, MP-1 Media Protection Policy and Procedures, MP-4 Media Storage
- ISAO270019 – Section 10.1

Guidance Flow:


Start
Secure by Design
Sharing Data
Data Protection
Encryption
Backups
End

RIIO-2 Cyber Resilience Guidelines B3.d Mobile Data

RIIO-2 Cyber Resilience Outcome Description for B3.d Mobile Data:

You should protect data on mobile devices that is important to the delivery of the essential service.

RIIO-2 Cyber Resilience Guidance:

1. **Identify Mobile Devices** – It is known which mobile devices hold data important to the delivery of the essential service.
   a) All mobile devices, including engineering laptops and maintenance laptops, that hold data important to the delivery of the essential service should be identified and catalogued as part of the asset management process.
   b) There should be processes and procedures to manage the storage of data on any third party or contractor devices.
   c) The catalogue of mobile devices holding critical data should be reviewed periodically, at least annually or in accordance with the management system.

2. **Mobile Data Policy** – The requirements to protect data that is important to the delivery of the essential services and is stored on mobile devices are defined.
   a) There should be a policy and procedures defined and implemented to secure data stored on mobile devices.

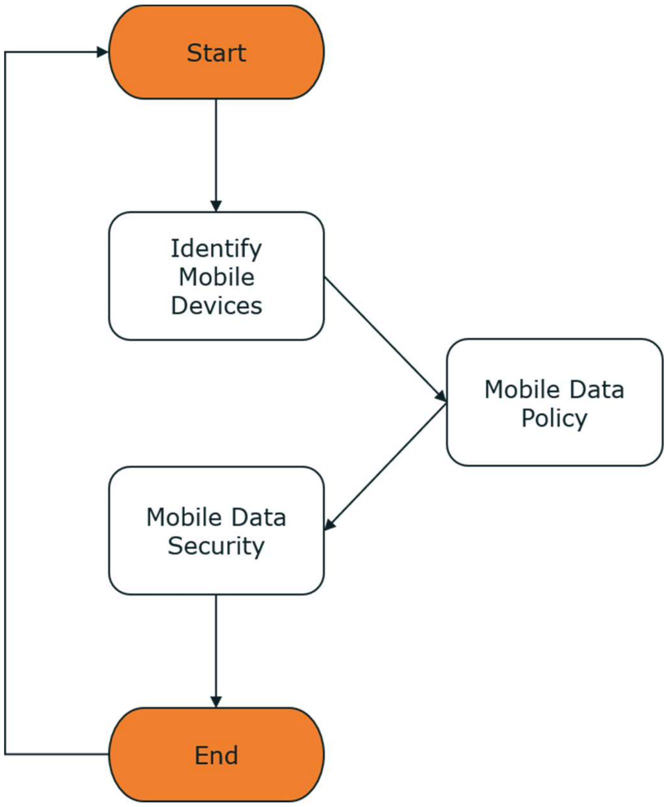
3. **Mobile Data Security** – Data stored on mobile devices that is important to the delivery of the essential services is appropriately secured.
   a) A risk assessment to identify the risks associated with important data being stored on mobile devices should be conducted.
   b) Based on the risk assessment, implement commensurate security controls (e.g. data encryption and device authentication).
   c) Risk assessments should be reviewed periodically, in accordance with policy.

References and Further Guidance:

- OG86 Appendix 2 - B3 Data Security
- IEC 62443/ISA99 3-3 – SR 2.3 Use Control for Portable and Mobile Devices
- ISO27019 – Sections 6.2.1 & 10.1
- ISA99 Part 4 Protection of data at rest

- NCSC End user device (EUD security guidance)
- NIST FIPS 140-2

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B3.e Media Equipment Sanitisation

RIIO-2 Cyber Resilience Outcome Description for B3.e Media Equipment Sanitisation:

You should appropriately sanitise data from the service, media or equipment before disposal.

RIIO-2 Cyber Resilience Guidance:

1. **Asset Inventories** – All devices (including removable media, laptops and mobile devices) that store data important to the delivery of the essential services should be identified and catalogued. For additional information please refer to the A3.a Asset Management section.
   a) Asset inventories should be maintained detailing which devices hold data important to the delivery of the essential service. This can include but should not be limited to:
      - Laptops (e.g. for engineering activities such as backup and recovery);
      - Mobile devices (e.g. for use by engineers in the field such as data acquisition);
      - Removable media (e.g. Collect or transfer a file or data to or from the OT such as collecting alarm data for analysis);
      - Other OT equipment such as Programmable Logic Controllers (PLCs, Human Machine Interfaces (HMIs), Remote Terminal Units (RTUs), engineering workstations, servers, “smart” instruments and industrial IoT devices, hand-held programming devices and mobile devices (e.g. tablets).

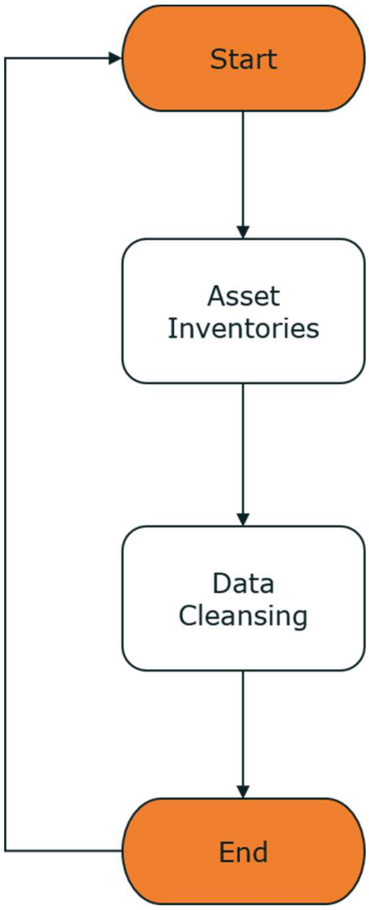
2. **Data Cleansing** – There is a robust process to sanitise data important to the delivery of the essential services from all devices, equipment and removable media before disposal or redeployment as part of the asset management lifecycle.
   a) There should be a policy and procedure defined and implemented to sanitise data from devices to manage security risks during the process of decommissioning and disposal (e.g. physical destruction, cryptographic erasure, data erasure).
   b) There should be detailed, step-by-step instructions for the different technology types.

References and Further Guidance:

- NIST SP800-82 R2 – Section 6.2.10, IA-3 Device Identification and Authentication, MP-6 Media Sanitization
- OG86 - Appendix 2 A3 Asset Management, B3 Data Security

- ISO 27019 – Section 8.3

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B4.a Secure by Design

RIIO-2 Cyber Resilience Outcome Description for B4.a Secure by Design:

You design security into the network and information systems that supports the delivery of essential services. You minimise their attack surface and ensure that the delivery of the essential service should not be impacted by the exploitation of any single vulnerability.

RIIO-2 Cyber Resilience Guidance:

1. **Secure by Design** – Appropriate expertise is employed to design secure networks and information systems supporting your essential services.
   a) The company should ensure that systems are secure by design through:
      - Persons with appropriate expertise in OT and security architecture are responsible for review and input;
      - Understanding business drivers (strategy/plans/regulation/safety, etc.), hazard, threat and vulnerability identification, risk assessment and controls identification;
      - An in-depth understanding of the need for the safety, resilience and reliability of the essential service;
      - Sufficient authority or support to ensure that the risks are managed and design patterns are adhered to.

2. **Network Segregation** – The networks and information systems supporting your essential services are segregated into appropriate security zones.
   a) The design of the OT systems should specify and implement a multi-layer security architecture that is segregated into zones based upon risk and function.
   b) The design should also consider supporting and ancillary systems (e.g. Uninterruptable Power Suppliers, HVAC) to ensure they are appropriately secured.
   c) Appropriate network segregation and access controls (logical and physical) should be implemented to protect the OT networks and zones against malfunction, mistake and malicious activity.
   d) The use of remote access to the networks and systems should be carefully designed to restrict access to the minimum required assets and data.

3. **Network Data Flows** – The networks and information systems are designed to have simple data flows internally between systems and interfaces with external systems and, where possible, between devices, to enable effective monitoring.

a) Any connections to external networks or other control systems should only be through managed interfaces consisting of appropriate boundary protection devices, including but not limited to physical or logical solutions providing encryption, network access control lists etc.

b) Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site.

c) As part of a multi-layer protection strategy, higher impact control systems should be partitioned into separate zones utilising controlled conduits to restrict or prohibit network access in accordance with security policies and procedures and an assessment of risk.

4. **Resilient Networks** – The networks and information systems supporting your essential service are designed to be easy to recover.

a) It should be possible to recover the essential service within the agreed Recovery Time Objective, Recovery Point Objective and Maximum Tolerable Period of Disruption to a known good, safe, state after an incident.

b) The design should ensure that:

- All required information for configuration, access control, safe start and operation, recovery procedures, etc. are documented;
- Backups are taken containing all required operational data, configurations, current encryption keys, passwords, etc. at suitable intervals;
- Log data is available to assist in incident diagnosis and recovery.

5. **Attack Mitigation** – Content-based attacks are mitigated for all inputs to operational systems that effect the essential service.

a) The design should defend against content-based attacks (the ability of an attacker to compromise systems by installing malware/trojans/logic bombs, sending corrupted or out-of-range commands, etc.) and the risk managed.

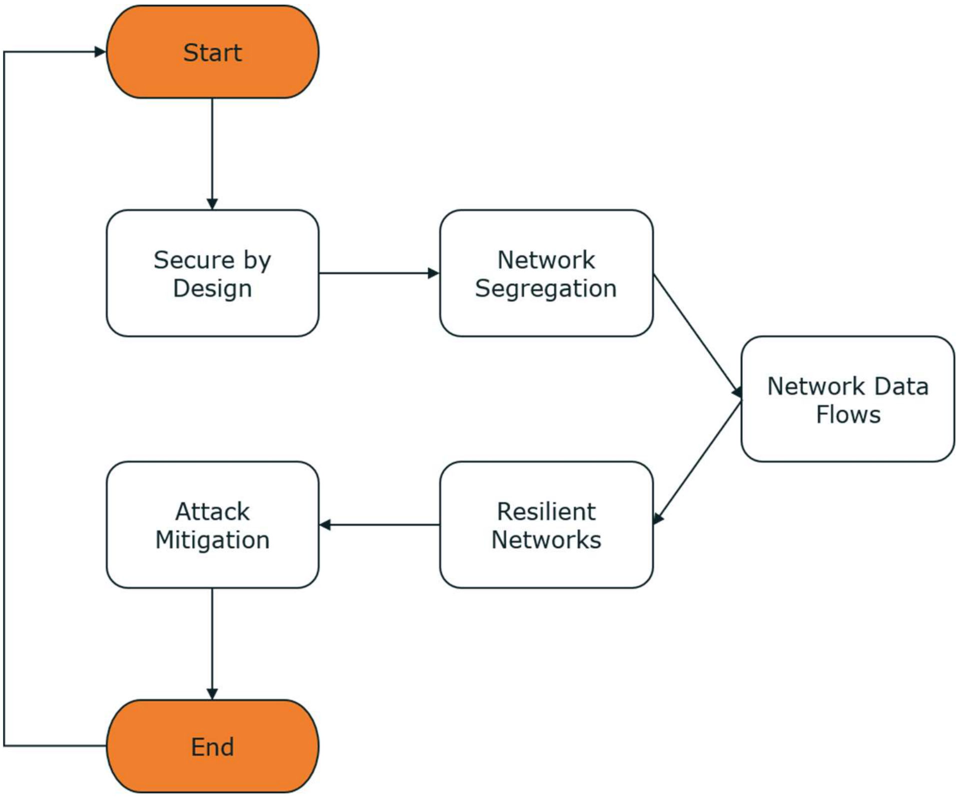
b) Design options include, but are not limited to:

- Tools to defend systems from unauthorised installation and execution of software;
- Use of content inspection and file format conversion toolsets at domain and zone boundaries;
- Input validation and verification techniques;
- OT protocol inspection technology;
- Use of cryptographic functions for authentication and non-repudiation.

References and Further Guidance:

- NIST 800-82 R2 – Appendix G: PL-7 Security Concept of Operations, PL-8 Information Security Architecture, SA-8 Security Engineering Principles, SA-17 Developer Security Architecture and Design
- OG86 – Appendix 2 - B4 System Security
- IEC62443-1-1 – Sections 5.2, 5.5, 5.9, 6.4, 6.5
- IEC62443-3-3 – SR 5.2 Zone Boundary Protection
- NIST 800-53 R4 – Section 2.6, Appendix D: AU-9 Protection of Audit Information, CP-9 Information System Backup, MP-1 Media Protection Policy and Procedures, MP-4 Media Storage
- ISO27001 – Sections 14.1 & 14.2
- NCSC Cyber security design principles
- NCSC 6 security architecture 'anti-patterns'

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B4.b Secure Configuration

RIIO-2 Cyber Resilience Outcome Description for B4.b Secure Configuration:
You securely configure the network and information systems that support the delivery of essential services.

RIIO-2 Cyber Resilience Guidance:

1. **Secure Configuration** – The security configuration and maintenance requirements for all assets is defined and documented.
   a) Requirements to consider for security configurations may include, but are not limited to:
      - Asset hardening;
      - Firewall and network equipment configurations;
      - Access control;
      - Remote access.

   b) Requirements to consider for security maintenance may include, but are not limited to:
      - Methods for carrying out maintenance tasks;
      - Performing security updates (e.g. patching and signature updates), performing backup etc.

2. **Asset Management** – There is a set of records for assets which need to be configured and maintained to ensure the essential service is secure.
   a) Asset inventories should be held and maintained to include security configuration and maintenance. This could be based on, but is not limited to, the asset's criticality to protect the safety, reliability, resilience or security of the essential service.

3. **Configuration Management** – The security configuration(s) are applied to all assets.
   a) A process should be implemented to apply the appropriate security configurations to all assets.
   b) Security configurations should be tested in suitable environments and further held and applied in a secure fashion.

4. **Secure Builds** – Secure builds exist for systems, networks or endpoints that need to be configured to maintain the security of the essential service.
   a) An appropriate and secure baseline build should be developed for all systems and components, including hardware and software to implement the specified configuration.

b) A process should be implemented to ensure that any functionality or application that does not support a user or business need is removed or disabled and the master baseline build profile for that device is updated.

5. **Secure Configuration Management** – The security configuration of assets which need to be carefully configured is actively managed.
   a) A procedure should be implemented to ensure that the secure build profile is managed by a configuration control process and any deviation from the standard build should be documented and approved.
   b) This procedure should ensure that changes to the build profile and to the configuration of live systems are managed to ensure systems and documentation are synchronised.

6. **Change Management** – There is an effective change management process that ensures all changes to network or system configuration are secure and comply with the security configuration requirements.
   a) Changes which may affect the security configuration of an asset, network or system, should only be undertaken with appropriate review and authorisation.
   b) Where possible, the change management process should be integrated with other change management processes. This can include but is not limited to:
      - Management of Change (MoC) – authorise change;
      - Risk assessment – to assess any new risks presented by the change;
      - Permit to Work system – manage change tasks.

7. **Software Management** – Only approved software should be installed on networks and information systems supporting your essential service.
   a) A process should be implemented to gain approval of software prior to deployment within the OT environment. This can include, but is not limited to:
      - Testing the security of software (e.g. code review or penetration testing);
      - Testing the integrity of software for install (e.g. installation in a test environment);
      - Vendor approval.
   b) Installation of software should be subject to the change management process.

8. **Account Permissions** – Non-privileged accounts cannot change settings which would impact security.
   a) User permissions should limit the ability of non-privileged accounts users to change access permissions, account permissions, install software, disable security software, etc., and be enforced across all systems and devices.

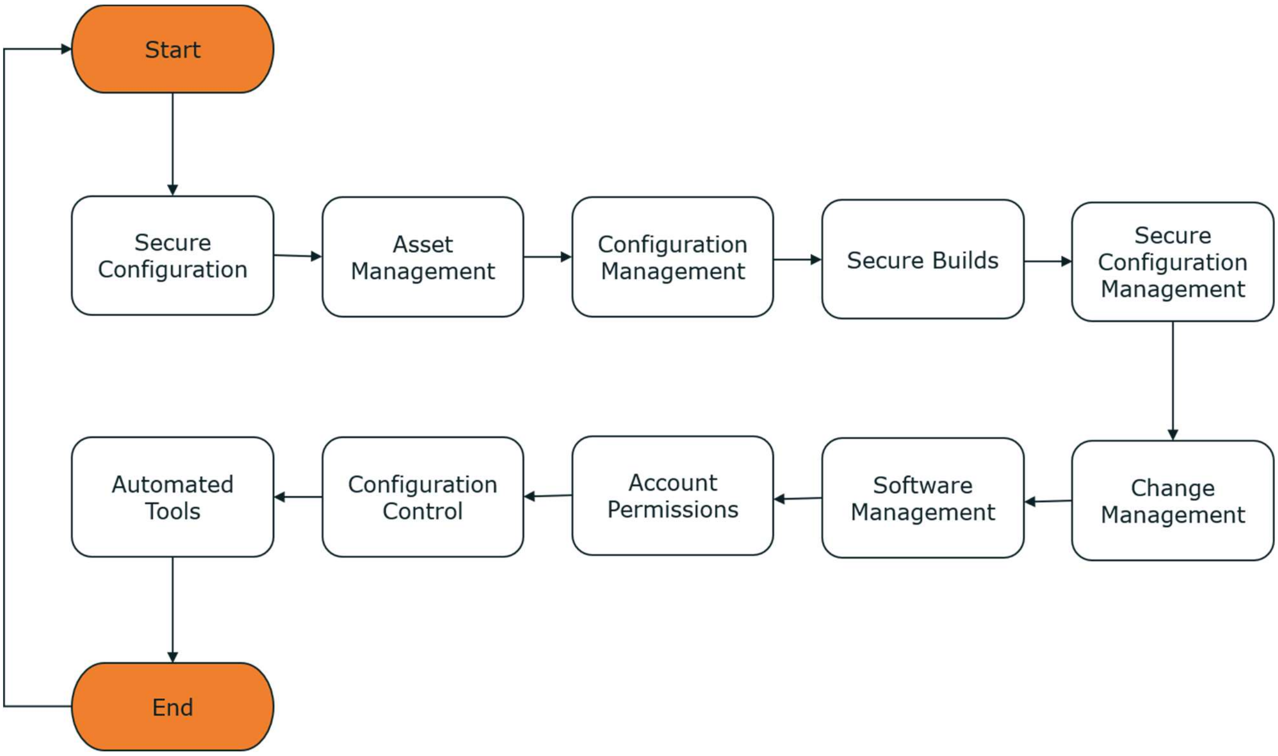
9. **Configuration Control** – The networks and information systems supporting your essential service are regularly reviewed or monitored and validated to confirm the expected configurations and secure settings are applied.
    a) Security configurations should be regularly reviewed, in accordance with company policy, or as part of a change.
    b) Validation techniques can include but are not limited to:
    - Reviewing and comparing configurations against master baseline build profiles;
    - Testing functionality of systems to check for desired interoperability.

10. **Automated Tools** – The operation of automated decision-making technologies, including advanced control, if in use, are well understood.
    a) Where automated decision making can affect an essential service, it should be possible to understand the data, process and thresholds used to make automated decisions so that it can be reproduced, audited and malicious changes detected.
    b) For decisions based on pre-determined and unchanging behaviour the company should understand the exact hardware, firmware, software, and configuration of individual systems (this may be achieved with detailed configuration and asset management) and monitor for any unplanned changes.
    c) Where systems use some element of machine learning and the decision-making process changes over time the model used should be auditable, so that malicious changes can be detected. This can identify cases where changes have been made directly, or where malicious or misleading data has been used for learning.

References and Further Guidance:

- NIST SP800-82 R2 – Sections 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9
- NIST SP800-82 R2 – Appendix G: CM-2 Baseline Configuration, PL-7 Security Concept of Operations, PL-8 Information Security Architecture, SA-8 Security Engineering Principles,
- OG86 - Appendix 2 - B4 System Security
- IEC 62443/ISA99 3-3 – SR 7.6 Network and Security Configuration Settings, SR 7.7 Least Functionality

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B4.c Secure Management

RIIO-2 Cyber Resilience Outcome Description for B4.c Secure Management:
You manage your organisation's network and information systems that support the delivery of essential services to enable and maintain security.

RIIO-2 Cyber Resilience Guidance:

1. **Dedicated Management Devices** – There should be dedicated devices used for the maintenance and security management of networks and information systems supporting your essential service.
   a) Policy and guidance (B2 refers) should be developed, maintained and implemented regarding the:
      - Separation of normal user functionality from maintenance and security management functionality. This includes all accounts capable of causing an impact on the delivery of essential services;
      - Use of separate user accounts with stronger identity and access requirements for system administration functions.

   b) The dedicated maintenance and security management devices are segregated and secured to a level commensurate with those networks and information systems they maintain. For example, there may be engineering laptops or dedicated maintenance devices used across the estate, which should be managed independently from corporate systems and networks.

2. **Unauthorised Software Management** – Effective technical, procedural and physical security measures are in place to prevent, detect and remove unauthorised software and malware on networks and information systems supporting your essential service.
   a) Policy and guidance should be developed, maintained and implemented regarding the:
      - Hardening of OT assets, recognising the need to secure a system by reducing its inherent vulnerabilities;
      - The deployment, monitoring and maintenance of protective monitoring, intrusion detection and anti-malware functions on assets and at domain/network boundaries;
      - Removal of unauthorised software and malware once detected.

   b) Where automated monitoring and detection cannot be used, alternative compensating controls should be implemented.

3. **Authorised Privileged Users** – Networks and information systems supporting your essential service are only administered and maintained by authorised privileged users.
   a) Policy and guidance should be developed, maintained and implemented regarding the separation of duties to manage the risks of abuse or compromise of privileged administration accounts and malicious activity. This includes, but is not limited to:
      - System management;
      - Configuration management;
      - Network security;
      - Protective monitoring and incident response;
      - Ensuring security personnel do not administer audit functions or have access to event log data.

   b) There should be a defined and documented approval process for granting personnel access to privileged accounts and systems.

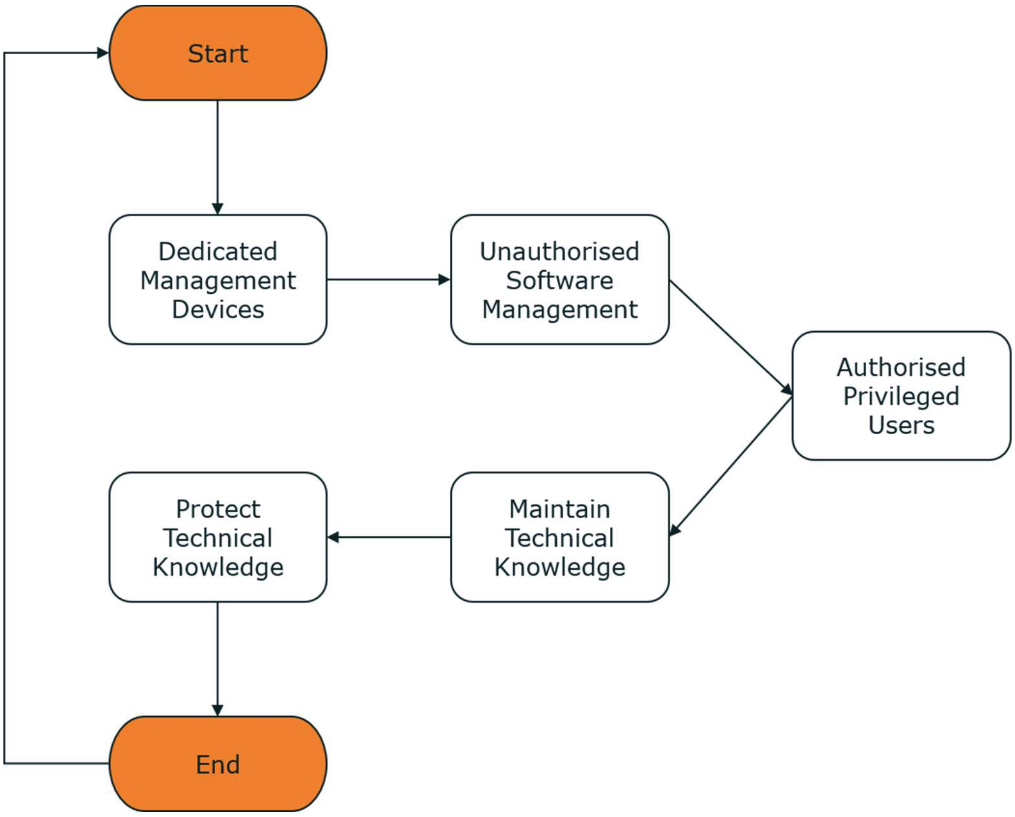
4. **Maintain Technical Knowledge** – Technical knowledge about networks and information systems supporting your essential service is reviewed and updated periodically.
   a) The technical knowledge, such as documentation and network diagrams, held on the networks and information systems supporting your essential service and its location should be known and catalogued.
   b) Technical knowledge should be reviewed and updated periodically, in accordance with company policy, or on a significant change.

5. **Protect Technical Knowledge** – Technical knowledge about networks and information systems supporting your essential service is appropriately stored and secured.
   a) An information classification scheme should be developed and implemented for the technical knowledge about the networks and information systems supporting your essential service.
   b) The information classification scheme should provide guidance to assign the appropriate classification, control access, store, transmit, and dispose of or destroy information.

References and Further Guidance:

- NIST SP800-82 R2 – Section 6.2.5
- OG86 Appendix 2 - B1 Protection Policies and Processes
- NIST 800-53 R4 – Appendix D: AC-5 Separation of Duties, SC-1 System and Communications Protection Policy and Procedures, SC-3 Security Function Isolation, MA-1 System Maintenance Policy and Procedures
- IS27001 – Sections 12.1.2, 14.2.2

Guidance Flow:


Start
Dedicated Management Devices
Unauthorised Software Management
Authorised Privileged Users
Maintain Technical Knowledge
Protect Technical Knowledge
End

RIIO-2 Cyber Resilience Guidelines B4.d Vulnerability Management

RIIO-2 Cyber Resilience Outcome Description for B4.d Vulnerability Management:
You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.

RIIO-2 Cyber Resilience Guidance:

1. **Research Vulnerabilities** – Publicly-known vulnerabilities relevant to the networks and information systems supporting your essential service are monitored and analysed to understand your exposure.
   a) A process should be implemented to maintain awareness of relevant vulnerabilities in the networks and information systems supporting your essential service. Sources of information includes, but is not limited to:
      - Government and industry information sources:
        - NCSC – providing advice relevant to operators of essential services directly and through the Cyber Information Sharing Partnership (CiSP) portal;
        - ICS CERT – from US Department of Homeland Security which provides focused advice on OT technologies;
        - MITRE CVE – a non-profit organisation providing the Common Vulnerability and Exposures database and which has become the de facto standard for Information Security Vulnerability nomenclature;
        - Law enforcement agencies – including police and specialist cybercrime units;
        - Regulators – sector specific information;
        - NCSC information exchanges;
        - Industry information exchanges e.g. E3CC and ISACs.
      - Commercial organisations:
        - Vendors;
        - Specialised threat intelligence organisations.
      - Internal sources:
        - Passive or active scanning and testing.
      - Others:
        - Security researchers;
        - Specialised forums and mailing lists (e.g. SCADASec).

2. **Horizon Scanning –** It is expected that the company be made aware of a new vulnerability or threat, they have the ability to ascertain the associated risk within their environment, within a period defined by their policy.

3. **Assess Vulnerabilities** – Vulnerabilities in the networks and information systems supporting your essential service are assessed, prioritised and mitigated.
   a) There should be a process implemented to assess known vulnerabilities in the networks and information systems supporting your essential service.
   b) The process should assess the risk associated with the vulnerability, including the likelihood of exploitation and the potential impact if exploited.
   c) The process should prioritise vulnerabilities for remediation based on the risk:
      - Identified vulnerabilities should be mitigated according to their priority;
      - Mitigations can be technical, procedural and physical measures.
   d) Where a system cannot be patched (e.g. system is unsupported), alternative compensating controls to mitigate the risk should be considered (e.g. the unsupported system connects to another system outside the boundary which can be patched).
   e) For vulnerabilities where it is decided not to mitigate, there should be a process to ensure these are documented as accepted and managed as a residual risk.

4. **Track Vulnerabilities** – Both publicly announced and privately notified vulnerabilities in the networks and information systems supporting your essential service are tracked.
   a) There should be a vulnerability management plan developed to ensure that vulnerabilities identified within networks and information systems are tracked through to remediation.
   b) Each vulnerability that is identified should be assigned an owner which is documented in the plan.

5. **Temporary Mitigations** – Some vulnerabilities that are not exposed outside the system boundary/security zone of the networks and information systems supporting your essential service may have temporary mitigations for an extended period.
   a) Temporary mitigations may be required for an extended period due to:
      - Operational reasons (e.g. change requires system shutdown and is being deferred until a planned maintenance routine);
      - Technical reasons (e.g. change is not compatible with existing system or infrastructure);
      - Age of system (e.g. system is coming towards end of life and change is not approved due to cost vs benefit/time).

b) Temporary mitigations and other compensating controls should always be implemented as the lack of exposure is insufficient mitigation on its own.

c) Where temporary mitigations are required for an extended period, these should be monitored and regularly reviewed, in accordance with the risk balance case.

6. **Obsolete Technology** – Obsolete and/or unsupported networks and information systems supporting your essential service may have temporary mitigations for vulnerabilities while pursuing migration to supported technology.

    a) The networks and information systems supporting your essential service which are obsolete or unsupported should be identified and catalogued.

    b) Temporary mitigations and alternative compensating controls should be managed as a programme where necessary while progressing migration to supported technology.

    c) The company may decide to continue operate some obsolete or unsupported systems for an extended period. Where this approach is followed, a comprehensive and holistic physical-cyber risk assessment should be conducted to ensure an appropriate level of security is maintained for the essential service.

7. **Vulnerability Checks** – There are regular tests or assessments undertaken to fully understand the vulnerabilities in the networks and information systems supporting your essential service.

    a) Vulnerability assessments should be carried out on a regular basis, in accordance with policy.

    b) Techniques can include but are not limited to:

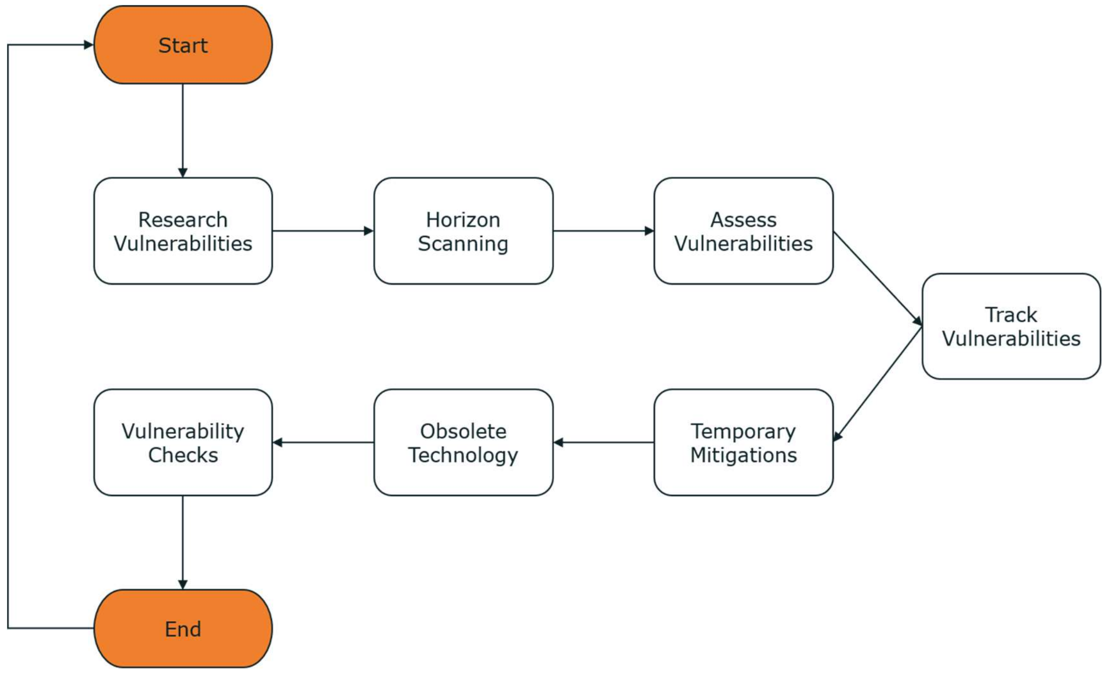
        - Application and software review;
        - Desktop and configuration reviews;
        - Operating system and network vulnerabilities reviews;
        - System and network architecture reviews.

Special Note: Due to the sensitive nature of OT networks and systems, operators need to carefully consider their approach to the testing of live OT, as system operation, availability and safety could be affected. Assurance could be gained without this additional risk by testing against non-operational environments or by testing individual components in a laboratory environment.

References and Further Guidance:

- NIST SP 800-82 R2 – CA-8 Penetration Testing, RA-5 Vulnerability Scanning, SI-7 Software, Firmware and Information Integrity
- OG86 – Appendix 2: B4 System Security, C2 Proactive Security Event Discovery
- ISO 27019 – Section 12.6
- NCSC – "Vulnerability Management" from guidance repository

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B5.a Resilience Preparation

RIIO-2 Cyber Resilience Outcome Description for B5.a Resilience Preparation:
You should be prepared to restore your essential service following disruption.

RIIO-2 Cyber Resilience Guidance:

1. **Recovery Plan** – The networks and information systems and supporting technologies required to restore your essential service are known, documented and in line with company, Business continuity, disaster recovery processes and risk management processes.
   a) The networks and systems, including their underlying technologies, and supporting technologies (e.g. Uninterruptible Power Supply (UPS) and Heating, Ventilation, and air conditioning (HVAC), Physical access controls) which are required to provide the essential service should be identified, understood and documented.
   b) This should include an understanding of the minimum set of networks, systems and resources required restore and operate your essential service.
   c) The company should ensure this aligns with Business Continuity Planning expectations.

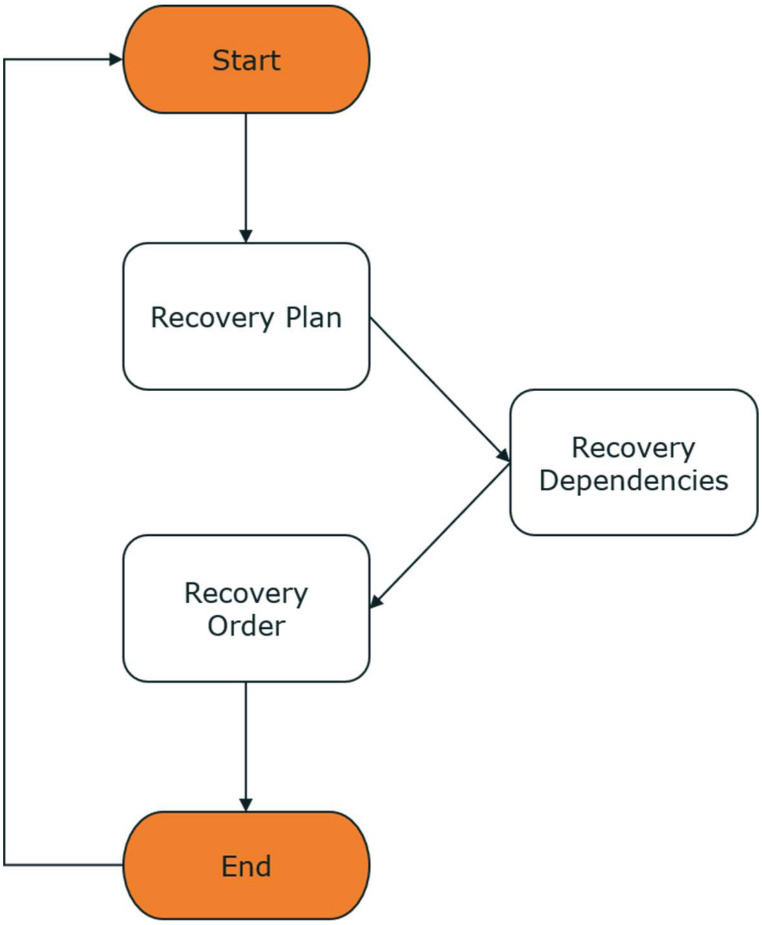
2. **Recovery Dependencies** – The interdependencies between the networks and information systems and the supporting technologies are understood and documented.
   a) The company should identify and document interdependencies:
      - Between the networks and systems supporting your essential service.
      - On supporting technologies.
      - On upstream and downstream third-party networks and systems.
      - Internal and external service and support providers.

3. **Recovery Order –** The sequence and order in which supporting technologies, the networks and systems to restore the essential service are known and documented. This should be aligned with company risks, disaster recovery and business continuity processes.
   a) There should be documentation identifying the order in which resources, supporting technologies and the networks and information systems supporting your essential service are needed to restore and operate your essential service.
   b) Escalation triggers and paths to facilitate restoration if required to overcome problems should be identified and documented.

References and Further Guidance:

- NIST 800-82 R2 – Section 6.2.6, Appendix G: CM-8 Information System Component Inventory, CP-1 Contingency Planning Policy and Procedures, CP-2 Contingency Plan, CP-4 Contingency Plan Testing, CP-10 Information System Recovery and Reconstitution
- OG86 – Appendix 2: B5 Resilient Networks and Systems
- IEC 62443/ISA99 2-1 – Section A.3.4.3.8
- IEC62443-3-3 – SR 7.3 Control System Backup, SR 7.4 Control System Recovery and Reconstitution, SR 7.5 Emergency Power, SR 7.8 Control System Component Inventory
- ISAO27001 – Sections 17.1, 17.2

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B5.b Design for Resilience

RIIO-2 Cyber Resilience Outcome Description for B5.b Design for Resilience:

You should design the network and information systems supporting your essential service to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.

RIIO-2 Cyber Resilience Guidance:

1. **Design for Resilience** – The networks and information systems supporting your essential services are segregated into appropriate security zones.
    a) The design of the OT systems should specify a defence-in-depth system/security architecture that is segregated into zones based upon risk and function.
    b) The design should consider supporting and ancillary systems such as UPS, HVAC, Safety Instrumented Systems, Fire & Gas systems, etc. to ensure they appropriately secured.
    c) Appropriate network segregation and access controls (logical and physical) should protect the OT networks and zones against malfunction, mistakes and malicious activity.
    d) The use of remote access to the networks and systems should be carefully designed to restrict access to the minimum required assets and data.

2. Identify Limitations – Resource limitations should be identified and, where appropriate, mitigated either technically or with compensating controls.

a) The company should identify resource limitations through, for example, risk assessment and, architecture and design reviews. Resource limitations may be technical (e.g. power, networks, legacy equipment, HVAC) or people (e.g. skilled personnel).

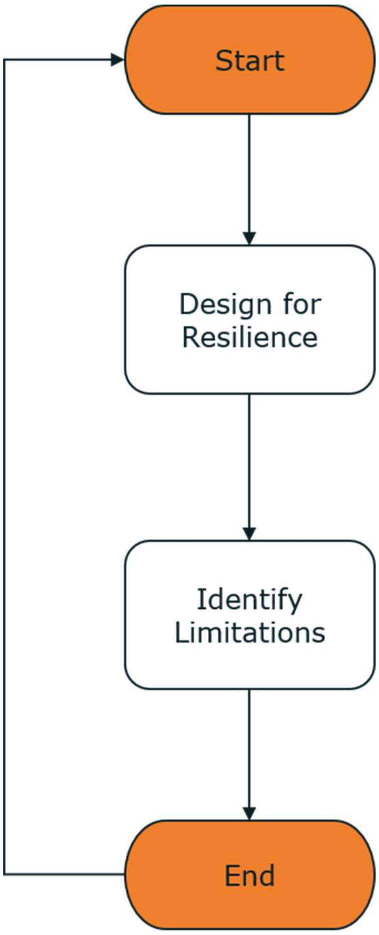
b) Appropriate mitigations or alternative compensating controls for the identified limitations should be identified, included in the design and risks assessed as part of the company risk management process.

References and Further Guidance:

- NIST SP800-82 R2 – Sections 5.1, 5.5, 5.13
- OG86 - Appendix 2: B4 System Security, B5 Resilient Networks and Systems
- IEC 62443/ISA99 3-3 – Section 7.1
- IEC 62443-3-3 - Section 9.1

- ISO 27019 – Section 13.1.3

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B5.c Backups

RIIO-2 Cyber Resilience Outcome Description for B5.c Backups:

You hold accessible and secured current backups of data and information needed to recover.

RIIO-2 Cyber Resilience Guidance:

1. **Backups** – There are backups of all systems, software, configurations, data and other relevant information required to enable recovery of individual devices or entire networks and systems supporting your essential services.
   a) The company should develop, maintain and implement policy and guidance to ensure backups are performed for:
      - IT and OT systems, communications and networks relevant for the operation of the essential service;
      - Supporting technologies (e.g. UPS and HVAC);
      - Security appliances and services;
      - Third party stored data.

   b) The company should consider retaining sufficient historical backups to enable restoration to a previous known-good state.
   c) The company should maintain appropriate records to manage backups.

2. **Security of backups** – Backups are appropriately secured and protected.
   a) The organisation should define and implement appropriate measures to secure and protect physical backups through the use of off-site or alternate sites storage.
   b) The media should be logically assured to protect against potential compromise as part of malicious or accidental activity, or environmental damage.
   c) The media should be protected at each location to the level required to manage the risks to the data they hold and the potential impact if they are lost or compromised.

3. **Availability of backups** – Backups are accessible if an extreme event occurs.
   a) The organisation should develop, maintain and implement policies and guidance on storing backup media:
      - At locations where an incident or disaster of any type would not lead to loss or compromise of the backup media for IT and OT systems associated with the delivery of essential services;

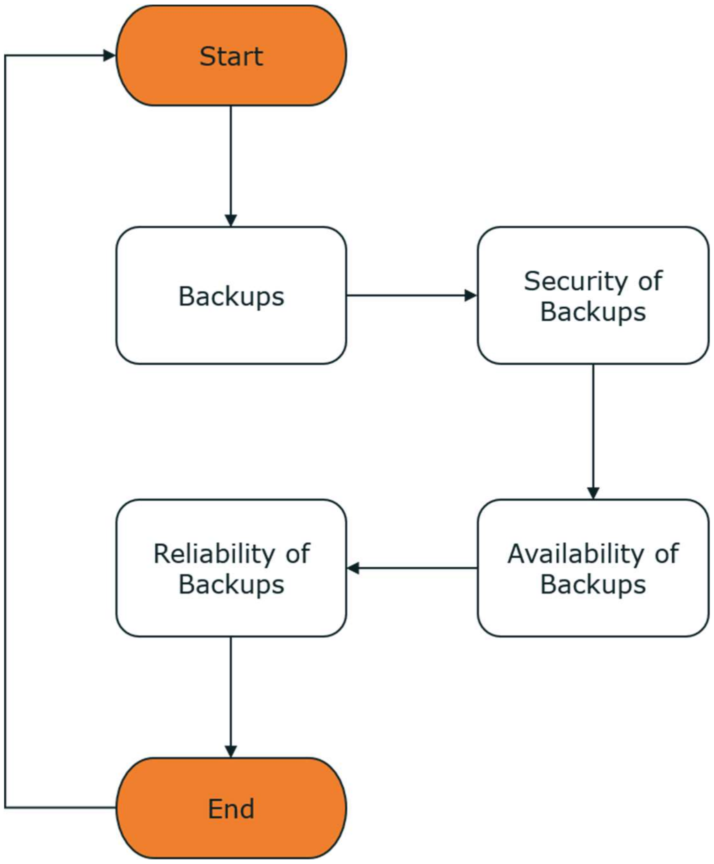
- Ensuring backup media is secure yet readily accessible by authorised personnel at each physical location where it is kept in the event of an extreme event or security incident.

4. **Reliability of backups** – Backups are routinely tested to ensure the backup process is functioning correctly and the backups are useable.
   a) The organisation should develop, maintain and implement policies and guidance on testing backup media to ensure that:
      - The backup process is capturing all the required operational and configuration data to allow full recovery;
      - The media could be used to recover assets to operate essential services in the event of an incident;
      - The documented restoration procedures are checked to ensure they work;
      - The backup recovery strategy should consider a range of restoration options and restoration order. This should include timing depending upon the criticality from installed standby equipment in other locations, hardware spares and software backups through to equipment that is not backed up;
      - The assets could be recovered within the Recovery Time Objective (RTO) and to the Recovery Point Objective (RPO), aligned with organisational response plans and policy requirements;
      - The recovery systems and components should be reliable and effective;
      - The personnel responsible to the backup and recovery process should be competent to recover backup media.
      - Changes to processes relating to the management of backup media are subject to change control and risk assessment.

References and Further Guidance:

- NIST 800-82 R2 – CP-9 Information System Backup, CP-10 - Information System Recovery and Reconstitution, CM-8 - Information System Component Inventory
- OG86 – Appendix 2 B5 Resilient Networks and Systems
- IEC 62443-3-3 – SR 7.3, Control System Backup, SR 7.4 Control System Recovery and Reconstitution
- ISO/IEC 27001 – Sections A.10.5, A.14.1
- ISO/IEC 27019 – Section 12.3

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines B6.a Cyber Security Culture

RIIO-2 Cyber Resilience Outcome Description for B6.a Cyber Security Culture:
You develop and pursue a positive cyber security culture.

RIIO-2 Cyber Resilience Guidance:

1. **Communicate Priorities and Objectives** – Executive management clearly communicate to all relevant personnel the organisation's cyber security priorities and objectives for the networks and information systems supporting your essential service.
   a) The company should have a clearly defined cyber security policy that is endorsed by the company's executive management team.
   b) The company should ensure that this security policy and approach are clearly communicated to all relevant personnel, including third parties.

2. **Positive Security Culture** – The company displays positive cyber security attitudes, behaviours and expectations.
   a) The company's leadership and personnel demonstrably comply with the organisation's security policy and procedures.
   b) A strong security culture is embedded as "business as usual".
   c) The level of security should be appropriate to the information or system being protected to both maximise compliance and minimise unnecessary restrictions.

3. **Availability of Security Information** – Personnel can easily access information about cyber security relevant to their role.
   a) The company should make cyber security policies, standards, procedures and work instructions easily accessible to all relevant personnel.
   b) The company can ensure relevant personnel have easily accessible technical knowledge about the networks and information systems supporting your essential service.
   c) The company should also ensure the remediations and sanctions in the event of a security breach are available, known and understood.

4. **Understand Individual Contribution to Security** – Personnel understand the contribution they can make as individuals to the security of the networks and information systems supporting your essential service.

a) Personnel should understand their roles and responsibilities relating to security of the networks and information systems supporting your essential service.

b) Relevant roles and responsibilities have clearly defined security contributions.

c) Training and awareness (see B6.b) should be developed to support individual knowledge and the fostering of a positive security culture.

5. **Security Incident Process** – There is an easily accessible and understood method to raise a cyber-security issue and that personnel are confident in its use.

a) There is a simple and clearly defined, documented and communicated process for raising cyber security issues.

b) Personnel are demonstrably aware of the process to raise a cyber-security issue and are confident to do so.

6. **Assess and Review Culture and Understanding** – A variety of methods will be employed to assess the security culture and personnel understanding of the required reactions in the event of different security incidents.

a) Options which could be used include, but are not limited to:

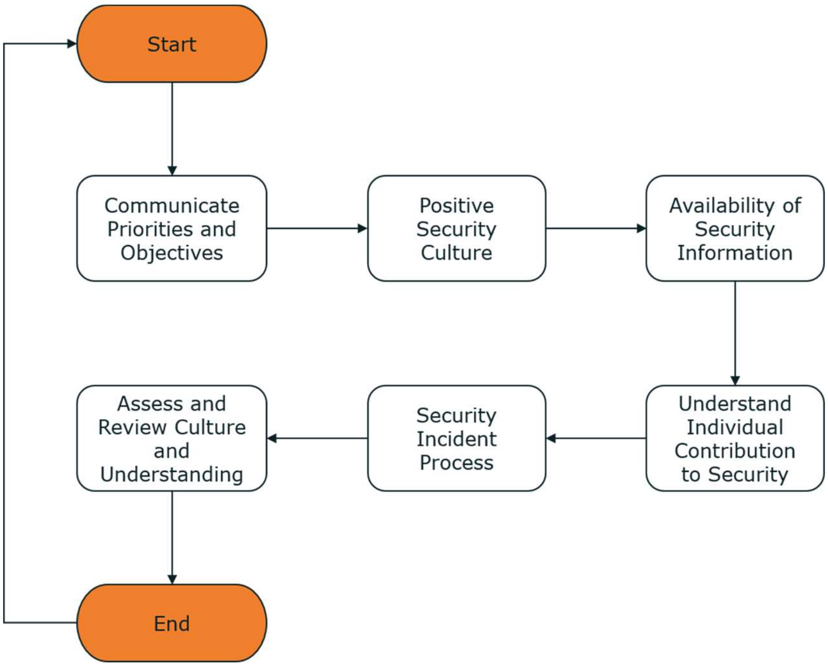
- Phishing simulations;
- Practical tests (e.g. leaving an unlabelled USB stick around);
- Surveys.

b) The company should review the security awareness programme, in accordance with company policy, to ensure all actives remain relevant, up-to-date and continue to support the development of a positive security culture.

References and Further Guidance:

- NIST SP800-82 R2 – Section 6.2.2
- OG86 Appendix 2 B6 Staff Awareness and Training
- ISO 27001 – Clause 7
- ISO27019 – Section 7.2.2
- NCSC Growing positive security cultures
- CPNI SeCuRE 4 Assessing security culture

Guidance Flow:


Start
Communicate Priorities and Objectives
Positive Security Culture
Availability of Security Information
Understand Individual Contribution to Security
Security Incident Process
Assess and Review Culture and Understanding
End

RIIO-2 Cyber Resilience Guidelines B6.b Cyber Security Training

RIIO-2 Cyber Resilience Outcome Description for B6.b Cyber Security Training:

The people who operate and support your essential service are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed.

RIIO-2 Cyber Resilience Guidance:

1. **Cyber Security Awareness Training** – There are defined and appropriate cyber security training and awareness activities for all relevant roles for security of the networks and information systems supporting your essential service.
   a) A cyber security training and awareness programme should be established to either provide training or ensure training has occurred for all relevant personnel, including third parties, to ensure they have the appropriate knowledge and skills for the secure operation of the networks and information systems supporting your essential service.
   b) The training should cover:
      - The potential operational impact of cyber incidents to the organisation and to the population that it serves;
      - The need for all staff to be diligent in compliance with security policies and to their local implementation procedures;
      - The need for staff to report and challenge staff who disregard security policies;
      - The protection of passwords and tokens used for authentication purposes;
      - The meaning of protective markings or classifications used to indicate how information or systems should be protected.
   c) Training should be relevant to the defined roles and certain roles, as identified in A1.b, are expected to require additional, role-specific, training packages.
   d) Role specific training should consider technical, process, operational and interpersonal training needs.
   e) The company could carry out a training needs analysis to define the relevant training.

2. **Recording Cyber Security Training** – For specified roles and cyber security topics where knowledge and awareness needs to be kept up-to-date and maintained, relevant cyber security training is tracked and refreshed at suitable intervals.

a) Training record should be kept using an appropriate solution e.g. Learning Management System.

b) Training records should be reviewed periodically, to ensure awareness and training is kept up-to-date in accordance with the training programme.

c) The training programme is periodically reviewed, at least annually or in accordance with company policy, and updated if necessary.

3. **Varied Training Methods** – A range of techniques are used to effectively teach and communicate to the relevant personnel.

   a) Techniques can include but are not limited to:

   - Email (e.g. simulated phishing email scenario);
   - Instructor-led classroom training;
   - PowerPoint presentation/video;
   - Interactive workshop or game;
   - Hands-on training;
   - Computer-based and e-learning training;
   - Coaching and mentoring.

   b) The company should identify opportunities to integrate security awareness training into other development programmes to raise awareness among key staff groups; e.g. project managers, service managers, procurement and operational staff, and reinforce the message that security is relevant to everyone.

4. **Validate Training Effectiveness** – The effectiveness of the training and communications is routinely evaluated.

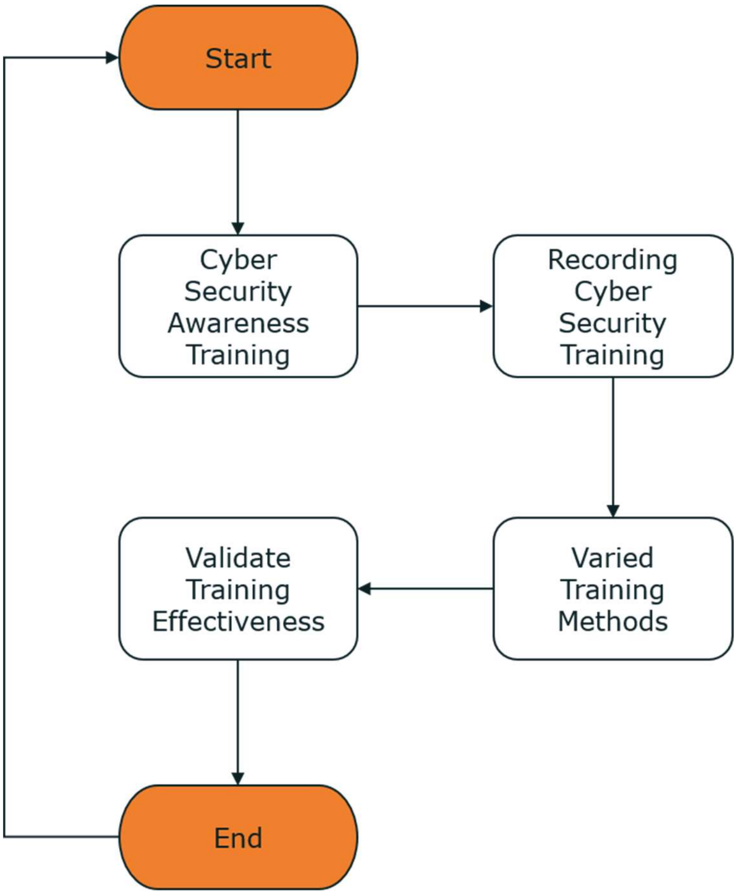
   a) The effectiveness of the training and awareness programme should be measured and reviewed periodically, in accordance with company policy, and inform the appropriate updates of the programme.

   b) The company should use an appropriate range of techniques to measure the effectiveness of training and communications.

References and Further Guidance:

- NIST SP800-82 R2 – Section 6.2.2
- OG86 - Appendix 2 B6 Staff Awareness and Training
- ISO 27019 – Section 7.2.2

Guidance Flow:


Start
Cyber Security Awareness Training
Recording Cyber Security Training
Varied Training Methods
Validate Training Effectiveness
End

RIIO-2 Cyber Resilience Guidelines C1.a Monitoring Coverage

RIIO-2 Cyber Resilience Outcome Description for C1.a Monitoring Coverage:

You monitor the security status of the networks and systems supporting the delivery of essential services in order to detect & respond potential security issues and to track the ongoing effectiveness of protective security measures

RIIO-2 Cyber Resilience Guidance:

1. **Define monitoring strategy** – There is a monitoring strategy which defines the objectives and requirements for monitoring and this is informed by an understanding of your networks and information systems supporting your essential service.
   a) The company should develop, document and maintain a strategy for monitoring, which should cover, but not be limited to:
      - Monitoring objectives;
      - Scope;
      - Rationale;
      - Event logging approach and requirements;
      - Event analysis approach and requirements;
      - Approach to aligning threat intelligence with monitoring;
      - Approach to aligning incident response with monitoring;
      - Approach to aligning vulnerability management with monitoring.

   b) The company should ensure that the use of security monitoring tools and scanning techniques does not adversely impact the operational performance of the essential service (e.g. performing passive monitoring with custom industrial controls systems (ICS) and OT systems).

2. **Confirm scope and deploy monitoring** – Monitoring data is collected from, at least, the critical networks and systems supporting your essential service.
   a) It may not be possible to monitor all parts of all systems due to limitations in technology, communications, etc. However, monitoring should be in place for critical elements of the networks and information systems supporting your essential services. The monitoring scope should include, but not be limited to:
      - Control centres;
      - Supporting enterprise systems, networks & databases;

- Engineering workstations & data historians;
- Critical PLCs;
- Supervisory Control and Data Acquisition (SCADA) systems;
- Distributed Control Systems (DCS);
- Firewalls & network switches;
- Energy Management Systems (EMS);
- Single points of failure systems;
- Critical network zones or conduits;
- Egress or ingress zones (inbound and outbound communications traffic);
- Safety instrumented systems (SIS);
- Unauthorised assets connected to the SCADA & ICS network;
- IT & OT specific protocols & ports;
- Specific monitoring of key assets (e.g. domain controllers, engineering workstations, assets accessed from non-ICS networks, assets used for file transfer by portable media, perimeter devices, etc.);
- Unexpected shutdowns or reboots;
- For perimeter devices – repeated denied connections, configuration changes, management console access.

b) The company should employ automated tools to support near real-time analysis of events (e.g. intrusion detection systems customised and tailored for ICS/SCADA environments).

c) In situations where there is no way to monitor inbound and outbound communications traffic, the company should employ compensating controls to provide a monitoring capability on a separate system.

d) The company should define monitoring response (both automated and manual) playbooks.

3. **Validate successful monitoring** – There is justified confidence that monitoring should detect the presence of known indicators of compromise on the networks and systems supporting your essential service.

a) The company should assure and document testing and validation of the monitoring systems.

b) Monitoring could include integration with Security Operation Centres (SOCs) for continuous analysis and incident response capabilities.

c) The company should employ automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

d) Assurance may be achieved through, but is not limited to:

- Commissioning and acceptance tests;
- Periodic compliance audits;
- SOC integration & testing;
- Penetration tests;
- Incident response plan tests.

e) The monitoring systems should be updated regularly to maintain their effectiveness.

4. **Ensure monitoring of privileged users** – Monitoring is conducted of all privileged activity for the networks and information systems supporting your essential service for suspicious or undesirable activity.

a) The company should design and implement additional logging requirements for privileged users, such as System Administrators and Operators, in the networks and information systems supporting your essential service.

b) This should include any privileged shared user IDs, third parties' access and contractors.

5. **Focus monitoring of network gateways and critical devices** – Extensive monitoring is performed of network gateways and host-based monitoring for critical devices, where possible.

a) The company should implement extensive monitoring of all network gateways, particularly between the networks and systems supporting your essential service and other networks and systems e.g. corporate IT and external.

b) The company should also consider implementing extensive monitoring of conduits between different security zones within the networks and information systems supporting your essential service.

c) The company should implement, where possible, host-based monitoring on critical devices such as, but not limited to, the core devices of the control systems e.g. engineering workstations, operator stations, SCADA master servers, etc.

6. **Include monitoring as part of the critical asset lifecycle** – All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.

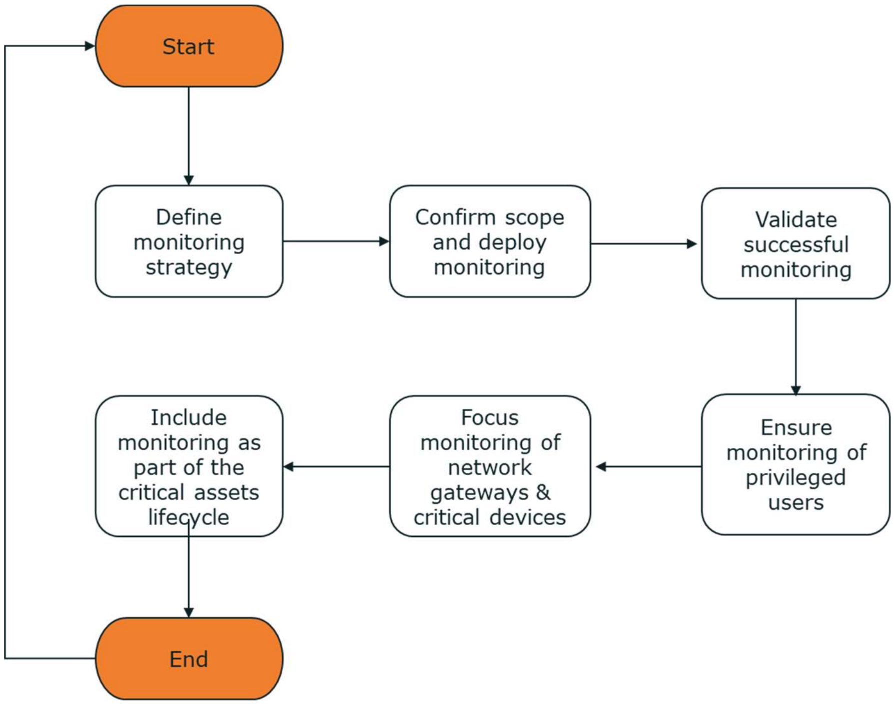
a) The company should ensure that monitoring requirements are included in the design and development of new systems or significant modifications.

b) Monitoring should be included as part of the asset management lifecycle and security requirements for critical systems.

References and Further Guidance:

- NIST 800-82 R2 – CA-7 Continuous Monitoring, MA-1 System Maintenance Policy and Procedures, SC-3 Security Function Isolation, SI-3 Malicious Code Protection, SI-4 Information System Monitoring
- OG86 – Appendix 2 C1 Security Monitoring
- IEC 62443-2-1 – Sections 4.3.4.3 System Development and maintenance, 4.3.3.3 Physical and environmental security
- ISO/IEC 27001 – Section A.10.10 Monitoring
- ISO/IEC 27019 – Section 12.4 Logging and monitoring

Guidance Flow:


Start
Define monitoring strategy
Confirm scope and deploy monitoring
Validate successful monitoring
Ensure monitoring of privileged users
Focus monitoring of network gateways & critical devices
Include monitoring as part of the critical assets lifecycle
End

RIIO-2 Cyber Resilience Guidelines C1.b Securing Logs

RIIO-2 Cyber Resilience Outcome Description for C1.b Securing Logs:

Logging data should be held securely and read access to it should be granted only to accounts with a business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.

RIIO-2 Cyber Resilience Guidance:

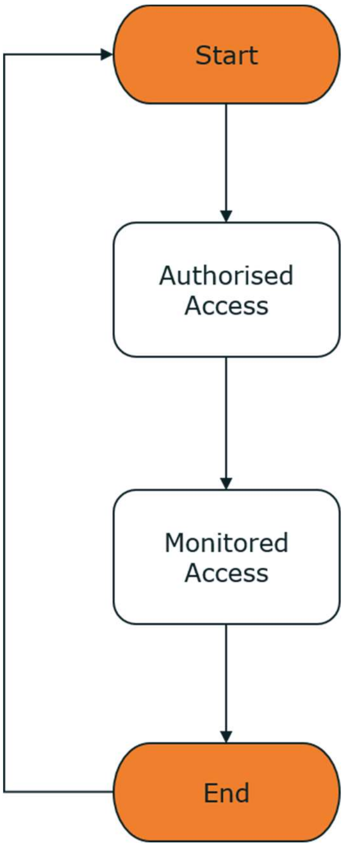
1. **Authorised Access** – Only authorised personnel can view logging information.
   a) There should be a policy and procedures defined and implemented to ensure only authorised users are permitted to view or copy logging data.
   b) No users should be able to delete or modify logging data within the defined and documented data retention period.

2. **Monitored Access** – Access to logging data is monitored and backed up appropriately.
   a) There should be a policy and procedures defined and implemented to monitor logging data.
   b) At a minimum, security monitoring of logging data should identify unauthorised attempts to access, modify or delete logging data.
   c) Security monitoring of logging data should be reviewed in accordance with policy.

References and Further Guidance:

- NIST SP800-82 R2 – Section 5.16
- OG86 - Appendix 2 C1 Security Monitoring
- IEC 62443/ISA99 3-3 – SR 3.9 Protection of Audit Information, SR 6.1 Audit Log Accessibility
- ISO 27019 – Section 12.4.2

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines C1.c Generating Alerts

RIIO-2 Cyber Resilience Outcome Description for C1.c Generating Alerts:

Evidence of potential security incidents contained in your monitoring data should be reliably identified and should trigger security alerts.

RIIO-2 Cyber Resilience Guidance:

1. **Detect and create security alerts** – Alerts are generated on suspicious activity within the networks and information systems supporting your essential service.
   a) In-line with the security monitoring strategy, the company should design and implement an appropriate monitoring capability consisting of appropriate tools, processes and personnel.
   b) Security alerts and logs should be generated for all systems supporting essential services. The scope should include, but not be limited to:
      - Engineering and operator workstations;
      - Critical Programmable Logical Controllers (PLCs);
      - Supervisory Control and Data Acquisition (SCADA) systems;
      - Distributed Control Systems (DCS);
      - Firewalls & network switches;
      - Data historians and databases;
      - Energy Management Systems (EMS);
      - Single points of failure systems;
      - Safety instrumented systems (SIS);
      - All unauthorised assets connected to the SCADA and Industrial Control Systems (ICS) network;
      - Key assets (e.g. domain controllers, assets accessed from non-ICS networks, assets used for file transfer by portable media, perimeter devices, gateways, etc.);
      - Endpoint protection, antivirus or anti malware services;
      - Supporting enterprise systems.

   c) The capability should use a wide range of signatures and indicators of compromise to help identify and analyse suspicious activity, at least in the critical areas of the networks and systems supporting your essential services.

2. **Map alerts to assets in scope** – Alerts should be resolved to assets in the networks and systems supporting your essential service.

   a) The monitoring and alerting systems should be designed and implemented such that it is possible to trace alerts to individual assets impacted to aid investigation and response.
   b) Assets should be mapped, updated and aligned according to organisational asset management processes.

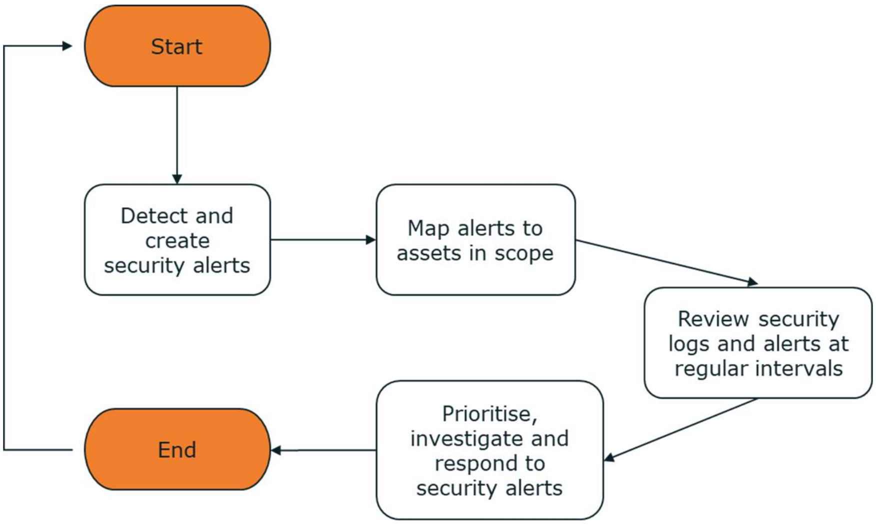
3. **Review security logs and alerts at regular intervals** – As defined in the monitoring strategy, security logs are reviewed regularly and, if possible, alerts should be reviewed almost continuously, in real time.
   a) The company should employ automated tools to support near real-time analysis of events (e.g. Security information and event management (SIEM), event aggregation tools).
   b) Alerts should be tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms and false positives.
   c) Systems in scope should be reviewed at appropriate intervals, in accordance with company policy, to ensure that they are successfully generating all required security alerts and events.

4. **Prioritise, investigate and respond to security alerts** – Security alerts relating to the networks and systems supporting your essential service should be prioritised, investigated and an appropriate action taken.
   a) Alerts should be triaged according to defined criticality, to determine the priority for investigation aligned with organisational incident management and response processes.
   b) Prioritised alerts should be investigated to assess the potential impact on essential services following organisational incident management and response processes.
   c) Investigation and event correlation may require involvement of IT, OT specialists and third parties.
   d) Based on the investigation appropriate actions should be identified and executed.
   e) Actions should be recorded, managed and monitored for completion.
   f) Where applicable, the process of prioritising, investigating and taking appropriate action against alerts is integrated with other operational/management service protection processes (automated and manual response playbooks), which can include but is not limited to:
      - Security incident management and response;
      - Risk assessment and management;
      - Remediation activities;
      - Business continuity and disaster recovery.

References and Further Guidance:

- NIST 800-82 R2 – Appendix G: CA-7 Continuous Monitoring, SI-3 Malicious Code Protection, SI-4 Information System Monitoring
- OG86 – Appendix 2 C1 Security Monitoring
- IEC 62443-2-1 – Section 4.3.4.3 System Development and maintenance
- ISO/IEC 27001 – Section A.10.10 Monitoring
- ISO/IEC 27019 – Section 12.4 Logging and monitoring

Guidance Flow:


Start
Detect and create security alerts
Map alerts to assets in scope
Review security logs and alerts at regular intervals
Prioritise, investigate and respond to security alerts
End

RIIO-2 Cyber Resilience Guidelines C1.d Identifying Security Incidents

RIIO-2 Cyber Resilience Outcome Description for C1.d Identifying Security Incidents:

You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.

RIIO-2 Cyber Resilience Guidance:

1. **Threat intelligence information should be selected** – Threat sources are selected and reviewed from a variety of sources appropriate to the likely threats and the company's business needs.
   a) The company should select appropriate sources of threat intelligence in order to inform the identification of security incidents as part of the incident management process. Sources could include, but should not be limited to:
      - National Cyber Security Centre (NCSC);
      - Cyber Security Information Sharing Partnership (CiSP);
      - Information exchanges and industry groups;
      - Information Sharing and Analysis Centre (ISACs);
      - Original equipment manufacturers (OEMs) and sector specific vendors;
      - Specialist third party providers;
      - Specialised forums, security feeds and mailing lists (e.g. SCADASec, ICS-CERT).

   b) Selected threat intelligence sources should be integrated and utilised as part of organisational incident response processes.

2. **Updates are received for all signatures** – All signature based protective technologies are received for the networks and systems supporting your essential service, within the company policy.
   a) The company should ensure updates are received and verified from trusted sources (e.g. vendor website).
   b) All signature updates should be reviewed and prioritised for deployment, informed by relevant threat intelligence, within an appropriate timeframe (e.g. within 24 hours of receipt) in accordance with company policy.

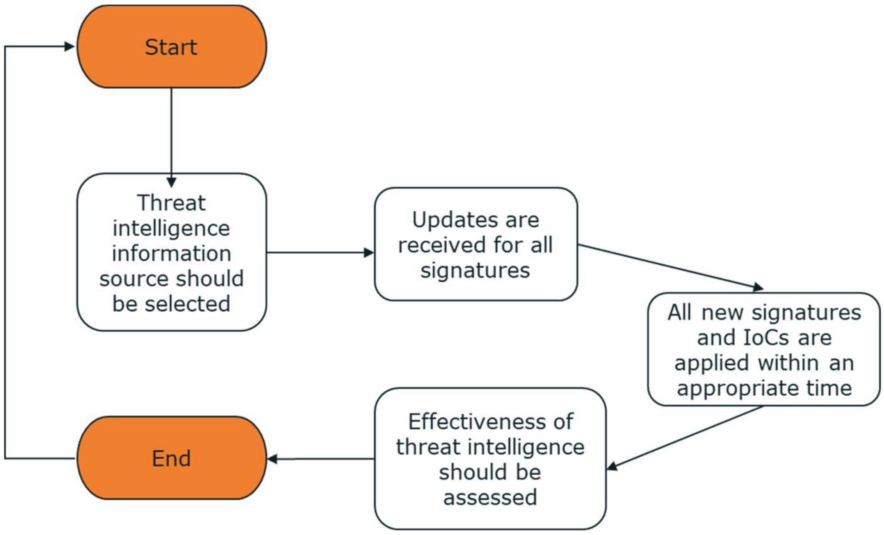
3. **All new signatures and Indications of Compromise (IoCs) are applied within an appropriate time** – Updates are implemented, based on risk and according to company policy.
   a) Updates should be applied within an appropriate timeframe dependent on the assigned priority for deployment (e.g. anti-virus and anti-malware signatures, intrusion detection systems updates)
   b) A risk assessment should be carried out prior to deployment where the signature update has the potential to adversely impact the networks and information systems supporting your essential service. Any risks should be managed according to organisational risk management policy and processes.

4. **The effectiveness of using threat intelligence should be assessed** – Threat information to identify security issues in the networks and information systems supporting your essential service is assessed.
   a) The company should review the use of threat intelligence on a regular basis, according to company policy.
   b) The review could consider whether the intelligence received was:
      - Appropriate and relevant;
      - Actionable;
      - Useful in informing the identification of security incidents according to organisational processes.

References and Further Guidance:

- NIST 800-82 R2 – Appendix G: CA-7 Continuous Monitoring, SI-3 Malicious Code Protection, SI-4 Information System Monitoring, IR-1 Incident Response Policy and Procedures, IR-4 Incident Handling
- OG86 – Appendix 2 C1 Security Monitoring
- IEC 62443-2-1 – Sections 4.3.4.3 System Development and maintenance, 4.3.4.5 Incident planning and response
- ISO/IEC 27001 – Sections A.10.10 Monitoring, A.13.2 Management of information security incidents and improvements
- ISO/IEC 27019 – Section 12.4 Logging and Monitoring

Guidance Flow:


Start
Threat intelligence information source should be selected
Updates are received for all signatures
All new signatures and IoCs are applied within an appropriate time
Effectiveness of threat intelligence should be assessed
End

RIIO-2 Cyber Resilience Guidelines C1.e Monitoring Tools & Skills

RIIO-2 Cyber Resilience Outcome Description for C1.e Monitoring Tools & Skills:

Monitoring staff skills, tools and roles, including any that are out-sourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential services they need to protect.

RIIO-2 Cyber Resilience Guidance:

1. **Determine Monitoring Coverage** – The requirements for monitoring coverage and to support and enable incident response are defined and appropriate tools and techniques identified.
   a) Industrial control systems (ICS) monitoring could be achieved through a variety of tools and techniques that could include, but not be limited to:
      - Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS), which should be tailored and customised to ICS (e.g. covering all necessary proprietary and custom IT & ICS protocols, performing passive monitoring to avoid potential performance issues);
      - Malicious code protection monitoring (e.g. endpoint protection, anti-malware & anti-virus);
      - Networks & boundary protection monitoring;
      - Identity & Access Management monitoring tools (e.g. including session monitoring/recording, privileged, shared and critical user IDs tracking);
      - Establish tools to monitor systems supporting critical services (e.g. Active directory, historians, databases, third party access).

   b) Monitoring devices should be strategically deployed within the control system. (e.g. at selected perimeter locations and near systems supporting critical applications) to collect essential information according to the organisational monitoring coverage strategy.

   c) Monitoring mechanisms may also be deployed at ad hoc locations within the control system to track specific transactions and events.

   d) Monitoring tools should make use of all logging data collected to pinpoint activity within an incident to facilitate effective monitoring of the networks and information systems supporting your essential service.

e) Where possible all logging sources should be enabled and the logs collected in order (or accurately time-stamped) to better inform the investigation and incident response process.

f) Monitoring tools should include appropriate reporting mechanisms to allow for a timely response to events and security incidents according to organisational incident response processes.

g) To keep the reporting focused and the amount of information to a level that could be processed by the recipients, mechanisms such as integration and monitoring through Security Operation Centres (SOC) and Security Information and Event Management (SIEM) systems should be applied to correlate individual events into aggregate reports which establish a larger context in which the raw events occurred to support incident response activities.

h) Additionally, these mechanisms could be used to track the effect of security changes to the control system. Having forensic tools pre-installed could facilitate incident analysis and response.

2. **Establish Monitoring Team** – Personnel are in place who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and system performance.

   a) The monitoring personnel could be employees or third parties on premises or provided as part of a managed service.

   b) Monitoring personnel should have appropriate security vetting and background checks.

3. **Develop Reporting Chain** – Monitoring personnel should report to an appropriate part of the organisation.

   a) Monitoring personnel should report into the appropriate part of the organisation that is able to provide the necessary resources and authority to investigate security monitoring data, alerts and incidents. This could be, for example, IT, OT, Operations, Information Security and potential third parties.

4. **Define Roles and Skills** – Monitoring personnel have defined roles and skills/competence requirements that, together with other personnel such as operators, system administrators and third parties, are able to cover all parts of the monitoring and investigation process.

   a) Appropriate roles should be defined and assigned to perform the analysis, investigation and reporting activities.

   b) The personnel should have appropriate training in OT and security knowledge to perform their role.

5. **Operational Awareness** – Monitoring personnel should be aware of essential services assets in scope and can identify and prioritise alerts or investigations that relate to them.
   a) Monitoring personnel should be sufficiently aware of the essential services and the networks in scope and information systems supporting them to effectively identify, prioritise and investigate alerts, engaging other personnel or third parties where necessary.

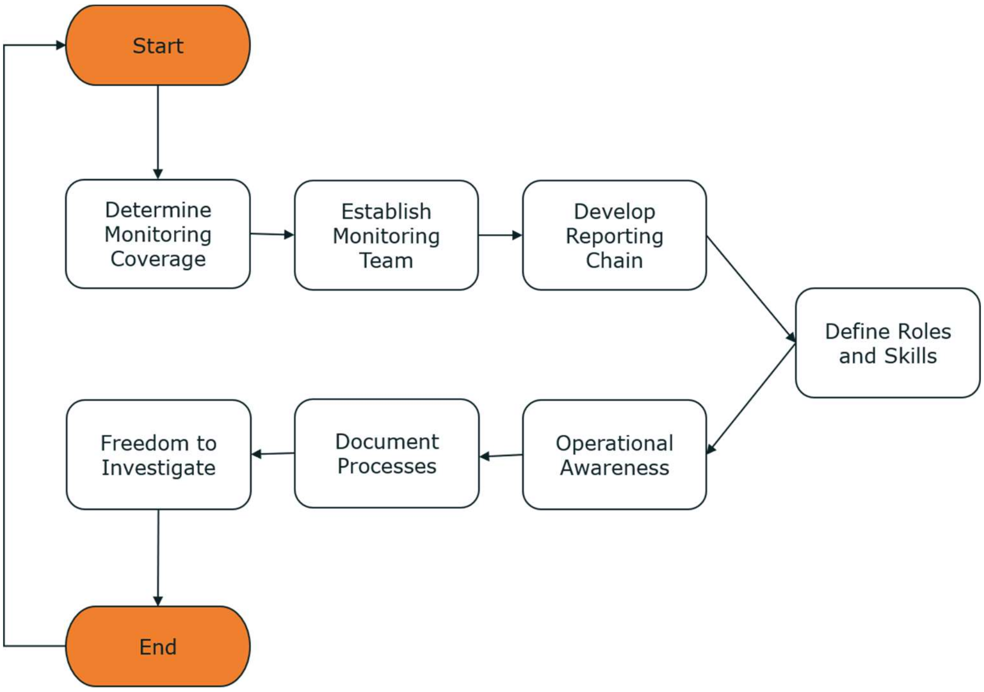
6. **Document Processes** – Monitoring personnel follow documented processes, procedures and workflows for the analysis, investigation and reporting of monitoring alerts.
   a) Standard workflows and playbooks should be defined and documented to cover the analysis, investigation and reporting activities (internal and external).
   b) A workflow should exist to ensure that reportable regulatory events, can be identified and reported to the Competent Authority (CA), within 72 hours of becoming aware of the incident.

7. **Freedom to Investigate** – Monitoring personnel are empowered to look beyond the fixed process to investigate and understand non-standard threats.
   a) This could be achieved by developing their own investigative techniques and making new use of data in order to continually enhance monitoring capabilities.
   b) As incidents may vary and novel, difficult to detect, techniques may be employed by adversaries, personnel conducting monitoring investigations should be permitted to conduct their own investigations which go beyond the documented workflows and playbooks where appropriate.

References and Further Guidance:

- NIST 800-82 R2 – Appendix G: CA-7 Continuous Monitoring, SI-4 Information System Monitoring
- IEC 62443-3-3 – Section 10.4, SR 6.2 Continuous Monitoring
- IEC 62443-2-1 – Section 4.3.4.3 System Development and maintenance
- ISO/IEC 27001 – Section A.10.10 Monitoring
- ISO/IEC 27019 – Section 12.4 Logging and monitoring

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines C2.a System Abnormalities for Attack Detection

RIIO-2 Cyber Resilience Outcome Description for C2.a System Abnormalities for Attack Detection:

You should define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.

RIIO-2 Cyber Resilience Guidance:

1. **Understanding Normal Behaviour** – There should be a good understanding of normal behaviour of the critical networks and systems supporting your essential service to permit effective detection of abnormal behaviour which may indicate malicious activity.
   a) The company should baseline the normal and expected behaviours of the networks and systems supporting your essential service. This may use, but should not be limited to:
      - Statistical analysis to establish modes, median and normal operations values.
      - Techniques and tools for monitoring to detect deviations from normal that would indicate compromise or failure of countermeasures, for example:
        - Network usage and connections.
        - User access.
        - Protocol anomalies.
        - Security policy.
        - Services running.
        - Network connections.
      - Unusual but potentially acceptable activity, volumes and times of activity that are authorised activity that must not be blocked as false positives.
      - Unusual use cases that should be investigated as potential Indicators of Compromise.

   b) The level of logging and monitoring required to establish and periodically update normal and abnormal activity should be defined.

2. **Develop Abnormality Descriptions** – System abnormality descriptions should be developed from past attacks, threat intelligence and consideration of the nature of likely attacks on your networks and information systems supporting your essential service.
   a) The company should develop descriptions of abnormal behaviours in systems, networks and people, which may potentially be indicators of compromise.

b) These descriptions should be informed by past attacks in your sector or other relevant incidents, security monitoring, threat intelligence and potential failure modes on the networks and systems supporting your essential service.

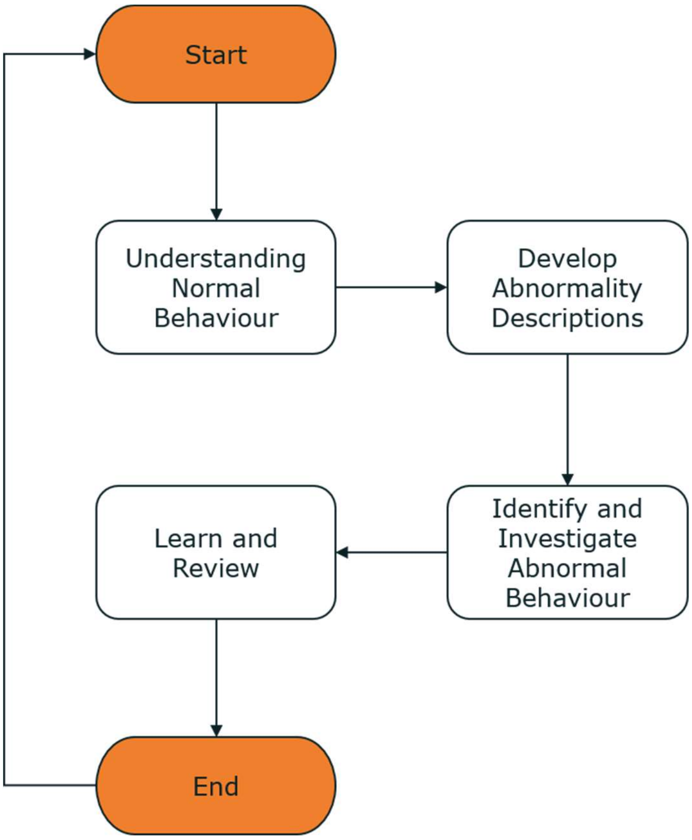
3. **Identify and Investigate Abnormal Behaviour** – The system abnormality descriptions should be used to identify potential malicious activity on your networks and information systems supporting your essential service.
   a) The company may consider using anomaly detection technology, monitoring and/or threat hunting techniques to identify malicious activity on the networks and information systems supporting your essential service.

4. **Learn and Review** – The system abnormality descriptions should be updated to reflect changes in your networks, systems and current threat intelligence.
   a) The abnormality descriptions should be reviewed and updated, if required, following events such as, but not limited to:
      - Any internal or relevant external incident.
      - Receipt of new and relevant threat intelligence.
      - Significant changes to the networks and systems supporting your essential service.
      - Significant changes to operating conditions.

References and Further Guidance:

- NIST 800-82 R2 – Appendix G: IR-5 Incident Monitoring, SI-2 Flaw Remediation, SI-4 Information System Monitoring
- OG86 – Appendix 2 C2 Proactive Security Event Discovery
- IEC62443-1-1 – Section 5.6.5
- ISAO27002 – Sections 13.1.1, 14.2.5

Guidance Flow:


Start
Understanding Normal Behaviour
Develop Abnormality Descriptions
Identify and Investigate Abnormal Behaviour
Learn and Review
End

RIIO-2 Cyber Resilience Guidelines C2.b Proactive Attack Discovery

RIIO-2 Cyber Resilience Outcome Description for C2.b Proactive Attack Discovery:

You should use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.

RIIO-2 Cyber Resilience Guidance:

1. **Exception Monitoring** – The critical networks and systems supporting your essential service are routinely monitored and searched for abnormalities indicative of malicious activities.
   a) Enhanced monitoring should be carried out on critical assets on a routine basis, in accordance with the policy. Abnormalities may include, but are not limited to:
      - Failed login attempts.
      - Policy violations.
      - Unexpected system behaviour.
      - Out of hours use from user accounts.
      - Unexpected use of software.
      - Processes or scripts running that do not reflect a core business use.

   b) The use of threat hunting techniques, network and host intrusion detection solutions specifically tailored for OT may be considered.
   c) Where it is not possible to implement monitoring for all the networks and information systems supporting your essential service, organisations should identify critical elements (e.g. control centres) and implement routine monitoring for these critical elements.

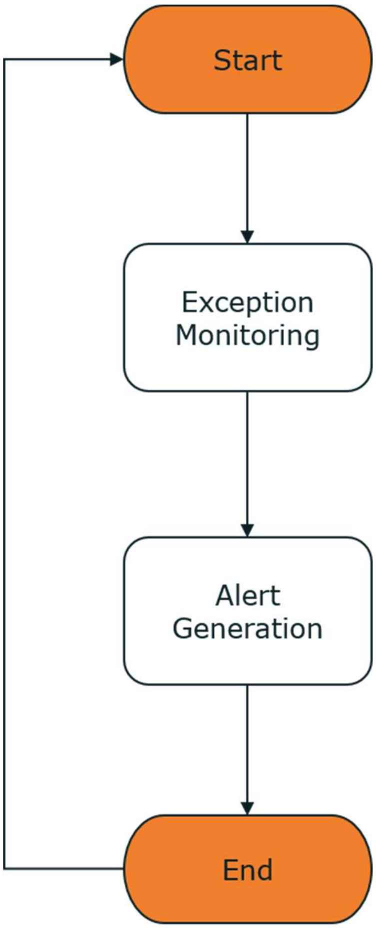
2. **Alert Generation** – Alerts are generated when abnormalities are detected and that these are addressed through the security alert and incident response investigation processes.
   a) Monitoring systems should be tuned to collect events and generate relevant alerts and to reduce false negatives. These alerts should be investigated through the normal alert investigation processes. Follow C1.e Monitoring Tools & Skills and C1.a Monitoring Coverage guidelines for additional details and supporting information.

References and Further Guidance:

- NIST SP800-82 R2 – Sections 5.16, 5.17, Appendix G: IR-5 Incident Monitoring, SI-4 Information System Monitoring

- OG86 - Appendix 2 C2 Proactive Security Event Discovery

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines D1.a Response Plan

RIIO-2 Cyber Resilience Outcome Description for D1.a Response Plan:

You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential service and covers a range of incident scenarios.

RIIO-2 Cyber Resilience Guidance:

1. **Develop Incident Response Plan** – A documented incident response plan exists for each major asset based on an understanding of the security risks to the networks and information systems supporting your essential service.
   a) The company should have a set of documented and approved incident response plans, whose scope covers all the networks and information systems supporting your essential service.
   b) The incident response plans should be informed by the company's understanding of the security risks to the networks and information systems supporting your essential service.

2. **Validate Response Plan Coverage** – The incident response plan is comprehensive and should cover the whole incident management lifecycle.
   a) The incident response plans should address the whole incident management lifecycle from preparing to respond to an incident, responding to an incident and post-incident follow-up. Incident response plans should form part of wider Business Continuity Planning considering:
      - Business impact classification and prioritisation of OT assets;
      - Required response to events that would activate the plan;
      - Procedures for operating the systems' basic functionalities in a manual mode, if possible, until normal operational conditions are restored;
      - Updated documentation (manuals, configurations, procedures, vendors contact lists, network diagrams etc.);
      - Personnel list for authorised physical and logical access to the systems;
      - System components restoration order/sequence;
      - Offsite backups recall and restoration procedures;
      - Procedures for liaison with the authorities as per the organisation's Business Continuity Plan (BCP);
      - Procedures to characterise and classify events as reportable security incidents;
      - Procedures to report security incidents to management.

b) The incident response plans should include, but are not limited to:
- Defining the structure and organisation of the incident response capability;
- Defining the members and their roles and responsibilities;
- Defining the general methodology to detect, contain, eradicate and recover to normal operational conditions;
- Identifying the information, tools and resources, including third parties, required to support the plans;
- Procedures for escalation of incident response;
- Internal and external reporting procedures.

3. **Consider Known Attack Patterns** – The incident response plan includes scenarios of known attack patterns to allow anticipation of likely next steps in the attack and enable appropriate response, and how to respond to novel attack patterns.

   a) To aid effective incident response, the organisation should develop relevant scenarios based on:
   - Risk assessments;
   - Past incidents;
   - Threat intelligence;
   - Threat modelling;
   - Vulnerability assessments;
   - Known attack patterns.

4. **Align to other Response Plans** – Where applicable, the incident response plans are aligned with and linked to other response plans to ensure coordinated response across the company and with relevant third parties.

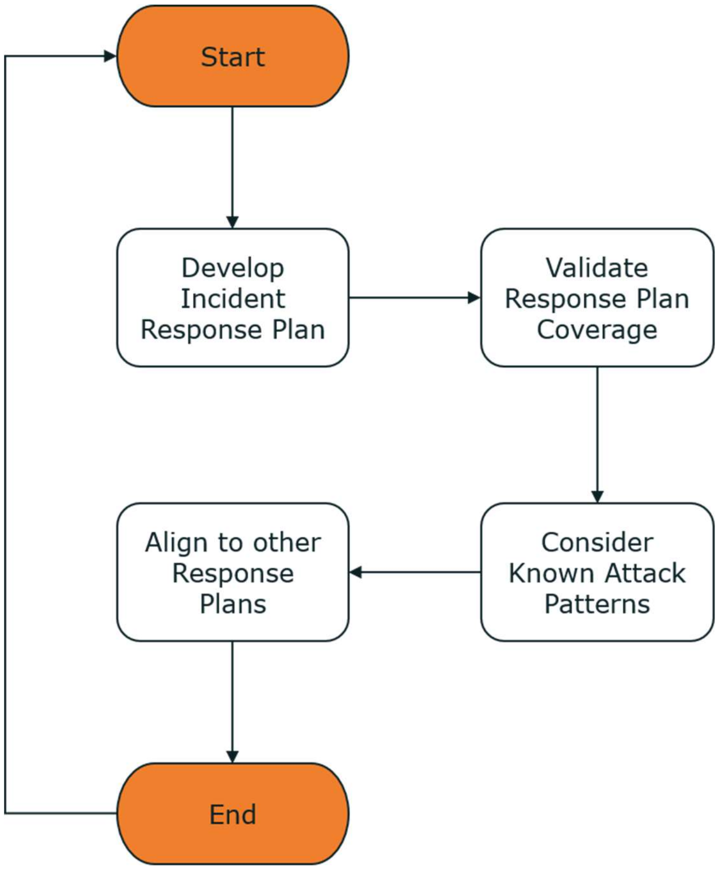
   a) Where applicable, the incident response plans are aligned and integrated with other response plans including, but not limited to:
   - Emergency response;
   - Crisis management;
   - Business continuity;
   - Capacity management;
   - Financial management;
   - Physical management;
   - Safety management;
   - Disaster recovery;
   - Upstream and downstream supply chain response and continuity plans.

b) The plans are regularly reviewed, according to company policy, and improved upon based on scenarios, impact, related incidents and changes within the management of the essential service.

References and Further Guidance:

- NIST SP 800-53 Rev. 4 Appendix D: CP-2 Contingency Plan, IR-8 Incident Response Plan, IR-4 Incident Handling
- OG86 – Appendix 2 D1 Response and Recovery Planning
- ISA 62443-2-1:2009 Sections 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8, 4.3.2.5.3, 4.3.4.5.1
- ISO/IEC 27001:2013 Sections A.16.1.6, A.16.1.1, A.17.1.1, A.17.1.2
- ISO 27019 – Section 16
- NIST CSF PR.IP-9

Guidance Flow:


Start
Develop Incident Response Plan
Validate Response Plan Coverage
Consider Known Attack Patterns
Align to other Response Plans
End

RIIO-2 Cyber Resilience Guidelines D1.b Response and Recovery Capability

RIIO-2 Cyber Resilience Outcome Description for D1.b Response and Recovery Capability:

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

RIIO-2 Cyber Resilience Guidance:

1. **Identify Response Team Members** – The members of the incident response team and supporting resources are identified and will be made available, if required.
   a) All appropriate roles and resources (e.g. office space, communications,) are identified within the incident response plans. This may consist of a core team, which could be extended with other appropriate internal and/or external personnel.
   b) The core team should include personnel familiar with the operation and management of the essential services and the networks and information systems supporting your essential service.
   c) The incident response team leader should have associated manual of authority, in order to make and take decisions.
   d) The incident response team roles and responsibilities should be formalised (e.g. by inclusion in job descriptions) to ensure personnel are made available when required.

2. **External Support Arrangements** – There are arrangements in place to augment your incident response capability with external support, if required.
   a) The incident response plans should identify potential external support to respond to an incident. The external support may include, but is not limited to:
      - National Technical Authority;
      - Specialist cyber security incident response and digital forensics providers;
      - Law enforcement.

   b) Where external support is deemed to be required, clear terms of engagement should be drafted in order to give preference to contending priorities such as maintaining chain of custody or restoration of services.
   c) Special arrangements should be pre-agreed with vendors such as OEMs, in order to gain commitment during times of incident response, irrespective if there are multiple external entities affected.

d) Where external support may be required, the company should ensure appropriate contractual arrangements are in place.

e) The processes to activate augmentation of the incident response capability should be defined and documented, including both during normal working hours and out-of-hours contact arrangements.

3. **Documented Triage Process** – Those identifying a potential incident and those performing triage for an incident, are following a documented and established procedure.

   a) There should be a defined and documented procedure to enable first responders to triage events. The procedure could include, but not be limited to:

   - Decision trees;
   - Criteria;
   - Incident severity classification;
   - Escalation procedure if additional expertise is required to triage the event.

4. **Response Team Skills** – The response team members have the skills, knowledge and authority required to respond appropriately, to limit the impact on your essential service.

   a) The company should ensure that all response team members have the appropriate knowledge and skills to perform their incident response roles. This may require training to develop specialist skills required for incident response, as well as incident response exercises and rehearsals.

   b) The company should give the incident response team the authority needed to respond in an appropriate and timely manner to incidents.

5. **Incident Response Information** – The information required to enable informed response decisions is known and can be made available to the incident response team.

   a. To ensure that response decisions can be made, the appropriate information should be made available to the incident response teams which may include, but is not limited to:

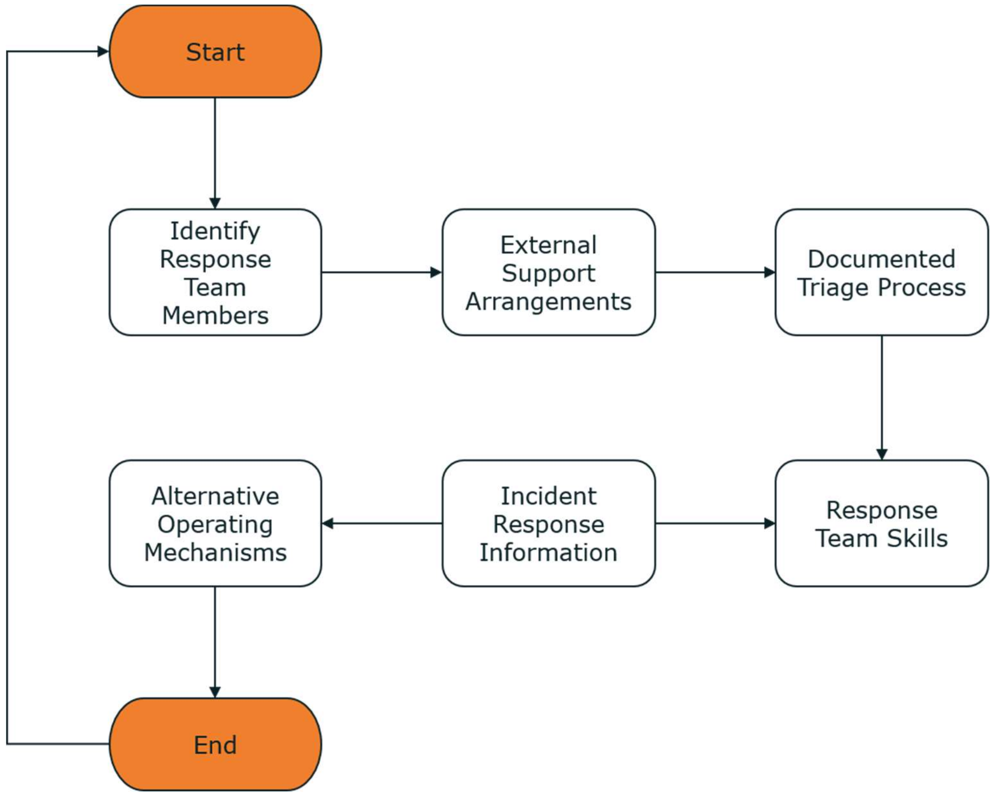
   - Incident response plan and supporting procedures;
   - Playbooks and workflows;
   - Monitoring and alert information;
   - System information and network diagrams;
   - Asset register with a list of critical sites and systems;
   - Escalation path and authorisation requirements;
   - Supporting tools;
   - External contact information;
   - Communication plans;
   - Criteria to close out incidents.

6. **Alternative Operating Mechanisms** – Alternative operating mechanisms are available to allow continued delivery, possibly at a reduced level, of your essential service where primary systems are not available.
    a. Where the delivery of the essential service is impacted and where deemed appropriate, the organisation should establish alternative operating mechanisms which can be readily activated to enable continued delivery of the service.
    b. Alternative operating mechanisms may require delivery at a reduced level and/or the use of alternative service providers.
    c. Where the delivery of the essential service has not been impacted, in order to reduce the attack surface and likelihood of compromise, the organisation may choose to limit connectivity and or information exchange using ancillary mechanisms to and from the OT environment.

References and Further Guidance:

- NIST SP 800-53 Rev. 4 Appendix D: CA-2 Security Assessments, CA-7 Continuous Monitoring, PM-14 Testing, Training, and Monitoring, IR-4 Incident handling, IR-5 Incident Monitoring, IR-8 Incident Response Plan, CP-2 Contingency Plan, CP-3 Contingency Training, IR-3 Incident Response Testing, PE-6 Monitoring Physical Access, RA-5 Vulnerability Scanning, SI-4 Information System Monitoring
- ISA 62443-2-1:2009 Sections 4.4.3.1, 4.2.3.10, 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4
- ISO/IEC 27001:2013 Sections A.6.1.1, A.16.1.1, A.16.1.2

Guidance Flow:


Start
Identify Response Team Members
External Support Arrangements
Documented Triage Process
Response Team Skills
Incident Response Information
Alternative Operating Mechanisms
End

RIIO-2 Cyber Resilience Guidelines D1.c Testing and Exercising

RIIO-2 Cyber Resilience Outcome Description for D1.c Testing and Exercising:

Your organisation carries out exercises to test response plans, using past incidents that affected your organisation and others', and scenarios that draw on threat intelligence and your risk assessment.

RIIO-2 Cyber Resilience Guidance:

1. **Incident Response Exercises** – Exercises of the incident response plans for security incidents involving the networks and information systems supporting your essential service are carried out regularly.
   a) The company should prioritise and conduct tests of the incident response plans based upon credible and relevant cyber security threats and previous incidents.
   b) Exercises could include, but are not limited to:
      - Orientation/walkthroughs;
      - Table-top exercises;
      - Functional testing of sections of the plans;
      - Full scale test of all elements;
      - Activation of DR plans;
      - Communications tests – suppliers, emergency services, media, etc.;
      - Any other tests required to meet legal & regulatory requirements.

   c) Each plan should include the process for Return to Normal Operations after an incident has occurred.
   d) Exercises should be used to:
      - Test they are accurate, complete and effective;
      - Train the incident response team;
      - Train new personnel;
      - Provide refresher training.

   e) Records of all testing should be kept for an appropriate period in accordance with legal and regulatory requirements.

2. **Credible Scenarios** – Documented exercise scenarios are based on actual incidents experienced by your and other organisations, on threat intelligence and/or experience.

3. **Maintain Scenarios –** Exercise scenarios are reviewed and updated to keep them relevant and effective.
    a) Exercise scenarios should be reviewed regularly and updated, if necessary, in accordance with company policy to:
    - Test they are still effective;
    - Incorporate changes or new threats or experience;
    - Incorporate changes to contacts, procedures, augmentation, etc.;
    - Maintain alignment with other relevant plans such as Business Continuity, Crisis Management, etc.

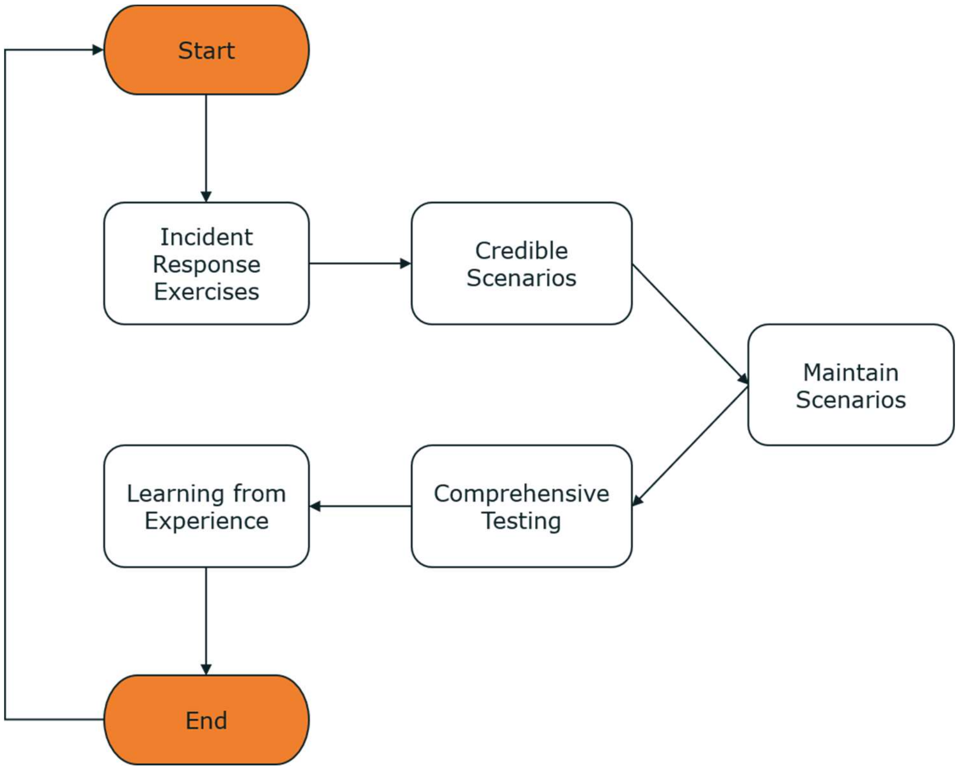
4. **Comprehensive Testing –** Exercises should test all parts of the incident response lifecycle and the responses appropriate to the exercise's scenario.
    a) The company should design exercises to test all elements of the incident response lifecycle.
    b) Tests do not have to test all elements together. Individual component tests can be designed to provide end-to-end assurance of the incident response lifecycle.
    c) Testing should provide assurance that the incident response plan can meet the defined recovery objectives.

5. **Learning from Experience –** Findings from exercises are documented and used to implement appropriate changes to the incident response plans, protective security of the networks and information systems supporting your essential service.
    a) The company should document a review of each exercise to identify findings and lessons learned which confirm what went well, and areas for improvement in the incident response plans and capabilities.

References and Further Guidance:

- NIST SP 800-53 Rev. 4 Appendix D: CM-2 Baseline Configuration, CP-4 Contingency Plan Testing, IR-3 Incident Response Testing, PM-14 Testing, Training and Monitoring, CA-2 Security Assessments, CA-7 Continuous Monitoring, PL-2 System Security Plan, RA-5 Vulnerability Scanning, SI-4 Information System Monitoring, CP-2 Contingency Plan, IR-4 Incident Handling, IR-8 Incident Response Plan
- ISA 62443-2-1:2009 Sections 4.3.2.5.7, 4.3.4.5.11, 4.4.3.4, 4.3.4.5.10
- ISA 62443-3-3:2013 SR 3.3 Software Functionality Verification
- ISO/IEC 27001:2013 Sections A.12.1.4, A.17.1.3, A.16.1.6

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines D2.a Incident Root Cause Analysis

RIIO-2 Cyber Resilience Outcome Description for D2.a Incident Root Cause Analysis:

Your organisation should identify the root causes of incidents you experience, wherever possible.

RIIO-2 Cyber Resilience Guidance:

1) **Develop policies** – The company should have a policy for investigating the root cause of incidents.
2) **Regularly perform root cause analysis** – Root cause analysis should be routinely conducted following an incident as part of the incident investigation and response process.
   a) The purpose of the analysis should be clear to all stakeholders and just enough to balance lessons learned and not hindering restoration of services.
   b) Where required by law enforcement entities, evidence should be kept in a state where chain of custody is maintained.
   c) Forensic analysis should be compared against last known good states.
   d) The company should consider whether the team conducting incident root cause analysis should be independent.
   e) The company should have call-off contracts with external specialists to lead or augment the root cause analysis team.
   f) OEMs should be involved throughout the process to assist and direct the process where required.

3) **All available relevant data should be made available to the team carrying out the root cause analysis.**
   a) This should include, but not be limited to:
      - Incident response plan and supporting procedures;
      - Restoration prioritisation;
      - Logs, monitoring and alert information;
      - System information and network diagrams;
      - Asset register with a list of critical sites and systems;
      - Forensic information e.g. device images, memory dumps, packet captures;
      - Incident handling logs and records;
      - Physical and logical access records.

b) The root cause analysis team will likely require specialist investigation technologies, techniques, processes to help with the investigation. These should have minimal linkages and connections with company systems until such time that they are required. These are privileged technologies that should not be accessible by others outside of the analysis team.

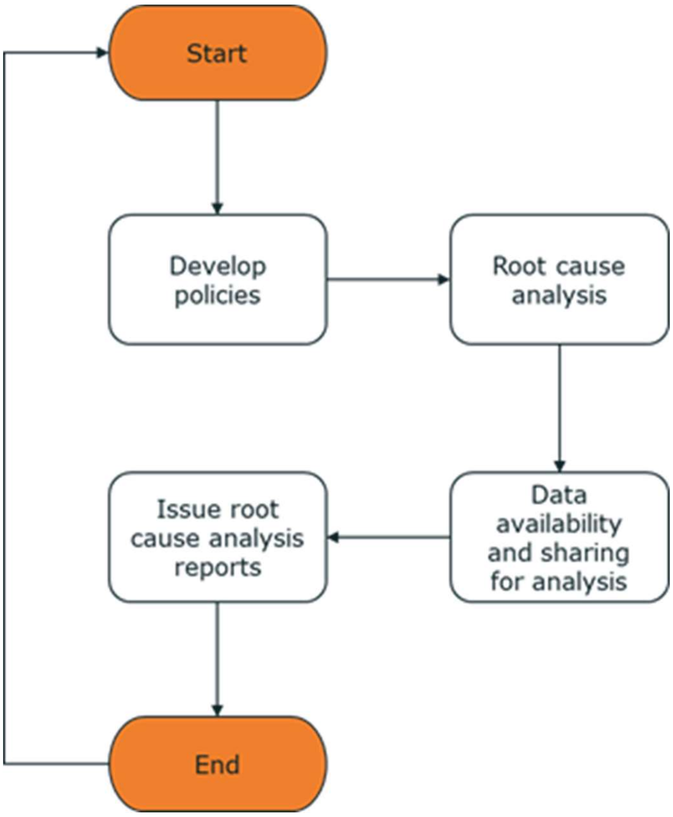
c) The root cause analysis process should ensure a comprehensive analysis.

4) **Issue root cause analysis reports –** For each incident analysed, a report should be issued to appropriate stakeholders and authorities detailing the findings and recommendations. Where appropriate, an annual report should be produced summarising trends and making further recommendations if appropriate.

References and Further Guidance:

- OG86 – Appendix 2 D1 Response and Recovery Planning
- ISO27002 – Section 17.1.3

Guidance Flow:


Start
Develop policies
Root cause analysis
Data availability and sharing for analysis
Issue root cause analysis reports
End

RIIO-2 Cyber Resilience Guidelines D2.b Using Incidents to Drive Improvements

RIIO-2 Cyber Resilience Outcome Description for D2.b Using Incidents to Drive Improvements:

Your organisation should use lessons learned from incidents to improve your security measures.

RIIO-2 Cyber Resilience Guidance:

1. **Lessons Learned Process** – There should be a documented process that ensures lessons learned from security incidents involving the networks and information systems supporting your essential service are identified, documented and acted upon.
   a) Following each incident or exercise, a lessons learned exercise should be carried out to identify any opportunities to improve incident response capability, processes and plans.

2. **Scope of Lessons** – The lessons learned process should cover technology, people, processes and management.
   a) The lessons learned exercise should identify opportunities for improvement in people, processes and technology related to the networks and information systems supporting your essential service to:
      - Enhance security and reduce likelihood of future incidents;
      - Improve the incident response capability in order to minimise the impact of future incidents.

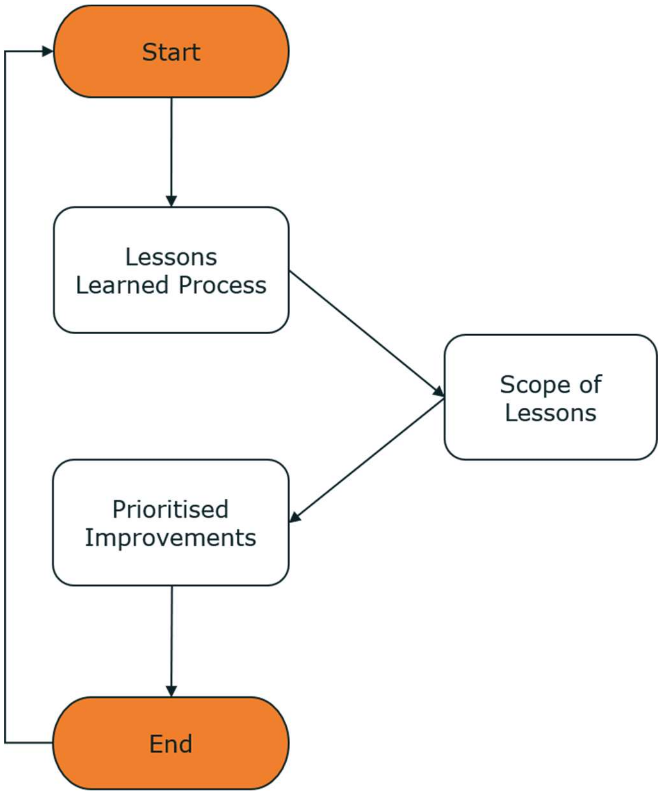
3. **Prioritised Improvements** – Improvements identified in the lessons learned should be prioritised and implemented in an appropriate timescale.
   a) The lessons learned exercise should capture any findings and develop improvement actions, priorities and action owners.

References and Further Guidance:

- OG86 - Appendix 2 D2 Lessons Learned
- IEC 62443/ISA99 2-1 – Section A.3.4.5.4
- NCSC D2 Lessons learned

- SICS Section 5.3.2 Establishing Response capabilities

Guidance Flow:



RIIO-2 Cyber Resilience Guidelines Supplementary – OT Replacement

Key points from Chapter 6 of the Decision RIIO-2 Sector Specific Methodology Decision (SSMD) – Core Document 24 May 2019:

6.4: *Companies also need to ensure that their assets are secure. This may require security upgrades to be implemented at critical sites, and investment in flood defences to continue where needed. Critical assets also need protecting where vulnerable to third party damage. Companies are also required to protect their network and information systems from failure, which includes securing them against cyber-attack.*

6.103: *For both plans [Business IT Security Plan and Cyber Resilience Plan], Ofgem is not expecting these to include the cost of general technology refresh or end of life replacement. Ofgem expects such projects to form part of more general system investment plans, which should already include appropriate cyber security measures.*

6.105: *In general, both plans [Business IT Security Plan and Cyber Resilience Plan] should include efficient, appropriate and proportionate measures, to deliver necessary enhancements to the overall security and resilience of the systems and networks used to operate essential services. When submitting these plans, a clear and coherent strategy with a robust risk-based approach to assessing and managing risk must be taken. Current risks, vulnerabilities, threats and mitigation options are expected to be documented, together with the relative benefits of the options considered.*

RIIO-2 Cyber Resilience Guidance:

The following RIIO-2 guidance applies to the Cyber Resilience Scope (please see associated Supplementary - Operational Technology Scope document), describing the key elements expected to be included within the business case for OT replacement. The network company should have explored and documented all other options, before considering OT replacement, in order to maintain proportionate and appropriate security. In addition, when considering OT replacement all areas of the CAF should be considered, with special focus on; A2.a Risk Management Process, A3.a Asset Management, A4.a Supply Chain, B4.a Secure by Design, B4.b Secure Configuration and B5.b Design for Resilience. A company considering making significant changes to OT, their related systems and associated security controls, should develop a business case including, but not limited to:

7. **Business Strategy & Direction** – Describe the overall context of asset changes, affecting the OT environment, in line with the company's business plans and associated response and capacity capability changes.

8. **Asset / OT classification** – Link asset classification, with the above business plan and criticality, in terms of Critical National Infrastructure (CNI) category and importance. Describe its function (for example; control systems, safety systems, instrumentation, etc.), its type (for example Alarm Receiving Centre) and outage impact.

9. **Asset / OT life** – Utilising a recognised methodology, describe both the asset life and OT components (including relevant supporting systems), with its associated current lifecycle position. Please note that for RIIO-2, Ofgem uses the Network Asset Risk Metric (NARM) to ensure companies maintain the health of critical assets, using the price control funding provided for this purpose. Should a company justify OT replacement due to Cyber risks, then a historical context on why this has not been previously initiative should be provided.

10. **Asset / OT risk assessment** – Utilising a recognised risk methodology, attack path and threat modelling, assess both the asset and associated OT components in terms of impact and probability, with an associated narrative:
    m) To a Cyber-attack, including any known scenarios, specific threat or previous historic company supporting evidence;
    n) To a non-related Cyber issue, such as a reliability caused outage, including any specific historic company supporting evidence.

11. **Mitigation options** – In addition to the OT replacement option, describe against the risks other mitigation options, which could include additional or compensating security controls. Specifically, has consideration been given to segmenting the OT architecture, reducing the attack surface or performing additional security monitoring, across the OT environment. Describe why these options are not deemed appropriate and/or proportionate.

12. **Define specifications** – Describe the approach taken to develop OT specific improvement specifications, to ensure security by design (please refer to the associated standards referenced) for any mitigation or replacement options. Please note, that as set out in 6.103 of the SSMD, it is not expected that investment will be required, under these plans, for a like for a like replacement – as this will fall within Business as Usual (BAU).

13. **Prioritisation & Planning** – Describe detailed planning behind proposed investments in the OT Cyber Resilience plan, with a milestone timetable, by combining the classification, risk assessment, useful life, mitigation options and time to benefit ratio.

14. **Budget** – Provide a breakdown of requested funding in terms of; Design, Build, Test, Commission, Training, Support and Maintenance, with associated Capex and Opex breakdown by asset; including, but not limited to:
    a) OT hardware / software costs;
    b) OT implementation costs;
    c) Endpoint or server hardware / software costs;
    d) Endpoint or server implementation costs.
    e) Network hardware / software costs;
    f) Network implementation costs.
    g) Security control hardware / software costs;
    h) Security control implementation costs.

15. **Cost Benefit Assessment (CBA)** – In order to demonstrate the proposed OT Cyber Resilience plan is appropriate and proportionate, the range of options considered (including the counterfactual of doing nothing) should be justified against the monetised reduction in risk delivered by the plan; this should be set out in terms of the reduced likelihood and potential economic impact of existing measures being compromised. In addition, will the investment assist in extending asset life, lowering support costs, or provide any other benefits?

16. **Delivery reporting** – Describe how and what the company will report on, against key performance indicators, risk reduction and delivery schedule.

References and Further Guidance:

- NIST 800-82 R2 – Guide to Industrial Control Systems (ICS) Security
- OG86 - Cyber Security for Industrial Automation and Control Systems (IACS) Edition 2
- IEC 62443; Security for Industrial Automation and Control Systems; 4 Parts.
- NIST 800-53 R4 – Recommended Security Controls for Federal Information Systems and Organizations
- ISO/IEC 27001; Information technology – Security techniques – Information security management systems - Requirements

- ISA-TR84.00.09-2013- Security Countermeasures Related to Safety Instrumented Systems (SIS)

RIIO-2 Cyber Resilience Guidelines Supplementary – Operational Technology (OT) Scope

Key points from the Decision RIIO-2 Sector Specific Methodology – Core Document 24 May 2019:

6.99: *[….] network companies are invited to submit Business Plans in December 2019 for Transmission, Gas Distribution and the ESO, covering the RIIO-2 period, which include the following two sections:*

- *A Business IT Security Plan (which would be considered BAU expenditure) – focused primarily on IT security for business systems, and*
- *A Cyber Resilience Plan – which is expenditure focused primarily on Operational Technology (OT), in response to the NIS Regulations.*

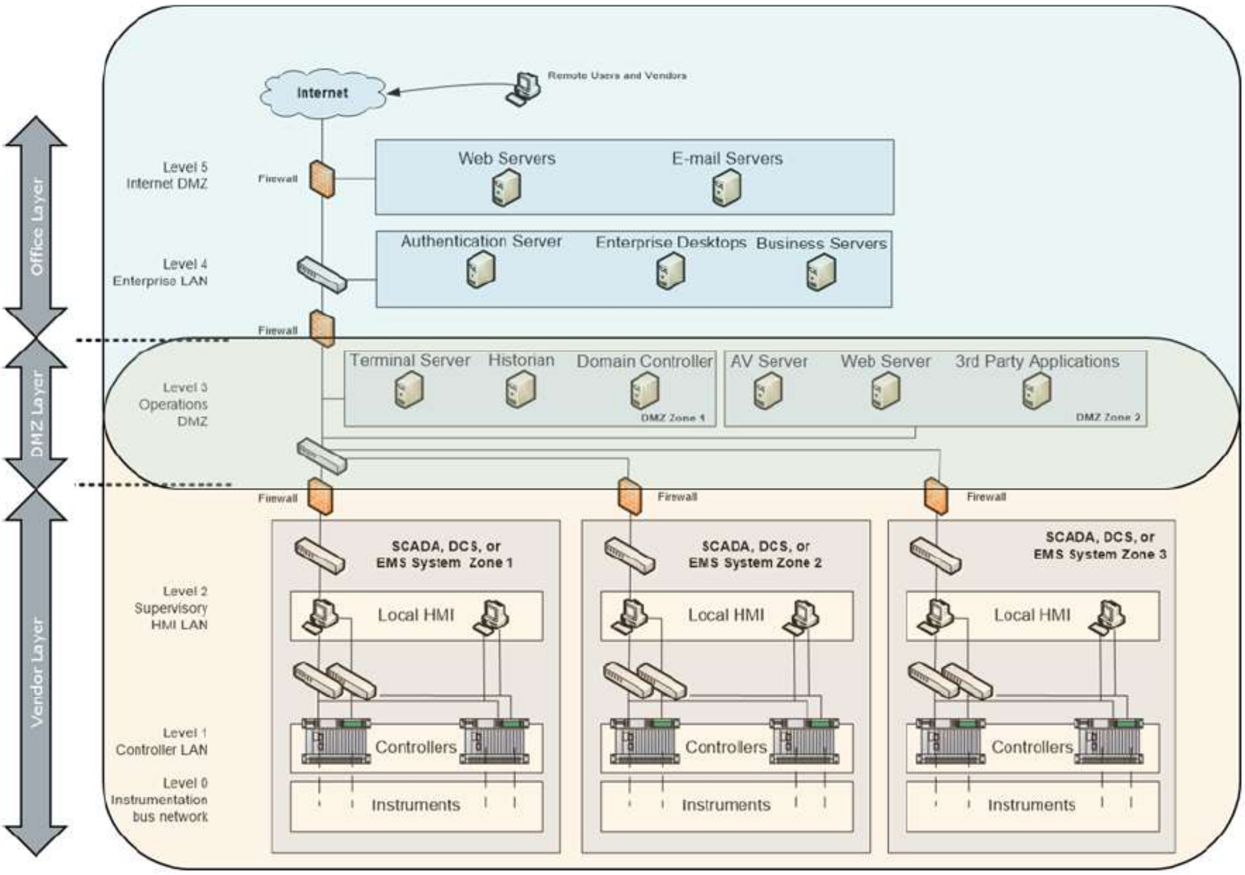
6.104: *For the Cyber Resilience Plan, IT [Information Technology] Security measures for the business domain are generally considered out of scope. However, Ofgem will consider crossover within the Cyber Resilience Plan, where an associated risk is highlighted, for example around the interconnection between business IT and OT.*

RIIO-2 Cyber Resilience Guidance:

1. The network companies would have submitted their scope for NIS regulations with respect to the services that they are delivering in 2018. This was based on the guidance published by Ofgem NIS Competent Authority and review sessions held with the Operator of Essential Service. As a reminder, the scope typically followed what's described below (but not limited to) to Operational Technology (OT) and supporting systems, which a network company may deem critical for the provision of the essential service:
    - Distributed Control System;
    - Supervisory Control and Data Acquisition Systems;
    - Gas Turbine Control System;
    - Steam Turbine Control System;
    - Water Treatment Plant System;
    - Cooling Water Makeup System;
    - Common Services (Auxiliary) System;
    - Coal plant System;
    - Generator Protection Systems;
    - Fire Safety Systems;

- Emergency Shutdown Systems;
- Switching System;
- Engineering Systems;
- Communication Systems;
- Plant Information Systems;
- Remote Terminal Units;
- Programmable Logic Controllers;
- Plant based Heating Ventilation and Air Conditioning;
- IT Systems deemed critical by the business for the delivery of essential services;
- Trading systems.

2. In relation to the Purdue Enterprise Reference Architecture depicted below, the components listed under Level 0, 1, 2 are considered under OT. Level 3, listed in this example as DMZ layer, may or may not be considered, depending on how the system is architected, owned and managed. Typically, any conduit entering the zone for Level 2 and Level 3 is considered in scope. Logical or physical indirect connections or interfaces through persistent or non-persistent means are typically in scope.



3. There are a number of security controls, which may be managed by IT for the OT environment (or vice versa), for example Security Monitoring. It is expected that network companies are able to identify and cost associate the appropriate split on these shared services. Such costs must not be attributed in both Business IT Security Plans and Cyber Resilience plans. Where major upgrades, re-architecture or replacement is required for networks, predominantly for cyber resilience purposes, this must be justified, alongside business benefits and opportunities of doing so.

References and Further Guidance:

- NIST 800-82 R2 – Guide to Industrial Control Systems (ICS) Security
- OG86 - Cyber Security for Industrial Automation and Control Systems (IACS) Edition 2
- IEC 62443; Security for Industrial Automation and Control Systems; 4 Parts.
- NIST 800-53 R4 – Recommended Security Controls for Federal Information Systems and Organizations