UK Government

CAF Overlay for the Load Control sub-sector

Date: March 2026
Version: Final for consultation

Important Note:
This document is in draft and is published to signal DESNZ policy intent and for consultation. Industry should not rely on nor take action as a result of this draft guidance beyond providing feedback as part of the ongoing consultation exercise.

This supplementary guidance will be finalised following consultation.

Table of Contents

Load Control CAF Overlay

1 Introduction

This guidance is for load controllers operating in the load control energy sub-sector of Great Britain (GB). This includes load controllers within the Domestic and Small Non-Domestic Consumer-Led Flexibility (CLF) sector, as well as those managing grid scale Industrial and Commercial (I&C) loads.

It is intended for load controllers required to measure their compliance with either the Tier 1 (equal to or greater than 300MW) or Tier 2 (less than 300MW) Load Control Cyber Assessment Framework[1] (CAF) Profiles.

Effective use of the load control CAF profile and this supplementary guidance should support organisations in understanding and demonstrating how they meet their security duties as set out at Condition 9 of the Standard Conditions of the Load Control Licence[2], or their statutory duties as Operators of Essential Services (OES) under the Network and Information Systems (NIS) Regulations[3].

1.1 Purpose and Approach

The primary aim of this document is to assist Load Control organisations in achieving an appropriate and proportionate level of cyber security for the network and information systems essential to their activity. This applies whether services are managed via cloud-based Application Programming Interface (API) platforms or Operational Technology (OT) and Industrial Control Systems (ICS).

It provides load control sector-specific guidance to relevant Load Controllers and OES which will assist them to achieve and demonstrate the security outcomes in the respective applicable CAF profile.

1.1.1 Collaboration and Profile Development

The Load Control CAF Profiles resulted from close collaboration between Industry, the Department for Energy Security and Net Zero (DESNZ) and the NCSC. This collaborative approach, and consultation with Industry, is intended to ensure the defined cyber outcomes are both robust and practical across the diverse technology stacks within the sector.

1.1.2 Profile Foundation

This guidance directly supports each Load Control CAF Profile, which are built upon the CAF. The CAF is designed to align with established international cyber security good practice frameworks, such as the NIST Cybersecurity Framework and the ISO 27000 series, which should benefit organisations already adhering to such frameworks.

1.1.3 Tiered Cyber Outcomes:

A tiered approach has been developed by DESNZ to ensure proportionality across the load control energy sector. This guidance serves both tiers:

- **Load Control Tier 2 CAF Profile:** Intended for organisations subject to a load control license and managing an aggregate load below 300MW. This profile outlines essential, foundational security practices that are proportionate to the scale and risk of their operations. Establishing this baseline provides a strong foundation for alignment with more stringent requirements as organisations grow or their systemic importance increases.
- **Large Load Control Tier 1 CAF Profile:** Intended for organisations managing an aggregate load equal to or greater than 300MW. These organisations are to be regulated as Operators of Essential Services under the Network and Information Systems Regulations, as outlined in the Cyber Security and Resilience Bill (CSRB)[4]. These requirements are more comprehensive, reflecting the

[1] https://www.ncsc.gov.uk/collection/cyber-assessment-framework
[2] https://assets.publishing.service.gov.uk/media/6937f1fb5cc812f50aa41e19/standard-conditions-load-control-licence.pdf
[3] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
[4] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/large-load-controllers

complexities of large-scale CLF platforms and OT / ICS based grid scale energy resources, and the broader systemic risk inherent in larger-scale load control operations.

More details on the DESNZ approach to load control licensing can be found in the SSES consultation[5] and the supporting guidance listed in Chapter 1.4.

1.2 Supporting Documents

This CAF Overlay guidance forms part of a broader collection of regulatory and technical documents supporting compliance with cyber security requirements set out in Condition 9 of the Load Control Licence and, where applicable, relevant obligations for OES under NIS Regulations.

These documents are intended to be read as a bundle to provide a comprehensive view of obligations, technical expectations, and procedural requirements for the load control sector.

- **DESNZ Policy Guidance for the Implementation of the Load Control Licence and the Network and Information Systems Regulations *[to be published following consultation]*:** This is the primary policy document for the load control sub-sector. It establishes the overarching regulatory framework for the implementation of the licensing regime, including the methodology for the 300 MW designation threshold and the defined methodology for the calculation of aggregated load. It provides the definitive policy link between the Standard Conditions of the Load Control Licence and the statutory requirements of the NIS Regulations, with a view to ensuring a consistent approach to cyber security across both regulatory tiers. This guidance is intended to be published following the DESNZ consultation.

- **DESNZ Scoping Guidance for the Load Control Subsector:** This document provides the technical methodology for defining the functional boundary of a load control system. It offers guidance for organisations already operating within the Downstream Gas and Electricity (DGE) sector where they undertake load control activities, as well as organisations entering the load control sub-sector that are new to cyber regulation. It provides the framework for identifying and isolating the components of the essential service from wider enterprise services, as well as assisting in the identification of relevant ESAs and other assets that fall within the technical scope of the load control function.
- **Standard Conditions of the Load Control Licence:** These are the licence conditions issued under the Electricity Act 1989. They set out the mandatory obligations with Condition 9 and Condition 10 defining the statutory requirements for cyber security and operational load control checks[6]
- **Large Load Control Tier 1 & Load Control Tier 2 CAF Profiles:** These profiles provide a tailored set of outcomes and indicators used to assess the extent to which a load control organisation has implemented security measures that are appropriate and proportionate to the risks posed to their operations and the wider grid. By mapping expectations against the NCSC CAF Contributing Outcomes (COs), the profiles establish the technical benchmark used by the regulator to verify compliance within each regulatory tier.
- **CAF Overlay for the Load Control sub-sector (this document):** This document provides a technical interpretation of the NCSC CAF COs and Indicators of Good Practice (IGPs). It offers practical examples of the evidence required across the people, process, and technology dimensions, assisting load control organisations in understanding the technical benchmarks used by the regulator to verify compliance.
- **The NCSC Cyber Assessment Framework Collection[7]:** This collection is provided by the NCSC, the UK's national technical authority for cyber security. It represents the primary technical standard upon which the load control profiles are built, providing the foundational objectives and principles for managing cyber security risks to essential functions, ensuring a structured and outcome-based approach to resilience[8].
- **NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain v3.0[9]:** This document is a procedural guide provided by Ofgem to assist organisations designated as an OES. It provides the formal framework for performing statutory duties under the NIS Regulations, including incident reporting and the setting of security objectives.

[5] https://www.gov.uk/government/consultations/smart-secure-electricity-systems-sses-programme-draft-load-control-licence-regulations-and-conditions/sses-proposals-on-load-control-licence-regulations-and-licence-conditions-accessible-webpage
[6] https://assets.publishing.service.gov.uk/media/6937f1fb5cc812f50aa41e19/standard-conditions-load-control-licence.pdf
[7] https://www.ncsc.gov.uk/collection/cyber-assessment-framework https://www.ncsc.gov.uk/collection/cyber-assessment-framework
[8] https://www.ncsc.gov.uk/collection/cyber-assessment-framework
[9] www.ofgem.gov.uk/sites/default/files/2026-01/NIS_Guidance_for_Downstream_Gas_and_Electricity_Operators_of_Essential_Services_in_GB_v3.0.pdf

- **DESNZ Policy Guidance for the Implementation of the Network and Information Systems Regulations**[10]**:** This is a policy-level document provided by the DESNZ which provides a comprehensive summary of the compliance landscape for an OES. It defines the specific roles and responsibilities of the Competent Authorities, being Ofgem and DESNZ, and outlines how regulatory oversight and enforcement will be conducted. The document provides guidance on the application of the incident reporting thresholds, provides the necessary templates for notification, and contains the relevant contact information required for an OES to fulfil its statutory duties.
- **NIS Security Assurance Guidance (Concept) for Downstream Gas & Electricity**[11]**:** This document supports the wider programme of inspection activity conducted under Regulation 16 of the NIS Regulations. It is intended for an OES and approved cyber security consultancies to help manage a structured cycle of verification activities. The guidance details the expected outcomes for three core assurance pillars, being independent CAF based audits, operational exercising to test incident response capabilities, and technical testing, which includes vulnerability assessments and penetration testing of essential systems.

2 Scope Summary

This section defines the technical scope that governs the applicability of each Load Control CAF Profile.

2.1 Technical Scope

The technical application of this guidance pertains specifically to the network and information systems essential for the delivery of load control activities. The scope encompasses the core functional systems and the supporting infrastructure required for secure and reliable operation, as these dependencies are integral to the security of the essential load control service.

2.1.1 Essential Service Functionality

The primary focus of this guidance is the load control service, which is defined as the function of controlling the flow of electricity into and out of relevant Energy Smart Appliances (ESAs) by way of load control signals. The scope is determined by any system, data flow, or interface that enables the management of this flow, as well as any system capable of adjusting or processing these signals.

This includes the consumer-facing interfaces, such as mobile applications or web portals, which allow consumers to select flexibility services and define configuration options for their participating assets. This functional scope applies regardless of the underlying technology stack, whether implemented via traditional Information Technology (IT), OT, ICS, or IoT architectures.

The following examples represent the core functional requirements but are indicative and not limited to:

- **Core Load Control Platforms:** Centralised systems used to manage flexibility, aggregate load, and to generate load control signals.
- **Communication Interfaces:** Connectivity layers, gateways, and protocols used to transmit signals to relevant ESAs, including those managed by intermediaries.
- **Consumer-Facing Interfaces:** Applications or portals that facilitate the interaction between the provider and the consumer-led flexibility assets.
- **Processing and Adjustment Systems:** Any infrastructure authorised to adjust or process load control signals before they reach the intended asset.

It is the responsibility of each load control organisation to perform a detailed functional analysis of their specific architecture to identify and document all systems that contribute to the essential service.

2.1.2 Supporting Infrastructure and Dependencies

The scope also encompasses the supporting infrastructure. These are the systems and services providing critical support for the secure and reliable operation of the essential service. This includes any

[10] https://assets.publishing.service.gov.uk/media/6530f1459274590000df959e3/implementation-of-the-network-and-information-systems-regulations-guidance.pdf
[11] https://www.ofgem.gov.uk/sites/default/files/2025-07/Ofgem-NIS-Security-Assurance-Guidance-Concept-for-DGE-Sector.pdf

systems used to configure, update, monitor, and maintain core components, encompassing security tools and administrative endpoints.

Organisations are expected to evaluate their specific dependencies and determine which supporting systems are within scope. Examples of these critical dependencies include, but are not limited to:

- **Identity and Access Management (IdAM):** Systems used to authenticate operators or facilitate system-to-system connections.
- **Security Monitoring and Logging:** Infrastructure used for the detection, triage, and investigation of security events.
- **Administrative Infrastructure:** Endpoints and networks used to configure, update, and maintain core components.

2.1.3 Logical Functional Boundaries and Regulatory Obligations

For organisations already operating within the DGE sub-sector, it is necessary to identify and define the logical boundary between existing essential services designated under the load control service. Organisations may deliver multiple regulated activities within the same sector (for example, generation or supply) and must therefore clearly distinguish the systems and functions that constitute their load control service. Where load control is designated as an essential service under NIS, organisations must comply with the relevant statutory duties as an OES in respect to that function.

Load controllers are responsible for determining the extent to which any common or shared systems, data, and processes previously managed under other DGE OES scopes, and are now required for compliance with the NIS duties specific to Load Control. This necessitates the definition of a clear functional boundary between the load control service infrastructure and:

- Existing OES systems and their associated regulatory scope.
- Shared Enterprise backend systems and general business environments.
- Shared or common supporting services that are not unique to the load control function.

These logical functional views ensure that cyber security measures are targeted specifically at the load control functionality. They support the identification of systems relevant to load control service for purpose of meeting applicable obligations.

The scope for these profiles is intended to exclude consumer owned ESAs deployed at the domestic and small non-domestic level, as baseline device-level security for these assets is addressed through separate regulations[12]. However, systems and interfaces used by load controllers to manage, communicate with, or control these ESAs remain in scope.

In the context of Industrial and Commercial load control, the intention is similarly to exclude the ESA devices themselves, with secondary legislation defining the relevant device types in context, while maintaining focus on the systems used to control and manage them. Accurately defining this scope is fundamental to ensure cyber security efforts are appropriately targeted at the network and information systems supporting the load control. Detailed methodology for defining the functional boundary and identifying supporting infrastructure is provided in the **DESNZ Scoping Guidance for the Load Control Sub-sector.**

[12] https://www.gov.uk/government/consultations/smart-secure-electricity-systems-sses-programme-first-phase-energy-smart-appliances-regulations/smart-secure-electricity-systems-sses-programme-first-phase-energy-smart-appliances-regulations-consultation-document-accessible-webpage

3 Assessing Appropriateness of Security Measures

3.1 Regulatory Obligations

The requirement to implement "appropriate and proportionate" technical and organisational measures is a mandatory duty. Organisations must ensure their technical and organisational measures satisfy the following where it applies to them:

- **NIS Regulation 10(1) & 10(2):** OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of their network and information systems on which their essential service relies; as well as taking appropriate and proportionate measures to prevent or minimise the impact of incidents affecting the security of the network and information systems used for the provision for an essential service.
- **Licence Condition 9.3 & 9.4:** Load Control licensees must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which it's licenced activities rely, as well taking appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of licensed activities.

3.2 Adopting a Risk-Based Approach

To determine what is 'appropriate', load control organisations must identify and manage the specific risks inherent in their technical architecture and operational role. This requires an active risk management process that evaluates how a compromise of the core load control functionality could impact both the organisation and the wider energy system, ensuring that security resources are prioritised where they are most effective.

In alignment with the NCSC CAF and recognised risk management methodologies, such as ISO 27005[13] or NIST SP 800-30[14], the selection of security controls must be evidence based and driven by a documented assessment. This process should be informed by the functional, systems, site, and dependency views of the essential service established during the scoping exercise, as detailed in the **DESNZ Scoping Guidance for the Load Control Sub-sector**.

3.3 Risk Perspectives

The following perspectives are intended to support organisation's in determining whether their cyber security measures are appropriate, by helping them identify and asses the key risks relevant to their load control service. These perspectives should be used to inform risk assessments and guide decisions on the selection and implementation of security measures. Using these dimensions as analytical lenses, grounded in the scoping viewpoints, is essential to accurately evaluate the threat level, the resulting risk exposure, and the specific security controls required to determine what is an appropriateness measure. These lenses are not intended to be exhaustive.

While these perspectives provide a framework for an effective assessment, they are not intended to be an exhaustive list of all possible risk factors. The relevance of each dimension, and the depth of analysis required, will vary depending on the specific operational, technical, and organisational context of each provider.

3.3.1 Environmental and Threat Perspectives

- **The Threat Landscape:** Maintaining a comprehensive understanding of the relevant Tactics, Techniques, and Procedures (TTPs) applicable to the sub-sector. This includes identifying the tools and methodologies used to target or disrupt load control infrastructure, ensuring that risk

[13] https://www.iso.org/standard/80585.html
[14] https://csrc.nist.gov/pubs/sp/800/30/r1/final

assessments are informed by the evolving nature of technical threats rather than static actor categories.

- **Hazard-Driven Risks:** Assessing non-malicious but high-impact events, such as extreme weather, natural hazards, or physical infrastructure failures, which could adversely affect the network and information systems supporting the essential service.
- **The Technology Landscape:** Recognising that as technology evolves, new vulnerabilities regularly emerge, necessitating a proactive and adaptable approach to security.

3.3.2 Operational and Technical Perspectives

- **The Operational Environment:** Accounting for the complexity of the specific technology stack, including the highly distributed attack surface, reliance on internet-facing architectures, cloud-native services, and third-party APIs.
- **Secure Load Control Platforms:** Recognising that centralised platforms used to aggregate and control distributed assets are critical and attractive targets. The security, resilience, and the security of their interfaces are essential.
- **Integrity of Data:** Assessing the validity and reliability of any data used to make load control decisions, even if that data resides outside the scope of the primary load control platform.

3.3.3 Supply Chain and Lifecycle Perspectives

- **Supply Chain Security and External Dependencies:** Managing risks associated with third-party suppliers of both the Load Control Platform and the distributed assets. Providers should conduct appropriate due diligence covering a manufacturers security posture, vulnerability management, and incident response capabilities.
- **Secure Development Lifecycle (SDLC):** Where a load control provider develops in-scope software, security should be embedded throughout the entire development process, often referred to as Secure by Design. This includes adhering to secure coding principles, input validation, and independent security testing prior to deployment.
- **Managing Vendor Access:** Implementing robust controls over third-party privileged access to in-scope systems, ensuring that vendor support access is aligned to the risk-based identity and access management approach used for internal privileged users.

3.3.4 Organisational Maturity Perspectives

- **Organisational Context:** The Load Controller's size, resources, and existing cyber security maturity, particularly for organisations establishing foundational security capabilities.
- **Protection of Sensitive Consumer Data:** Managing the collection, processing, and storage of sensitive consumer data, such as energy consumption patterns and personal data, in compliance with UK GDPR and the Data Protection Act 2018.
- **Organisational Growth and Scalability:** Designing security measures in line with NIS obligations and scalability for both Tier 1 and Tier 2 operators to facilitate a well-managed transition between the two tiers.

3.3.5 Consequence and Sector Perspectives

- **High-Impact Scenarios:** Performing a robust impact analysis to understand the consequences of potential incidents on consumers and the resilience of the wider energy system. Organisations are expected to evaluate both inherent and residual risk to determine the effectiveness and appropriateness of their security posture.
- **Sector-Level and Cascading Risks:** Considering the organisation's position within the wider energy system and the potential for incidents to affect numerous participants through shared dependencies, common technology stacks, or coordinated threat activity targeting the sub-sector.

4 Assessing Proportionality of Security Measures

While consideration of whether a measure is appropriate should help define the effectiveness of a security measure against a specific risk, proportionality governs the scale, depth, and rigour of its implementation. This chapter outlines how load control organisations should determine a proportionate level of security, ensuring that the burden of protection is balanced against the potential impact of service disruption.

4.1 Factors Driving Proportionality

Proportionality is a relative measure that requires an organisation to justify the effort and resources dedicated to security based on the scale of their operations and the risk posed to the security of the network and information systems on which these operations rely. The following factors serve as the primary drivers for determining the required level of security rigour.

4.1.1 Operational Scale and Growth

The volume of aggregate load under management is the primary indicator of a load controller's footprint within the sub-sector. Proportionality requires that the rigour of security measures scales in accordance with the growth of the managed load. Security measures should be designed with scalability in mind, facilitating an incremental increase in maturity as the service grows, rather than waiting for a threshold to be exceeded before enhancing protections.

4.1.2 Risk and Threat Evolution

The depth and robustness applied to meeting outcomes must be directly informed by the prevailing threat environment and the assessed level of risk. This determination dictates the required strength of the security measures and the level of operational persistence necessary to ensure that outcomes remain effective. This is not a static assessment, as the measures required today may become insufficient if Tactics, Techniques, and Procedures (TTPs) evolve or new vulnerabilities emerge. An implementation previously considered sufficient may require additional depth if the likelihood, or potential impact, of a specific threat increases significantly.

4.1.3 Systemic Ecosystem Impact

Proportionality must account for the consequences of service failure within the wider energy ecosystem. The rigour of security must scale with the potential impact on the national grid, ensuring that organisations with greater systemic significance maintain a level of maturity that reflects their critical role in the stability of the energy system.

These drivers are fundamentally addressed through the use of the tiered CAF profiles. As set out in the DESNZ policy guidance (to be finalised following consultation), these profiles represent a pre-determined analysis where the designation breakpoints identify the specific point at which the systemic impact and operational scale necessitate a shift in the expected depth and breadth of security outcomes.

5 Evidential Requirements

5.1 Purpose of Evidence

The relevant authority(ies) may require an organisation to provide evidence of the appropriate and proportionate measures in order to assess compliance with NIS or the relevant licence condition(s). This documentation must clearly articulate the rationale behind the organisation's security posture.

This evidence base should provide a transparent audit trial that links the identified threats and operational scale to the specific measures selected to meet the required cyber control outcomes. Organisations should focus on demonstrating that the relevant CAF outcomes are met. Where different or alternative

controls are implemented to achieve those outcomes, the documentation must provide a robust evidence base to demonstrate why the chosen approach is appropriate to the risk and proportionate to the impact.

Load control providers should demonstrate that they are meeting their security duties as set out in the NIS regulations or in Condition 9 of the Standard Conditions of Load Control Licence.

The primary purposes of maintaining and presenting evidence are:

- **To Support Self-Assessment:** Load controller's will be expected to conduct self-assessments of their cyber security posture. Robust evidence is necessary to substantiate the judgments made during these self-assessments regarding the achievement of CAF contributing outcomes.
- **To Facilitate Independent Assurance:** Conformance with the Load Control CAF Profile will be subject to an enduring assurance framework, involving independent audits. This evidence will be essential for auditors (e.g., NCSC Assured Service Providers or a selected auditor) to verify the provider's security measures and their effectiveness.
- **To Demonstrate Due Diligence:** Maintaining appropriate evidence demonstrates that the CLF provider has taken its cyber security obligations seriously and has a structured approach to managing risks.
- **To Inform Continuous Improvement:** The process of gathering and reviewing evidence can help identify areas for improvement within the organisation's Cyber Security Management System (CSMS).

5.2 Nature of Evidence

Evidence can take many forms. It is not solely about generating new documents for compliance purposes but rather about being able to show, through existing or appropriately created documentation and records, that security policies are defined, processes are followed, and controls are effectively implemented and managed.

Examples of evidence types include, but are not limited to:

- **Documented Policies and Procedures:** E.g., security policies, incident response plans, data handling procedures, access control policies.
- **System Design and Configuration Documents:** E.g., network diagrams for in-scope Load Control NIS, secure build configurations for Load Control NIS.
- **Screenshots:** Where export of data and configuration settings proves challenging, screenshots may be accepted as supporting evidence where they clearly capture the relevant information for review.
- **Records and Logs:** E.g., training records, risk registers, asset inventories, change management records, security event logs, audit logs from Load Control Platforms.
- **Reports:** E.g., risk assessment reports, vulnerability scan results, penetration test reports, internal audit reports.
- **Meeting Minutes:** Where key security decisions or reviews have taken place (e.g., risk review meetings, governance meetings).
- **Contractual Agreements:** With third-party suppliers, detailing security responsibilities.

The key is that the evidence should be relevant, current, and sufficient to support the assertion that a specific CAF outcome is being met. Further detail examples are in Annex A.

5.3 Evidential Expectations for Tier 2 Load Controllers

For Tier 2 Load Controller's, the evidential expectations will be proportionate to their scale, the complexity of their services, and the requirements of the Tier 2 Load Control CAF Profile. It is acknowledged that many Tier 2 providers may be on a cyber security maturity journey. While robust evidence is still required, the expectations below reflect this developmental context.

- **Focus on Essential Documentation:** Evidence should clearly demonstrate that foundational security policies and processes are in place and being followed.
- **Pragmatic Record Keeping:** Records should be sufficient to show that key activities (like risk assessments, essential training, or incident logging) are occurring.
- **Leverage Existing Documentation:** Where possible, existing business documentation can be used or adapted to serve as evidence, rather than creating entirely new sets of documents solely for CAF purposes.
- **Clarity and Accessibility:** Evidence should be organised and accessible, allowing the provider to easily demonstrate its security posture during self-assessment or a Cyber Resilience Audit (CRA)[15] or other recognised CAF-aligned audit or assurance methodologies.

This CAF Overlay provides examples of the types of evidence that would typically be expected to see for each CAF Contributing Outcome.

5.4 Maintaining Evidence

Cyber security is not a one-time activity, and neither is the maintenance of evidence. Load controller's should ensure that their evidence is:

- **Kept Up to Date**: Reflecting the current state of their security measures and systems.
- **Monitored & Reviewed Periodically:** As part of their Cyber Security Management System (CSMS) review and continuous improvement processes.
- **Securely Stored**: Protecting the confidentiality and integrity of sensitive security documentation.
- **Available:** Key evidence required for incident response and recovery (e.g., system configuration details, network diagrams, BCDR plans) should be stored in a manner that ensures it is accessible during a cyber incident, even if primary systems are unavailable.

5.5 Regulatory Assurance and Evidential Requirements

Assessment against each Load Control CAF Profile will be subject to an enduring assurance framework, which may involve independent audits conducted by NCSC Assured Service Providers using the Cyber Resilience Audit scheme or a similar Authority endorsed mechanism.

Load controllers should be aware that the Competent Authorities may request additional or alternative evidence to gain sufficient assurance that security outcomes are being met appropriately and proportionately.

Furthermore, organisations that are, or become, subject to the Load Control Tier 1 CAF Profile as a result of being deemed or designated as an OES under the NIS Regulations, will face more formal and stringent evidential requirements as part of that regulatory framework. Maintaining robust, well organised evidence from the outset will facilitate a smoother transition should an organisation move from being in scope of a Tier 2 profile to a Tier 1 OES Profile.

6 Technology Lifecycle & Obsolescence

The security and resilience of the load control service depend on the effective management of the technology lifecycle. This chapter outlines the expectations for managing assets, software, and systems from initial procurement through to decommissioning, with a specific focus on mitigating the risks associated with technical obsolescence. Providers should actively manage the security lifecycle of all in-scope hardware and software components, particularly concerning obsolete components.

[15] https://www.ncsc.gov.uk/schemes/cyber-resilience-audit/introduction

6.1 Defining Obsolescence

A technology component is considered obsolete from a security perspective when it is no longer receiving security updates from the original vendor or manufacturer to address new vulnerabilities. This also includes cases where reliance on third-party provided compensating controls or patches, such as those from an Independent Software Vendor (ISV) or community source, is insufficient for comprehensive risk mitigation.

6.2 Risk Assessment and Compensating Controls

When an in-scope technology component is identified as obsolete, a risk assessment should be conducted to understand the specific unmitigated vulnerabilities. If immediate replacement is not feasible, proportionate compensating controls should be implemented to mitigate the risk. These may include, but are not limited to, network segmentation, physical or logical isolation, the implementation of Perdue based zones and conduits to secure OT / ICS and / or enhanced protective monitoring.

Providers should maintain sufficient evidence and assurance to demonstrate to the relevant authority(ies) that these compensating controls are effective, continuously operational, and materially reduce the identified risk. It should be noted that having obsolete hardware in scope does not remove the requirement to be compliant with each respective CAF profile.

6.3 Cryptographic Agility

Load controllers should seek to design and operate their load control systems in such a way that offers cryptographic agility. This enables the infrastructure to readily support alternative post-quantum cryptographic algorithms, ensuring long-term resilience against evolving computational threats.

6.4 Asset Inventory and Lifecycle Management

Providers must maintain an up-to-date asset inventory that tracks hardware, software, and firmware versions, along with known end-of-support dates. This inventory must extend to third-party dependencies, including software libraries and APIs, to ensure that the entire technology stack is monitored for obsolescence. This proactive approach is necessary to identify obsolete components before they pose a risk to the essential service.

6.5 Managing Unsupported Devices

For consumer-owned technology, the load controller’s assurance plan should outline the specific circumstances under which the load controller will cease to use a device as part of its licensed service due to unacceptable security risk. This decision-making process must be clearly linked back to the organisation’s risk assessment to ensure that the security of the load control service is maintained.

7 Cyber Security Management Systems

7.1 The CSMS and CAF Relationship

A Cyber Security Management System, or CSMS, is the comprehensive set of policies, processes, governance structures, and controls established by an organisation to manage and reduce cyber security risks to its essential systems and services. For load controller’s, the CSMS protects the network and information systems essential for the delivery of the load control service.

It is important to understand the distinction between the management system and the assessment framework:

- The **CSMS** is the organisation's internal documented system of security management, it is what the organisation does to manage cyber risk.
- A **Load Control CAF Profile** is a framework of expected security contributing outcomes required to be met by the provider to assess the effectiveness of their CSMS.

- A CAF self-assessment, or an independent audit, is an evaluation of the CSMS, not a substitute for it. A mature CSMS should naturally produce the evidence required to demonstrate achievement of the CAF outcomes.

7.2 Scope of the CSMS

The CSMS must effectively govern the technical and organisational scope of the load control service. While an organisation may use a single, overarching CSMS for its entire organisation, it must be able to demonstrate how that system identifies and mitigates the specific risks associated with the load control service.

The primary function of the CSMS is to provide a structured, repeatable approach for the ongoing management of cyber security risks. By implementing effective risk mitigations as part of standard operational activity, the CSMS enables the organisation to meet the objective security outcomes defined in the relevant Load Control CAF Profile. These outcomes serve as the common standard against which the effectiveness of the CSMS is assured across the five CAF objectives:

- Objective A: Managing Security Risk
- Objective B: Protecting Against Cyber Attack
- Objective C: Detecting Cyber Security Events
- Objective D: Minimising the Impact of Cyber Security Incidents
- Objective E: Physical Security

8 Load Control CAF Overlay

Section 8 outlines the relevant authority(ies) interpretations of the CAF IGPs. These interpretations are presented as a Load Control CAF Overlay. The interpretations describe the type and nature of security measures that the authorities would typically expect to see implemented by a load control organisation to meet the overarching security outcome, regardless of the scale of load control. These interpretations should be read in conjunction with the relevant Load Control CAF profile.

NCSC have produced the IGPs to describe the typical circumstances in which an organisation might be considered to have achieved a contributing outcome. Use of the word ‘typical’ acknowledges that there are circumstances in which security outcomes may be better achieved via alternative means. The Load Control CAF overlay has been produced on the same basis, meaning that the inclusion of an interpretation of an IGP does not imply that it is mandatory. The interpretations are provided on a non-binding basis with the intention of guiding load control organisations toward achieving and demonstrating attainment of the security outcomes.

The term ‘network and information systems’ is used repeatedly throughout the CAF tables and the overlay. In every instance, the term is being used to describe network and information systems that are within the essential system scope.

The NCSC's CAF provides a structured approach that load control providers can use to assess their security posture and guide the implementation of appropriate measures. Specific risks to the load control ecosystem and potential impacts to CNI have been assessed with a view to ensuring the profiles are tailored to what is considered appropriate and proportionate for the sector.

When using the CAF Overlay and the relevant Load Control CAF Profile, the provider should:

- **Focus on Outcomes:** The primary goal is to achieve the Contributing Outcomes (COs), as these are the detailed requirements that collectively satisfy the overarching CAF Objectives and underlying principles.
- **Utilise IGPs:** The Indicators of Good Practice detailed in the CAF and interpreted in the Load Control CAF Overlay provide guidance on how outcomes may be achieved. They function as guidance points intended to inform expert judgment rather than as a prescriptive checklist.

- **Justify Approach:** Where a provider implements controls that go beyond the IGPs due to their risk assessment or chooses an alternative technical approach for compensating controls, they should be prepared to justify why their chosen measures are appropriate and proportionate in achieving the expected cyber outcome.

8.1 The Role of Indicators of Good Practice

The NCSC CAF describes the achievement levels for contributing outcomes using Indicators of Good Practice (IGPs). The CAF states that for an outcome to be assessed as Achieved or Partially Achieved, it is expected that all the relevant indicators would normally be present. While this can seem binary, it is important to provide context, particularly regarding the appropriate and proportionate nature of the required security measures.

It is worth reaffirming that the IGPs are indicators only. They provide examples of effective security measures but are not an exhaustive or prescriptive checklist. The appropriateness and proportionality of any given control must be determined by the organisation's specific risk assessment.

An organisation’s risk assessment will drive the selection of security measures. There may be circumstances where an organisation identifies threats that necessitate the implementation of controls that go beyond the standard IGPs, or conversely, where an organisation can demonstrate that an outcome has been met through alternative or compensating controls better suited to their specific technologies. In all instances where the implemented approach deviates from or extends beyond the IGPs, providers should document the rationale as part of their assurance evidence.

The focus of any assessment should always be on whether the organisation is achieving the required security outcome effectively. The IGPs and the interpretations in this guidance offer pathways to do so, but the ultimate measure is the successful achievement of the outcome itself. Detailed guidance on assessing appropriateness and proportionality is provided in the subsequent chapters of this document.

8.2 CAF IGP Indexing

To ensure precision during assessment and cross-referencing, this guidance uses a structured indexing system to reference specific Indicators of Good Practice (IGPs). The referencing convention is structured to clearly identify the Objective, Principle, Contributing Outcome, Achievement Level, and the specific IGP line item. The format is as follows:

[Objective].[Principle].[Contributing Outcome].[Achievement Level].[IGP Number]

Component	Description	Example
[Objective]	A, B, C, or D.	A
[Principle]	The Principle number (1-6).	1
[Contributing Outcome]	The Outcome letter (a, b, c, etc.).	a
[Achievement Level]	A (Achieved), PA (Partially Achieved), or NA (Not Achieved).	A
[IGP Number]	The sequential number of the IGP statement within that achievement column.	4
Full Example	Direction set at board-level is translated into effective organisational practices...	A1.a.A.4
Full Example	The security elements of projects or programmes are solely dependent on the completion of a risk management assessment...	A2.a.NA.4

Table 7-1 IGP Indexing

In the forthcoming tables, any specific reference made to an IGP will follow this convention.

8.3 Application of Overlay and Interpretations

The guidance and interpretations detailed in Chapter 8 are intended to be profile agnostic. They provide the descriptive detail for the Indicators of Good Practice (IGPs) regardless of the specific expected outcomes defined for an organisation in the CAF profile. These interpretations represent the types of measures that the Competent Authority consider appropriate and proportionate for each IGP.

This guidance should not be read in isolation. It should be used alongside the specific Load Control CAF Profile assigned to the organisation and the supporting documents listed in Chapter 1.20. By consulting the IGP interpretations in conjunction with their profile, organisations can understand the specific rigour and nature of the security measures expected of them to achieve the required outcomes.

To support the diverse range of technical models and the designation of OES within the sector, the guidance is structured into distinct areas:

- **General Interpretations**: These are non-specific to a technology stack. They cover the standard expectations for the technology environments common across the sector.
- **OT and ICS Specific Interpretations:** For providers whose load control functions involve ICS or OT, typical in grid-scale BESS and VPPs, specific guidance and evidence requirements are provided. These address the unique safety, reliability, and physical integrity constraints associated with control hardware.

This structure allows providers to extract the specific technical and sectoral requirements relevant to their unique operating model while ensuring they meet the outcome levels defined in their assigned profile and NIS designation status.

9 Objective A: Managing Security Risk

9.1 CAF Objective A Outcomes

CAF Objective A: **Appropriate organisational structures, policies, processes and procedures in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.**

9.2 Objective A Extended Guidance**:**

Objective A establishes the foundational organisational security posture required to support the cyber resilience of the load control service. It requires moving beyond ad-hoc security measures toward a systematic, documented, and repeatable process for identifying, assessing, and managing the unique cyber risks associated with load control activities.

For any load control provider, achieving the outcomes within this objective is a foundational prerequisite for effective security. This requires a clear focus on the following overarching areas:

- **Strategic Governance and Safety Integration:** Ensuring security is governed by a deliberate, documented system with clear lines of accountability, driven by senior leadership. For organisations managing grid-scale assets, this includes the integration of security governance with existing operational safety and engineering management structures to ensure that cyber security measures do not adversely affect the physical safety or integrity of the energy system.
- **Threat-Informed Risk Management:** Ensuring that risk assessments are not static but are informed by an understanding of adversary Tactics, Techniques, and Procedures (TTPs) specific to the Load Control technology stack. This involves a multidisciplinary approach, drawing on expertise from IT, OT, and engineering teams to identify how technical vulnerabilities could translate into operational disruption.
- **Lifecycle Asset and System Visibility:** Maintaining a comprehensive and up-to-date understanding of all assets (data, people, and systems) required to deliver the essential function. This includes understanding the interdependencies between core load control platforms, supporting infrastructure, and the communication interfaces used to command distributed assets.

- **Ecosystem and Supply Chain Oversight:** Recognising that security is a collective responsibility, requiring systematic management of third-party dependencies. This extends from cloud service providers and software developers to the interfaces with Energy Smart Appliances (ESAs), ensuring that the integrity of the wider energy ecosystem is considered in risk treatment decisions.

A robust implementation of Objective A provides the necessary organisational structures and risk-based context required to justify the selection and implementation of security measures in subsequent objectives. The effectiveness of the protective measures in Objective B, the detection capabilities in Objective C, and the recovery plans in Objective D is fundamentally dependent on the rigour of the governance and risk management processes established here.

9.3 Principle A1: Governance

9.3.1 Principle A1 Extended Guidance:

Principle A1: **The organisation has appropriate management policies, processes and procedures in place to govern its approach to the security of network and information systems.**

Effective governance is the critical first principle within Objective A because it provides the top-down direction, authority, and accountability for security. It ensures that security is treated as a core business function, driven and overseen by the executive level, rather than a purely technical issue managed in isolation.

This principle establishes the framework in which risk can be managed effectively, by defining the strategic direction they should follow (board direction, A1.a), who is responsible (roles, A1.b) and who makes decisions (decision-making, A1.c). Without strong governance, even the best technical security efforts can lack direction, resources, and risk reduction impact.

The governance structure must encompass the entire scope of the essential service, ensuring that senior leadership has sufficient visibility into the security posture of both internal platforms and any third-party dependencies that facilitate load control.

For organisations with significant operational technology (OT) or engineering components, governance processes must ensure that cyber security decisions are fully aligned with operational safety and engineering management requirements to prevent security measures from adversely affecting the physical integrity of the energy system.

9.3.2 A1.a Board Direction

A1.a – Board Direction	
You have effective organisational security management led at board level and articulated clearly in corresponding policies.	
Not achieved: At least one of the following statements is true	Achieved: All the following statements are true
A1.a.NA.1 The security of network and information systems related to the operation of essential function(s) is not discussed or reported on regularly at board level.	**A1.a.A.1** Your organisation's *approach and policy* relating to the security of network and information systems supporting the operation of your essential function(s) are *owned and managed* at board-level. These are communicated, in a meaningful way, to risk Management decision-makers across the organisation.
A1.a.NA.2 Board-level discussions on the security of network and information systems are based on partial or out-of-date information, without the benefit of expert guidance.	**A1.a.A.2** *Regular* board-level *discussions on the security* of network and information systems supporting the operation of your essential function(s) take place, based on timely and accurate information and *informed by expert guidance*.

A1.a.NA.3 The security of network and information systems supporting your essential function(s) are not driven effectively by the direction set at board-level.	**A1.a.A.3** There is a board-level individual who has overall accountability for the security of network and information systems and drives regular discussion at board-level.
A1.a.NA.4 Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.	**A1.a.A.4** Direction set at board-level is translated into *effective organisational practices* that *direct and control* the security of network and information systems supporting your essential function(s).
	A1.a.A.5 The board has the information and understanding needed in order to effectively discuss how the security and resilience of network and information systems contributes to the delivery of essential function(s) and what the potential impact from compromise of those systems would be.
	A1.a.A.6 Security is recognised as an important enabler for the resilience of your essential function(s) and considered in all relevant discussions.

IGP Ref	IGP Interpretation
A1.a.A.1 *A1.a.A.4*	***[approach and policy] [effective organisational practices]*** • 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. You are confident that these organisational practices deliver the intended security benefits and have a means of monitoring and demonstrating their effectiveness. • A management system exists which clearly defines your approach to managing the security of networks and information systems that support your essential function.
A1.a.A.1 *A1.a.A.4*	***[owned and managed] [direct and control]*** • The management system clearly defines the governance roles, responsibilities and the chain of accountability. • The management system is reviewed in accordance with company policy and updated, as necessary, to ensure it is in line with the latest threats and the approved risk appetite. • The security management system is integrated into the company's wider Corporate Management System (CMS), compliance structures and performance reporting processes.
A1.a.A.2	***[regular]*** Senior management supply the board with scheduled (planned and periodic) feedback on the security of networks and information systems supporting the delivery of your essential function.
A1.a.A.2	***[informed by expert guidance]*** This feedback should be prepared by suitably qualified and experienced personnel from within the organisation or by third parties.
A1.a.A.2	***[discussions on security]*** Discussions and reports should include, but not be limited to: • cyber security risk status and trajectory • cyber security risks associated with the organisation's supply chain • cyber security risks associated with the organisation's interactions with other participants in the load control eco-system • cyber security performance (supported by key performance indicators) • incidents experienced within the organisation • incidents experienced in the industry or similar industries • progress against improvement plans • any changes to relevant cyber security threats.

IGP Ref	OES / OT / ICS Specific IGP Interpretation

A1.a.A.1 *A1.a.A.4*	***[approach and policy] [effective organisational practices]*** • 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. You are confident that these organisational practices deliver the intended security benefits and have a means of monitoring and demonstrating their effectiveness. • A management system exists which clearly defines your approach to managing the security of networks and information systems that support your essential function.

IGP	Examples of Evidence to support IGPs
A1.a.A.1 *A1.a.A.4*	A suite of policy documentation that combine to form a security management system. Some organisations may use elements of internationally recognised standards and frameworks such as, but not limited to ISO 9001, ISO 27001 or ISO 55000 to contribute to their cyber security management system. In these instances, Licensee's should be able to explain how these elements integrate with other security related organisational processes to form a complete security management system.
A1.a.A.1 A1.a.A.4	Evidence (in the form of meeting minutes or reports) that the implementation of the security management system is monitored by your company's compliance structures (e.g. company compliance committee or equivalent).
A1.a.A.1 A1.a.A.4	Evidence (e.g. meeting minutes, directives) that the board is actively engaged in security management (e.g. provision of direction and guidance after the review of performance indicators).
A1.a.A.2	Relevant status reports and meeting minutes

References and Further Guidance	
• A.1 Governance - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	GV.PO-01, GV.RR-01
• ISO 27001/27002:2022 Control:	5.1, 5.4
• NIST SP 800-53 Rev. 5 Control:	CA -1, PL-1, PM-1

9.3.3 A1.b Roles and Responsibilities

A1.b Roles and Responsibilities	
Your organisation has established roles and responsibilities for the security of network and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.	
Not achieved: At least one of the following statements is true	Achieved: All the following statements are true
A1.b.NA.1 Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis.	A1.b.A.1 *Key roles and responsibilities* for the security of network and information systems supporting your essential function(s) have been *identified*. These are reviewed regularly to ensure they remain *fit for purpose.*
A1.b.NA.2 Staff are assigned security responsibilities but without adequate authority or resources to fulfil them.	A1.b.A.2 *Appropriately capable* and knowledgeable staff fill those roles and are given the *time, authority, and resources* to carry out their duties.
A1.b.NA.3 Staff are unsure what their responsibilities are for the security of the essential function(s).	A1.b.A.3 There is *clarity* on who in your organisation has overall accountability for the security of the network and information systems supporting your essential function(s).

IGP Ref	IGP Interpretation

A1.b.A.1	***[Key roles and responsibilities][Identified][fit for purpose]*** Being 'fit for purpose' means that you are confident that the roles and responsibilities that you have identified are sufficient to deliver the security management plan. This means that you should be able to associate all the activities and tasks listed in your security management plan with specific roles in your organisation.
A1.b.A.1	***[identified]*** Key roles and assigned personnel are published internally and kept-up to-date. Individuals who are employed in roles with security responsibilities are fully aware of those responsibilities - this may be achieved by documenting these responsibilities in job specifications and organisational charts.
A1.b.A.1	***[Key roles]*** Roles can include, but are not limited to: • Managers and senior leaders who are risk owners and who are responsible and accountable for elements of the security management system. • Enterprise Information Technology (EIT) and Internet of Things (IoT) personnel who have responsibilities for securing the Enterprise IT networks that are connected to the Load Control environment and for maintaining and configuring gateways and boundary devices for Load Control networks. • Additional resources who may be in the legal, human resources and customer support and have responsibilities for implementing administrative controls.
A1.b.A.2	***[appropriately capable]*** You have baselined the minimum levels of qualification and experience required to effectively discharge the security responsibilities associated with each role. You are confident that the incumbents in each of your security roles meets this baseline, or there is a training plan in place to close the gap.
A1.b.A.2	***[time, authority and resources]*** Personnel should be provided with sufficient information, financial, physical, and human resources to discharge their security responsibilities.
A1.b.A.3	***[clarity]*** A tool such as a responsible, accountable, consulted, and informed (RACI) matrix should be used to document and communicate responsibilities and accountabilities.

IGP Ref	Examples of Evidence to support IGPs
A1.b.A.1	A master list of security roles and responsibilities that is maintained as part of the security management system (this is often achieved in a RACI table format).
A1.b.A.1	The job specifications for each of the roles defined in the master list of security roles and responsibilities should clearly define the associated security responsibilities.
A1.b.A.2	The baseline level of qualification and experience for each security role should be documented (possibly in the job specification and organisational chart).
A1.b.A.2	Evidence of the employment, or procurement, of a sufficient number of individuals to fill roles that have security responsibilities
A1.b.A.3	A clear chain of accountability which cascades down from board level and is documented in an appropriate format (such as a RACI matrix and skill gap analysis).

References and Further Guidance	
• A.1 Governance - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	GV.RR-02
• ISO 27001/27002:2022 Control:	5.2, 6.2
• NIST SP 800-53 Rev. 5 Control:	PM-1, PS-1

9.3.4 A1.c Decision Making

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 functions are considered in the context of other organisational risks.

Not achieved: At least one of the following statements is true	Achieved: All the following statements are true
A1.c.NA.1 What should be relatively straightforward risk decisions are constantly referred up the chain, or not made.	**A1.c.A.1** Senior management have *visibility* of key risk decisions made throughout the organisation.
A1.c.NA.2 Decision-makers are unsure of what senior management's risk appetite is, or only understand it in vague terms such as "averse" or "cautious".	**A1.c.A.2** Risk management decision-makers understand their responsibilities for making *effective and timely decisions* in the *context of the risk appetite* regarding the essential function(s), as set by senior management.
A1.c.NA.3 Risks are resolved informally (or ignored) at a local level when the use of a more formal risk reporting mechanism would be more appropriate.	**A1.c.A.3** Risk management decision-making is *delegated and escalated* where necessary, across the organisation, to people who have the skills, knowledge, tools and authority they need.
A1.c.NA.4 Decision-makers are unable to justify their risk management decisions.	**A1.c.A.4** Risk management decisions are *regularly reviewed* to ensure their continued relevance and validity.
A1.c.NA.5 Organisational structure causes risk decisions to be made in isolation. (e.g. engineering and IT do not talk to each other about risk).	
A1.c.NA.6 Risk priorities are too vague to make meaningful distinctions between them. (e.g. almost all risks are rated 'medium' or 'amber').	

IGP Ref	IGP Interpretation
A1.c.A.1	***[visibility]*** Risk registers are maintained and are reviewed and approved on a scheduled basis e.g. Monthly by individuals with sufficient authority to make the necessary risk management decisions.
A1.c.A.2	***[effective and timely decisions]*** The organisation's policy and processes relating to the management of risk should be published as part of the organisation's security management system. These policies and processes should be easily accessible and support effective decision making.
A1.c.A.2	***[context of risk appetite]*** • Your organisation's risk appetite should be agreed by the board. The risk appetite should take account of the CAF profiles that are issued by DESNZ. • Your risk appetite should be reviewed periodically and at least annually in accordance with company policy, or due to any significant change in threat level. Any changes should be promptly communicated to relevant personnel.
A1.c.A.3	***[delegated and escalated]*** • Suitable governance structures and scheduled activities (such as risk reviews) are in place to support the delegation and escalation of risk management decision making to the appropriate level. • Risk management decision-makers have the necessary authority and resources to make decisions and drive risk management activities in line with the guidance from the board. • Decision makers are given appropriate support by senior management.
A1.c.A.4	***[regularly reviewed]*** Reviews should be performed both periodically (e.g., annually, as part of the overall governance process) and event-driven, specifically when new threat intelligence (A2.b), major changes to architecture, or findings from assurance activities (A2.c) necessitate validation that the current residual risk remains within the board-defined risk appetite.

IGP Ref	Examples of Evidence to support IGPs

A1.c.A.1	Risk registers that have been formally approved and accepted by those managers who are responsible and accountable for the risks.
A1.c.A.2	A documented risk appetite statement, and a process that explains how you manage situations where risk treatment decisions informed by your own risk appetites deviate from the relevant CAF profile. Note: This is covered in more detail in Section 5 & 6 of this document
A1.c.A.3	A schedule of risk management activities (e.g. risk identification workshops, risk reviews).
A1.c.A.3	Minutes of previously held risk management activities.
A1.c.A.3	Appropriate financial delegations/budgets have been delegated to allow timely and effective management of risk.
A1.c.A.4	A schedule of risk management activities (e.g. risk identification workshops, risk reviews, risk assessments and risk treatments).
A1.c.A.4	Minutes from previously held risk management meetings/activities

References and Further Guidance	
• A.1 Governance - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory	GV.RM-01, GV.RM-02
• ISO 27001/27002:2022 Control	5.3, 5.35
• NIST SP 800-53 Rev. 5 Control	PM-9, PM-28

9.4 Principle A2: Risk management

9.4.1 Principle A2 Extended Guidance:

Principle A2 puts the governance established in A1 into practice through the Risk Management function. It transitions an organisation from a general awareness of cyber risk to a detailed, threat-informed understanding of the threats, vulnerabilities, and potential impacts on its essential service.

The CAF defines the requirement for contributing outcome **A2.b (Understanding Threat)**, which necessitates proactive engagement with threat intelligence. This means moving beyond reliance on generic or retrospective risk analysis and instead focusing on:

- **Intelligence-Led Decisions:** Actively using up-to-date knowledge about attacker TTPs, sector-specific threats, and the methods of capable and well-resourced threat actors to inform risk treatment decisions.
- **Attack Path Analysis:** Applying techniques to develop an understanding of the Load Control environment or platform from an adversary's perspective, enabling the anticipation of probable attack methods.
- **Proportionate Defences:** Ensuring that the implemented security controls (in Objectives B, C, and D) are demonstrably effective against the actual threat level identified in the risk assessment, which may necessitate controls beyond the standard baseline IGPs.

A structured and continuously assured risk management process is essential for driving proportionate security decisions and targeting defensive investments effectively. This threat-led approach ensures the organisation maintains the capability to understand and defend against evolving cyber threats, acknowledging that risk management is a dynamic and continuous process.

Risk assessments should be multidisciplinary, integrating with existing safety and operational risk frameworks to ensure that the potential for physical impact on grid stability or equipment is accurately reflected in the risk profile.

9.4.2 A2.a Risk Management Process

A2.a Risk Management Process

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of your essential function(s) and communicating associated activities.

Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
A2.a.NA.1 Risk assessments are not based on a clearly defined set of threat assumptions.	**A2.a.PA.1** Your organisational process ensures that security risks to network and information systems *relevant to essential function(s)* are *identified, analysed, prioritised, and managed.*	**A2.a.A.1** Your organisational process ensures that security risks to network and information systems *relevant to essential function(s) are identified, analysed, prioritised and managed.*
A2.a.NA.2 Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner.	**A2.a.PA.2** Your risk assessments are informed by an *understanding of known and well understood threats and vulnerabilities* in network and information systems supporting your essential function(s).	**A2.a.A.2** Your approach to risk is focused on the *possibility of adverse impact* to your essential function(s), leading to a *detailed understanding* of how such impact might arise as a consequence of *possible threat actor actions* and the *security properties* of your network and information systems supporting your essential function(s).
A2.a.NA.3 Risk assessments for network and information systems supporting your essential function(s) are a "one-off" activity or not done at all.	**A2.a.PA.3** The output from your risk management process is a *clear set of security requirements* that will address the risks in line with your organisational approach to security.	**A2.a.A.3** Your risk assessments are based on a *clearly understood set of threat assumptions*, informed by an *up-to-date understanding* of threats to network and information systems supporting your essential function(s), your sector and *wider national infrastructure.*
A2.a.NA.4 The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.	**A2.a.PA.4** Significant conclusions reached in the course of your risk management process are *communicated* to key security decision-makers and *accountable individuals.*	**A2.a.A.4** Your risk assessments are informed by an *understanding of the vulnerabilities* in the network and information systems supporting your essential function(s).
A2.a.NA.5 There is no systematic process in place to ensure that identified security risks are managed effectively.	**A2.a.PA.5** You conduct risk assessments when significant events potentially affect the essential function(s), such as replacing a system or introducing *new or emergent technologies* or a change in the cyber security threat.	**A2.a.A.5** The output from your risk management process is a *clear set of traceable and prioritised security requirements* that will address the risks in line with your organisational approach to security.
A2.a.NA.6 Systems are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).		**A2.a.A.6** Significant conclusions reached in the course of your risk management process are *communicated* to key security decision-makers and *accountable individuals.*

A2.a.NA.7 Security requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of network and information systems supporting your essential function(s).		**A2.a.A.7** Your risk assessments are dynamic and *readily updated* in the light of relevant changes which may include technical changes to network and information systems, supporting your essential function(s), change of use, the introduction of new or emergent technologies or new threat information.
A2.a.NA.8 Risks remain unresolved on a register for prolonged periods of time awaiting senior decision- making or resource allocation to resolve.		**A2.a.A.8** The *effectiveness* of your risk management process is *reviewed* regularly, and improvements made as required
		A2.a.A.9 You anticipate technological developments that could be used to adversely impact network and information systems supporting your essential function(s).

IGP Ref	IGP Interpretation
A2.a.A.1 *A2.a.PA.1*	***[relevant to essential function]*** You have fully captured and documented your CLF scope in accordance with the direction provided in the current version of Supplementary Guidance for CLF Operators. Your license scope takes account of the requirement for you to deliver the licenced services in accordance with relevant licences, regulations and network codes.
A2.a.A.1 *A2.a.PA.1*	***[identified, analysed, prioritised and managed]*** • You have had regard to the NCSC's guidance on risk management and have selected a risk identification and assessment methodology that is appropriate to the systems in scope • You have recognised that, for those network architectures that include a conduit between the EIT and Load Control networks, the systems on your load control network have a dependency on the security services (boundary protection, access control, SIEM etc) provided by your EIT networks. You have included these IT security services within your CLF scope. • You have taken account of common risks in your sub-sector (such as those associated with the use of particular equipment types and communications methods) and of context specific risks (such as those associated with your particular network topologies and equipment configurations). You have used multi-disciplinary teams to ensure a comprehensive capture of context specific organisational risks in accordance with your selected risk assessment methodology. • Your risk management process is clearly explained in your security management system, and the outputs of your risk management activities are documented. • You have considered the risk of single cyber-attacks, multiple and coordinated near simultaneous attacks at the risk identification and assessment stage. • You periodically, at least annually or upon any material change to the organisation, threat landscape or systems, review your risk assessments to consider changes in the cyber security landscape or scope.

A2.a.A.2	***[possibility of adverse impact]*** • Your risk assessments take account of the potential for adverse impacts to the delivery of your licensed service and for adverse impacts that may impact other Operators of CLF services, DNOs and NESO (typically referred to as cascading impacts) and have prioritised them accordingly. • You have identified risks originating on the systems of other CLF services on which you have dependencies. You have taken measures to control these risks where it is practical and feasible to do so.
A2.a.A.2	***[detailed understanding]*** • You have employed a system-driven risk assessment methodology to identify the possibility of adverse impacts to the essential function. The organisation has fully captured and documented this risk assessment and is able to explain and justify it to auditors. • The organisation's cyber risk assessment panel is multi-disciplinary, such that the risk assessment is as complete as is feasible.
A2.a.A.2	***[possible threat actor actions]*** You understand the Tactics, Techniques and Procedures that attackers may employ against your systems. You conduct attack modelling (using a resource such as the MITRE ATT&CK framework) to identify the specific techniques that an adversary could employ.
A2.a.A.2	***[security properties]*** • You have fully captured the existing security properties (the security function/capability provided by the controls) of your systems and understands how these properties contribute to controlling risk. • You have considered the effectiveness of these security controls against the attack models you have developed and have identified where enhanced security controls will be required to match these threats.
A2.a.A.3	***[clearly understood set of threat assumptions]*** You have conducted and documented a threat assessment. Your assumptions include the possibility that your organisation is subject to attacks from threat actors ranging in capability from basic to advanced (e.g. from commodity attacks to espionage and targeted attacks from malicious actors such as hostile states and criminals)
A2.a.A.3	***[up to date understanding]*** • You review your threat assumptions, based on changes to the threat landscape. For example, in response to geo-political events, evidence of new cyber-attack campaigns that are relevant to your sector, or the disclosure of significant new vulnerabilities. • You participate in cross-sector information sharing forums and draw on NCSC's threat intelligence (e.g. through CISP). You make use of all available services provided by NCSC and you are in receipt of an appropriate Threat Intelligence feed (e.g. MISP or a commercial equivalent). • You have a means of prioritising new threat intelligence and updating risk assessments accordingly.
A2.a.A.3	***[wider national infrastructure]*** Your threat assumptions should consider cascading and systemic risks that may originate from, or be directed at, other parts of CNI that cross DSR / CLF sector boundaries. This includes risks related to dependencies on telecommunications, cloud service providers, and the wider electricity system operators.
A2.a.A.5	***[clear set of traceable and prioritised security requirements]*** The output security requirements should be traceable back to the specific risks identified in the assessment, providing a clear audit trail and rationale. They should be prioritised based on the criticality of the risk they address and their alignment with the organisation's established risk appetite, ensuring high-impact risks are managed first.

A2.a.A.6	***[communicated][accountable individuals***] Residual risks (those risks that remain after risk treatment) are captured on the risk register and approved by accountable individuals. The means of approval is formal and documented. Therefore, the approval should be accompanied by a documented justification. This justification should clearly articulate the business rationale for accepting the risk, demonstrating that the accountable individual has balanced the potential impact of the risk against factors such as the cost, technical feasibility, and operational impact of further mitigation. This ensures that all risk acceptance is a conscious, transparent, and defensible business decision
A2.a.A.7	***[readily update]*** having efficient mechanisms in place for continuous environmental monitoring and risk review, such as integrating automated threat intelligence feeds (e.g., CiSP, MISP, or commercial equivalents) or routinely using automated vulnerability scanners. This demonstrates the organisational agility required to respond promptly to critical changes in the threat landscape or technical architecture.
A2.a.A.8	***[effectiveness][reviewed]*** The organisation's cyber risk management process is subject to an appropriate level of oversight. This may take the form of a formal Quality Assurance process, a regulatory compliance committee or another form of internal or external audit.
A2.a.PA.2	***[understanding of known and well understood threats and vulnerabilities]*** This requires actively maintaining a process that identifies and manages vulnerabilities at a component level (often via asset and configuration management) and integrating this with knowledge of commonly observed attack patterns, vectors, and the TTPs of adversaries. This can be supported by frameworks like MITRE ATT&CK and relevant Threat Intelligence services or feeds
A2.a.PA.3	***[clear set of security requirements]*** Deficiencies in your security controls that are identified through your risk assessment and vulnerability management processes are assessed against your risk appetite. Those risks that required treatment are captured in the organisation's cyber improvement plan.
A2.a.PA.5	***[new or emergent technologies]*** This includes adopting technologies like Artificial Intelligence / Machine Learning components for control or optimisation, new IoT device platforms, or significant changes to foundational cloud services or architectures (e.g., serverless, containerisation). This guidance should also apply to traditional on-premise network and data centre architecture where new software-defined components, virtual4isation, or modern security tooling are introduced, as these could materially change the risk profile of the essential service. Risk assessments should specifically address AI-Related Risk as part of this review.

IGP Ref	Examples of Evidence to support IGPs
A2.a.A.1 *A2.a.PA.1*	A documented risk management process.
A2.a.A.1 *A2.a.PA.1* *A2.a.A.2*	A comprehensive risk register that has taken account of the risks posed by the full range of threat actors.
A2.a.A.3	Evidence of consideration (e.g. updates to risk assessments) of changes to the threat landscape.
A2.a.A.3	Evidence that the organisation participates in cross sector information sharing initiatives and is in receipt of regular threat intelligence.

References and Further Guidance	
• A.2 Risk management - NCSC.GOV.UK	
• NCSC Early Warning : https://www.ncsc.gov.uk/section/active-cyber-defence/early-warning	
• NCSC CISP: https://www.ncsc.gov.uk/cisp/home	
• NIST CSF 2.0 Subcategory:	ID.RA-05, ID.RA-06
• ISO 27001/27002:2022 Control:	5.7, 8.8
• NIST SP 800-53 Rev. 5 Control:	RA-3, PM-9

9.4.3 A2.b Understanding Threat

A2.b Understanding Threat		
You understand the capabilities, methods and techniques of threat actors and what network and information systems they may compromise to adversely impact your essential function(s). This information is used to inform security and resilience risk management decisions, adjusting, enhancing or adding security measures to better defend against threats.		
Not achieved: At least one of the following statements is true	Partially Achieved All the following statements are true	Achieved All the following statements are true
A2.b.NA.1 You are unable to perform threat analysis.	**A2.b.PA.1** You perform threat analysis and understand how *common threats* apply to network and information systems supporting your essential function(s).	**A2.b.A.1** You perform *detailed threat analysis* and understand how this applies to network and information systems supporting your essential function(s), in the context of your sector and wider national infrastructure.
A2.b.NA.2 You do not understand the threats to network and information systems supporting your essential function(s).	**A2.b.PA.2** You understand common types of cyber-attacks, including the methods and techniques, and how these might apply to network and information systems supporting your essential function(s). This understanding is kept up to date.	**A2.b.A.2** Your detailed understanding of threat includes the methods and techniques available to *capable and well-resourced threat actors* and how they could be used systematically against network and information systems supporting your essential function(s).
A2.b.NA.3 You do not have a clearly defined set of threat assumptions.	**A2.b.PA.3** You anticipate what threat actors might target in network and information systems to cause an adverse impact to your essential function(s).	**A2.b.A.3** You use appropriate techniques to *develop an understanding* of network and information systems supporting your essential function(s) *from a threat actor's perspective*. You anticipate probable attack methods and techniques, targets and objectives and develop plausible scenarios.
A2.b.NA.4 You do not use your understanding of threat to inform your risk management decisions.	**A2.b.PA.4** Your understanding of threat is informed by common incidents.	**A2.b.A.4** You understand the different steps a capable and well-resourced threat actor would need to take to reach the probable target(s).
	A2.b.PA.5 You apply your understanding of threat to inform your risk management decision-making.	**A2.b.A.5** You identify and justify what measures can be used at each step to reduce the likelihood of the threat actor reaching the probable target(s) or achieving their objective(s).
		A2.b.A.6 You maintain a detailed understanding of current threats (e.g. by threat intelligence and proactive research).

		A2.b.A.7 You apply your detailed understanding of threat to inform your risk management decision-making.
		A2.b.A.8 You have documented the steps required to undertake detailed threat analysis.

IGP Ref	IGP Interpretation
A2.B.A.1	***[detailed threat analysis]*** You employ organisation-specific threat analysis (using frameworks such as MITRE ATT&CK or Cyber Kill Chain) to develop tailored threat models. This analysis should go beyond general industry trends to identify specific attacker objectives and the TTPs most likely to be employed against the CLF environment's unique technology stack and operational context.
A2.B.A.2	***[capable and well-resourced threat actors]*** This refers to sophisticated adversaries such as Advanced Persistent Threat (APT) groups and highly organised cyber-criminal organisations. These actors have a demonstrated capacity to overcome standard security controls, adapt tactics, techniques, and procedures (TTPs), and execute persistent, multi-stage attacks. This requires focusing threat analysis on protecting the entire attack surface and key supply chain elements from a systematic compromise.
A2.B.A.3	***[develop an understanding][from a threat actor's perspective]*** This covers the use of techniques (such as Attack Path Analysis or red-teaming exercises) to systematically map the environment as an adversary would. The result should be documented, plausible scenarios (e.g., loss of control, data exfiltration) detailing the TTPs a capable threat actor would use to reach the target(s) and outlining the defensive measures that can be deployed at each step.
A2.b.PA.1	***[common threats*]** Common threats are well-documented and broadly recognised adversarial TTPs, often linked to commodity malware, known attack campaigns, or generic social engineering attempts impacting multiple sectors. The analysis should focus on readily available, validated and authoritative threat intelligence sources (e.g., NCSC advisories, common CWE / CVEs).

IGP Ref	Examples of Evidence to support IGPs
A2.b.A.1	A formal Threat Intelligence Strategy document.
A2.b.A.1 / A2.b.A.8	Evidence that personnel conducting threat analysis are suitably qualified and experienced (e.g. training records, certifications, or CVs highlighting relevant sector experience).
A2.b.A.2	A formal Threat Assessment Document that includes assumptions on the range of threat actors and their likely Tactics, Techniques, and Procedures (TTPs).
A2.b.A.3	Documented Attack Path Analysis or a set of Plausible Attack Scenarios tailored to the Load Control environment.
A2.b.A.3	Reports from assurance activities, such as red team exercises, which were explicitly scoped using the developed threat models.
A2.b.A.4	Risk Register entries or change records showing where threat analysis has directly informed a specific security requirement or control change.
A2.b.A.5	Records demonstrating that your organisation participates in cross-sector information sharing forums.
A2.b.A.8	Documented methodology for detailed threat analysis and developing threat models (e.g., citing MITRE ATT&CK or Cyber Kill Chain frameworks).
A2.b.PA.1	Evidence of subscription or active membership to relevant threat intelligence feeds (e.g., NCSC CiSP access, MISP).

References and Further Guidance

- A.2 Risk management - NCSC.GOV.UK

• NCSC.GOV.UK: https://www.ncsc.gov.uk/guidance/risk-management-principles-and-guidance	
• MITRE ATT&CK Framework: Enterprise: https://attack.mitre.org/	
• NCSC CiSP (Cyber Security Information Sharing Partnership): https://www.ncsc.gov.uk/cisp/home	
• NIST CSF 2.0 Subcategory:	ID.RA-02, ID.RA-03, ID.RA-08, DE.AE-07
• ISO 27001/27002:2022 Control:	5.7, 5.38
• NIST SP 800-53 Rev. 5 Control:	RA-1, RA-3, RA-5, PM-15

9.4.4 A2.c Assurance

A2.c Assurance	
You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to the operation of network and information systems supporting your essential function(s)	
Not achieved: At least one of the following statements is true	Achieved: All the following statements are true
A2.c.NA.1 A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value.	**A2.c.A.1** You *validate* that the security measures in place to protect the network and information systems supporting your essential function(s) are effective and remain effective for the lifetime over which they are needed.
A2.c.NA.2 Assurance methods are applied without appreciation of their strengths and limitations.	**A2.c.A.2** You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of network and information systems supporting your essential function(s).
A2.c.NA.3 Assurance is assumed because there have been no known problems to date.	**A2.c.A.3** Your confidence in the security as it relates to your technology, people, and processes can be *justified to, and verified by, a third party.*
	A2.c.A.4 *Security deficiencies uncovered* by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.
	A2.c.A.5 The *methods used for assurance are reviewed* to ensure they are working as intended and remain the most appropriate method to use.

IGP Ref	IGP Interpretation

A2.c.A.1	***[validate]*** Validation of the technology, people and process that constitutes an organisations security measures requires:
	• **Technology** – You employ a mix of the following:
	  • maintenance of accurate configuration records and periodic documentation and system checks (at least annually) to ensure that devices are correctly configured in accordance with standard builds and physical security.
	  • vulnerability assessments (see contributing outcome A2.a)
	  • penetration testing.
	
	Your use of these validation techniques is cognisant of the risks associated with each and the relative importance of the security function provided by specific element being validated. Meaning that devices and services with a high degree of security functionality, such as boundary protection devices, will be subject to the full range of techniques.
	
	People – The organisation:
	  • preform personnel screenings.
	  • requires its people to undertake appropriate cyber security training periodically, and at least annually.
	  • may choose to employ human behavioural testing (e.g. simulated phishing emails) to reinforce training.
	
	Process – The organisation uses a mix of internal and in the case of Tier 1 external audits to validate the correct implementation of security processes.

A2.c.A.3	• ***[justified to, and verified by, a third party]***
	  • the organisation may choose to employ an independent auditor to verify the effectiveness of its security measures. Doing so may provide the organisation with confidence that the security measures are effective and may be taken into consideration during inspections.
	  • The organisation should be prepared to justify the effectiveness of its security measures during an inspection. The organisation should collate and archive its assurance and verification documentation in such a way that they can be used as examples of evidence during an inspection.

A2.c.A.4	• ***[security deficiencies uncovered]*** the organisation can provide evidence that recommendations made via assurance activities and findings made during validation activities have been recorded. These recommendations and findings have either been actioned, are in the process of being actioned, or have been refuted.
A2.c.A.5	• ***[methods used for assurance are reviewed]*** the organisation has evolved its assurance methods as its Security Management System has matured and become established. Initial assurance activity should be focused on ensuring that the processes employed are meeting their objectives. Later stage assurance activity should be focused on refining and optimising processes and checking that they are aligned to best practise.

IGP Ref	Examples of Evidence to support IGPs
A2.c.A.1	Asset registers in accordance with Contributing Outcome A3.
A2.c.A.1	Documented configuration management processes and records.
A2.c.A.1	Documented vulnerability management processes and records.
A2.c.A.1	Results of automated vulnerability scans (where appropriate).
A2.c.A.1	Results of penetration tests (where appropriate).
A2.c.A.1	Employee cyber security training plan and records.
A2.c.A.1	Results of any security relevant internal or external audits.
A2.c.A.3	Copies of reports commissioned from third parties (audit results, technical testing results).
A2.c.A.3	A suitable document repository, which is accessible by key members of staff, such that relevant evidence can be easily presented on request.
A2.c.A.4	Up to date configuration management records that demonstrate that recommendations and findings have been actioned.
A2.c.A.4	Up to date cyber improvement plans that demonstrate that those recommendations and findings with longer implementation timeframes have been programmed.
A2.c.A.5	Records (e.g. version records) demonstrating that the Security Management System is being periodically updated (at least annually) and improved.

References and Further Guidance	
• A.2 Risk management - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	ID.IM-01, ID.IM-02
• ISO 27001/27002:2022 Control:	5.35, 5.36, 8.29
• NIST SP 800-53 Rev. 5 Control:	CA-2, CA-7

9.5 Principle A3 Asset Management

9.5.1 Principle A3 Extended Guidance:

Principle A3: **Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).**

This establishes the fundamental asset visibility required for effective risk management (Principle A2). Adequate protection of the load control service is contingent upon a comprehensive understanding of every integral asset, as risks cannot be managed effectively against assets of which the organisation is not aware.

The scope of asset management must encompass the entire operational ecosystem necessary to deliver the service, spanning both traditional information technology and the specialised components used to monitor and control load. Effective implementation requires the organisation to move beyond simple equipment registers toward a managed, lifecycle-based process that provides a clear view of how assets are interconnected and supported.

For Load Control providers, the approach to asset management must account for the diverse nature of the distributed assets being managed:

- **Scope and Ownership:** A clear distinction must be made between assets under the provider's direct operational control and those that reside within the consumer or third-party domain. While domestic Energy Smart Appliances (ESAs) typically sit outside the direct management boundary, the infrastructure used to interface with them remains critical.
- **Operational Criticality:** For grid-scale operations, such as Virtual Power Plants or Grid scale BESS, asset management must reflect the increased systemic importance of the underlying industrial control and operational technology components.
- **Logical and Data Assets:** Asset management must extend to logical assets that are critical for the secure operation of the service. This includes sensitive data, software versions, and cryptographic material (such as keys and certificates) used for device authentication and secure communication across the Load Control ecosystem.
- **Interdependence and Lifecycle:** Managing assets supporting the essential function requires an understanding of their dependencies and their service life. For grid-scale infrastructure, this must account for the significant difference in lifecycle between physical plant assets and the software or control systems that manage them. This ensures that risks associated with aging, legacy, or obsolete components are identified and managed before they impact the security of the service.

A robust asset management process is the prerequisite for subsequent security measures, including vulnerability management, configuration control, and incident response. It provides the foundational visibility required to justify that security controls are correctly targeted and proportionate to the identified risks.

9.5.2 A3.a Asset Management

A3.a Asset Management	
Everything required to deliver, maintain or support network and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	
Not achieved: At least one of the following statements is true	Achieved: All the following statements are true

E1.a.NA.1 Inventories of assets relevant to the network and information systems supporting your essential function(s) are incomplete, non-existent, or inadequately detailed.	**E1.a.A.1** All assets *relevant to the secure operation* of network and information systems supporting your essential function(s) are *identified and inventoried (at a suitable level of detail).* The inventory is kept up to date.
E1.a.NA.2 Only certain domains or types of assets are documented and understood. Dependencies between assets are not understood (such as the dependencies between EIT, IoT and OT).	**E1.a.A.2** *Dependencies on supporting infrastructure* (e.g. power, cooling etc) are recognised and recorded.
E1.a.NA.3 Information assets, which could include personally identifiable information or other sensitive information, are stored for long periods of time with no clear business need or retention policy.	**E1.a.A.3** You have prioritised your assets according to their importance to the operation of network and information systems supporting your essential function(s)
E1.a.NA.4 Knowledge critical to the management, operation, or recovery of network and information systems supporting your essential function(s) is held by one or two key individuals with no succession plan.	**E1.a.A.4** You have assigned responsibility for managing all assets, including physical assets, relevant to the operation of network and information systems supporting your essential function(s).
E1.a.NA.5 Asset inventories are neglected and out of date.	**E1.a.A.5** Assets relevant to network and information systems supporting your essential function(s) are *managed with cyber security in mind throughout their lifecycle*, from creation through to eventual decommissioning or disposal.

IGP Ref	IGP Interpretation
A3.a.A.1	***[relevant to the secure operation]*** the asset inventory captures the following asset types: • the components of all systems and sub-systems named in your scope. This should specifically include any systems with the capability to exert load control, such as load control platforms and dispatch engines. • the sources of data required to operate, maintain and restore these systems and sub-systems. These could include manuals, configuration management records, device images. • the people and contract services required operate, maintain and restore the systems. People should include those with niche (or possibly unique) knowledge of your systems who would be impossible to replace at short notice, e.g. developers of bespoke applications on which your services rely. • all ancillary systems that are necessary to support the secure and reliable operation of the network and information systems (e.g. UPS, backup generation, cooling).
A3.a.A.1	***[identified and inventoried]*** the asset capture process is comprehensive, and you have a high degree of confidence that it is complete. You have used an appropriate range of tools and techniques to ensure completeness; these could include automated discovery tools and manual survey. The information is captured in a suitable format and is easily searchable, spreadsheets may prove to be adequate, however, larger organisations may wish to consider dedicated asset management solutions.

A3.a.A.1	***[suitable level of detail]*** a suitable level of detail is that which allows the organisation to manage the assets through life. Information is expected to include, but is not limited to: • the location of assets • a unique identifier • asset criticality relating to the assets' importance to the delivery of the essential function • asset criticality relating to the assets' importance to the delivery of network security. You should be able to filter for devices that provide security enhancing functionality, and devices on the network boundary that are externally accessible. This will allow you to ensure that these devices are appropriately configured and patched. • list of ancillary equipment required for maintenance and configuration • list of firmware, operating systems and application software, including End of Life (EOL) dates • details of known vulnerabilities/non-conformities against configuration management and patching policies. These vulnerabilities and non-conformities should be carried across to the risk register. • identify and document dependencies between assets to understand interconnection and assess potential security risks and impacts. For devices which are obsolete you have captured the following additional information (this information may be captured in the asset register, risk register, or vulnerabilities register – the choice of which will depend on your own processes): • list of the firmware, operating systems and application software that is obsolete • list of CVEs relevant to any software • risks of continued use of these devices • list of measures taken to reduce the likelihood and impact of compromise • details of the plans to upgrade, replace or remove obsolete devices.
A3.a.A.2	***[dependencies on supporting infrastructure]*** all dependencies are captured in the asset register and you can cross-reference these dependencies with risks you have identified under Principle E2 – Broader network and information systems resilience risks.
A3.a.A.5	***[managed with cyber security in mind throughout their life cycle]*** You make full use of your asset registers and configuration management databases as part of your cyber security management system. You ensure that: • asset registers are up to date • asset registers are regularly reviewed and audited and obsolete devices are identified • Obsolete devices are appropriately managed • routine cross-reference new Common Vulnerabilities and Exposures (CVEs) and supplier security advisories with the devices and software employed on your networks. When relevant CVEs/advisories are identified you are able to quickly locate affected devices and schedule the necessary patches. • the specification of security requirements for devices in the design and procurement processes (see B4.b) • the use of standardised secure device configurations, i.e. baseline/gold builds (see B4.b).

IGP Ref	Examples of Evidence to Support IGPs
A3.a.A.1	Comprehensive asset register.
A3.a.A.1	linkages between any vulnerabilities that are recorded/flagged in the asset register and the appropriate risk register and cyber improvement plan (if relevant).
A3.a.A.2	Risks relating to dependencies on supporting infrastructure have been recorded in the appropriate risk register.
A3.a.A.5	use of a method that allows for easy identification of devices that are obsolete (such as the use of date based conditional formatting in the asset).

A3.a.A.5	Configuration management and patching records that demonstrate that the necessary patching is taking place.
A3.a.A.5	evidence that the risks identified through good asset management (e.g. the identification of obsolete devices and devices that remain unpatched) have been transferred to the appropriate risk registers.

References and Further Guidance	
• A.3 Asset management - NCSC.GOV.UK	
• CISA: Asset Visibility and Vulnerability Management: https://www.cisa.gov/news-events/directives/bod-23-01-improving-asset-visibility-and-vulnerability-detection-federal-networks	
• CIS Controls (Inventory & Control): https://www.cisecurity.org/controls/inventory-and-control-of-software-assets	
• NIST CSF 2.0 Subcategory:	ID.AM-01, ID.AM-02, ID.AM-08
• ISO 27001/27002:2022 Control:	5.9, 5.10, 5.11
• NIST SP 800-53 Rev. 5 Control:	CM-8, SA-3

9.6 Principle A4 Supply Chain

9.6.1 Principle A4 Extended Guidance:

Principle A4: **The organisation understands and manages security risks to network and information systems supporting the operation of essential functions that arise as a result of dependencies on suppliers. This includes ensuring that appropriate measures are employed where third party services are used.**

This addresses the security risks that arise from dependencies on external suppliers. For load control services, the supply chain is often extensive and complex, involving cloud service providers, software developers, managed service providers, and hardware manufacturers. Effective supply chain management ensures that the security of the essential service is not compromised by the vulnerabilities or failings of a third party.

While technical and operational functions may be outsourced, accountability for the security of the essential function remains with the organisation. To manage these risks effectively, the strategy should focus on the following areas:

- **Supplier Visibility and Risk Assessment (A4.a):** Maintaining a comprehensive understanding of all suppliers that support the delivery of the load control service. This involves identifying direct suppliers and, where necessary, critical sub-contractors whose failure could impact the service. Risk assessments must consider the level of access a supplier has to the technology stack, the sensitivity of the data they handle, and the long-term viability of the supplier. This includes assessing the risk of a supplier going out of business or a manufacturer no longer being able to support critical components.
- **Security Requirements in Procurement (A4.b):** Ensuring that security is a core consideration throughout the procurement lifecycle. This means defining clear, proportionate security requirements in contracts and ensuring that these obligations are enforceable. These requirements should cover incident notification, the right to audit, and adherence to recognised security standards. Procurement strategies should also account for the risk of market exit or insolvency, ensuring that measures such as escrow agreements or secondary support arrangements are considered for critical infrastructure.
- **Continuous Assurance:** Moving beyond initial assessments toward a model of regular assurance. There should be processes to verify that suppliers are maintaining the agreed security standards throughout the life of the contract, particularly when there are significant changes to the service or the threat landscape.

Particular attention must be paid to the provenance and ongoing support of the software and hardware components that facilitate command-and-control functions. This ensures that the integrity of the wider

energy ecosystem is considered when managing third-party dependencies, particularly where those dependencies involve the long-term maintenance of operational infrastructure.

For grid-scale operations, supply chain risk management must explicitly address the challenges of legacy or unsupported assets where original equipment manufacturers or software vendors may no longer provide support or security updates.

9.6.2 A4.a Supply Chain

A4.a Supply Chain		
You understand and effectively manage the risks associated with suppliers to the security of network and information systems supporting the operation of your essential function(s).		
Not achieved:	**Partially Achieved**	**Achieved**
At least one of the following statements is true	All the following statements are true	All the following statements are true
A4.a.NA.1 You do not know what data belonging to you is held by suppliers, or how it is managed.	**A4.a.PA.1** You understand the *general risks* suppliers may pose to network and information systems supporting your essential function(s).	**A4.a.A.1** You have a *deep understanding* of your supply chain, including sub-contractors and the *wider risks* it faces.
A4.a.NA.2 Elements of the supply chain network and information systems supporting your essential function(s) are subcontracted and you have little or no visibility of the sub-contractors.	**A4.a.PA.2** You know the *extent of your supply chain* that supports network and information systems supporting your essential function(s)., including sub-contractors.	**A4.a.A.2** You consider factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub- contract and their *approach to cyber security*. This informs your risk assessment and procurement processes.
A4.a.NA.3 You have no understanding of which contracts are relevant and / or relevant contracts do not specify appropriate security obligations.	**A4.a.PA.3** Suppliers to network and information systems that support your essential function(s) can demonstrate appropriate and proportionate levels of cyber security within the context of common threats.	**A4.a.A.3** Your approach to supply chain risk management considers the risks to network and information systems supporting your essential function(s) arising from supply chain subversion by *capable and well-resourced threat actors.*
A4.a.NA.4 Suppliers have access to network and information systems supporting your essential function(s) that is unrestricted, not monitored or bypasses your own security controls.	**A4.a.PA.4** You understand which contracts are relevant and you *include appropriate security obligations* in relevant contracts.	**A4.a.A.4** Critical suppliers to network and information systems supporting your essential functions(s) can demonstrate appropriate and proportionate levels of cyber security within the context of capable and well-resourced threat actors.
	A4.a.PA.5 You are aware of all third-party connections and have *assurance* that they meet your organisation's security requirements.	**A4.a.A.5** You have confidence that information held by suppliers that is essential to the operation of network and information systems supporting your essential function(s) is *appropriately protected* from capable and well-resourced threat actors.

	A4.a.PA.6 Your approach to security incident management considers incidents that might arise in your supply chain.	**A4.a.A.6** You understand which contracts are relevant and you include *appropriate security obligations* in relevant contracts.
	A4.a.PA.7 You *have confidence* that information held by suppliers that is necessary for the operation of network and information systems supporting your essential function(s) is *appropriately protected* from *common threats*.	**A4.a.A.7** You have a *proactive approach to contract management* which may include a contract management plan for relevant contracts.
		A4.a.A.8 Customer / supplier ownership of *responsibilities* is laid out in contracts.
		A4.a.A.9 All network connections and *data sharing with third parties are managed effectively* and proportionately.
		A4.a.A.10 When appropriate, your incident management process and that of your suppliers provide *mutual support* in the resolution of incidents.

IGP Ref	IGP Interpretation
A4.a.A.1	***[deep understanding]*** you have mapped and documented your supply chain; you update this documentation as new information becomes available (e.g. through contract documentation and supplier engagements) and can demonstrate that your understanding of your supply chain continually evolves. Your approach to understanding your supply chain is risk-based, meaning that you have a greater level of understanding, control and oversight regarding those elements of your supply chain that you assess as presenting the greatest risk.
A4.a.A.1	***[wider risks]*** wider risks refers to external or indirect factors that, while not directly related to cyber security risks, could have significant impact on the performance of your networks and systems or on the procurement of services required to support your operations. Examples of such risks include insolvency, geopolitical restrictions and sanction lists.
A4.a.A.2	***[approach to cyber security]*** You should evaluate a supplier's genuine maturity, covering their security governance structure, technical controls (e.g., patching, logging), security culture, and adherence to relevant industry standards (e.g., ISO 27001, Cyber Essentials Plus, ETSI EN 303 645) as it relates to the products or services they provide to your essential function.
A4.a.A.3	***[capable and well-resourced threat actors]*** Assurance against this level of threat requires the supplier to demonstrate robust security controls designed to resist Advanced Persistent Threats (APTs), state-sponsored adversaries, and sophisticated cyber-criminal groups.
A4.a.A.7	***[proactive approach to contract management]*** you monitor your suppliers to ensure that they are meeting their security obligations. This monitoring could take the form of engagement meetings or could extend to audits.
A4.a.A.8	***[responsibilities]*** you have clearly specified your requirements for security properties of devices and services in your procurement documentation. You have confirmed that your supplier understands the specification. Where necessary, the contract details which party is responsible for installing, configuring, testing and maintaining the security functionality of devices.

A4.a.A.9	***[data sharing with third parties is managed effectively]*** • You maintain Interface Control Documents (ICDs) which detail all network connections with third parties. Network connections could include, but are not limited to, vendor access for remote support and maintenance, customers, outsourced service providers, electricity companies. • You have risk assessed each network connection with third parties and have employed appropriate controls. • You share the minimum amount of data required for the third party to meet their obligations and maintain an Information Asset Register detailing which information is held by which suppliers.
A4.a.A.10	***[mutual support]*** you understand the circumstances in which breaches of your security will impact your suppliers and the circumstances in which breaches of your supplier's security will impact your essential service. You have agreements in place to inform each other in the event of these circumstances, and where necessary, will share resources with the aim of minimising the impact to all parties.
A4.a.PA.1	***[general risks]*** You have conducted an assessment in which you have: • identified the suppliers whose products or services could have an impact on your essential service. • categorised your suppliers by type (e.g. OEM, Systems Integrator, Software Supplier, Cloud Service Provider) and considered the nature of the risks (e.g. introduction of malware, deliberate misconfiguration) associated with each type.
A4.a.PA.2	***[extent of your supply chain]*** you have conducted an assessment in which you have identified the suppliers whose products or services could have an impact on your essential service.
A4.a.PA.3	***[include appropriate security obligations]*** you have created a standard set of security clauses for inclusion within contractual agreements. You select the appropriate security obligations for all new contracts, at contract renewal for existing contracts and insert them as required.
A4.a.PA.4	***[appropriate security obligations]*** you have created a standard set of security clauses for inclusion within contractual agreements. You select the appropriate security obligations for all new contracts and insert them as required.
A4.a.PA.5	***[assurance]*** you recognise that third-party connections to your systems should be carefully managed and assured due to the risk that they pose. You are aware of the specific security controls that your suppliers have put in manage these risks and you have processes in place to ensure that your suppliers are maintaining these controls and abiding by all relevant processes.
A4.a.PA.7	***[common threats]*** In this context, common threats are equivalent to the widely recognised known and well understood threats defined in A2.a. This demonstrates that suppliers can protect against general, unsophisticated attack vectors, such as phishing, commodity malware, and the exploitation of publicly disclosed, unpatched vulnerabilities.
A4.a.PA.7	***[have confidence]*** you have agreements in place with all suppliers with which you share information: • The agreements detail the measures that suppliers will take to secure your data. Ideally these agreements will be contractual, but they may also be best endeavours up until the point at which the contract is re- negotiated. • The security measures that your suppliers are taking is appropriate for the nature of the information shared and you have assurances that the measures are being implemented in accordance with your agreement. • These measures may include (but are not limited to), requirements for suppliers to have achieved an appropriate cyber security standard (such as cyber-essentials plus, ISO 27001 etc). • Instances where there is not the confidence should be recorded in the risk register and proactively managed.
A4.a.PA.7	***[appropriately protected]*** the security measures that your suppliers are taking is appropriate for the nature of the information shared. You require those suppliers that hold your most sensitive data and those directly involved in load control to meet more demanding cyber security requirements than those who hold less sensitive data sets.

IGP Ref	Examples of Evidence to support IGPs
A4.a.A.1	A comprehensive supply chain risk assessment which assesses the specific cyber risks associated with each of your suppliers.
A4.a.A.4	Documentation of the minimum security standards required for critical suppliers, including evidence (e.g., certification, audit reports) of supplier compliance with those standards against capable and well-resourced threat actors.
A4.a.A.4	Records of assurance reviews focusing on the supplier's governance, culture, and security controls to evaluate their genuine approach to cyber security.
A4.a.A.5	information asset register detailing which suppliers are holding key information relating to your network and information systems.
A4.a.A.5	Measures to assure the cyber security of key suppliers. These measures may include use of questionnaires, mandating minimum security standards for suppliers (such as Cyber Essentials Plus), use of a supply chain cyber risk scoring service.
A4.a.A.6 A4.a.PA.3 A4.a.PA.7	A standard set of security clauses that relate to custody of sensitive information, including load control information.
A4.a.A.7 A4.a.PA.3 A4.a.PA.7	Evidence that these clauses have been included in recently issued contracts.
A4.a.A.8	Supplier contracts with clearly specified security requirements.
A4.a.A.9	Network diagrams which clearly indicate information exchanges which cross the organisations network boundaries and the security controls that are in place.
A4.a.A.9	Interface Control Documents (ICDs) which document the nature of the data that is being shared with third parties
A4.a.A.10	Supplier contracts with clearly specified incident management responsibilities.
A4.a.PA.1 A4.a.PA.2	A register of suppliers, categorised by type and providing details of the nature of the risks associated with each.
A4.a.PA.3	An assessment of the contracts of all suppliers on your supplier register which identifies the contracts that are missing key security clauses, and opportunities to update them (e.g. for inclusion at contract re-let).
A4.a.PA.4	The register of suppliers should clearly identify which suppliers have remote access to your systems. The register should also include the controls that your suppliers and your own organisation have put in place to mitigate the risks. You can demonstrate that you routinely, at least annually or if there is a material change to the supply arrangements and/or supplier relationship, liaise with these suppliers and have mechanisms in place (these may include audit checks, connection logs) to ensure that the remote connections are being managed in accordance with the agreement between your organisation and your supplier. Any residual risks should be proactively managed.

References and Further Guidance	
• A.4 Supply Chain - NCSC.GOV.UK	
• How to assess and gain confidence in your supply chain... - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	GV.SC-05, GV.SC-07
• ISO 27001/27002:2022 Control:	5.19-5.22
• NIST SP 800-53 Rev. 5 Control:	SA-12, SR-1

9.6.3 A4.b Secure Software Development and Support

A4.b Secure Software Development and Support		
You actively maximise the use of secure and supported software, whether developed internally or sourced externally, within network and information systems supporting the operation of your essential function(s).		
Not achieved:	**Partially Achieved**	**Achieved**
At least one of the following statements is true	All the following statements are true	All the following statements are true
A4.b.NA.1 Your software supplier(s) is unaware of the composition and provenance of software provided to you.	**A4.b.PA.1** Your software supplier leverages *secure development principles and practices*.	**A4.b.A.1** Your software supplier(s) leverages an *established secure software development framework* (e.g. NIST Secure Software Development Framework (SSDF), Microsoft Secure Development Lifecycle (SDL)).
A4.b.NA.2 Software, including updates and patches, undergoes little to no testing.	**A4.b.PA.2** Your software supplier(s) can demonstrate a limited understanding of the *composition and provenance of software* provided to you.	**A4.b.A.2** Your software supplier can demonstrate a thorough understanding of the composition and provenance of software provided to you, including any third-party components used in the development of that software, and those components are being monitored for new vulnerabilities throughout the lifespan of the product.
A4.b.NA.3 Updates and patches often introduce new problems or fail to address existing issues.	**A4.b.PA.3** You consider the *security of environments* (e.g. development, test and production), including source code and repositories, used in the production of software to be *appropriate and proportionate within the context of common threats*.	**A4.b.A.3** You consider the *security of environments* (e.g. development, test, and production), including source code and repositories, used in the production of software to be appropriate and proportionate within the context of *capable and well-resourced threat actors*.
A4.b.NA.4 Vulnerabilities are discovered in software despite the negligible difficulty of implementing mitigations.	**A4.b.PA.4** The *testing regime* uses a range of different approaches (e.g. static and dynamic analysis, unit and integration testing and point in time assessments) that verify all aspects of the development lifecycle covering both functional and non-functional testing.	**A4.b.A.4** The software development lifecycle is informed by a detailed and up to date understanding of threat and applies appropriate techniques, such as threat modelling, to identify and assess potential vulnerabilities and attack vectors.
	A4.b.PA.5 You have arrangements in place with your software supplier to receive timely security updates, patches and notifications.	**A4.b.A.5** You can *attest to the authenticity and integrity of software*, including updates and patches.
	A4.b.PA.6 Software, including updates and patches, is obtained from your supplier(s) via secure channels.	

	A4.b.PA.7 Your software supplier(s) has processes in place to identify, report and mitigate security vulnerabilities.	
	A4.b.PA.8 You have arrangements in place with your software supplier to be notified of any significant events that may adversely impact network and information systems supporting your essential function(s).	
	A4.b.PA.9 If open-source software is used, you have taken appropriate and proportionate steps to establish and maintain sufficient confidence in its security for its use.	
	A4.b.PA.10 You have appropriate support and maintenance arrangements in place.	

IGP Ref	IGP Interpretation
A4.b.A.1	***[established secure software development framework]*** This demonstrates formal process maturity and includes adherence to frameworks such as, but not limited to, the NIST Secure Software Development Framework (SSDF), the Microsoft Security Development Lifecycle (SDL), or relevant controls derived from OWASP SAMM.
A4.b.A.3 A4.b.PA.3	***[security of environments]*** The security for all environments should be segmented and proportionate to the data criticality. This requires using separate authentication/access controls, enforcing least privilege for developers, and preventing production data from being used in lower, less-secured environments unless adequately anonymised or tokenised.
A4.b.A.4	***[capable and well-resourced threat actors]*** Threats posed by sophisticated groups such as State Actors and Advanced Persistent Threats (APTs), as well as highly organised Cyber-Criminal Groups. In the context of the supply chain, this requires securing development and testing environments against deliberate, targeted compromise (supply chain subversion) to inject malicious code into the final product.
A4.b.A.5	***[attest the authenticity and integrity of software]*** This requires using cryptographic signing mechanisms (e.g., code signing) for all production software, updates, and patches to verify that the software delivered to the operational environment has originated from a trusted source and has not been tampered with since it was built and approved.
A4.b.PA.1	***[secure development principles and practices]*** This includes foundational practices such as using secure coding standards, performing peer code reviews for security defects, applying the principle of least privilege in application design, and ensuring sensitive data is handled securely throughout the development and testing process.
A4.b.PA.2	***[composition and provenance of software]*** This requires detailed knowledge of the software's components, which is typically demonstrated by maintaining a Software Bill of Materials (SBOM) that lists all internal, external, and third-party commercial or open-source libraries. Provenance refers to the auditable record of the software's origin, build, and integrity verification through the pipeline.

A4.b.PA.3	***[appropriate and proportionate within the context of common threats]*** For development environments, this means securing systems sufficiently against opportunistic threats like phishing, commodity malware, and general misconfiguration, focusing on controls such as strong authentication, basic network segregation, and anti-malware solutions.
A4.b.PA.4	***[testing regime]*** An effective testing regime should include a mix of the following: Static Application Security Testing (SAST) on source code, Dynamic Application Security Testing (DAST) on running applications, penetration testing, and security regression testing to verify fixes for previously identified vulnerabilities.

IGP Ref	Examples of Evidence to support IGPs
A4.b.A.1	A documented Secure Software Development Lifecycle (SDLC) Policy or Framework (e.g., NIST SSDF or Microsoft SDL), detailing security gates at every phase.
A4.b.A.1	Evidence of a vulnerability disclosure program for software and the associated records demonstrating timely mitigation of identified flaws.
A4.b.A.1	Records from security reviews that specifically focus on assessing the supplier's approach to cyber security (A4.a) for software development.
A4.b.A.5	Requirements or contractual clauses mandating the supply of a Software Bill of Materials (SBOM) to verify software composition and provenance.
A4.b.A.5	Policy documents and technical configurations proving the implementation of cryptographic signing mechanisms (code signing) for all production software, updates, and patches.
A4.b.PA.1	Assurance reports from suppliers confirming the segregation and security controls (e.g., access lists, strong authentication) within their development, test, and production environments.
A4.b.PA.1	Documentation of the secure configurations and least privilege access controls applied to the build servers, code repositories, and developer workstations.
A4.b.PA.4	Records of security testing activities integrated into the continuous integration/continuous delivery (CI/CD) pipeline, including SAST (Static Analysis) and DAST (Dynamic Analysis) results.

References and Further Guidance

- A.4 Supply Chain - NCSC.GOV.UK
- Secure software development - NCSC.GOV.UK: https://www.ncsc.gov.uk/collection/secure-development
- NIST Secure Software Development Framework (SSDF): https://csrc.nist.gov/projects/ssdf
- OWASP Software Assurance Maturity Model (SAMM): https://owasp.org/www-project-samm/
- OWASP Top Ten (for secure coding standards): https://owasp.org/www-project-top-ten/

• NIST CSF 2.0 Subcategory:	PR.SD-01, PR.SD-02, PR.DS-10
• ISO 27001/27002:2022 Control:	8.27, 8.28, 8.29
• NIST SP 800-53 Rev. 5 Control:	SA-3, SA-11, SA-15

10 Objective B: Protecting Against Cyber Attack

10.1 CAF Objective B Expected Outcome.

Proportionate security measures are in place to protect the network and information systems supporting essential functions from cyber-attack.

10.2 Objective B Extended Guidance:

Objective B is the practical implementation of the risk management activities established in Objective A. While Objective A focuses on understanding and planning, Objective B is the stage where the organisation builds and operates its defences.

The core requirement of this objective is the implementation of appropriate and proportionate technical and procedural controls. For a load control provider, this entails securing a diverse and distributed ecosystem that includes central load control platforms, consumer applications, and sensitive data flows, while managing the security of the interfaces with in-scope ESAs, whether those connections are direct or facilitated via third party APIs.

As established in the preceding chapters, the concept of proportionality is fundamental. The CAF Objective B defines the specific expected outcomes that provide a robust and essential foundation for the service. The primary goal is to ensure that all implemented security measures are demonstrably effective against the specific threats and vulnerabilities identified during the risk management process in Objective A.

This requires the organisation to ensure that its protective controls are not merely present, but are correctly configured, maintained, and consistently applied across the full technical stack supporting the load control service.

10.3 Principle B1: Service Protection Policies, Processes and Procedures

10.3.1 Principle B1 Extended Guidance:

This first principle within Objective B acts as the bridge between governance and technical execution. It ensures that protective security measures are guided by formally documented and consistently applied policies, processes, and procedures. This principle provides the foundational framework for satisfying the requirements of the NIS Regulations, specifically Regulation 10(1) and 10(2), alongside relevant Licence Conditions.

Principle B1 focuses on the development and implementation of a suite of cyber security policies that define the organisation's approach to securing its network and information systems. To ensure these policies are appropriate and proportionate, the strategy should account for the specific nature of the load control service being provided:

- **Policy and Process Development (B1.a):** A comprehensive set of policies must be documented from the outset. For providers managing grid-scale or industrial assets, these policies should be aligned with the National Energy Security Strategy and must be tailored to address "Cyber-Physical" risks to ensure technical security does not override operational safety or physical integrity. For providers focused on the domestic market, the policy framework should prioritise the security of aggregate load manipulation and the protection of consumer data and privacy.
- **Policy and Process Implementation (B1.b):** This addresses the need to fully embed processes across the organisation. Effective implementation involves moving beyond simple monitoring of policy compliance toward a formal evaluation of the security effectiveness of all policies. This ensures they

are deeply integrated across the business and that any deviations are addressed promptly to maintain the integrity of the essential service.

- **Vulnerability Disclosure Policy:** In line with sectoral expectations and NCSC guidance, the policy framework should include a clear and accessible vulnerability disclosure process. This is particularly relevant for providers with public-facing interfaces or consumer applications, as it allows external researchers and stakeholders to report identified flaws in a controlled manner, ensuring the organisation can remediate vulnerabilities before they can be exploited.
- **Continuous Review and Evolution:** Effective policies are not static but must be regularly reviewed and updated to reflect changes in the technical architecture, the threat landscape, and the organisation's risk appetite. This evolution ensures that the defensive posture remains effective against increasingly sophisticated attack methods and shifting sectoral requirements.

The implementation of these policies should be supported by clear procedures that provide step by step guidance on how to meet the required security standards. Regular training and awareness programmes ensure that all personnel understand their responsibilities and have the necessary skills to follow the defined processes, providing the necessary assurance to the Competent Authority.

10.3.2 B1.a Policy & Process Development

B1.a Policy & Process Development		
You have developed and continue to improve a set of cyber security and resilience policies, processes and procedures that manage and mitigate the risk of adverse impact to network and information systems supporting your essential function(s).		
Not achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
B1.a.NA.1 Your policies, processes and procedures are absent or incomplete.	**B1.a.PA.1** Your policies, processes and procedures document your *overarching security governance* and risk management approach, technical security practice and *specific regulatory compliance.*	**B1.a.A.1** You *fully document* your *overarching security governance* and risk management approach, technical security practice and *specific regulatory compliance*.
B1.a.NA.2 Policies, processes and procedures are not applied universally or consistently.	**B1.a.PA.2** You review and update policies, processes and procedures in response to major cyber security incidents.	**B1.a.A.2** Cyber security is integrated and embedded throughout policies, processes and procedures and key performance indicators are reported to your executive management.
B1.a.NA.3 People often or routinely circumvent policies, processes and procedures to achieve business objectives.		**B1.a.A.3** Your organisation's policies, processes and procedures are developed to be *practical, usable and appropriate* to *mitigate the risk of adverse impact* to network and information systems supporting your essential function(s).
B1.a.NA.4 Your organisation's security governance and risk management approach has no bearing on your policies, processes and procedures.		**B1.a.A.4** Policies, processes and procedures that *rely on user behaviour* are practical, appropriate and achievable.

B1.a.NA.5 System security is totally reliant on users' careful and consistent application of manual security processes.		**B1.a.A.5** You review and update policies, processes and procedures at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident.
B1.a.NA.6 Policies, processes and procedures have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period.		**B1.a.A.6** Any changes to the essential function(s) or the threat it faces triggers a review of policies, processes and procedures.
B1.a.NA.7 Policies, processes and procedures are not readily available to staff, too detailed to remember, or too hard to understand.		**B1.a.A.7** Your systems are designed so that they *remain secure* even when user security policies, processes and procedures are not always followed.

IGP Ref	IGP Interpretation
B1.a.A.1	***[fully document]*** you have a suite of documentation that describe the policies, processes and procedures you employ as part of your security management system. This documentation is easily accessible and is used by your security practitioners to guide their security related activities.
B1.a.A.1 B1.a.PA.1	***[overarching security governance]*** your suite of documentation covers cyber, physical and personnel security and describes how these 3 pillars integrate to implement a holistic security system.
B1.a.A.1	***[specific regulatory compliance]*** you can map your policies and processes to specific CAF contributing outcomes. Your policies and processes include registers and logs that allow you to demonstrate that you are actively using them to deliver the relevant security outcomes. Relevant registers and logs are archived and provide the evidence you require to demonstrate that your security management is both appropriate and proportionate.
B1.a.A.3	***[practical, usable and appropriate]*** • if you have used policy and process templates that you have found on-line, you have tailored them such that they are relevant to your operating context. Meaning that they consider the specific hardware, software, and support contracts that you employ. • Your policies and processes are sufficiently thorough to meet the desired security outcome, without being so onerous as to make them unrealistic.
B1.a.A.3	***[mitigate the risk of adverse impact]*** This reinforces that policies are not simply compliance documents but should be explicitly designed and evaluated based on their effectiveness in demonstrably reducing the likelihood and impact of the security risks identified in Objective A.
B1.a.A.4	***[rely on user behaviour]*** In instances where your processes are dependent on human behaviour, it should be reasonable to assume that those behaviours will be adhered to by staff. It is unreasonable to claim that security outcomes are being met through cumbersome processes that are easily circumvented.

B1.a.A.7	***[remain secure]*** • This indicator addresses the risk that policies reliant on human behaviour can be circumvented. To ensure systems remain secure, an organisation should therefore implement a programme of assurance to verify that its policies and processes are being followed effectively. This moves beyond passive, layered controls and involves actively looking for evidence of compliance. • This assurance programme should include a range of appropriate and proportionate activities, such as technically monitoring for policy violations (e.g., credential sharing), conducting management-led audits of high-risk processes, and using controlled tests (like phishing simulations) to validate the effectiveness of security awareness training. By implementing such a programme, an organisation can provide robust evidence that its systems are designed to remain secure, even when faced with human error.

IGP Ref	Examples of Evidence to support IGPs
B1.a.A.1	A suite of up-to-date policy, process and procedures that combine to form a security management system. This documentation should be owned by suitably qualified and trained individuals and should be subject to periodic (at least annually) review and update.
B1.a.A.1	Elements of this suite should address cyber, physical and personnel security.
B1.a.A.1	A complete set of up-to-date registers and logs that evidence the implementation of your policies and procedures (e.g. risk registers with records of amendments / updates).
B1.a.A.3	A set of policy and processes that reference the specifics of your operating context.
B1.a.A.3 B1.a.A.4	A set of logs and registers associated with each of your processes that evidence that they are being thoroughly implemented.

References and Further Guidance	
• B.1 Service protection policies and processes - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	GV.PO-01, GV.PO-02
• ISO 27001/27002:2022 Control:	5.1, 5.37
• NIST SP 800-53 Rev. 5 Control:	PL-1, AC-1

10.3.3 B1.b Policy and Process Implementation

B1.b Policy and Process Implementation		
You have successfully implemented your security policies, processes and procedures and can demonstrate the security benefits achieved.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B1.b.NA.1 Policies, processes and procedures are ignored or only partially followed.	**B1.b.PA.1** *Most of your policies, processes and procedures are followed* and their *application is monitored*.	**B1.b.A.1** All your *policies, processes and procedures* are followed, their *correct application* and security *effectiveness* is evaluated.

B1.b.NA.2 How your policies, processes and procedures support the resilience of your essential function(s) is not well understood.	**B1.b.PA.2** *Your policies, processes and procedures are integrated with other organisational policies*, processes and procedures, including *HR assessments of individuals' trustworthiness.*	**B1.b.A.2** *Your policies, processes and procedures are integrated with other organisational policies*, processes and procedures, *including HR assessments of individuals' trustworthiness*.
B1.b.NA.3 Staff are unaware of their responsibilities under your policies, processes and procedures.	**B1.b.PA.3** *All staff are aware of their responsibilities* under your policies, processes and procedures	**B1.b.A.3** Your policies, processes and procedures are effectively and appropriately communicated across all levels of the organisation resulting in good staff awareness of their responsibilities.
B1.b.NA.4 You do not attempt to detect breaches of policies, processes and procedures.	**B1.b.PA.4** All breaches of policies, processes and procedures with the potential to adversely impact the essential function(s) are fully investigated. Other *breaches are tracked, assessed for trends* and action is taken to understand and address.	**B1.b.A.4** *Appropriate action* is taken to address all breaches of policies, processes and procedures with potential to adversely impact the essential function(s) including *aggregated breaches.*
B1.b.NA.5 Policies, processes and procedures lack integration with other organisational policies, processes and procedures.		
B1.b.NA.6 Your policies, processes and procedures are not well communicated across your organisation.		

IGP Ref	IGP Interpretation
B1.b.A.1	***[policies and processes are followed] [correct application]*** You can measure the extent to which your policies and processes are being followed and you maintain records of instances of policy violations. For example, you maintain records of Acceptable Use Policy (AUP) violations (e.g. instances of shared passwords) and unauthorised use of removable media.
B1.b.A.1	***[effectiveness]*** You review your policies and processes to ensure that they continue to contribute to the relevant security outcomes. For example, your patching status gives you a clear understanding of how effective your patching policy is being implemented.
B1.b.A.2 B1.b.PA.2	***[policies and processes are integrated with other organisational policies]*** you have identified instances where wider business processes can be integrated with security specific processes, thereby improving their effectiveness. This is particularly relevant for ESA environments where Identity and Access Management (IdAM) controls are likely to be distinct from the enterprise IdAM enterprise controls. Examples include, but are not limited to: • HR notify the appropriate IdAM system manager for all Joiner, Mover and Leaver (JML) events. • System permissions are reviewed in the event of disciplinary action.
B1.b.A.2 B1.b.PA.2	***[HR assessments of individual's trustworthiness]*** you follow the guidance in the following documentation: • BS7858 – Security screening of individuals employed in a security environment. Code of Practice (or local equivalents)

B1.b.A.4	***[Appropriate action]*** In the event of a security policy breach you consider the following actions: • completion of Post Incident Reviews • provision of additional training to prevent further breaches • commencement of disciplinary action where breaches are sufficiently serious, or repeated.
B1.b.A.4	***[aggregated breaches]*** You periodically review (at least annually) the set of all breaches/policy violations with a view to identifying patterns and determining whether individual breaches may be indicators of a more sophisticated, longer-term, and multi-stage campaign.
B1.b.PA.1	***[Most of your policies and processes are followed]*** you are confident that more than half of your policies and processes are being fully implemented. However, because many of your processes and policies are new, you are finding that they require more time to bed-in before you can be confident that they are being correctly applied and effective. You are actively taking steps to improve standards of application where necessary
B1.b.PA.1	***[application is monitored]*** you can measure the extent to which your policies and processes are being followed and you maintain records of instances of policy violations.
B1.b.PA.3	***[All staff are aware of their responsibilities]*** you ensure that all your staff receive adequate training, such that they are aware of all security policies and processes that are relevant to their roles, and they have the skills to be able to implement those policies and processes.
B1.b.PA.4	***[breaches are tracked and assessed for trends]*** you can measure the extent to which your policies and processes are being followed and you maintain records of instances of policy violations.

IGP Ref	Examples of Evidence to support IGPs
B1.b.A.1 B1.b.PA.1 B1.b.PA.4	A register of policy and process violations the records of remedial actions.
B1.b.A.1	A complete set of up-to-date logs and registers that evidence the implementation of your policies and procedures (e.g. risk registers with records of amendments/updates).
B1.b.A.1	A set of status reports/dashboards that are used to manage and monitor your key security processes.
B1.b.A.2 B1.b.PA.2	A communication chain between the relevant department and IdAM administrators (for both IT and IoT systems) detailing JML events.
B1.b.A.2 B1.b.PA.2	Details of the processes used to implement BS7858
B1.b.A.4	A central log of all process and policy violations and breaches.
B1.b.A.4	Any completed post incident reviews.
B1.b.PA.1 B1.b.PA.4	Details of actions taken to improve levels of policy compliance.
B1.b.PA.3	A security management system training plan.
B1.b.PA.3	Personnel records demonstrating that training has been satisfactorily completed.

References and Further Guidance	
• B.1 Service protection policies and processes - NCSC.GOV.UK	
• BSI BS 7858:2019 - Screening of individuals working in a secure environment. Code of practice	
• NIST CSF 2.0 Subcategory:	GV.OV-03, ID.IM-03
• ISO 27001/27002:2022 Control:	5.36, 6.3
• NIST SP 800-53 Rev. 5 Control:	CA-1, AT-1

10.4 Principle B2: Identity and Access Control

10.4.1 Principle B2 Extended Guidance:

Principle B2 is a critical protective measure, ensuring that only verified and authorised users and systems can interact with the load control service. In this context, robust access control is paramount for preventing unauthorised command and control of the system and protecting sensitive consumer data. This principle governs who gets access, what they can access, and how that access is managed and monitored throughout its lifecycle, whether for an interactive user or a system-to-system API.

To manage identity and access effectively, the organisation should focus on the following strategic areas:

- **Identity Verification and IdAM (B2.a and B2.d):** Establishing robust procedures to verify the identity of all users and systems before granting access. This involves a formal Identity and Access Management (IdAM) framework that manages the lifecycle of identities, ensuring that access rights are granted based on the principle of least privilege and are promptly revoked when no longer required.
- **Device Management (B2.b):** This outcome focuses on the requirement to have full trust and visibility in the devices used to access and manage the networks, information systems, and data supporting the load control service. The specific scope of managed devices is determined through the scoping exercise, targeting those assets used by personnel or automated systems to administer the platform or issue operational commands. By ensuring these management devices are known and securely configured, the organisation prevents them from being used as a vector for unauthorised interaction with the essential function. There is no expectation for device-level management of consumer-owned hardware under this principle.
- **Privileged User Management (B2.c):** Given the potential impact of unauthorised command and control, the management of privileged access requires heightened oversight. This includes implementing strict controls over accounts with administrative rights, ensuring that privileged activities are performed through secure channels, and maintaining comprehensive logs of all privileged actions.
- **Proportionate Authentication and Auditing:** The level of authentication, such as the use of Multi-Factor Authentication (MFA), and the depth of log correlation and auditing should be determined by the organisation's risk assessment. As the scale of the service or the threat landscape evolves, the implementation of more advanced authentication and monitoring techniques ensures that the security posture remains effective against increasingly sophisticated attacks.

A well-implemented identity and access control framework ensures that the organisation can demonstrate that its systems are accessed only by legitimate entities and that all interactions with the load control platform are accountable and authorised.

10.4.2 B2.a Identity Verification, Authentication

B2.a Identity Verification, Authentication		
You robustly verify, authenticate and authorise access to network and information systems supporting your essential function(s).		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.

B2.a.NA.1 Initial identity verification is not robust enough to provide an acceptable level of confidence of a user's identity profile.	**B2.a.PA.1** Your *process of initial identity verification* is robust enough to provide a reasonable level of confidence of a user's *identity profile* before allowing an authorised user access to network and information systems that support your essential function(s).	**B2.a.A.1** Your *process of initial identity verification* is robust enough to provide a high level of confidence of a user's *identity profile* before allowing an authorised user access to network and information systems that support your essential function(s).
B2.a.NA.2 Authorised users and systems with access to networks or information systems on which your essential function(s) depends cannot be individually identified.	**B2.a.PA.2** All authorised users and systems with access to network and information systems supporting your essential function(s) are individually identified and authenticated.	**B2.a.A.2** Only *authorised and individually authenticated* users can *physically access* and *logically connect* to your network or information systems on which your essential function(s) depends.
B2.a.NA.3 Unauthorised individuals or devices can access your network or information systems on which your essential function(s) depends.	**B2.a.PA.3** The number of authorised users and systems that have access to network and information systems is *limited to the minimum necessary* to support your essential function(s).	**B2.a.A.3** The number of authorised users and systems that have access to network and information systems is *limited to the minimum necessary* to support your essential function(s).
B2.a.NA.4 The number of authorised users and systems that have access to your network and information systems are not limited to the minimum necessary.	**B2.a.PA.4** You use *additional strong authentication mechanisms*, such as multi-factor authentication (MFA), for *privileged access* to all network and information systems that operate or support your essential function(s).	**B2.a.A.4** You use *additional strong authentication mechanisms*, such as multi-factor (MFA), for all user access, *including remote access*, to all network and information systems that operate or support your essential function(s).
B2.a.NA.5 Your approach to authenticating users, devices and systems does not follow up to date best practice.	**B2.a.PA.5** You individually authenticate and authorise all remote access to all your network and information systems that support your essential function(s).	**B2.a.A.5** The list of users and systems with access to network and information systems supporting and delivering the essential function(s) is reviewed on a regular basis, at least every six months.
	B2.a.PA.6 The list of users and systems with access to network and information systems supporting and delivering the essential function(s) is reviewed on a regular basis, at least annually.	**B2.a.A.6** Your approach to authenticating users, devices and systems follows up to date best practice.
	B2.a.PA.7 Your approach to authenticating users, devices and systems follows up to date best practice.	

IGP Ref	IGP Interpretation
B2.a.A.1 B2.a.PA.1	***[process of initial identity verification]*** your pre-employment checks are sufficient to establish the identity of your employees.

B2.a.A.1 B2.a.PA.1	***[identity profile]*** your pre-employment check policy specifies the identity profile required for each role. The identity profile relates to the level of confidence you require in an individual's declared identity, for example Government's identify profile guidance. You are not required to follow the Government's identity profile guidance prescriptively, however, you should be able to demonstrate that the identity profiles you use are appropriate to the level of access that you are granting to your systems.
B2.a.A.2	***[authorised and individually authenticated]*** You understand, and have documented, which roles (and associated individuals) are authorised to access each system. Wherever feasible, your systems require that users are individually authenticated.
B2.a.A.2	***[physically access]*** your physical security management system has been designed to restrict physical access to your networks and information systems. Your physical security measures have been designed to complement your logical access controls. For example, enhanced physical access controls are employed to limit access to your most sensitive systems.
B2.a.A.2	***[logically connect]*** your network and information systems all have an appropriate authentication mechanism for both local and remote access.
B2.a.A.3 B2.a.PA.3	***[limited to the minimum necessary]*** you enforce the principle of least privilege, and you actively manage your Access Control Lists in response to Joiner, Mover and Leaver events (see B1.b)
B2.a.A.4 B2.a.PA.4	***[Additional Strong Authentication][for privileged access]*** This requires the use of multi-factor methods that are demonstrably resilient against modern attack techniques (e.g., phishing, MFA prompt bombing). Strong authentication should prioritise technologies such as hardware tokens or modern phishing-resistant protocols over simple SMS or push notifications, especially for privileged and remote access.
B2.a.A.4	***[including remote access]*** any user requiring a remote connection to your network and information systems should do so via a mechanism that enforces additional authentication mechanisms. Additional authentication refers to mechanisms that are in addition to passwords or numbers. Where users require remote access to your networks, they will be required to pass through a minimum of two discrete authentication mechanisms. The first to gain access to the corporate network and the second to gain access from the corporate network to the nis network.

IGP Ref	Examples of Evidence to support IGPs
B2.a.A.1 B2.a.PA.1	An identity and access management policy that details the process of initial identity verification.
B2.a.A.1 B2.a.PA.1	A documented pre-employment check process that follows BS7858 (see **B1.b**).
B2.a.A.1 B2.a.PA.1	You have confirmed that any 3rd party organisations with access to your systems employ suitably robust identity verification processes.
B2.a.A.2	An identity and access management policy that details the process for approving authorisations and detailing the process for maintaining access control lists.
B2.a.A.2	A register of the mechanisms providing authentication services for all network and information systems supporting your essential function (this may be recorded as a field in your asset registers).
B2.a.A.2	Where domain level authentication services are being employed, the service on the essential networks and supporting enterprise networks should be separate. IoT systems should not rely on services from the EIT domain for authentication and authorisation.
B2.a.A.2	In cases where logical and physical access controls do not meet best practice, the risks should be recorded in your risk register with evidence of compensating controls.
B2.a.A.3 B2.a.PA.3	An identity and access management policy that details how you implement the principle of least privilege on your networks and information systems. Examples may include Roles Based or Attribute Based Access Control schemes (RBAC, ABAC). In instances where you rely on system specific IdAM mechanisms your access management policy should detail the processes you employ for each separate system.

B2.a.A.4 B2.a.PA.4	A register of the mechanisms providing authentication services for all network and information systems supporting your essential function (this may be recorded as a field in your asset registers).
B2.a.A.4	Network diagrams clearly showing the IdAM services that control remote access.

References and Further Guidance	
• B.2 Identity and access control - NCSC.GOV.UK	
• BSI BS 7858:2019 - Screening of individuals working in a secure environment. Code of practice	
• Identity profiles - GOV.UK (www.gov.uk)	
• NIST CSF 2.0 Subcategory:	PR.AA-01, PR.AA-02, PR.AA-03
• ISO 27001/27002:2022 Control:	5.16, 5.17, 8.5
• NIST SP 800-53 Rev. 5 Control:	IA-1, IA-2, IA-8

10.4.3 B2.b Device Management

B2.b Device Management		
You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential function(s)		
Not achieved: At least one of the following statements is true.	Partially Achieved All the following statements are true.	Achieved All the following statements are true.
B2.b.NA.1 Users can connect to your network and information systems supporting your essential function(s) using devices that are not corporately owned and managed.	**B2.b.PA.1** Only *corporately owned and managed devices* can access your essential function(s) network and information systems.	**B2.b.A.1** All *privileged operations* performed on your network and information systems supporting your essential function(s) are conducted from highly trusted devices, such as Privileged Access Workstations, *dedicated solely* to those operations.
B2.b.NA.2 Privileged users can perform privileged operations from devices that are not corporately owned and managed.	**B2.b.PA.2** All *privileged operations* are performed from *corporately owned and managed devices*. These devices provide sufficient separation, using a risk-based approach, from the activities of standard users.	**B2.b.A.2** You either obtain *independent and professional assurance* of the security of third-party devices or networks before they connect to your network and information systems, or you only allow third-party devices or networks that are dedicated to supporting your network and information systems to connect.
B2.b.NA.3 You have not gained assurance in the security of any third-party devices or networks connected to your systems.	**B2.b.PA.3** You have sought to understand the security properties of third- party devices and networks before they can be connected to your systems. You have taken appropriate steps to mitigate any risks identified.	**B2.b.A.3** You perform certificate-based device identity management and only allow known devices to access systems necessary for the operation of your essential function(s).

B2.b.NA.4 Physically connecting a device to your network and information systems gives that device access without device or user authentication.	**B2.b.PA.4** The act of connecting to a network port or cable does not grant access to any systems.	**B2.b.A.4** You perform regular scans to detect unknown devices and investigate any findings.
	B2.b.PA.5 You are able to detect unknown devices being connected to your network and information systems and investigate such incidents.	

IGP Ref	IGP Interpretation
B2.b.A.1 B2.b.PA.2	***[privileged operations] [Dedicated solely]*** • You have a process to ensure that devices such as Privileged Access Workstations (PAWs) that temporarily connect to your systems for the purpose of system management (e.g. commissioning, configuring and maintaining) are only used for these purposes. This process extends to third party suppliers as well as your own staff. • The primary control objective is strict logical and technical segregation of high-risk administrative tasks from general user activity (e.g., email or web browsing). While a physical PAW is the most direct solution, this outcome can be achieved using equivalent controls such as hardened Bastion Hosts, Session Jump Servers, or Privileged Access Management (PAM) systems that enforce session isolation. All solutions should ensure that privileged access sessions are routed through a single, monitored gateway, logging every action to provide a comprehensive audit trail.
B2.b.A.2	***[independent and professional assurance]*** • Your default policy is that no 3rd party devices connect to your network or systems. Wherever possible, you supply 3rd parties with the devices and software that they need to enable them to complete their tasks and these devices remain under your supervision. • However, in cases where it is essential for 3rd parties to use their own devices, you have a process to minimise the risk they present to your network. This process may include, but is not limited to, scanning for malware and limiting the software installed to only that which is necessary for the task. • You do not accept the assurances of the 3rd party that their devices are secure. Where it is necessary for 3rd parties to connect their own devices to your systems, you subject those devices to a minimum set of checks which are conducted by your own staff prior to allowing connection.
B2.b.A.3	***[You perform certificate-based device identity management]*** You perform certificate-based device identity management where practicable.
B2.b.PA.1 B2.b.PA.2	***[corporately owned and managed devices]*** these devices may belong to your own organisation, or, to a third-party supplier. However, in both cases the devices should be governed by a formalised IT policy. This precludes the use of any privately owned devices (e.g. Bring Your Own Devices) and the use of any corporate devices to which an employee has administrative rights.

IGP Ref	Examples of Evidence to support IGPs
B2.b.A.1 B2.b.A.2 B2.b.PA.1	A policy document describing the use of Privileged Access Workstations (PAWs) or their equivalents (Bastion Hosts/Jump Servers) on the EIT environment, detailing how you control the use of these dedicated privileged devices
B2.b.A.1	A register of all your PAWs and their permitted use (this information is likely to captured in your asset register).
B2.b.A.1 B2.b.A.2	Evidence that third party suppliers are contractually bound to comply with your PAW policy.
B2.b.A.1 B2.b.A.2 B2.b.PA.2	Documentation of the strong technical controls that enforce segregation and dedication (e.g., firewall rules, network access control lists) ensuring PAWs/Bastion Hosts cannot be used for general activities like email or web browsing
B2.b.A.1 B2.b.A.2	Evidence that all privileged operations are performed from corporately owned and managed devices, which are strictly defined and monitored by EIT policy.
B2.b.A.3	Details of any certificate-based device identity management schemes that you employ.
B2.b.PA.1	A corporate mobile device management policy (which will typically be owned by your IT department).
B2.b.PA.2	Work instructions or Maintenance Task Procedures that specify the use of PAWS.

References and Further Guidance

• B.2 Identity and access control - NCSC.GOV.UK	
• NCSC Device Security Guidance: https://www.ncsc.gov.uk/collection/device-security-guidance	
• NCSC: Using an assured device to access sensitive data: https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management	
• NIST CSF 2.0 Subcategory:	PR.PS-01, PR.PS-03
• ISO 27001/27002:2022 Control:	8.1, 7.9
• NIST SP 800-53 Rev. 5 Control:	CM-2, MA-1

10.4.4 B2.c Privileged User Management

B2.c Privileged User Management		
You closely manage privileged user access to network and information systems supporting your essential function(s)		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B2.c.NA.1 The identities of the individuals with privileged access to network and information systems (infrastructure, platforms, software, configuration etc) supporting your essential function(s) are not known or not managed.	**B2.c.PA.1** All privileged user access to network and information systems supporting your essential function(s) strong authentication, such as multi-factor authentication (MFA).	**B2.c.A.1** Privileged user access to network and information systems supporting your essential function(s) is carried out from *dedicated separate accounts that are closely monitored and managed*.
B2.c.NA.2 Privileged user access to network and information systems supporting your essential function(s) is via weak authentication mechanisms (e.g. only simple passwords).	**B2.c.PA.2** The identities of the individuals with privileged access to network and information systems (infrastructure, platforms, software, configuration etc) supporting your essential function(s) are known and managed. This includes third parties.	**B2.c.A.2** The issuing of *temporary, time- bound rights* for privileged user access and / or external third- party support access is in place.
B2.c.NA.3 The list of privileged users has not been reviewed recently (e.g. within the last 12 months).	**B2.c.PA.3** Activity by privileged users is routinely reviewed and validated (e.g. at least annually).	**B2.c.A.3** Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process.
B2.c.NA.4 Privileged user access is granted on a system-wide basis rather than by role or function(s).	**B2.c.PA.4** Privileged users are only granted specific privileged user access rights which are essential to their business role or function.	**B2.c.A.4** All privileged user activity is routinely *reviewed, validated and recorded* for offline analysis and investigation
B2.c.NA.5 Privileged user access to network and information systems supporting your essential function(s) is via generic, shared or default name accounts.		

B2.c.NA.6 Where there are "always on" terminals which can perform privileged actions (such as in a control room), there are no additional controls (e.g. physical controls) to ensure access is appropriately restricted.		
B2.c.NA.7 There is no logical separation between roles that an individual may have and hence the actions they perform (e.g. access to corporate email and privilege user actions).		

IGP Ref	IGP Interpretation
B2.c.A.1	***[dedicated separate accounts that are closely monitored and managed]*** This amounts to: • privileged user access is conducted from dedicated privileged user accounts and devices which are not used for typical day- to-day functions (e.g. email, web browsing). • all privileged user actions are logged and you have defined SIEM rules that will detect suspicious and potentially damaging events. The rules that you have defined are system specific.
B2.c.A.2	***[temporary, time-bound rights]*** • You have processes in place which enforce 'just in time administration'. Just in time administration ensures that the privileged user is only permitted to access a system after they have been approved to do so for a specific purpose. Ideally, just in time administration should be enforced via technical means such as a Privileged Access Management (PAM) Service. • It may not be possible to implement a PAM on your IoT networks, where this is the case you should enforce just in time administration through alternative processes, such as a documented works request/permit to work. In certain circumstances, just in time administration can also be enforced by securing PAWs or required hardware in locked storage, release from storage would form part of the works request/permit to work process.
B2.c.A.4	***[reviewed, validated and recorded]*** You have tools and/or manual processes in place to ensure that logs of all privileged user actions in the IT and IoT environments are checked to confirm that they correspond to legitimate activity. All remote 3rd party connections are recorded and audit events are passed to a SIEM.

IGP Ref	Examples of Evidence to support IGPs
B2.c.A.1 B2.c.A.2	A privileged user access policy.
B2.c.A.1 B2.c.A.4	A logging and monitoring policy which specifically addresses privileged user monitoring.
B2.c.A.1	Work instructions or Maintenance Task Procedures specifying the use of dedicated, non-generic privileged accounts.
B2.c.A.2	Details of any Privileged Access Management (PAM) service that is being employed, or documentation detailing the use of Bastion Hosts/Session Jump Servers to enforce isolation for privileged access.
B2.c.A.2	Records demonstrating that temporary, time-bound rights (Just-in-Time access) are implemented for elevated privileges where technically feasible.
B2.c.A.4	Audit logs demonstrating that all privileged actions are routinely reviewed and correlated with known maintenance schedules or change requests.

B2.c.A.4	Evidence that privileged user and system activity logs are fed into a Security Information and Event Management (SIEM) tool for real-time monitoring and alerting.

References and Further Guidance	
• B.2 Identity and access control - NCSC.GOV.UK	
• Introduction to identity and access management - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	PR.AA-05
• ISO 27001/27002:2022 Control:	8.2
• NIST SP 800-53 Rev. 5 Control:	AC-3, AC-6

10.4.5 B2.d Identity and Access Management (IdAM)

B2.d Identity and Access Management (IdAM)		
You closely manage and maintain identity and access control for users, devices and systems accessing network and information systems supporting your essential function(s).		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B2.d.NA.1 Greater access rights are granted than necessary.	**B2.d.PA.1** You follow a *robust procedure* to verify each user and issue the *minimum required access rights*.	**B2.d.A.1** You follow a *robust procedure* to verify each user and issue the *minimum required access rights*, and the application of the procedure is regularly audited.
B2.d.NA.2 Identity validation and requirement for access of a user, device or systems is not carried out.	**B2.d.PA.2** You regularly review access rights and those no longer needed are revoked.	**B2.d.A.2** User access rights are reviewed both when people change roles via your joiners, leavers and movers process and at regular intervals - at least annually.
B2.d.NA.3 User access rights are not reviewed when users change roles.	**B2.d.PA.3** User access rights are reviewed when users change roles via your joiners, leavers and movers process.	**B2.d.A.3** All user, device and systems access to network and information systems supporting your essential function(s) *is logged and monitored.*
B2.d.NA.4 User access rights remain active when users leave your organisation.	**B2.d.PA.4** All user, device and system access to the systems supporting the essential function(s) is *logged and monitored*, but it is not compared to other log data or access records.	**B2.d.A.4** *You regularly review access logs* and correlate this data with other access records and expected activity.
B2.d.NA.5 Access rights granted to devices or systems to access other devices and systems are not reviewed on a regular basis (at least annually).		**B2.d.A.5** Attempts by unauthorised users, devices or systems to connect to network and information systems supporting your essential function(s) are alerted, promptly assessed and investigated are alerted, promptly assessed and investigated.

IGP Ref	IGP Interpretation
B2.d.A.1 B2.d.PA.1	***[robust procedure]*** You meet the outcomes for a Tier 2 Profile for B2.a
B2.d.A.2 B2.d.PA.2	***[minimum required access rights]*** • You ensure that staff only have access to the systems that they require to carry out their roles. You avoid providing 'blanket-access' to all systems for all staff. • You make full use of the functionality on all of your devices and, where the device allows, you issue permissions on the basis of the principal of least privilege and distinguish between standard and administrative users. This requires that you fully understand the user administration functionality on your devices and that you have correctly configured it so as to provide access protection to critical functions
B2.d.A.3 B2.d.PA.4	***[logged and monitored]*** You have a process to monitor user access to all your systems. Ideally this process will be automated, and you will be able to monitor logs from a central SIEM.
B2.d.A.4	***[regularly review access logs]*** In cases where you have implemented SIEM tooling, and have configured alerts, this would typically be considered as reviewing access logs in real-time. In cases where you are reliant on copying access event logs, and are reviewing them manually, you have a scheduled (planned and periodic) process to complete this activity.

IGP Ref	Examples of Evidence to support IGPs
B2.d.A.1 B2.d.PA.1	Relevant IdAM policies and proof, in the form of your critical systems.
B2.d.A.1 B2.d.PA.1	Your IdAM policies clearly define the degree to which you are able to limit permissions on each of your devices and demonstrates that you're making full use of this functionality.
B2.d.A.3 B2.d.PA.4	SIEM tooling that covers all essential NIS systems (including the cloud platform and its access logs) to meet the comprehensive logging requirement (B2.d.A.3).
B2.d.A.3 B2.d.A.4 B2.d.PA.4	Demonstration of a process to manually check logs on systems that are not integrated with a SIEM tool.
B2.d.A.4	Records demonstrating alerting and investigation procedures for unauthorised access attempts, proving that access logs are actively monitored and actioned.
B2.d.A.4	Audit reports confirming that access logs are regularly reviewed and correlated with other access records and expected activity.

References and Further Guidance	
• B.2 Identity and access control - NCSC.GOV.UK	
• Introduction to identity and access management - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	PR.AA-05
• ISO 27001/27002:2022 Control:	5.18
• NIST SP 800-53 Rev. 5 Control:	AC-2, AC-5

10.5 Principle B3: Data Security

10.5.1 Principle B3 Extended Guidance:

Principle B3 addresses the protection of data throughout its entire lifecycle. For a load control provider, this includes both sensitive consumer information and the critical operational data used to issue commands to the platform. The scoping exercise is fundamental to this principle, as it defines the boundaries of the load control service and identifies the specific data assets and flows that require protection while in transit, in use, or at rest.

The scope of this principle applies primarily to the data handled within the provider's internal systems and cloud platforms. Security for consumer-premise ESAs and the data they handle locally is addressed through separate product security regulations and standards, such as ETSI EN 303 645, which focus on the hardware and software integrity of the device itself.

To ensure robust data protection, the organisation should focus on the following core areas:

- **Understanding and Cataloguing Data (B3.a):** This involves identifying and cataloguing all important data assets and mapping their associated flows and storage locations, as determined by the scoping exercise. This understanding serves as the essential foundation for risk-based protection, ensuring that the organisation knows exactly where its sensitive information resides and how it moves across the ecosystem.
- **Technical Protection of Data (B3.b and B3.c):** There should be no ambiguity regarding the technical controls used to protect known data. This includes the consistent application of encryption and other protective measures for data in transit and data at rest. The organisation must have justified confidence that these controls are correctly implemented and effective against unauthorised access or interception.
- **Secure Media Sanitisation (B3.e):** Robust processes must be in place to ensure that data is securely removed from storage media when it is no longer required or when the hardware reaches its end of life. This prevents the accidental disclosure of sensitive information through the improper disposal of hardware components.

A comprehensive approach to Principle B3 ensures that all known data assets are subject to robust protective controls from the outset. While the process of mapping complex data flows may evolve as the service scales, the technical measures protecting identified data must be demonstrably effective to maintain the confidentiality and integrity of the load control service.

10.5.2 B3.a Understanding Data

B3.a Understanding Data		
You have a good understanding of data important to the operation of network and information systems supporting your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, uncontrolled release, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B3.a.NA.1 You have incomplete knowledge of what data is used by and produced in the operation of network and information systems supporting your essential function(s).	**B3.a.PA.1** You have identified and catalogued all the *data important to the operation* of network and information systems supporting your essential function(s), or that would *assist a threat actor.*	**B3.a.A.1** You have identified and catalogued all the *data important to the operation of* network and information systems supporting your essential function(s), or that would *assist a threat actor.*

B3.a.NA.2 You have not identified the important data on which network and information systems supporting your essential function(s).	**B3.a.PA.2** You have identified and catalogued who has access to the data important to the operation of network and information systems supporting your essential function(s).	**B3.a.A.2** You have identified and catalogued who has access to the data important to the operation of network and information systems supporting your essential function(s).
B3.a.NA.3 You have not identified who has access to data important to the operation of network and information systems supporting your essential function(s).	**B3.a.PA.3** You regularly review location, transmission, quantity and quality of data important to the operation of network and information systems supporting your essential function(s).	**B3.a.A.3** You maintain a current understanding of the location, quantity and quality of data important to the operation of network and information systems supporting your essential function(s).
B3.a.NA.4 You have not clearly articulated the impact of data compromise or lack of availability.	**B3.a.PA.4** You have identified all mobile devices and media that hold data important to the operation of network and information systems supporting your essential function(s).	**B3.a.A.4** You take steps to remove or minimise unnecessary copies or unneeded historic data.
	B3.a.PA.5 *You understand and document* the impact on your essential function(s) of all relevant scenarios, including unauthorised data access, *uncontrolled release*, modification or deletion, or when authorised users are unable to appropriately access this data.	**B3.a.A.5** You have identified all mobile devices and media that may hold data important to the operation of network and information systems supporting your essential function(s).
	B3.a.PA.6 You occasionally *validate* these documented impact statements.	**B3.a.A.6** You maintain a current *understanding of the data links used to transmit data* that is important to network and information systems supporting your essential function(s).
		B3.a.A.7 You understand the context, limitations and dependencies of your important data.
		B3.a.A.8 You *understand and document* the impact on your essential function(s) of all relevant scenarios, including unauthorised data access, *uncontrolled release*, modification or deletion, or when authorised users are unable to appropriately access this data.
		B3.a.A.9 You validate these documented impact statements regularly, at least annually.

IGP Ref	IGP Interpretation
B3.a.A.1 B3.a.PA.1	***[data important to the operation]*** The operation and management of your essential service will rely on multiple data sources. This data may include, but will not be restricted to, telemetry data required to maintain 'view' and 'control' of the system, system design and configuration data and system back-ups.

B3.a.A.1 B3.a.PA.1	***[assist a threat actor]*** Implementing a cyber security management system creates several documents that would be especially useful to a threat actor. These documents include, but are not limited to, network diagrams, asset registers, configuration management databases, vulnerability registers and attack path maps. Once these documents are created it is vital that they are adequately protected. Protection is achieved by understanding the types of data that could assist an attacker, marking all such documentation as sensitive (in accordance with your company policy) and ensuring that the data is stored and secured in a manner that is commensurate with the security marking.
B3.a.A.6	***[understanding of the data links used to transmit data]*** You maintain Interface Control Documents (ICD) for each system. These ICDs detail all the information that is shared between systems, across network boundaries (particularly between CLF and enterprise networks) and outside of the organisation. You have used this ICD to help inform your risk register. Your ICD captures any data that informs load control decisions e.g. to check validity and for anomalies: • Data/fields transmitted • Data recipient (system or organisation) • Data link (e.g. internal network, leased line, public network) • Transmission protocol including descriptions of protocol breaks used at boundaries • Criticality of data transmission, including an assessment of whether the essential service relies on the transmission • Security controls applied to the transmission, including details of any boundary devices that are traversed by the data.
B3.a.A.8 B3.a.PA.5	***[understand and document]*** your risk register should include risks associated with loss of Confidentiality, Integrity and Availability (CIA) of data important to the operation of the essential service.
B3.a.A.8 B3.a.PA.5	***[uncontrolled release]*** This considers managing the risk of unauthorised data disclosure or exfiltration, typically associated with a breach of data confidentiality. This explicitly reinforces the security outcome against data loss or leakage events and requires policies and technical controls (e.g., Data Loss Prevention (DLP), encryption of data in motion and at rest) to prevent such occurrences.
B3.a.PA.6	***[validate]*** You review your risk register in accordance with guidance issued at **A1.c.**

IGP Ref	Examples of Evidence to support IGPs
B3.a.A.1 B3.a.PA.1	A completed Information Asset Register (IAR). The Information Asset Register may be part of your main asset register, or it may be a discrete document. The IAR should include details of any data that informs load control decisions e.g. to check validity and for anomalies. : • 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), mobile media) • Technical security controls that have been applied to data stored on mobile devices (e.g. encryption) • Access control restrictions • Data backup requirements.
B3.a.A.1 B3.a.PA.1	Meeting minutes demonstrating that the IAR has been reviewed and revised where necessary.
B3.a.A.1 B3.a.PA.1	Documentation detailing the process for managing information that would assist a threat actor (e.g., network diagrams, asset registers), ensuring it is protected with appropriate access controls
B3.a.A.6	Interface Control Documents (ICDs) for all your systems.

B3.a.A.8 B3.a.PA.5	A risk register with entries that related to loss of CIA of critical data streams and where appropriate, historic data.
B3.a.A.8 B3.a.PA.5	Evidence of Data Loss Prevention (DLP) controls or equivalent measures applied to critical data sets to prevent unauthorised transfer or exfiltration.

References and Further Guidance	
• B.3 Data security - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	ID.AM-07
• ISO 27001/27002:2022 Control:	5.12, 5.13
• NIST SP 800-53 Rev. 5 Control:	SI-12, MP-3

10.5.3 B3.b Data in Transit

B3.b Data in Transit		
You have protected the transit of data important to the operation of network and information systems supporting your essential function(s). This includes the transfer of data to third parties.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B3.b.NA.1 You do not know what all your data links are, or which carry data important to the operation of the essential function(s).	**B3.b.PA.1** You have identified and *protected (effectively and proportionately)* all the *data links* that carry data important to the operation of your essential function(s).	**B3.b.A.1** You have identified and *protected (effectively and proportionately)* all the *data links* that carry data important to the operation of your essential function(s).
B3.b.NA.2 Data important to the operation of the essential function(s) travels without technical protection over non-trusted or openly accessible carriers.	**B3.b.PA.2** You apply appropriate *physical and / or technical means* (e.g. cryptography) to protect data that travels over non-trusted or openly accessible carriers, but you have limited or no confidence in the robustness of the protection applied.	**B3.b.A.2** You apply appropriate *physical and / or technical means* (e.g. cryptography) to protect data that travels over non-trusted or openly accessible carriers, with *justified confidence* in the robustness of the protection applied.
B3.b.NA.3 Critical data paths that could fail, be jammed, be overloaded, etc. have no alternative path.		**B3.b.A.3** Suitable *alternative transmission paths* are available where there is a significant risk of impact on the operation of the essential function(s) due to resource limitation (e.g. transmission equipment or function failure, or important data being blocked or jammed).

IGP Ref	IGP Interpretation
B3.b.A.1 B3.b.PA.1	***[protected (effectively and proportionately)]*** You have taken measures to protect your data that is commensurate with the consequence of compromise. For example, you have taken measures to assure the integrity of data flows that are critical to the safe operation of your CLF service, and you have taken measures to ensure the confidentiality of data that could assist and attacker.

B3.b.A.1 B3.b.PA.1	***[data links]*** You have taken account of all data links that carry important data, this includes networked transmission of data, use of removable media and the physical carriage of hard copy data.
B3.b.A.2 B3.b.PA.2	***[physical and / or technical means]*** This confirms that protection measures should be holistic, spanning both logical and environmental controls. Technical means include cryptography (e.g., TLS, VPNs) applied to data channels, while physical means include securing physical media and access to communication links, infrastructure hardware, and boundary devices.
B3.b.A.2	***[justified confidence]*** You have independently tested and validated the means you are using to protect your data to a recognised standard. It would be expected for organisations to have conducted technical testing of their networks to confirm that the encryption function on all data flows across non-trusted (e.g. public internet) or openly accessible carriers (e.g. wi-fi, radio links) have been correctly configured.
B3.b.A.3	***[alternative transmission paths]*** All data transmissions that have been identified as critical to the provision of the essential CLF service have been recorded in the relevant Interface Control Documents (ICD) and the risk register. You have assessed whether these transmission paths are sufficiently resilient. Where your assessments indicate that that there is significant risk of the failure or compromise you have considered the provision of multi- path and or modular redundant communication links.

IGP Ref	Examples of Evidence to support IGPs
B3.b.A.1 B3.b.PA.1	A set of data flow diagrams (or similar) of sufficient detail to show individual data links and the means of protection (e.g. VPN, radio link encryption).
B3.b.A.1 B3.b.PA.1	Interface Control Documents that specify the nature of the data links used for each interface.
B3.b.A.2 B3.b.PA.2	Documentation of physical security controls that protect communication infrastructure (e.g., locked server cabinets, restricted access to networking rooms)
B3.b.A.2	Independent 3rd Party Penetration test results which validate the robustness of the technical protection applied (e.g., testing encryption implementation).
B3.b.A.3	The provision of resilient communication designs where they are required.
B3.b.A.3	Business resilience or business continuity plans that address the need for maintenance and stand up of alternative solutions.

References and Further Guidance

• B.3 Data security - NCSC.GOV.UK	
• NCSC Using TLS to protect data: https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data	
• NIST CSF 2.0 Subcategory:	PR.DS-02
• ISO 27001/27002:2022 Control:	8.24, 8.21
• NIST SP 800-53 Rev. 5 Control:	SC-8, SC-13

10.5.4 B3.c Stored Data

B3.c Stored Data

You have protected stored soft and hard copy data important to the operation of network and information systems supporting your essential function(s).

Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.

B3.c.NA.1 You have no, or limited, knowledge of where data important to the operation of network and information systems supporting your essential function(s) is stored.	**B3.c.PA.1** All copies of *data important to the operation* of network and information systems supporting your essential function(s) are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy.	**B3.c.A.1** All copies of *data important to the operation* network and information systems supporting your essential function(s) are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy.
B3.c.NA.2 You have not protected vulnerable stored data important to the operation of network and information systems supporting your essential function(s) in a suitable way.	**B3.c.PA.2** You have applied suitable physical and / or technical means to protect this important stored data from unauthorised access, modification or deletion.	**B3.c.A.2** You have applied suitable physical and / or technical means to protect this important stored data from unauthorised access, modification or deletion.
B3.c.NA.3 Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.	**B3.c.PA.3** If cryptographic protections are used, you apply suitable technical and procedural means, but you have limited or no confidence in the robustness of the protection applied.	**B3.c.A.3** If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied.
	B3.c.PA.4 You have *suitable, secured backups of data* to allow the operation of network and information systems supporting your essential function(s) to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.	**B3.c.A.4** You have *suitable, secured backups of data* to allow the operation of network and information systems supporting your essential function(s) to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.
		B3.c.A.5 Necessary historic or archive data is suitably secured in storage.

IGP Ref	IGP Interpretation
B3.c.A.1 B3.c.PA.1	***[important to the operation]*** the operation and management of your Licensed CLF service will rely on multiple data sources. This data may include, but will not be restricted to ESA telemetry data, system design and configuration data, system back-ups.
B3.c.A.4 B3.c.PA.4	***[Suitable secured backups of data]*** You have taken account of principle B5.c.

IGP Ref	Examples of Evidence to support IGPs
B3.c.A.1 B3.c.PA.1	An Information Asset Register (IAR), as detailed at the interpretation of B3.a.
B3.c.A.2	Records demonstrating that the secured backups are complete, segregated, and regularly tested for restoration capability.
B3.c.A.2	Policy and configurations demonstrating the mandatory use of encryption for data at rest on all critical components (servers, databases, cloud storage).
B3.c.A.5	Evidence of physical controls protecting hard copy records or storage media containing critical system data.

References and Further Guidance	
• B.3 Data security - NCSC.GOV.UK	
• Ransomware-resistant backups - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	PR.DS-01
• ISO 27001/27002:2022 Control:	8.10, 8.24
• NIST SP 800-53 Rev. 5 Control:	SC-28, MP-4

10.5.5 B3.d Mobile Data

B3.d Mobile Data		
You have protected data important to the operation of network and information systems supporting your essential function(s) on mobile devices (e.g. smartphones, tablets and laptops).		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B3.d.NA.1 You don't know which mobile devices may hold data important to the operation of network and information systems supporting your essential function(s).	**B3.d.PA.1** You know which *mobile devices* hold data important to the network and information systems supporting your essential function(s).	**B3.d.A.1** *Mobile devices* that hold data that is important to the operation of network and information systems supporting your essential function(s) are *catalogued*, are under your organisation's control and configured according to best practice for the platform, with appropriate technical and procedural policies in place.
B3.d.NA.2 You allow data important to the operation of network and information systems supporting your essential function(s) to be stored on devices not managed by your organisation, or to at least equivalent standard.	**B3.d.PA.2** Data important to the operation of network and information systems supporting your essential function(s) is stored on mobile devices only when they have at least the security standard aligned to your overarching security policies.	**B3.d.A.2** Your organisation can remotely wipe all mobile devices holding data important to the operation of network and information systems supporting your essential function(s).
B3.d.NA.3 Data on mobile devices is not technically secured, or only some is secured.	**B3.d.PA.3** Data on mobile devices is *technically secured*	**B3.d.A.3** You have minimised this data on these mobile devices. Some data may be automatically deleted off mobile devices after a certain period.

IGP Ref	IGP Interpretation
B3.d.A.1 B3.d.PA.1	***[mobile devices][Catalogued]*** you understand which mobile devices (e.g. laptops, removable media) host important data and you have records of these devices in your Asset Inventory (**A3.a**). Your records and management processes enable you to manage them through life and assure the data that they host.
B3.d.PA.3	***[technically secured]*** You do not rely solely on people and processes to secure mobile devices. You have also implemented appropriate and proportionate technical measures to secure the data on your mobile devices. The technical measures employed will depend on the purpose for which the mobile device is employed and will need to be selected after risk assessment.

IGP Ref	Examples of Evidence to support IGPs

B3.d.A.1 B3.d.PA.1	An asset register, as detailed in interpretation of IGP of A3.a, which clearly identifies mobile devices.
B3.d.A.1 B3.d.PA.1	An Information Asset Register (IAR), as detailed in interpretation of IGP B3.a.11, which clearly identifies when important information is being hosted on mobile devices.
B3.d.A.1 B3.d.PA.1	A mobile device management policy covering all relevant mobile devices. This may amount to more than one policy if mobile devices are managed by separate departments (e.g. EIT and IoT teams).
B3.d.A.1	Evidence of technical security controls applied to mobile devices, such as mandatory disk/file encryption
B3.d.A.2	Records demonstrating the remote wipe capability is tested and functional.

References and Further Guidance	
• B.3 Data security - NCSC.GOV.UK	
• Device Security Guidance - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	PR.AA-06
• ISO 27001/27002:2022 Control:	8.1, 7.9
• NIST SP 800-53 Rev. 5 Control:	AC-19, PE-18

10.5.6 B3.e Media/Equipment Sanitisation

B3.e Media/Equipment Sanitisation

Before reuse and / or disposal you appropriately sanitise devices, equipment and removable media holding data important to the operation of network and information systems supporting your essential function(s).

Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B3.e.NA.1 Some or all devices, equipment or removable media that hold data important to the operation of network and information systems supporting your essential function(s) are reused or disposed of without sanitisation of that data.	**B3.e.PA.1** Data important to the operations of network and information systems supporting your essential function(s) is removed from all devices, equipment and removable media before reuse and / or disposal.	**B3.e.A.1** You *catalogue and track all devices that contain data* important to the operation of network and information systems supporting your essential function(s) (whether a specific storage device or one with integral storage).
		B3.e.A.2 Data important to the operation of network and information systems supporting your essential function(s) is removed from all devices, equipment and removable media before reuse and / or disposal using an *assured product or service*

IGP Ref	IGP Interpretation
B3.e.A.1	***[catalogue and track all devices that contain data]*** his requires maintaining a complete and accurate inventory, as defined in the Asset Management principle A3.a. This catalogue should include dedicated privileged access devices (B2.b) and all media containing critical data. Tracking should record the device's unique identifier, current location, and the full history of sanitisation or disposal throughout its lifecycle.

B3.e.A.2	***[assured product or service]*** This refers to using commercial tools, software, or third-party destruction services that are independently verified or certified to meet an agreed-upon standard for media sanitisation (e.g., permanent deletion, degaussing, physical destruction). Assurance should be sought against official guidance, such as the NCSC's Secure Sanitisation and Disposal of Storage Media guidance.
IGP Ref	**Examples of Evidence to support IGPs**
B3.e.A.1	A completed Information Asset Register (IAR). The Information Asset Register may be part of your main asset register, or it may be a discrete document. The IAR should include details of any assets reuse and / or disposal using an assured product or service to dispose.
B3.e.A.2	Contracts or agreements with third-party disposal services, providing assurance and certification of the data destruction process used for assets.
B3.e.A.2	Records of Sanitisation/Disposal for all catalogued devices, detailing the method used (e.g., physical destruction, cryptographic erasure) and date of destruction.

References and Further Guidance	
• B.3 Data security - NCSC.GOV.UK	
• NCSC: Secure sanitisation and disposal of storage media	
• UK GDPR guidance and resources	
• The UK's data protection legislation	
• NIST CSF 2.0 Subcategory:	PR.DS-08
• ISO 27001/27002:2022 Control:	7.14, 8.10
• NIST SP 800-53 Rev. 5 Control:	MP-6, SI-12

10.6 Principle B4 System Security

10.6.1 Principle B4 Extended Guidance

Principle B4 addresses the technical core of system protection, detailing how the Network and Information Systems supporting the load control service should be designed, configured, and managed to be resilient to cyber-attack. The scoping exercise is the essential starting point for this principle, as it identifies the specific boundary of the technical stack, including cloud environments, management interfaces, and communication paths that must be secured.

The implementation of this principle ensures that the technical architecture is inherently robust. For Load Control providers, the strategy for system protection should focus on the following areas:

- **Network Segregation and Boundary Control (B4.a):** This involves the logical or physical separation of systems based on their criticality and function. Many providers leveraging modern cloud platforms may find that robust network segregation is a natural outcome of following well-architected framework principles, but this must be formally verified to ensure that the load control platform is isolated from less secure environments.
- **Secure Configuration and Hardening (B4.b):** Ensuring that all systems within the scope of the service are configured according to security best practices to reduce the available attack surface.
- **Vulnerability Management (B4.d):** Establishing a proactive process for identifying, assessing, and remediating vulnerabilities within the software and hardware components of the service. This requires regular scanning and a clear lifecycle for the deployment of security patches, particularly for components that facilitate the command and control of distributed assets.
- **System Resilience and Availability (B4.c):** Designing the system to maintain its essential function even in the event of component failure or a localised cyber-attack. This involves ensuring there is sufficient redundancy and that the technical architecture can withstand attempts to disrupt the load control service.

The organisation's risk assessment is the primary driver for determining the depth and complexity of these technical controls. The goal is to ensure that the security posture is proportionate to the systemic importance of the load control service and that all protective measures are demonstrably effective against the identified threat landscape.

10.6.2 B4.a Secure by Design

B4.a Secure by Design		
You design security into the network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential function(s) should not be impacted by the exploitation of any single vulnerability.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B4.a.NA.1 Network and information systems supporting the operation of the essential function(s) are not appropriately segregated from other systems.	**B4.a.PA.1** You employ appropriate expertise to design network and information systems.	**B4.a.A.1** You employ appropriate expertise to design network and information systems supporting your essential function(s).
B4.a.NA.2 Internet services, such as browsing and email, are accessible from network and information systems supporting your essential function(s).	**B4.a.PA.2** You design *strong boundary defences where your network and information systems interface with other organisations* or the world at large.	**B4.a.A.2** Network and information systems are *segregated into appropriate security zones* (e.g. systems supporting the essential function(s) are segregated in a highly trusted, more secure zone).
B4.a.NA.3 Data flows between network and information systems supporting your essential function(s) and other systems are complex, making it hard to discriminate between legitimate and illegitimate / malicious traffic.	**B4.a.PA.3** You design *simple data flows* between your network and information systems and any external interface *to enable effective monitoring.*	**B4.a.A.3** The network and information systems supporting your essential function(s) are designed to have *simple data flows* between components to *support effective security monitoring.*
B4.a.NA.4 Remote or third-party accesses circumvent some network controls to gain more direct access to network and information systems supporting the essential function(s).	**B4.a.PA.4** You design to make network and information system recovery simple.	**B4.a.A.4** The network and information systems supporting your essential function(s) are *designed to be easy to recover.*
	B4.a.PA.5 All inputs to network and information systems supporting your essential function(s) are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks	**B4.a.A.5** *Content-based attacks are mitigated for all inputs* to network and information systems that affect the essential function(s) (e.g. via transformation and inspection / sanitisation and validation).
		B4.a.A.6 If *automated decision-making technologies* are in use, you design and apply appropriate restrictions to prevent actions that could have an adverse impact on your essential function(s).

IGP Ref	IGP Interpretation
B4.a.A.2	***[segregated into appropriate security zones]*** your network design is based around the segregation principle. You have grouped your services and systems that take account of their criticality. You have ensured that your Load Control networks, and any other systems that you have identified as being critical, are segregated from your enterprise systems.
B4.a.A.4	***[designed to be easy to recover]*** you have taken account of Principle B5: Resilient Networks and Systems.
B4.a.A.5	***[Content-based attacks are mitigated for all inputs]*** You should understand all possible paths by which data can be imported onto your networks and systems, including network connections (e.g., APIs, user uploads) and removable media. You should assume that content-based attacks are likely to originate from less trusted networks (e.g., the public internet, third-party systems) and, as a result, you should employ an appropriate blend of detective, defensive, and responsive measures at your network boundaries. Examples of these measures include: **Defensive Techniques (Preventing the attack):** • Input Validation: Validating all data inputs against a strict schema to ensure they conform to expected formats, lengths, and character sets. This is a primary defence for APIs. • Message Transformation / Protocol Break: Using a gateway to terminate an incoming connection, inspect and sanitise the content, and then forward a newly created, clean request to the internal system. • File Type Restriction: Allowing only specific, known-safe file types for any user or system uploads. • Rapid Patching: Ensuring that all systems and libraries used for data processing are promptly patched against known vulnerabilities. **Detective Techniques (Identifying an attack in progress):** • Content Inspection and Alerting: Using tools like a Web Application Firewall (WAF) or an API gateway to perform deep packet inspection on incoming traffic and generate alerts for known malicious payloads or patterns. • Behavioural Analysis: Monitoring for unusual patterns of data submission, such as a high volume of malformed requests from a single source, which could indicate an attempt to find a vulnerability. • Sandboxing: Automatically analysing file uploads or email attachments in an isolated sandbox environment to detect malicious behaviour before the file is made available to the end system or user. **Responsive Techniques (Reacting to a detected attack):** • Automated Blocking: Automatically blocking the source IP address of an attacker at the network edge (e.g., via the WAF) when a malicious pattern is detected. • Quarantining: Automatically moving any input that fails validation or is flagged as malicious to a secure quarantine area for later analysis, rather than rejecting it outright. • Incident Response Trigger: Automatically generating a high-priority alert in a security ticketing system to trigger a formal incident response playbook when a confirmed content-based attack is detected.
B4.a.A.6	***[automated decision-making technologies]*** This includes the use of Artificial Intelligence (AI) or Machine Learning (ML) components within the Load Control platform that automatically execute actions (e.g., forecasting, load shedding, control). Assurance should be in place to ensure these systems operate within safety parameters and that their decisions cannot be maliciously manipulated to cause an adverse impact.

B4.a.PA.2	***[strong boundary defences where your networks and information systems interface with other organisations]*** You have clearly identified all of the points of interconnection between your network and information systems and external organisations/third parties. These points of interconnection are equipped with a method of validating message format and content.
B4.a.PA.3	***[simple data flows],[to enable effective monitoring]*** Your data flows have been designed such that you are able to easily validate message format and content. Where necessary, you employ protocol breaks at network boundaries to transform data into the simplest format and perform validation of message format and content. You have considered the risks associated with importing data from various sources and have applied boundary protection that is commensurate with the risk. For example, you have applied higher levels of boundary protection and monitoring to data that is being imported from outside of your organisation.

IGP Ref	Examples of Evidence to support IGPs
B4.a.A.2	Network diagrams that clearly show all the networks and information systems that are in-scope, the zones that they are part of and DMZs.
B4.a.A.2	Documentation and network diagrams demonstrating the strict segregation of the NIS from Internet services (e.g., dedicated firewall rules blocking browsing/email protocols).
B4.a.A.3 B4.a.A.5 B4.a.PA.3	A set of Interface Control Documents (ICDs) for your in-scope systems that conform with the interpretation B3a.
B4.a.A.3 B4.a.A.5 B4.a.PA.3	A set of data flow diagrams (or similar) of sufficient detail to show data flows between network segments, and the means of validating message format and content.
B4.a.A.3 B4.a.PA.3	Details of a logging and monitoring strategy that details how data flows between network segments are monitored and that conforms with the guidance provided at C1.a.
B4.a.A.5	Technical control documentation showing the use of transformation, sanitisation, and validation controls (e.g., Web Application Firewalls, API gateways) at all network boundaries.
B4.a.A.6	(If applicable): Architectural documentation and operational logs demonstrating the security constraints and monitoring applied to any systems using automated decision-making technologies.
B4.a.PA.2	Network diagrams that show points of interconnection between network and information systems and external organisations/third parties.
B4.a.PA.3	A set of Interface Control Documents (ICDs) for your in-scope systems.

References and Further Guidance	
• B.4 System security - NCSC.GOV.UK	
• Pattern: Safely Importing Data - NCSC.GOV.UK	
• Content based attack protection - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	PR.IR-01
• ISO 27001/27002:2022 Control:	8.22, 8.27
• NIST SP 800-53 Rev. 5 Control:	SC-7, SA-8

10.6.3 B4.b Secure Configuration

B4.b Secure Configuration		
You securely configure the network and information systems that support the operation of your essential function(s).		
Not achieved:	Partially Achieved	Achieved

At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B4.b.NA.1 You haven't identified the assets that need to be carefully configured to maintain the security of network and information systems supporting your essential function(s).	**B4.b.PA.1** You have identified and documented the *assets that need to be carefully configured* to maintain the security of network and information systems supporting your essential function(s).	**B4.b.A.1** You have identified, documented and *actively manage* (e.g. maintain security configurations, patching, updating according to good practice) the *assets that need to be carefully configured* to maintain the security of network and information systems supporting your essential function(s).
B4.b.NA.2 Policies relating to the security of operating system builds or configuration are not applied consistently across your network and information systems relating to your essential function(s).	**B4.b.PA.2** *Secure platform and device builds* are used across the estate.	**B4.b.A.2** *All platforms conform* to your secure, defined baseline build, or the latest known good configuration version for that environment.
B4.b.NA.3 Configuration details are not recorded or lack enough information to be able to rebuild the system or device.	**B4.b.PA.3** Consistent, secure and minimal system and device configurations are applied across the same types of environment.	**B4.b.A.3** You closely and effectively manage changes in your environment, ensuring that network and information systems configurations are secure and documented.
B4.b.NA.4 The recording of security changes or adjustments that affect your essential function(s) is lacking or inconsistent.	**B4.b.PA.4** Changes and adjustments to security configuration at security boundaries of network and information systems supporting your essential function(s) are *approved and documented.*	**B4.b.A.4** You regularly review and validate that your network and information systems have the expected, secure settings and configuration.
B4.b.NA.5 Generic, shared, default name and built-in accounts have not been removed or disabled.	**B4.b.PA.5** You verify software before installation is permitted.	**B4.b.A.5** Only permitted software can be installed.
B4.b.NA.6 Standard users are able to change settings that would adversely impact the security of network and information systems supporting your essential function(s).	**B4.b.PA.6** Generic, shared, default name and built-in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed. *Service accounts are appropriately protected.*	**B4.b.A.6** If *automated decision-making technologies* are in use, *their operation is well understood*, and decisions can be replicated.
	B4.b.PA.7 Standard users are not able to change settings that would adversely impact the security of network and information systems supporting your essential function(s).	**B4.b.A.7** Generic, shared, default name and built-in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed. *Service accounts are appropriately protected.*

IGP Ref	IGP Interpretation

B4.b.A.1	***[actively manage]*** You have documented policies and processes that describe how you manage device configuration. These policies and processes include, but are not limited to: • baseline ('gold') builds for commonly used devices/platforms. • a means of ensuring that only permitted software is installed on devices. • maintenance of patch and configuration files You follow these processes and ensure that your assets are correctly configured and updated with the latest approved patches in a timely manner. Where it is not possible to update devices to the latest approved patch level (for reasons of down-time or safety) you: • maintain a register of missed patches (as part of configuration management register/database) • monitor the risks associated with lack of patching as part of your routine risk assessment updates • have a documented plan to install missing patches as soon as is reasonably practicable or, • adopt additional risk reduction measures to minimise any residual risk where patching cannot be carried out. • maintain a register of obsolete platforms/devices (as part of configuration management register/database).
B4.b.A.1 B4.b.PA.1	***[assets that need to be carefully configured]*** assets include the in-scope systems themselves and the network devices that provide network functionality and security (e.g. switches, firewalls, VPN software, etc). Any assets that form part of a network boundary are prioritised.
B4.b.A.2	***[All platforms conform]*** all in scope network and information systems, and the wider network devices that provide network functionality and security are appropriately configuration managed.
B4.b.A.6	***[automated decision making, their operation is well understood]*** This explicitly includes systems utilising AI or ML components that are embedded within the platform to perform automated functions and / or tools that automate configuration management or security responses for the licensed service. The operation is well understood requires that the core logic (the ML model or programme) driving these automated decisions is auditable, documented, and subject to change control. You should ensure that the system's decisions are predictable and that any attempt to maliciously manipulate the underlying logic or training data to cause an adverse impact can be detected and prevented.
B4.b.PA.2	***[secure platform and device builds]*** you use well understood, consistent and secured baseline/gold builds across your environments. These builds are suitably hardened.
B4.b.PA.4	***[approved and documented]*** you implement configuration management policies that govern configuration changes. Technical documentation of the networks and information systems is up to date.
B4.b.PA.6	***[Service accounts are appropriately protected]*** All system-level or non-human accounts used for automated processes, inter-service communication, or running applications should be secured using technical controls like strong, unique, and complex passwords/keys that are regularly rotated, restricted access (least privilege), and isolated from human user accounts. Passwords should be stored in a secured vault or managed by a secret management tool.

IGP Ref	Examples of Evidence to support IGPs
B4.b.A.1 B4.b.PA.1 B4.b.PA.4	A configuration management and patching policy, with associated processes. These processes describe how: • a case of misconfiguration or out of date patching is identified. • tickets are raised to complete any re-configuration or patching that is required. • your configuration register/database is updated to reflect the completion of the tickets.

B4.b.A.1 B4.b.A.2 B4.b.PA.1 B4.b.PA.2 B4.b.PA.4	A configuration management register/database that captures all configurable devices and their configuration status. This register/database may be a component of your asset-register or may be a stand-alone document.
B4.b.A.1 B4.b.PA.1	Documented baseline builds and build images.
B4.b.A.1 B4.b.A.2 B4.b.PA.1	An asset register that conforms to Interpretation at A3.a
B4.b.A.1 B4.b.PA.1	Audit logs demonstrating compliance with secure baseline builds across the NIS estate.
B4.b.A.6	Backups of all current ‘known good’ configurations of devices.
B4.b.A.6	Audit Documentation for Automated Logic. If AI/ML components are used within the NIS for configuration validation or automated decision-making, evidence should include documentation that details the logic, security constraints, and monitoring in place to detect malicious manipulation of the model or its training data.
B4.b.PA.6	Policy and technical configurations detailing the securing of Service accounts, including password complexity, rotation, and use of secret management tools.
B4.b.PA.7	Evidence of technical controls (e.g., application whitelisting, UAC settings) that prevent standard users from making security-impacting changes.

References and Further Guidance

• B.4 System security - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	PR.PS-01
• ISO 27001/27002:2022 Control:	8.9
• NIST SP 800-53 Rev. 5 Control:	CM-6, CM-7

10.6.4 B4.c Secure Management

B4.c Secure Management		
You manage your organisation's network and information systems that support the operation of your essential function(s) to enable and maintain security.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B4.c.NA.1 Your systems and devices supporting the operation of the essential function(s) are administered or maintained from devices that are not corporately owned and managed.	**B4.c.PA.1** Your systems and devices supporting the operation of the essential function(s) are only administered or maintained by authorised privileged users from *devices sufficiently separated*, using a risk-based approach, from the activities of standard users.	**B4.c.A.1** Your systems and devices supporting the operation of the essential function(s) are only administered or maintained by authorised privileged users from *highly trusted devices, such as Privileged Access Workstations,* dedicated solely to those operations.
B4.c.NA.2 You do not have good or current technical documentation of your network and information systems.	**B4.c.PA.2** Technical knowledge about network and information systems, such as documentation and network diagrams, is regularly reviewed and updated.	**B4.c.A.2** You regularly review and update technical knowledge about network and information systems, such as documentation and network diagrams, and ensure they are securely stored.
	B4.c.PA.3 You prevent, detect and remove malware, and unauthorised software. You use technical, procedural and physical measures as necessary.	**B4.c.A.3** You prevent, detect and remove malware, and unauthorised software. You use technical, procedural and physical measures as necessary.

IGP Ref	IGP Interpretation
B4.c.A.1	***[highly trusted devices, such as Privileged Access Workstations]*** The principle of using a "highly trusted device" is to ensure that all privileged administrative actions originate from a hardened, isolated, and monitored environment that is segregated from high-risk activities like email and general web browsing. While a physical Privileged Access Workstation (PAW) is an example, this outcome can also be effectively achieved through various contemporary architectural patterns. These include, but are not limited to: • Secure Administrative Hosts: Utilising hardened bastion hosts or jump servers as the sole, mandatory gateway for all administrative access. • Privileged Access Management (PAM) Solutions: Implementing comprehensive PAM tools that broker all privileged sessions, providing credential protection, session isolation, and detailed auditing. The key consideration is not the specific technology used, but the demonstrated effectiveness of the chosen solution in segregating administrative sessions from common threats and ensuring all privileged activity is logged and auditable.
B4.c.PA.1	***[Devices sufficiently separated]***The key consideration is not the specific technology used, but the demonstrated effectiveness of the chosen solution in segregating administrative sessions from common threats and ensuring all privileged activity is logged and auditable.

IGP Ref	• Examples of Evidence to support IGPs

B4.c.A.1	Documented build and configuration standards for that environment, detailing hardening requirements and software restrictions.
B4.c.A.2	A formal policy mandating that all privileged access should originate from the designated secure administrative environment.
B4.c.A.2	Sample logs (e.g., from a bastion host, PAM tool, or firewall) demonstrating that privileged sessions originate exclusively from the secure environment.
B4.c.A.3	Network diagrams clearly illustrating the segregation of the secure administrative environment from general user networks.
B4.c.A.3	Live technical controls (e.g., firewall rules, network access control lists) that enforce this segregation.
B4.c.A.4	Audit records proving that privileged activity is comprehensively logged and can be traced to a unique, authenticated user account.
B4.c.A.5	Evidence of a documented process for the secure version control and storage of technical documentation.
B4.c.PA.1	Identity and Access Management (IAM) configurations defining which specific roles are authorised to use the secure environment.
B4.c.PA.1	Meeting the baseline for Tier 2 B2.c Privileged User Management.

References and Further Guidance	
• B.4 System security - NCSC.GOV.UK	
• NCSC: Secure System Administration: https://www.ncsc.gov.uk/collection/secure-system-administration	
• NIST CSF 2.0 Subcategory:	PR.PS-02, PR.PS-03
• ISO 27001/27002:2022 Control:	7.13, 8.18
• NIST SP 800-53 Rev. 5 Control:	MA-1, PL-2

10.6.5 B4.d Vulnerability Management

B4.d Vulnerability Management		
You manage known vulnerabilities in your network and information systems to prevent adverse impact on your essential function(s).		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B4.d.NA.1 You do not understand the exposure of network and information systems supporting your essential function(s) to publicly-known vulnerabilities.	**B4.d.PA.1** You *maintain a current understanding of the exposure* of network and information systems supporting your essential function(s) to publicly-known vulnerabilities.	**B4.d.A.1** You *maintain a current understanding of the exposure* of network and information systems supporting your essential function(s) to publicly-known vulnerabilities.
B4.d.NA.2 You do not mitigate externally exposed vulnerabilities promptly.	**B4.d.PA.2** Announced vulnerabilities for all software packages used in network and information systems supporting your essential function(s) are tracked, *prioritised* and *externally exposed* vulnerabilities are mitigated (e.g. by patching) promptly.	**B4.d.A.2** Announced vulnerabilities for all software packages used in network and information systems supporting your essential function(s) are tracked, *prioritised* and mitigated (e.g. by patching) promptly.

B4.d.NA.3 You have not recently tested to verify your understanding of the vulnerabilities of network and information systems supporting your essential function(s)	**B4.d.PA.3** Some vulnerabilities that are not externally exposed have *temporary mitigations* for an extended period.	**B4.d.A.3** You *regularly test* to fully understand the vulnerabilities of network and information systems supporting your essential function(s) and verify this understanding with third-party testing.
B4.d.NA.4 You have not suitably mitigated systems or software that is no longer supported.	**B4.d.PA.4** You have temporary mitigations for unsupported systems and software while *pursuing migration to supported technology.*	**B4.d.A.4** You actively maximise the use of supported software, firmware and hardware in your network and information systems supporting your essential function(s).
B4.d.NA.5 You are not pursuing replacement for unsupported systems or software.	**B4.d.PA.5** You *regularly test* to fully understand the vulnerabilities of network and information systems supporting your essential function(s).	

IGP Ref	IGP Interpretation
B4.d.A.1 B4.d.PA.1	***[maintain a current understanding of the exposure]*** you have a process of identifying known vulnerabilities for your network and information systems. You use a range of sources including subscribing to vendor security notices, monitoring threat intelligence sources and websites hosting common vulnerabilities and exposures data. You are able to quickly identify the network and information systems that are affected by these vulnerabilities and exposures.
B4.d.A.2 B4.d.PA.2	***[prioritised]*** The means by which you record vulnerabilities allow you to prioritise them according to risk. You use this prioritised vulnerability data to inform your risk management process and your system management and patching process.
B4.d.A.3 B4.d.PA.5	***[regularly test]*** You undertake scheduled (planned and periodic) test activity for your IT and CLF environments at least annually and on major system changes / updates. Test activity includes penetration testing and vulnerability scans. You schedule your testing according to risk and you prioritise your networks' boundary devices. Your approach to testing takes account of the risk of testing in a live environment and you have considered approaches such as testing your baseline builds/gold builds in a lab environment.
B4.d.PA.2	***[externally exposed]*** You do not accept temporary mitigations and/or risk acceptance to vulnerabilities and exposures that are exposed to the IT network boundary, or the IT/internet boundary. All such vulnerabilities and exposures at your network boundaries are patched in accordance with targets stipulated in your patching policy.
B4.d.PA.3	***[temporary mitigations]*** • You understand which of your assets cannot be patched to remove vulnerabilities and, where they remain in use, you have made a risk-based decision to do so. Your risk-based decision has taken account of the criticality of the system and any temporary mitigations that are in place. The residual risk is being owned at the appropriate level. (Note: this does not apply to devices exposed to external network segments). • The mitigations chosen will depend on circumstances, however they may include further network segregation and/or measures to ensure that the vulnerable system only receives trusted data. In circumstances where the risk is demonstrably low it may be reasonable to accept rather than mitigate/treat the residual risk.
B4.d.PA.4	***[pursuing migration to supported technology]*** You understand how long you are likely to continue to carry the risk of unsupported systems and your security improvement plan identifies when the unsupported technology will be replaced.

IGP Ref	Examples of Evidence to support IGPs
B4.d.A.1 B4.d.PA.1	Your configuration management registers/databases are being regularly updated with applicable vulnerabilities and exposures (i.e., those that affect your network and information systems).
B4.d.A.1 B4.d.A.2 B4.d.PA.1 B4.d.PA.2	Your configuration management registers/databases are built such that you can use filters to identify the networks and information systems that may be exposed to new vulnerabilities (meaning you can filter for all platforms that are running particular specific software versions).
B4.d.A.1 B4.d.PA.1 B4.d.PA.3	Your configuration management registers/databases contain details of networks and information systems that remain exposed to vulnerabilities and provide details of any compensating controls/temporary mitigations that you have implemented.
B4.d.A.1	Evidence of a formal process for tracking, prioritising, and mitigating announced vulnerabilities specifically for software packages used within the load control environment.
B4.d.A.2	Records demonstrating that systems, software, firmware, and hardware are actively assessed for and migrated from an unsupported status.
B4.d.PA.4	A security improvement plan detailing the improvement activity that will provide a full mitigation for the identified vulnerabilities.
B4.d.PA.5	A security testing policy that details how you test IT and load control environments. This policy will describe how you intend to use internal and/or third-party resources to conduct testing and will define the scope of tests and the interval at which they occur.
B4.d.PA.5	Copies of all test results from the point at which your security testing policy was introduced.

References and Further Guidance	
• B.4 System security - NCSC.GOV.UK	
• Vulnerability Management - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	ID.RA-01, ID.RA-08
• ISO 27001/27002:2022 Control:	8.8
• NIST SP 800-53 Rev. 5 Control:	RA-5, SI-2

10.7 Principle B5 Resilient Networks and Systems

10.7.1 Principle B5 Extended Guidance

Principle B5 focuses on building resilience into the load control service to ensure it can withstand and recover from cyber-attacks and system failures. This principle provides the practical framework for meeting the statutory requirements of the NIS Regulations, specifically Regulation 10(1) and 10(2), and the obligations set out in Licence Conditions 9 and 10. These regulatory pillars require providers to take appropriate and proportionate measures to minimise the impact of incidents and ensure the continuity of the essential service.

The scoping exercise is the critical foundation for this principle, as it identifies the essential functions, systems, and data that must be prioritised for protection and rapid restoration. This principle is closely integrated with the wider protective suite. Resilience preparation and design are the practical realisation of the security by design concepts established in Principle B4, while backup strategies build directly upon the data protection requirements of Principle B3.

To ensure effective resilience, the organisation should focus on the following core areas:

- **Resilience Preparation and Design (B5.a and B5.b):** This involves architecting the load control platform to be inherently resilient, ensuring that critical components have redundancy that is proportionate to the risk of service disruption. The system should be designed to fail gracefully without compromising the wider energy network. This is a proactive requirement where security and availability are considered at the earliest stages of system design to satisfy the requirement for service continuity in an appropriate manner.
- **Validation and Testing (B5.a):** An untested recovery plan represents only a theoretical capability. Effectiveness is demonstrated through a structured testing regime that is appropriate to the complexity of the service. This moves from foundational validation, such as tabletop exercises to confirm the integrity of the plan, toward more advanced functional testing. This includes technical validation such as the test restoration of critical databases and complex simulations like failing over to secondary cloud regions or infrastructure.
- **Backups and Data Integrity (B5.c):** Establishing robust backup processes for all critical operational data and system configurations identified during the scoping exercise. The organisation must ensure that backups are not only performed regularly but are also protected from being compromised in the same event that affects the primary systems, for example, through the use of offline or immutable storage.

The depth, frequency, and scale of resilience testing should be driven by the organisation's risk assessment to ensure the approach remains proportionate. The goal is to move beyond documenting what is needed for restoration to a state where the underlying architecture is demonstrably resilient and recovery procedures are proven through practical exercise, providing the necessary assurance required by the Competent Authority.

10.7.2 B5.a Resilience Preparation

B5.a Resilience Preparation		
You are prepared to restore the operation of your essential function(s) following adverse impact to network and information systems.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.

B5.a.NA.1 You have limited understanding of all the elements that are required to restore operation of network and information systems supporting your essential function(s).	**B5.a.PA.1** *You know* all network and information systems, and underlying technologies, that are *necessary to restore the operation* of your essential function(s) and understand their interdependence.	**B5.a.A.1** You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness. Appropriate use is made of different test methods (e.g. manual fail-over, table-top exercises, or red-teaming).
B5.a.NA.2 You have not completed business continuity and disaster recovery plans for network and information systems, including their dependencies, supporting the operation of the essential function(s).	**B5.a.PA.2** You know the order in which systems need to be recovered to efficiently and effectively restore the operation of the essential function(s).	**B5.a.A.2** You use your security awareness and threat intelligence sources to identify new or heightened levels of risk, which result in immediate and potentially temporary security measures to enhance the security of your network and information systems (e.g. in response to a widespread outbreak of very damaging malware).
B5.a.NA.3 You have not fully assessed the practical implementation of your business continuity and disaster recovery plans.		

IGP Ref	IGP Interpretation
B5.a.PA.1	***[You know][necessary to restore the operation]*** • For a Load Control provider, fulfilling this indicator goes beyond simply creating a list of systems. The phrase "know all network and information systems...necessary to restore" implies having justified confidence that the identified systems, data, and their interdependencies are correct and sufficient. • This confidence cannot be achieved through documentation alone; it should be grounded in validation. Therefore, as part of meeting this indicator at the 'Partially Achieved' baseline, it is expected that an organisation will have conducted, at a minimum, foundational testing of its business continuity and disaster recovery (BCDR) plans. This does not require the comprehensive, threat-led exercises described under the 'Achieved' state. Rather, it requires evidence that the core assumptions of the BCDR plan have been tested for practicality. This could include: • Tabletop exercises to walk through the documented plan and confirm that the identified roles, responsibilities, and system recovery sequences are logical and understood. • Basic technical validation of key components, such as performing a test restoration of critical data from backups (as required by B5.c) to ensure their integrity and usability for recovery. • An untested plan represents only a theoretical capability. By conducting this foundational testing, an organisation can provide assurance that it truly "knows" what is necessary for restoration and has a practical basis for its resilience planning.

IGP Ref	Examples of Evidence to support IGPs
B5.a.A.1	The BCDR documented plan itself, clearly identifying the critical systems, data, interdependencies, and the prioritised sequence for recovery of the licensed CLF service.
B5.a.A.3	A document or log demonstrating that any issues, gaps, or incorrect assumptions identified during testing have been formally captured and are tracked for remediation to improve the BCDR plan.
B5.a.A.4	Evidence that the BCDR plan has been walked through with relevant personnel. This could include meeting invitations, minutes, and a summary report detailing the scenario, discussion points, and outcomes.
B5.a.A.4	Records of foundational technical tests, such as a report confirming the successful test restoration of critical data or system configurations from backups.
B5.a.A.4	Evidence of formal procedures for deploying immediate and temporary security measures when new or heightened levels of risk are identified through security awareness and threat intelligence sources (e.g., pre-approved actions for isolating critical systems, emergency patching policies).

References and Further Guidance	
• B.5 Resilient networks and systems - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	ID.IM-04
• ISO 27001/27002:2022 Control:	5.29, 5.30
• NIST SP 800-53 Rev. 5 Control:	CP-2, CP-1

10.7.3 B5.b Design for Resilience

B5.b Design for Resilience		
You design network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B5.b.NA.1 Network and information systems supporting the operation of your essential function(s) are not appropriately segregated.	**B5.b.PA.1** Network and information systems supporting the operation of your essential function(s) are *logically separated from your business systems* (e.g. they reside on the same network as the rest of the organisation but within a DMZ).	**B5.b.A.1** Network and information systems supporting the operation of your essential function(s) are segregated from other business and external systems by *appropriate technical and physical means* (e.g. separate network and system infrastructure with independent user administration).
B5.b.NA.2 Internet services, such as browsing and email, are accessible from network and information systems supporting the essential function(s).	**B5.b.PA.2** Internet services, such as browsing and email are not accessible from network and information systems supporting your essential function(s).	**B5.b.A.2** Internet services, such as browsing and email, are not accessible from network and information systems supporting your essential function(s).
B5.b.NA.3 You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential function(s).	**B5.b.PA.3** *Resource limitations* (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.	**B5.b.A.3** You have identified and mitigated all resource limitations (e.g. bandwidth limitations and single network paths).

		B5.b.A.4 You have identified and mitigated any geographical constraints or weaknesses. (e.g. systems that your essential function(s) depends upon are replicated in another location, important network connectivity has alternative physical paths and service providers).
		B5.b.A.5 You review and update assessments of dependencies, resource and geographical limitations and mitigations when necessary.

IGP Ref	IGP Interpretation
B5.b.A1	***[appropriate technical and physical means]*** The objective of this indicator is to ensure the systems supporting the licensed service are robustly isolated from less trusted environments, such as corporate networks or the public internet, thereby preventing unauthorised access and lateral movement by an attacker. The CAF example of "separate network and system infrastructure" describes one method of achieving this outcome, often associated with physical separation or air-gapping. While effective, this is not the only acceptable approach and may be disproportionate or impractical for organisations utilising contemporary, cloud-based architectures. The security outcome of segregation can be met through the implementation of robust, well-architected, and assured logical controls that provide an equivalent level of isolation. Examples of appropriate technical means include, but are not limited to: • Cloud Network Virtualisation: The use of separate Virtual Private Clouds (VPCs) or Virtual Networks (VNets) to create logically isolated environments for the licensed service systems. • Strict Access Control: Enforcing strict ingress and egress rules using network security groups, firewall policies, and private endpoints to ensure that only authorised and expected traffic can flow between the segregated environment and other networks. • Identity-Based Segmentation: Utilising separate identity management systems or distinct, strictly controlled portions of a central system (e.g., separate organisational units with no trust relationships, different tenants) for user and service administration. • Software-Defined Segmentation and Micro-segmentation: Implementing more advanced, dynamic controls where network access policies are not tied to static IP addresses but are defined and enforced in software. This approach, often a core component of a "Zero Trust" architecture, allows for very granular isolation (micro-segmentation) of individual workloads or applications. Access decisions are made dynamically based on a range of attributes, such as user identity, device health, application labels, and the specific process attempting to communicate. The key consideration is not the physical nature of the separation, but the demonstrable effectiveness of the chosen controls. The organisation should be able to provide evidence and assurance that its logical segregation is strong, has no unintended bypasses, and is actively monitored and maintained.

B5.b.PA.1	***[logically separated from your business systems]*** your network design is based around the segregation principle. You have grouped your services and systems into logical segments that take account of their criticality. You have ensured that your CLF networks, and any other systems that you have identified as being critical, are segregated from your enterprise systems.
B5.b.PA.3	***[Resource limitations]*** You have analysed your network infrastructure and identified single points of failure and choke points. You are planning upgrades to resolve these issues where the risk they pose exceeds your risk appetite.

IGP Ref	Examples of Evidence to support IGPs
B5.b.A.1	Policy-as-Code (PaC) or Infrastructure-as-Code (IaC) Definitions: Files from a version control system (e.g., Git) containing the code used to define and enforce segmentation policies.
B5.b.A.1	Micro-segmentation Policy and Rule Sets: Exported policies or screenshots from the specific micro-segmentation tool. This should clearly show rules that define allowed traffic between individual workloads or applications based on labels or attributes, not just IP addresses.
B5.b.A.1	Attribute and Labelling Schema: Documentation defining the organisation's schema for labels and attributes used in policy decisions. For example, a data dictionary explaining what labels mean and how they are applied to workloads.
B5.b.A.1	Dynamic Policy Enforcement Logs: Specific log samples that demonstrate access being granted or denied based on dynamic attributes.
B5.b.A.1	Zero Trust Architecture Documentation: If the implementation is part of a wider "Zero Trust" strategy, the high-level design documents for that architecture would be relevant.
B5.b.A.1	Identity and Access Management (IAM) policy documents and role definitions that demonstrate separate administrative domains or strictly controlled, limited permissions between environments.
B5.b.A.1	Results from a recent penetration test or security audit conducted by an independent third party, specifically validating that the logical segregation controls are effective and have no bypasses.
B5.b.A.1	Sample audit logs from network devices or cloud services showing that traffic is being controlled in line with policies (e.g., logs of denied traffic attempts).
B5.b.A.1	Change management records demonstrating that any modifications to segregation controls (e.g., firewall rule changes) follow a formal review and approval process.
B5.b.A.2	Technical access control lists (ACLs) or firewall policies that enforce the segregation required by B5.b.PA.2 and B5.b.A.2, specifically blocking all protocols related to Internet services, browsing, and email from the Network and Information Systems.
B5.b.A.3	Exported configurations or screenshots of cloud networking rules (e.g., Network Security Groups, firewall policies, VPC peering configurations) that enforce the documented segregation and redundancy.
B5.b.PA.1	High-level and detailed network architecture diagrams illustrating the logical separation of environments (e.g., separate VPCs/VNets for the licensed service vs. corporate IT).
B5.b.PA.3	Entries in risk registers where lack of network and information system resilience presents a risk to the essential service in the event of a loss of connectivity.
B5.b.PA.3	Evidence (e.g. risk register entries, mitigation plans) demonstrating that resource limitations (e.g. single network paths) have been identified and are being mitigated.

References and Further Guidance

- B.5 Resilient networks and systems - NCSC.GOV.UK
- NCSC Network Architectures: https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/network-architectures
- NCSC Network security fundamentals: https://www.ncsc.gov.uk/guidance/network-security-fundamentals

• NCSC Architecture and configuration: https://www.ncsc.gov.uk/collection/10-steps/architecture-and-configuration	
• NIST CSF 2.0 Subcategory:	PR.IR-03, PR.IR-04
• ISO 27001/27002:2022 Control:	8.14, 8.22
• NIST SP 800-53 Rev. 5 Control:	CP-6, SC-5

10.7.4 B5.c Backups

B5.c Backups		
You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s) following an adverse impact to network and information systems.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B5.c.NA.1 Backup coverage is incomplete and does not include all relevant data and information needed to restore the operation of your essential function(s).	**B5.c.PA.1** You have *appropriately secured backups* (including data, configuration information, software, equipment, processes and knowledge). These backups will be accessible to recover from an extreme event including *ransomware attack.*	**B5.c.A.1** Your *comprehensive, automatic and tested* technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event.
B5.c.NA.2 Backups are not frequent enough for the operation of your essential function(s) to be restored effectively.	**B5.c.PA.2** You *routinely test backups* to ensure that the backup process function(s) correctly and the backups are usable.	**B5.c.A.2** Backups of all important data and information needed to recover the essential function(s) are made, *tested, documented and routinely reviewed*.
B5.c.NA.3 Your restoration process does not restore your essential function(s) in a suitable time frame.		

IGP Ref	IGP Interpretation
B5.c.A.1	***[comprehensive, automatic and tested]*** Your backup policy details how backups of all of the software, configurations, data and other relevant information for your network and information systems are maintained. You have employed automatic backup procedures wherever it is appropriate to do so. The creation of back-ups should be part of your engineering change management process and scheduled through any computerised maintenance management system (CMMS) established for work scheduling.
B5.c.A.2	***[tested, documented and routinely reviewed]*** You follow a documented process for confirming that your set of backups is complete and that you are able to efficiently use these backups to restore your systems.

B5.c.PA.1	***[appropriately secured backups]*** you maintain a set of backups that are secured off-line. The core security outcome of this indicator is to ensure that backups are stored in a manner that protects them from the same event that might compromise the primary systems. A primary threat in this context is ransomware, which often seeks to encrypt or delete backups to prevent recovery, but this also includes regional service failures or catastrophic administrative errors. While securing backups off-line or in an air-gapped physical environment is a valid and highly effective method for on-premise platforms, it is not the only one. For organisations utilising cloud-based architectures, an equivalent or greater level of resilience can be achieved through robust logical and architectural controls. The goal is to create a separation, be it administrative, logical, or geographical, that prevents a single attack or failure from affecting both the live system and its ability to be recovered. Appropriate contemporary methods for securing cloud-based backups to ensure resilience and recovery include, but are not limited to: • Geo-Redundant Storage: Utilising native cloud services to automatically replicate backups to a separate, geographical region, with consideration of which geo-locations Government considers appropriate for the handling of UK sensitive data. This protects against a large-scale regional outage affecting the primary data centre. • Logically Segregated Storage with Immutability: Storing backups in dedicated, isolated cloud storage (e.g., a separate storage account) where immutability policies (object locks) are enforced. This makes backup data unchangeable for a defined period, providing a powerful defence against ransomware that targets backup files. • Cross-Account/Subscription Replication: Replicating backups to a completely separate cloud account or subscription with a distinct set of credentials and identity management controls. This ensures that even a full compromise of the primary environment's administrative credentials does not grant access to destroy the backups. • Full Site or Service Replication: For services requiring very high availability, maintaining a full, replicated 'hot' or 'warm' standby of the service in a separate region. This replicated site functions as a near real-time backup, allowing for very rapid recovery. The chosen method should be appropriate for the technology in use and demonstrably effective at preventing the concurrent loss of both primary systems and their backups.
B5.c.PA.1	***[ransomware attack]*** Secured backups should employ mechanisms like immutability (write-once, read-many storage), air-gapping (physical or logical separation), or cross-account/geo-redundancy to prevent their modification or deletion in the event of a successful compromise of the live production environment. The recovery plan should explicitly test restoration following a simulated encryption event.
B5.c.PA.2	***[routinely test backups]*** You follow a documented process for confirming that your set of backups is complete and that you are able to efficiently use these backups to restore your systems.

IGP Ref	Examples of Evidence to support IGPs
B5.c.A.1	Documentation confirming the use of immutable storage, air-gapping, or logical segregation (cross-account/subscription replication) to protect backups from the effects of a ransomware attack.
B5.c.A.1	Change Management Records: Evidence that any changes to the backup configuration or policies follow a formal review and approval process.

B5.c.A.1	Cloud Configuration Records: Screenshots or exported configurations from the cloud provider's console clearly showing that backup data is being replicated to a different geographical region or a separate administrative account/subscription.
B5.c.PA.1	Backup and Recovery Policy: The formal policy document detailing the organisation's strategy, including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), and specifying the chosen technical solution for securing backups.
B5.c.PA.2	Test Results: Documentation from recent recovery tests that prove data can be successfully restored from the secured backup.

References and Further Guidance	
• B.5 Resilient networks and systems - NCSC.GOV.UK	
• Ransomware-resistant backups - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	PR.DS-11
• ISO 27001/27002:2022 Control:	8.13
• NIST SP 800-53 Rev. 5 Control:	CP-9

10.8 Principle B6 Staff Awareness and Training

10.8.1 Principle B6 Extended Guidance

Principle B6 addresses the critical human element of cyber security. It recognises that even the most advanced technical controls can be undermined if staff lack the awareness, knowledge, and skills to operate securely. The scoping exercise is a vital prerequisite for this principle, as it helps identify the specific roles and individuals whose actions directly impact the security and integrity of the load control service.

The implementation of this principle ensures that people are a strong link in the defensive chain. For load control providers, the strategy should focus on the following areas:

- **Cyber Security Culture (B6.a):** This involves moving beyond the mere dissemination of information to deeply embedding security into the organisation's core values and daily operations. A positive security culture ensures that staff at all levels feel empowered to report potential issues and understand how their individual behaviours contribute to the resilience of the load control service.
- **Cyber Security Training and Competence (B6.b):** The organisation must define and deliver training that is tailored to the specific risks identified in the load control environment. This includes ensuring that personnel with access to sensitive command and control functions receive specialised training. Effectiveness is maintained by tracking completion, refreshing content at suitable intervals, and routinely evaluating whether the training is being absorbed and applied in practice.
- **Adapting to Evolving Social Engineering Threats (B6.b):** The threat landscape is rapidly changing, with threat actors increasingly using technologies such as AI and deepfakes to perform sophisticated social engineering. This includes methods like voice cloning for help desk impersonation to compromise credentials and bypass security protocols. Training and awareness programmes must be continuously updated and routinely evaluated to ensure staff are equipped to recognise and respond to these evolving methods.

The development of these cultural and evaluation mechanisms should be guided by the organisation's own risk assessment. The goal is to ensure that the level of investment in training and awareness is appropriate to the complexity of the service and proportionate to the potential impact of a human-facilitated security breach on the wider energy network.

10.8.2 B6.a Cyber Security Culture

B6.a Cyber Security Culture
You develop and maintain a positive cyber security culture and a shared sense of responsibility.

Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B6.a.NA.1 People in your organisation don't understand what they contribute to the cyber security of network and information systems supporting your essential function(s).	**B6.a.PA.1** Your executive management understand and widely communicate the importance of a positive cyber security culture. Positive attitudes, behaviours and expectations are described for your organisation.	**B6.a.A.1** Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations.
B6.a.NA.2 People in your organisation don't know how to raise a concern about cyber security.	**B6.a.PA.2** All people in your organisation understand the contribution they make to the security of network and information systems supporting your essential functions(s).	**B6.a.A.2** People in your organisation raising potential cyber security incidents and issues are treated positively.
B6.a.NA.3 People believe that reporting issues may get them into trouble.	**B6.a.PA.3** All individuals in your organisation know who to contact and where to access more information about cyber security. They know how to raise a cyber security issue.	**B6.a.A.3** Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure.
B6.a.NA.4 Your organisation's approach to cyber security is perceived by staff as hindering the business of the organisation and may encourage poor security behaviours.	**B6.a.PA.4** You identify and address issues that inhibit people from behaving in a manner that supports your intended cyber security outcomes.	**B6.a.A.4** Your management is seen to be committed to and actively involved in cyber security.
B6.a.NA.5 Formal or informal incentives and rewards conflict with the promotion of positive security outcomes.		**B6.a.A.5** Your organisation communicates openly about cyber security, with any concern being taken seriously.
		B6.a.A.6 People across your organisation collaborate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.

IGP Ref	IGP Interpretation
	There are no specific interpretation of these outcomes and refers readers to Cyber security culture principles - NCSC.GOV.UK.
IGP Ref	**Examples of Evidence to support IGPs**
B6.a.A.1	Board or senior management meeting minutes showing detailed engagement with security topics beyond high-level risk reports.
B6.a.A.1	Evidence that senior leadership participates in and completes the same security awareness training required of all staff.
B6.a.A.2	Records of internal communications (e.g., all-staff emails, intranet articles, records from team meetings) where senior management reinforces the importance of cyber security.
B6.a.A.2	Cyber security exercises and simulations.
B6.a.A.3	Role descriptions that include specific security responsibilities for different positions.

B6.a.A.3	Roles and responsibility matrix (RACI); security responsibilities explicitly stated in job descriptions.
B6.a.A.5	Evidence of a formal mechanism (e.g., staff surveys, interviews, anonymous reporting) used to identify issues that inhibit secure behaviour and address them.
B6.a.A.6	Records demonstrating collaboration in security activities, such as cross-functional working groups on risk review or policy development.
B6.a.PA.1	A board-approved Cyber Security Policy that has been communicated to all staff.
B6.a.PA.1	Business objectives explicitly linked to cyber awareness.
B6.a.PA.4	A clear, documented, and accessible process for any member of staff to report a security concern or incident (e.g., a "report a concern" button or a dedicated email address).

References and Further Guidance	
• B6 Staff awareness and training - NCSC.GOV.UK	
• Cyber security culture principles - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	PR.AT-01
• ISO 27001/27002:2022 Control:	5.4, 6.3
• NIST SP 800-53 Rev. 5 Control:	AT-2, PL-4

10.8.3 B6.b Cyber Security Training

B6.b Cyber Security Training

The people who support the operation of network and information systems supporting your essential function(s) are appropriately trained in cyber security.

Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
B6.b.NA.1 There are teams who operate and support your essential function(s) that lack any cyber security training.	**B6.b.PA.1** You have defined appropriate cyber security training and awareness activities for all roles in your organisation, from executives to the most junior roles.	**B6.b.A.1** All people in your organisation, from the most senior to the most junior, follow appropriate cyber security training paths.
B6.b.NA.2 Cyber security training is restricted to specific roles in your organisation.	**B6.b.PA.2** You use a range of teaching and communication techniques for cyber security training and awareness to reach the widest audience effectively.	**B6.b.A.2** Each individuals cyber security training is tracked and refreshed at suitable intervals.
B6.b.NA.3 Cyber security training records for your organisation are lacking or incomplete.	**B6.b.PA.3** Cyber security information is easily available.	**B6.b.A.3** You routinely evaluate your cyber security training and awareness activities to ensure they reach the widest audience and are effective.
B6.b.NA.4 Training is used as a "silver bullet" for all user security behaviours.		**B6.b.A.4** You make cyber security information and good practice guidance easily accessible, widely available and you know it is referenced and used within your organisation.

B6.b.NA.5 The success of training is only measured by the number of people reached, rather than assessing whether it has a positive impact on security behaviours.		
B6.b.NA.6 Training materials contain out of date or contradictory information, or information that conflicts with other policies, processes or procedures.		

IGP Ref	IGP Interpretation
	There are no specific interpretation of these outcomes and refers readers to Cyber security culture principles - NCSC.GOV.UK.

IGP Ref	Examples of Evidence to support IGPs
B6.b.A.1	Records demonstrating that training content is reviewed at least annually and updated to ensure consistency with current security policies and the evolving threat landscape.
B6.b.A.2 B6.b.A.4	Records of completed training. This should include how failures are managed, additional training support, and tailored training for job roles.
B6.b.A.3	A formal, documented evaluation process that measures the positive impact on security behaviours (e.g., results of phishing simulations, log review of correct IdAM protocol usage, incident reporting rates).
B6.b.A.5	Documentation that identifies and addresses where training may be used inappropriately as a substitute for necessary technical controls.
B6.b.PA.1 B6.b.PA.2	Details of all cyber security training provided by your organisation. Ideally this would take the form of an organisational cyber security training plan.

References and Further Guidance	
• B6 Staff awareness and training - NCSC.GOV.UK	
• Cyber security culture principles - NCSC.GOV.UK	
• NIST CSF 2.0 Subcategory:	PR.AT-02
• ISO 27001/27002:2022 Control:	6.3
• NIST SP 800-53 Rev. 5 Control:	AT-3

11 Objective C: Detecting cyber security events

11.1 CAF Objective C Expected Outcome:

The organisation monitors the security status of network and information systems supporting the operation of essential function(s) in order to detect security events indicative of a security incident.

11.2 Objective C Extended Guidance:

Objective C marks a critical shift from prevention (Objective B) to detection. While Objective B aims to build robust defences, Objective C presumes that determined threat actors may still find a way through. The scoping exercise is fundamental to this objective, as it defines the specific technical and data landscape that must be monitored to achieve effective situational awareness.

The focus of this objective is to ensure the organisation can see what is happening on its network and information systems to detect malicious activity before it causes significant impact. For a load control provider, this requires visibility across a complex and distributed environment, including central cloud platforms, consumer applications, API interfaces, and communication paths.

The strategy for detection should focus on the following core areas:

- **Situational Awareness and Monitoring Strategy:** Establishing a coherent, risk-based plan for what needs to be monitored. Rather than just collecting logs, the goal is to understand what constitutes normal behaviour versus anomalous activity that requires investigation. This ensures that resources are focused on the most critical areas of the technical stack.
- **Distributed Visibility:** Ensuring that monitoring covers the entire ecosystem as defined in the scope. This includes not only internal systems but also the external interfaces and data flows that facilitate command and control functions. The level of visibility, and the resources applied to achieve it, must be appropriate to the service and proportionate to the risks identified in Objective A.
- **Proactive Security Event Discovery:** Moving beyond simple signature matching toward active methods of detection. This involves structured threat hunting and the use of threat-informed knowledge to search for unknown or sophisticated threats that may evade traditional automated alerts.

The primary goal of Objective C is to ensure that detection capabilities are built on a solid strategic foundation, evolving toward deep, proactive analysis that protects the integrity of the essential service and the wider energy network.

11.3 Principle C1 Security Monitoring

11.3.1 Principle C1 Extended Guidance

Principle C1 is the foundation of any detection capability. It covers the core activities of collecting the right data through logs, protecting that data, analysing it to generate meaningful alerts, and ensuring the organisation has the necessary tools and skills to respond to any detected anomalies. The scoping exercise is the essential starting point for this principle, as it defines the specific technical boundary and critical data flows that must be monitored to ensure the security of the load control service.

An effective monitoring capability is built on a strong strategic foundation. For load control providers, the approach to security monitoring should focus on the following areas:

- **Monitoring Strategy and Data Sources (C1.a):** A comprehensive monitoring strategy must be evidence-based and aligned with the outcomes of asset management, risk assessment, and the technical architecture of the systems being protected. This ensures that the organisation has a coherent plan for what it needs to monitor and why, focusing resources on the areas of greatest systemic risk.

- **Log Security and Alert Generation (C1.b and C1.c):** The integrity of the monitoring process depends on the security of the logs themselves. Technical controls must be in place to ensure that logs are protected from unauthorised access or tampering. Furthermore, the organisation must be able to generate meaningful alerts from this data, ensuring that malicious activity is identified promptly.
- **Triage and Personnel Skills (C1.d and C1.e):** Generating alerts is only effective if there is a robust process for investigation and triage. This requires personnel or partners with the necessary investigative skills and technical knowledge to understand the context of an alert and determine the appropriate response.
- **Behavioural Understanding and Threat Intelligence (C1.f):** Maturing a monitoring capability involves moving toward a deeper understanding of what constitutes normal user and system behaviour. By integrating threat intelligence, the organisation can enrich its monitoring data, allowing it to proactively investigate complex or non-standard threats that may otherwise go unnoticed.

The depth and complexity of these monitoring activities should be guided by the organisation's risk assessment. The goal is to move from a basic collection of logs toward a state where monitoring coverage is extensive and integrated with multiple intelligence sources, providing the necessary situational awareness to protect the essential function.

11.3.2 C1.a Sources and Tools for Logging and Monitoring

C1.a Sources and Tools for Logging and Monitoring		
The data sources and tools that you include in your logging and monitoring allow for timely identification of events which might adversely affect the security or resiliency of network and information system(s) supporting the operation of your essential function(s).		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
C1.a.NA.1 Data relating to the security and operation of network and information systems supporting your essential function(s) is not collected.	**C1.a.PA.1** *Data* relating to the security and operation of some areas of network and information systems supporting your essential function(s) is collected but coverage is *not comprehensive.*	**C1.a.A.1** Monitoring is based on an *thorough understanding* of network and information systems supporting your essential function(s), common *techniques used by threat actors*, and *awareness* of what logging and monitoring is required to *detect* potential security incidents that could *affect the operation* of your essential function(s).
C1.a.NA.2 You are not able to audit the activities of users and systems in relation to network and information systems supporting your essential function(s).	**C1.a.PA.2** Some user and system monitoring is done, but not covering a fully *agreed list* of *suspicious or undesirable behaviour*.	**C1.a.A.2** Your *monitoring data* provides enough *detail* to *promptly and reliably detect* security events, incidents and support investigations. that could affect the operation of your essential function(s).

C1.a.NA.3 You do not monitor traffic crossing your network boundary.	**C1.a.PA.3** You *monitor* traffic crossing your *network boundary* (including IP address connections as a minimum).	**C1.a.A.3** Extensive monitoring of *user and system activity* in relation to network and information systems that support your essential function(s) enables you to promptly detect policy violations, suspicious or undesirable user and system behaviour, deviations from normal / routine behaviour or *abnormalities indicative of adverse activity*.
C1.a.NA.4 Log data cannot be synchronised using an accurate common time source.	**C1.a.PA.4** Some but not all log datasets can be easily queried with search tools to aid in investigations.	**C1.a.A.4** Your logging and monitoring capability includes *host-based and network monitoring*
C1.a.NA.5 Logs are stored in locations where they are not readily available to authorised users and systems.	**C1.a.PA.5** Your monitoring tools work with most log data, with some configuration.	**C1.a.A.5** All *new* network and information systems supporting your essential function(s systems are considered as potential monitoring data sources to *maintain* a *comprehensive monitoring capability*.
C1.a.NA.6 Your monitoring tools cannot be configured to make use of new log streams as they come online.	**C1.a.PA.6** Your monitoring tools can make use of log data that would capture all common threats.	**C1.a.A.6** Log datasets are synchronised including using an accurate common time source so that separate datasets can be correlated in appropriate ways.
C1.a.NA.7 Your monitoring tools are only able to make use of a fraction of the log data being collected.	**C1.a.PA.7** You ensure log data is available for analysis when needed.	**C1.a.A.7** You enrich log data with other network and information systems data to provide a more comprehensive picture of actions and behaviours.
C1.a.NA.8 You do not understand where log data is stored or how long it should be stored for.		**C1.a.A.8** Your monitoring tools make use of log data to pinpoint activity.
C1.a.NA.9 You have no way of ensuring log data is being captured as expected and available when needed.		**C1.a.A.9** You regularly review the data sources and tools included in your logging and monitoring strategy to ensure it remains effective.

IGP Ref	IGP Interpretation
C1.a.A.1	***[thorough understanding]*** Your monitoring strategy should be directly informed by a documented understanding of your network architecture (**B4**), your assets (**A3**), and the risks posed to them (A2). A documented monitoring strategy is required and should cover monitoring objectives, scope, rationale, and how monitoring aligns with other security processes like incident response and vulnerability management.
C1.a.A.1	***[techniques used by threat actors]*** Part of the required ***[thorough understanding]*** is a specific knowledge of relevant adversary tactics. This explicitly links monitoring rules to intelligence, requiring the use of frameworks like MITRE ATT&CK to design custom detection rules, moving beyond generic IoCs to detecting specific adversary TTPs relevant to the CLF environment.

C1.a.A.1	***[awareness]*** The goal of your monitoring strategy is to achieve situational awareness. This means moving beyond simple log collection to a state where you can collect, analyse, and prioritise information to create actionable intelligence for responsible personnel. This enables effective reporting on the overall health of the networks and information systems. A mature approach will take a holistic view, monitoring for non-cyber issues that could impact the service (e.g., cloud service health) alongside cyber threats.
C1.a.A.1	***[detect]*** This is the core purpose of the monitoring capability. The tools and processes should be configured to reliably identify potential security incidents in the collected data. This requires active analysis and correlation, often with a Security Information and Event Management (SIEM) system, to identify events that require investigation.
C1.a.A.1	***[affect the operation]*** The entire monitoring process should be focused on events that could tangibly impact the delivery of the licensed service. The capability should be designed to detect threats that could lead to service disruption or degradation, enabling a proactive response that supports business continuity and recovery activities.
C1.a.A.2	***[monitoring data]*** This refers to the definition of use cases and technical requirements for monitoring coverage that are necessary to support effective incident response. The organisation should formally define what data it needs to collect from which assets to meet its security objectives.
C1.a.A.2	***[detail]*** The data collected should have sufficient ***[detail]*** to be useful. This is achieved by implementing a variety of appropriate and tailored tools and techniques, which could include: • Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS): Customised for the operating environment. • Malicious Code Protection Monitoring: Including endpoint protection and anti-malware solutions. • Network & Boundary Protection Monitoring: Analysing traffic at key ingress and egress points. • Identity & Access Management (IdAM) Monitoring: Including session monitoring and privileged user tracking. • Security Information and Event Management (SIEM): A central system to aggregate and correlate logs, turning raw data into meaningful security events.
C1.a.A.2	***[promptly and reliably detect]*** Monitoring tools should be strategically deployed within the architecture (e.g., at perimeters and near critical applications). The organisation should ensure that the use of these tools does not adversely impact the performance of the licensed service. For assets where active monitoring is not technically feasible or proportionate, alternative procedural and physical controls should be used to protect them from interference.
C1.a.A.3	***[user and system activity]*** A mature monitoring capability extends beyond general event logging to specific, deep monitoring of user & system activity. This is particularly important for privileged users (such as CLF System Administrators and CLF Platform Operators) who have access to more sensitive information and can potentially do greater damage than non-privileged users. This requires implementing additional, specific logging requirements for privileged roles to ensure that any malicious activity can be identified at the earliest possible time. For an EIT and IoT environment, this monitoring should be comprehensive for central cloud platforms and corporate IT systems.
C1.a.A.3	***[abnormalities indicative of adverse activity.]*** The requirement is to move beyond signature-based detection to User and Entity Behaviour Analytics (UEBA). Monitoring should establish a baseline of normal system and user traffic, and alert on deviations that suggest a compromise (e.g., a service account accessing a code repository or unusual data volume transfers).

C1.a.A.4	***[host-based and network monitoring]*** This involves deploying monitoring capabilities directly on critical endpoint devices. For a Load Control provider, this should be implemented where possible on assets such as, but not limited to: • The core servers, virtual machines, and containers that run the Load Control service. • Engineering, administrative, and operator workstations. • Key assets such as domain controllers or identity management systems.
C1.a.A.5	***[new]*** This ensures that monitoring is not a one-off project but is treated as an ongoing, living process. Monitoring requirements should be formally considered and included in the design, procurement, and change management processes for any new network and information systems supporting your essential functions systems or for significant modifications to existing ones.
C1.a.A.5	***[maintain a comprehensive monitoring capability]*** The programme should be regularly reviewed, at least annually, and updated to ensure it remains effective, with all changes managed through a formal process. This ensures that monitoring coverage evolves in step with the technical environment and the threat landscape.
C1.a.PA.1	***[Data]*** This term refers to the full spectrum of information and log sources that are collected for security monitoring purposes. To meet the 'Achieved' baseline, the scope of data collection cannot be determined in isolation; it should be comprehensive and based on a clear, documented monitoring strategy. This strategy is a direct output of foundational activities completed in other principles, including a comprehensive understanding of the assets that comprise the licensed service (A3 Asset Management) and a thorough assessment of the risks to those assets (A2 Risk Management). The data collected should be of sufficient quality and detail to enable the detection of threats to the licensed service.
C1.a.PA.1	***[not comprehensive]*** This term describes a state where an organisation's monitoring requirements and capability are understood and prioritised, but the collection of data does not yet cover all systems in scope. This is a characteristic of a 'Partially Achieved' state. Information relating to the security status of some lower-priority assets may be omitted. An organisation in this state should be able to demonstrate that it has an actively managed programme of improvement to expand its monitoring coverage over time, prioritised based on its risk assessment.
C1.a.PA.2	***[agreed list]*** This indicates that monitoring for user behaviour is not arbitrary but is based on a defined and formally agreed-upon set of detection rules. The creation of this list is an output of an analysis process where the organisation establishes a baseline of normal, expected user activity for its systems and then defines specific deviations to monitor. This analysis should be informed by the organisation's risk assessment and threat intelligence, with the resulting list of monitoring rules being formally documented, approved, and maintained.
C1.a.PA.2	***[suspicious or undesirable behaviour]*** This term refers to the specific types of activities that would be included on the **[*agreed list*].** These are actions that deviate from established baselines of normal user activity and could indicate a compromise or misuse of systems. The list of behaviours to monitor should be prioritised, focusing on privileged users first, given their greater potential to cause impact. Examples of such behaviours include, but are not limited to: • Anomalous Load Control actions or responses. • Unauthorised configuration changes to critical CLF platforms or applications. • Attempts by a user or process to escalate privileges. • The unauthorised addition or removal of software or system services. • Anomalous changes to important system files or data records.
C1.a.PA.3	***[monitor]*** This refers to the active observation and review of traffic and system logs. To be effective, monitoring requires having defined processes and the technical capability to interrogate the data being collected. It is not passive data collection. At a minimum, this includes monitoring IP traffic metadata (e.g., the 5-tuple of source/destination IP, source/destination port, and protocol) to understand traffic flows and identify anomalous connections.

C1.a.PA.3	***[network boundary]*** A network boundary is a logical or physical perimeter where systems of different trust levels interact. To effectively monitor a boundary, it should first be properly defined and architected using the principles of segregation outlined in Objective B4. Important network boundaries for a CLF provider include, but are not limited to: • Connections between your CLF service environment and the Internet. • The interfaces between your CLF production, test environments and corporate IT networks. • Interfaces to related but out of scope 3rd party CLF systems e.g. Energy trading platforms. • Gateways to any external third-party networks, such as those of partners or large customers.

IGP Ref	Examples of Evidence to support IGPs
C1.a.A.1	A documented process for creating and maintaining the agreed list of suspicious behaviours: This should include the baseline of normal activity and the risk-based criteria used to define what is monitored.
C1.a.A.1 C1.a.A.6	Network Architecture Diagrams: Clearly showing the defined network boundary points, security zones, and the locations of key monitoring sensors and logging points.
C1.a.A.4	Documentation of the baseline established for normal user and system traffic and the defined rules for triggering alerts on abnormalities indicative of adverse activity.
C1.a.A.4	Incident Response Records: Examples of incident reports where security monitoring data was successfully used to detect and investigate a real or simulated security event.
C1.a.A.6	Records of Log Assurance procedures showing ongoing validation that log feeds are active and that data is being ingested from all new NIS components.
C1.a.A.6	System and Tooling Configurations: Evidence of the technical configuration of monitoring tools (e.g., SIEM, IDS, EDR), showing what data sources are being ingested and what detection rules are active.
C1.a.A.6	For host-based monitoring, evidence of agent deployment and configuration on critical assets.
C1.a.A.6	Change Management Records: Demonstrating that new systems are formally assessed for monitoring requirements before being integrated into the licensed service environment.
C1.a.A.8	Logs and Alert Records: Sample logs and screenshots from various sources and alerts from the SIEM or other tools that demonstrate the monitoring system is operational and effective at detecting events.
C1.a.A.9	Documentation of the regular review process for the logging and monitoring strategy and its effectiveness.
C1.a.A.9	Assurance Reports: Results from independent penetration tests or audits (internal/external) that validate the effectiveness of detection controls and the monitoring capability.
C1.a.PA.1	A formal, documented Security Monitoring Strategy: This should detail the scope, objectives, and rationale for the monitoring programme and demonstrate its alignment with the organisation's risk assessment (A2) and system architecture (B4).

References and Further Guidance

• C.1 Security monitoring - NCSC.GOV.UK	
• NCSC Introduction to logging for security purposes: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes	
• NIST CSF 2.0 Subcategory:	DE.CM-01, DE.CM-09
• ISO 27001/27002:2022 Control:	8.16
• NIST SP 800-53 Rev. 5 Control:	AU-6, CA-7

11.3.3 C1.b Securing Logs

C1.b Securing Logs		
You hold log data securely and grant appropriate user and system access only to accounts with a business need. Log data is held for a suitable retention period, after which it is deleted.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
C1.b.NA.1 It is possible for log data to be easily edited or deleted by unauthorised users / systems or attackers.	**C1.b.PA.1** Only authorised users and systems can *access log data*	**C1.b.A.1** Appropriate access to log data is limited to those users and systems with a business need.
C1.b.NA.2 There is no control of the users and systems that can access log data	**C1.b.PA.2** There is some monitoring of access to log data (e.g. copying, deleting or modification, or even viewing).	**C1.b.A.2** The logging architecture has mechanisms, policies, processes and procedures to ensure that it *can protect itself from threats comparable to those it is trying to identify*. This includes protecting the function itself, and the data within it.
C1.b.NA.3 There is no monitoring of the access to log data.	**C1.b.PA.3** You have defined and implemented *retention periods for log data*.	**C1.b.A.3** Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered.
C1.b.NA.4 There are no policies covering access to log data.	**C1.b.PA.4** You have given legitimate reasons for accessing log data in your policies.	**C1.b.A.4** All actions involving log data (e.g. copying, deleting, modification, or even viewing) can be traced back to a unique user or system.
		C1.b.A.5 The integrity of log data is *protected, verified and any modification, including deletion, is detected and attributed*.

IGP Ref	IGP Interpretation
C1.b.A.2	***[can protect itself from threats comparable to those it is trying to identify]*** This requires the logging and security monitoring infrastructure (e.g., SIEM, log aggregators, forensic storage) to be secured to a level at least equal to the NIS they are protecting. This includes: placing the logging environment in a segregated, highly trusted security zone; implementing the principle of least privilege for administration; and enforcing immutable storage (C1.b.A.5) to resist tampering by capable threat actors who attempt to blind the organisation by destroying evidence.

C1.b.A.5	***[protected, verified and any modification, including deletion, is detected and attributed]*** Log data should be protected from unauthorised modification or deletion. This protection should be technical, not just procedural. In a modern cloud environment, this can be achieved through several robust technical means: • Immutable Storage: Utilising cloud storage features (e.g., AWS S3 Object Lock, Azure Blob Storage immutability policies) to make log files "write-once, read-many". This provides a high degree of assurance against ransomware and malicious or accidental deletion, as it prevents anyone, including administrators, from altering or deleting the logs for a defined retention period. • Segregated Log Archives: Architecturally separating the log storage from the production environment. This often involves sending logs to a dedicated, separate cloud account or logging service with its own strict access controls. This ensures that a full compromise of the primary production environment does not automatically grant the attacker the ability to access and tamper with the log archives. • Robust Access Controls: Applying strict, "deny-by-default" Identity and Access Management (IAM) policies that deny modification and deletion permissions for log data to all but a highly restricted break-glass or automated archival service role.
C1.b.PA.1	***[access log data]*** This term describes the capability for authorised users or systems to access and query [log data] as part of an incident response or troubleshooting process. It requires having a defined process and the necessary tools (e.g., a centralised logging platform with a query interface) to allow security personnel or system administrators to access and ***[view]*** logs from critical systems. This capability is fundamental to any incident response process as it allows for the analysis of events, reconstruction of timelines, and identification of indicators of compromise. Access should be based on roles, ensuring that only those with a legitimate need can view potentially sensitive log information.
C1.b.PA.3	***[retention periods for log data]*** a formal policy specifying the required storage duration for different classes of log data (e.g., security, access, operational). Retention periods should be based on a risk-based assessment and regulatory compliance needs (e.g., NIS Regulations, GDPR).

IGP Ref	Examples of Evidence to support IGPs
C1.b.A.1	Technical Configuration records (e.g., cloud storage policies) demonstrating the use of immutable storage or cryptographic hashing to ensure log integrity.
C1.b.A.1 C1.b.A.5	Technical Configuration for Protection: Depending on the method used to ensure logs are ***[protected]***, this could include: • Screenshots or exported configurations showing immutability policies (object locks) applied to cloud storage buckets containing logs. • Architectural diagrams and IAM policies demonstrating that logs are stored in a separate, segregated cloud account with restricted cross-account access. • Specific IAM policy documents that deny modify/delete permissions for log data to all standard administrative roles.
C1.b.A.1	Monitoring Alerts/Reports: Evidence from the monitoring system showing that the availability and synchronisation status of the time service is being tracked.
C1.b.A.4	Audit logs demonstrating monitoring of access to the log data repository itself, proving all viewing, copying, or deletion attempts are traceable to a unique user/system.
C1.b.A.5	Configuration of Integrity Detection: If using log hashing to detect ***[modification]***, evidence would include: • Documentation of the log hashing process. • Evidence of the secure, segregated storage location for the hashes. • Sample reports or logs from the automated comparison tool showing that integrity checks are being performed.

C1.b.PA.1	Access Control Policy for Logging Systems: A formal policy document that defines: • The roles and responsibilities for managing logging infrastructure. • The principle of least privilege for accessing log data. • The specific roles that have a legitimate *business need* to access logs and the rationale for that access. • The formal approval process for granting or modifying access to log data.
C1.b.PA.1	Evidence of Access Control: Role-Based Access Control (RBAC) Configuration: Screenshots or reports from the logging platform or cloud IAM system showing how access ***[is limited]***. This should clearly show different roles (e.g., 'SecurityAnalyst_ReadOnly', 'LogSystemAdmin') with different permission sets. Access Request and Approval Records: Examples of completed access request forms or service desk tickets showing the formal approval process for granting a user access to view log data for investigations.
C1.b.PA.3	A documented Log Retention Policy defining required storage duration based on risk and regulation.

References and Further Guidance	
• C.1 Security monitoring - NCSC.GOV.UK	
• NCSC: Logging for security purposes: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes	
• NCSC Principles for ransomware-resistant cloud backups: https://www.ncsc.gov.uk/collection/ransomware-resistant-backups/principles-for-ransomware-resistant-cloud-backups	
• NIST CSF 2.0 Subcategory:	PR.PS-04
• ISO 27001/27002:2022 Control:	8.15, 8.17
• NIST SP 800-53 Rev. 5 Control:	AU-9, AU-11

11.3.4 C1.c Generating Alerts

C1.c Generating Alerts		
Evidence of potential security incidents contained in your monitoring data is reliably identified and where appropriate triggers alerts.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
C1.c.NA.1 You do not apply updates to your detection security technologies in a timely way, after receiving them (e.g. AV signature updates, other threat signatures or Indicators of Compromise (IoCs)).	**C1.c.PA.1** You easily *detect the presence of Indicators of Compromise (IoCs)* on network and information systems supporting your essential function(s), such as *known malicious command and control signatures.*	**C1.c.A.1** You easily *detect the presence of Indicators of Compromise (IoCs)* on network and information systems supporting your essential function(s), such as *known malicious command and control signatures*, as well as abnormalities or behaviours indicative of adverse activity.
C1.c.NA.2 Security alerts relating to network and information systems supporting your essential function(s) are not prioritised.	**C1.c.PA.2** You apply some updates, new signatures and IoCs in a timely way.	**C1.c.A.2** You apply all updates, new signatures and IoCs promptly.

C1.c.NA.3 The enrichment of security alerts within network and supporting your essential function(s) cannot be performed.	**C1.c.PA.3** Security *alerts* relating to network and information systems that support your essential function(s) are *prioritised*.	**C1.c.A.3** Security *alerts* relating to all network and information systems supporting your essential function(s) are *prioritised* and this information is used to support incident management.
C1.c.NA.4 You do not confidently *detect the presence of IoCs* on network and information systems supporting your essential function(s), such as known malicious command and control signatures (e.g. because applying the indicator is difficult or your log data is not sufficiently detailed).	**C1.c.PA.4** The enrichment of alerts within network and information systems supporting your essential function(s) is performed but not as part of the original alert.	**C1.c.A.4** Alerts are routinely enriched within network and information systems supporting your essential function(s). The *enrichment of these alerts* is performed in almost real time and as part of the original alert.
C1.c.NA.5 You do not monitor for user or system abnormalities indicative of adverse activity.	**C1.c.PA.5** Detections and alerting rely on off the shelf tooling without customisation or users reporting events and potential incidents.	**C1.c.A.5** Alerts and the underlying detections are regularly *reviewed* and tested to ensure they are generated promptly and reliably, and it is possible to distinguish genuine security incidents from false alarms.
C1.c.NA.6 Logs are monitored infrequently.	**C1.c.PA.6** There is a documented and shared process for all users who support the operation of the essential function to report events and potential security incidents.	**C1.c.A.6** Alerts and the underlying detection rules are *customisable and tuned* to reduce false positives as well as optimising responses.
	C1.c.PA.7 Where appropriate, detections and alerting result in automated actions being taken. (e.g. malware identified by AV is quarantined).	***C1.c.A.7*** Detections and alerting may use off the shelf tooling and rules as well as custom tooling and / or rules.
	C1.c.PA.8 You monitor on an irregular basis for user or system abnormalities indicative of adverse activity.	***C1.c.A.8*** You *continuously monitor for user and system abnormalities* indicative of adverse activity generating alerts based on the results of such monitoring.
	C1.c.PA.9 Logs are monitored at regular intervals.	***C1.c.A.9*** Logs are monitored *continuously in near real time.*

IGP Ref	IGP Interpretation
C1.c.A.1 C1.c.PA.1	***[detect the presence of IoCs]*** This requires that an organisation's security monitoring systems can effectively process Indicators of Compromise (IoCs), which may come from threat intelligence feeds or internal analysis, and reliably detect them on the network. IoCs are the digital forensic artefacts that indicate a potential intrusion, such as known malicious IP addresses, file hashes, or command-and-control signatures. To achieve this, an organisation should have justified confidence that its monitoring capability is effective. Consistent with the principles of assurance established in **A2.b**, this confidence cannot be based on assumption; it should be earned through a programme of testing and validation. This validation should include activities such as: • Effective, standards based, testing and commissioning of monitoring and detection systems to ensure they are functioning as designed. • Integration with a capability for continuous analysis and response. This could be a formal in-house Security Operations Centre (SOC), a third-party Managed Detection and Response (MDR) service, or a clearly defined process where qualified internal staff are responsible for responding to critical alerts in a timely manner. • The use of automated tools and platform capabilities to enable a rapid response. While this can extend to dedicated Security Orchestration, Automation, and Response (SOAR) platforms, a proportionate and effective approach for many organisations is to leverage the built-in security features of their existing cloud and enterprise platforms. This includes configuring the native security tools (e.g., Microsoft Sentinel, Microsoft 365 Defender, AWS Security Hub) to take automated actions in response to high-confidence alerts, such as isolating a device, blocking a malicious IP address at the firewall, or disabling a compromised user account. • Regular updates to monitoring systems to maintain their effectiveness against emerging threats. • Documented penetration testing to independently verify the effectiveness of detection controls. Reviewing the performance of monitoring tools as part of broader incident response testing and exercises (as per **Principle D1.c**).
C1.c.A.1 C1.c.PA.1	***[known malicious command and control signatures]*** A mature investigation process uses a wide range of data points, not just simple alerts. This includes searching for specific [signatures and indicators of compromise] across all available log sources to identify related malicious activity. This demonstrates a proactive and in-depth approach to incident investigation.
C1.c.A.3 C1.c.PA.3	***[Alerts]*** In an 'Achieved' state, the resolution of Alerts resolved to network assets becomes a highly efficient process. This means having tooling and processes (such as a SIEM enriched with data from a Configuration Management Database or Asset Inventory) that allow alerts to be mapped to the specific asset that generated them in near-real time, enabling a much faster start to any investigation
C1.c.A.3 C1.c.PA.3	***[prioritised]*** Security alerts should be prioritised for investigation and response. This prioritisation cannot be arbitrary; it should be risk-based. The priority of an alert should be determined by factors such as the criticality of the asset involved (as defined in the asset management process, A3), the potential impact of the incident, and intelligence about the specific vulnerability or threat. For a 'Partially Achieved' state, this means that alerts relating to some critical functions, such as Load Control, or systems are effectively prioritised, even if the process is not yet applied universally across the entire estate.
C1.c.A.4	***[enrichment of these alerts]*** This requires automatically adding context from other systems (e.g., asset inventory, user identity, vulnerability data) to the raw alert data at the point of generation. When performed "as part of the original alert" (C1.c.A.4), it allows the human triage team to immediately assess severity and respond promptly

C1.c.A.6	***[customisable and tuned]*** You can modify detection rules to fit the specific needs and noise profile of the Load Control environment. Tuning is the essential, continuous activity of adjusting rule thresholds and logic to reduce false positives while ensuring genuine security incidents are reliably identified.
C1.c.A.8	***[continuously monitor for user and system abnormalities]*** This requires implementing User and Entity Behaviour Analytics (UEBA) principles to establish a dynamic baseline of normal activity for privileged users and critical services. This monitoring should be continuous to detect low-and-slow threats that rely on deviations from normal behaviour.
C1.c.A.9	***[Logs are monitored continuously in real time]*** In an 'Achieved' state, the review of logs moves from a periodic, scheduled activity to one that is continuous in real time. This is typically achieved through the use of automated tools like a SIEM, which constantly analyses incoming log streams against detection rules, and is often supported by a Security Operations Centre (SOC) function where personnel are actively watching for and triaging alerts as they are generated.

IGP Ref	Examples of Evidence to support IGPs
C1.c.A.1	Alert Management Policy/Procedure: A formal document detailing: • The process for how alerts are investigated. • The risk-based matrix or criteria used to ensure alerts are prioritised. • The defined schedule and responsibilities for when logs are reviewed, for systems not monitored in real-time. • The process for how new detection rules for suspicious activity or alerts are developed and deployed. • The strategy for how and when alerts are tested.
C1.c.A.1 C1.c.A.6	SIEM / Logging Platform Configuration: • Evidence showing that alerts can be resolved to network assets, for example by showing that asset data from a CMDB or inventory is enriching the log data. • Examples of active correlation rules designed to detect suspicious activity or alerts or specific signatures and indicators of compromise.
C1.c.A.4	Incident Response Plan: The section of the plan that details how alerts are triaged and escalated from the monitoring system into a formal incident response process.
C1.c.A.4	Alert and Investigation Records: • Sample records from a ticketing or case management system showing alerts being formally tracked, investigated, and resolved. • Investigation notes or reports showing the outcome of an investigation into a high-priority alert.
C1.c.A.5	Alert Testing and Validation Reports (C1.c.A.5) showing that detection rules are regularly reviewed and tested (e.g., using Breach and Attack Simulation tools) to ensure promptness and reliability.
C1.c.A.6	Query and Analysis Tooling: • Demonstration of the tools used to query log data from various sources. • Role-based access control configurations for these tools, showing who has the authority to query logs.
C1.c.A.8	Evidence of the monitoring setup (e.g., UEBA tooling logs) used for continuous monitoring of user and system abnormalities (C1.c.A.8).
C1.c.PA.4	Log Review Records: For systems where logs are manually reviewed, evidence that these reviews are taking place according to the defined schedule (e.g., checklists, sign-off sheets).

References and Further Guidance

- C.1 Security monitoring - NCSC.GOV.UK
- NCSC Incident Management: https://www.ncsc.gov.uk/section/about-ncsc/incident-management
- NCSC Building a SOC: Incidents: https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/incidents

• NCSC Building a SOC: Detection: https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/detection	
• NIST CSF 2.0 Subcategory:	DE.AE-08
• ISO 27001/27002:2022 Control:	8.16
• NIST SP 800-53 Rev. 5 Control:	AU-6, SI-4

11.3.5 C1.d Triage of Security Alerts

C1.d Triage of Security Alerts

You contextualise alerts with knowledge of the threat and your systems, to identify security incidents as well as responding to all alerts appropriately.

Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
C1.d.NA.1 You do not triage alerts from your detection security technologies (e.g. AV, IDS).	**C1.d.PA.1** You investigate and triage alerts from some security tools and take action.	**C1.d.A.1** You investigate and triage alerts from all security tools and take action.
C1.d.NA.2 You do not categorise alerts and incidents by type and priority / severity level.	**C1.d.PA.2** You have created, made available and use when appropriate, *Standard Operating Procedures (SOPs) / Playbooks / Runbooks* covering the most common use cases. These are regularly reviewed to ensure they remain effective.	**C1.d.A.2** You have created, made available and use when appropriate *Standard Operating Procedures (SOPs) / Playbooks / Runbooks* covering all plausible use cases. These are regularly reviewed to ensure they remain effective.
C1.d.NA.3 You do not have Standard Operating Procedures (SOPs) / Playbooks / Runbooks available for use during triage.	**C1.d.PA.3** You perform some triage and actions taken by monitoring and detection personnel are recorded.	**C1.d.A.3** You categorise alerts and incidents by type and priority / severity level.
C1.d.NA.4 You do not keep records of triage performed.	**C1.d.PA.4** You categorise alerts and incidents by type and priority / severity level.	**C1.d.A.4** You document all triage related activities performed by monitoring and detection personnel and these are *used to drive improvements.*
C1.d.NA.5 You do not have a sufficient understanding of normal user or system behaviour to make effective decisions within triage.	**C1.d.PA.5** Your understanding of normal user or system behaviour informs your decision making within triage.	**C1.d.A.5** Triage provides enough information for *subsequent activities to be prioritised* (e.g. the containment of damaging malware).
C1.d.NA.6 You do not triage alerts from your detection security technologies (e.g. AV, IDS).		**C1.d.A.6** Your understanding of normal user and system behaviour, and threats, is sufficient for effective decision making within triage.

IGP Ref	IGP Interpretation
C1.d.A.2 C1.d.PA.2	***[Standard Operating Procedures (SOPs) / Playbooks / Runbooks]*** These are the documented workflows that guide the actions of the triage team, specifying steps for initial investigation, escalation paths, and containment measures. The progression from "most common" (PA) to "all plausible" (A) use cases requires leveraging risk assessment (A2) and threat modelling (A2.b) to ensure critical but rare scenarios are covered.
C1.d.A.4	***[used to drive improvements]*** The output of the triage process is actionable. It should contain sufficient validated context (e.g., identity of the compromised user/system, initial containment priority, and assessed impact) to allow the Incident Response team (D1) to immediately commence containment without further delay or investigation.
C1.d.A.5	***[subsequent activities to be prioritised]*** This establishes a formal feedback loop. The logged triage actions provide data that should be analysed in the Lessons Learned (D2) process, ensuring the SOPs, monitoring rules, and training are continually refined based on real-world incident handling performance.

IGP Ref	Examples of Evidence to support IGPs
C1.d.A.2	A complete library of SOPs, Playbooks, and Runbooks covering a risk-based selection of scenarios, regularly reviewed for effectiveness.
C1.d.A.2 C1.a.A.4	Evidence that personnel utilise knowledge of normal user/system behaviour during decision-making (e.g., investigation reports noting deviation from baseline).
C1.d.A.3	Policy documentation mandating the categorisation and prioritisation of alerts based on the asset criticality (A3) and threat severity (A2.b).
C1.d.A.4	Triage records or case logs from the SIEM or ticketing system, demonstrating that every alert investigated includes: a priority/severity level, the action taken, and the outcome.
C1.d.A.4	Audit reports showing that the logs of triage activities are systematically reviewed to drive improvements in detection rules and SOPs.
C1.d.PA.2	Standard Operating Procedures (SOPs) or Playbooks covering common or high-risk alert scenarios.
C1.d.PA.3	Case logs demonstrating that alerts are investigated and the results are recorded.
C1.d.PA.4	Policy documentation for the categorisation and prioritisation of alerts.

References and Further Guidance

- C.1 Security monitoring - NCSC.GOV.UK
- NCSC Plan: Your cyber incident response processes: https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes
- NCSC Building a SOC https://www.ncsc.gov.uk/collection/building-a-security-operations-centre

• NIST CSF 2.0 Subcategory:	ID.RA-02, DE.AE-07
• ISO 27001/27002:2022 Control:	5.7
• NIST SP 800-53 Rev. 5 Control:	PM-15, SI-5

11.3.6 C1.e Personnel Skills for Monitoring and Detection

C1.e Personnel Skills for Monitoring and Detection

Monitoring and detection personnel skills and roles, including those outsourced, reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring and detection personnel have sufficient knowledge of network and information systems and the essential function(s) they need to protect.

Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
C1.e.NA.1 There are no personnel who perform a monitoring and detection function.	**C1.e.PA.1** Monitoring and detection personnel have some *investigative skills* and a basic understanding of the data they need to work with.	**C1.e.A.1** You have *monitoring and detection personnel* who are responsible for the *proactive and reactive analysis*, *investigation and reporting* of monitoring alerts including both security and performance.
C1.e.NA.2 Monitoring and detection personnel do not have the correct specialist skills.	**C1.e.PA.2** Monitoring and detection personnel can *report* to other parts of the organisation (e.g. security directors, resilience managers).	**C1.e.A.2** Monitoring and detection personnel have *defined roles and skills* that cover all parts of the monitoring and investigation process.
C1.e.NA.3 Monitoring and detection personnel are not capable of reporting against governance requirements.	**C1.e.PA.3** Monitoring and detection personnel are *capable* of following most of the required workflow(s).	**C1.e.A.3** Monitoring and detection personnel follow policies, processes and procedures that address all governance reporting requirements, internal and external.
C1.e.NA.4 Monitoring and detection personnel have a lack of awareness of the essential function(s) the organisation provides, what assets relate to those functions and hence the importance of the log data and security events.	**C1.e.PA.4** Monitoring and detection personnel are aware of some of the network and information systems and your essential function(s), and can manage alerts relating to them.	**C1.e.A.4** Monitoring and detection personnel are empowered to look beyond the fixed process to investigate and understand non-standard threats.
C1.e.NA.5 Monitoring and detection personnel have no awareness of other roles or tasks outside of security monitoring and detection that are relevant to the operation of your essential function(s).	**C1.e.PA.5** Monitoring and detection personnel have some understanding of the *operational context* (e.g. people, processes, network that support your *essential function(s)*) to enhance the security monitoring function.	**C1.e.A.5** Monitoring and detection personnel are aware of the network and information systems and your essential function(s), related assets and can identify and prioritise alerts and investigations that relate to them.
C1.e.NA.6 Monitoring and detection personnel are overwhelmed with the amount of data and alerts they have to work with. Alert / triage fatigue is present.	**C1.e.PA.6** Monitoring and detection personnel deal with their workload and cases effectively.	**C1.e.A.6** Monitoring and detection personnel drive and shape new log data collection and can make effective use of it.
		C1.e.A.7 Monitoring and detection personnel are capable of following all of the required workflow(s).

		C1.e.A.8 Monitoring and detection personnel have a sufficient understanding of the *operational context* (e.g. people, processes, network and information systems that support your essential function) to enhance the security monitoring function.
		C1.e.A.9 Monitoring and detection personnel deal with their workload and cases effectively as well as identifying areas for improvement.

IGP Ref	IGP Interpretation
C1.e.A.1	***[monitoring and detection personnel]*** This term, used in the 'Achieved' state, signifies a formalised function. It refers to having dedicated personnel, whether internal or outsourced, who are formally responsible for the security monitoring capability. The size and structure of this function will vary, but it should be resourced appropriately for the scale and risk profile of the organisation. Personnel should have a detailed understanding of the hardware, software, and architecture of the systems they are protecting.
C1.e.A.1	***[proactive and reactive analysis]*** This confirms that personnel should be skilled in both reactive investigation (responding to automated alerts) and proactive analysis (threat hunting and searching for anomalies, aligning with C2).
C1.e.A.1	***[investigation and reporting]*** This describes the core duties of the monitoring staff in a mature 'Achieved' state. Their responsibilities should cover the full lifecycle: the initial analysis of event data, the detailed investigation of potential incidents, and the formal reporting of findings to internal stakeholders and, where required, external authorities.
C1.e.A.2	***[defined roles and skills]*** An 'Achieved' state requires that monitoring staff have formally defined roles and skills or competency requirements. This ensures a structured and capable team.
C1.e.PA.1	***[investigative skills]*** This requires that staff responsible for monitoring possess the necessary competencies to perform their roles. At a 'Partially Achieved' level, this means having personnel with some foundational investigative skills and a basic understanding of the log data they need to work with. The organisation should understand the competency requirements for all roles involved in the monitoring lifecycle (design, implementation, operation) and be proactively addressing any identified skills gaps. Where specialist skills (e.g., advanced digital forensics) are not maintained in-house, the organisation should have arrangements in place with third parties to provide this capability when needed. This should be supported by internal training programmes that provide access to development systems, test beds, and learning materials appropriate to the complexity of the systems being managed.
C1.e.PA.2	***[report]*** This refers to the process by which monitoring staff can escalate potential security incidents. A formal process should exist to allow personnel to report their findings to other parts of the organisation, such as senior security management or incident response teams. For a 'Partially Achieved' state, clear lines of reporting and communication should be established to support this escalation based on the criticality of the finding. The process should involve relevant stakeholders to ensure any required action can be taken, and forums or working groups should be established to support the discussion and resolution of security issues.

C1.e.PA.3	***[capable]*** This indicates that monitoring staff are sufficiently skilled and equipped to follow the organisation's defined operational procedures and workflows. At the 'Partially Achieved' baseline, this means staff are capable of following most of the required workflows. The organisation should ensure staff are competent in using the monitoring tools and have access to the necessary documentation and guidance to perform their duties effectively. This capability is built by ensuring system functionality is well understood (in collaboration with vendors where necessary) and that this knowledge is translated into operational procedures and internal guidance.
C1.e.PA.5	***[operational context]*** This requires personnel to understand the business-critical processes running on the network and information systems supporting your essential function(s). Knowledge should extend beyond technical logs to include who operates the system, when specific maintenance windows occur, and why certain traffic patterns are routine, enabling better distinction between malicious and legitimate anomalies.
C1.e.PA.5	***[essential function(s)]*** Monitoring staff should understand the licensed essential functions the organisation provides and which assets relate to those functions. This contextual awareness is critical.

IGP Ref	Examples of Evidence to support IGPs
C1.e.A.1	Competency Framework / Role Descriptions: Formally defined roles and skills for all monitoring staff, including a competency matrix and a process for identifying and addressing skills gaps.
C1.e.A.2	Training and Awareness Plan: A comprehensive training program with records for all monitoring staff, covering advanced topics and including a process for evaluating training effectiveness.
C1.e.A.2	Training and Competency Records: Evidence of competency assessments and any arrangements with third-party specialists for advanced skills.
C1.e.A.3	Monitoring Tool Configuration: Evidence of advanced configuration that allows the tools to pinpoint activity by making use of all collected log data, including custom parsers and enrichment from other data sources.
C1.e.A.3	Policy on Tooling: A document outlining the strategy for selecting, implementing, and maintaining monitoring tools.
C1.e.A.3	System Documentation: Evidence that monitoring tools are documented in the asset inventory and that their functionality is understood and recorded.
C1.e.PA.6	Incident case metrics demonstrating effective workload management (C1.e.PA.6), such as low Mean Time to Acknowledge (MTTA) and evidence that the number of open cases is manageable.
C1.e.A.5	Documentation of cross-functional training, shadowing, or liaison roles that ensure detection personnel understand the operational context of the essential systems.
C1.e.A.6	Investigation Records: Examples of investigations into non-standard threats, demonstrating that staff are empowered to go beyond standard playbooks.
C1.e.A.7	Documentation demonstrating that all required workflows for triage and escalation are defined and adhered to.
C1.e.A.7	Incident Response and Escalation Procedures: A documented process showing how monitoring staff report findings and escalate them, covering the governance reporting requirements for internal and external communication.
C1.e.A.8	Management Reports: Reports provided to senior management on the performance of the monitoring capability, demonstrating an awareness of the essential function(s) and the risks to them.
C1.e.A.9	Continuous Improvement Records: Meeting minutes or change records showing how monitoring staff and tools drive and shape new log data collection, demonstrating a mature feedback loop.
C1.e.PA.1	Competency Framework / Role Descriptions: Documented roles and responsibilities showing who performs monitoring functions.

C1.e.PA.2	Training and Awareness Plan: A plan that outlines training for staff with monitoring responsibilities to ensure they have the basic investigative skills.
C1.e.PA.2	Training and Competency Records: Records showing that staff are capable of following workflows and have completed required training.
C1.e.PA.3	Monitoring Tool Configuration: Evidence that the monitoring tools are configured to ingest logging and log data from key sources.
C1.e.PA.4	Investigation Records: Sample records from a case management or ticketing system showing how alerts are managed and investigated.
C1.e.PA.5	Documentation of cross-functional training, shadowing, or liaison roles that ensure detection personnel understand the operational context of the essential systems.

References and Further Guidance	
• C.1 Security monitoring – NCSC.GOV.UK	
• NCSC Plan: Your cyber incident response processes: https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes	
• NCSC Building a SOC https://www.ncsc.gov.uk/collection/building-a-security-operations-centre	
• NIST CSF 2.0 Subcategory:	GV.RR-02
• ISO 27001/27002:2022 Control:	5.2, 6.3
• NIST SP 800-53 Rev. 5 Control:	AT-3, PM-13

11.3.7 C1.f Understanding User's and System's Behaviour, and Threat Intelligence (within Security Monitoring)

C1.f Understanding User's and System's Behaviour, and Threat Intelligence (within Security Monitoring)		
Threats to the operation of network and information systems, and corresponding user and system behaviour, are sufficiently understood. These are used to detect cyber security incidents.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
C1.f.NA.1 Your organisation has no sources of threat intelligence.	**C1.f.PA.1** You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security incidents).	**C1.f.A.1** You track the effectiveness of your threat intelligence and actively share feedback on the usefulness of Indicators of Compromise (IoCs) and other intelligence with the threat community (e.g. sector partners, threat intelligence providers, government agencies).
C1.f.NA.2 You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	**C1.f.PA.2** Your organisation may use *threat intelligence services*, but you do not necessarily choose sources or providers specifically *because of your business needs, or specific threats in your sector* (e.g. sector-based info share, software vendors, anti-virus providers, specialist threat intel firms, special interest groups).	**C1.f.A.2** When using *threat intelligence feeds,* these have been selected using risk-based and threat- informed decisions based on your business needs and sector.

C1.f.NA.3 You have no awareness of the steps necessary to make best use of *threat intelligence* for security monitoring.	**C1.f.PA.3** The *user and system abnormalities from past attacks* and threat intelligence, on your and other network and information systems*, are used to signify adverse activity*.	**C1.f.A.3** You make relevant, reliable and actionable threat intelligence available to the necessary users and systems promptly.
C1.f.NA.4 Threat intelligence is unreliable and / or is not actioned by the appropriate users or systems in a timely manner.	**C1.f.PA.4** You receive regular updates for all your detection security technologies (e.g. AV, IDS).	**C1.f.A.4** You *contextualise threat intelligence* and link it to the why and / or how attacks take place for security monitoring.
C1.f.NA.5 You have no established understanding of what abnormalities to look for that might signify adverse activities.		**C1.f.A.5** You understand normal *user and system abnormalities fully*, to such an extent that searching for system abnormalities is an effective way of detecting adverse activity (e.g. you fully understand which systems should and should not communicate and when).
C1.f.NA.6 You do not receive updates for all your detection security technologies (e.g. AV, IDS).		**C1.f.A.6** The user and system abnormalities you monitor for are based on the nature of adverse activities likely to impact network and information systems supporting the operation of your essential function(s).
C1.f.NA.7 You do not understand normal user and system behaviour sufficiently to be able to use abnormalities to detect adverse activity.		**C1.f.A.7** The user and system abnormalities indicative of adverse activity you use are regularly updated to reflect changes in network and information systems supporting your essential function(s) and current threat intelligence.
		C1.f.A.8 You possess the *capability to share threat intelligence* (e.g. ways to effectively detect adversaries) with the threat community / defender community (sector partners, threat intelligence providers, government agencies) when required.

IGP Ref	IGP Interpretation
C1.f.A.2	***[threat intelligence feeds]*** This expects that the organisation formally vets and selects intelligence sources based on their direct relevance to the CLF provider's specific business risks and the threat actors identified in the A2.b risk assessment.
C1.f.A.4	***[contextualise threat intelligence]*** This requires the security team to translate raw indicators into TTPs (Tactics, Techniques, and Procedures) using a framework like MITRE ATT&CK. Contextualisation proves the team understands why a threat is relevant to the CLF environment, allowing for the creation of effective, custom detection rules (C1.c).

C1.f.A.5	***[user and system abnormalities fully]*** This confirms the requirement for a mature User and Entity Behaviour Analytics (UEBA) capability. "Fully" implies that monitoring has established a robust, statistically sound baseline of activity for all privileged users and critical NIS components, enabling the detection of subtle, low-and-slow threats (deviations from normal behaviour)
C1.f.A.8	***[capability to share threat intelligence]*** This requires having the necessary governance and technical channels (e.g., CiSP membership, established communication links with regulators/sector partners) to share findings quickly when deemed necessary, ensuring a two-way flow of vital information.
C1.f.PA.2	***[threat intelligence service]*** Any structured source providing contextual and timely information regarding cyber threats, encompassing technical data (Indicators of Compromise - IoCs), tactical data (TTPs), and strategic data (actor motivations, campaigns). This service should be actively used and integrated into the workflow, going beyond passive reading of generic public news feeds.
C1.f.PA.2	***[because of your business needs, or specific threats in your sector]*** The PA state accepts the use of generic intelligence feeds (e.g., sector info share, AV provider reports) but requires the organisation to use them effectively to understand threat actor motives and TTPs against the CLF environment.
C1.f.PA.3	***[user and system abnormalities from past attacks][are used to signify adverse activity.]*** The application of Behavioural Analytics. It requires the team to translate learning from past attacks (internal or external) and intelligence reports into simple anomaly detection rules within their monitoring tools.

IGP Ref	Examples of Evidence to support IGPs
C1.f.A.1	Intelligence Application Records: Logs showing the correlation of internal monitoring data with external threat intelligence feeds, demonstrating that actionable intelligence is promptly integrated into detection tools.
C1.f.A.4	Threat Context Documentation: Triage or investigation reports that explicitly contextualise an alert by mapping the event to an adversary's Tactics, Techniques, and Procedures (TTPs), often citing a framework like MITRE ATT&CK.
C1.f.A.5	Behavioural Baselines and Models: Documentation of the quantitative baseline established for normal user and system activity (e.g., normal login times, common inter-service communication patterns) used to identify abnormalities.
C1.f.A.5	UEBA Tooling Configuration: Configuration records for User and Entity Behaviour Analytics (UEBA) or equivalent SIEM components that prove the system is actively monitoring and alerting on deviations from the normal baseline.
C1.f.PA.1	Evidence of subscription to threat intelligence feeds relevant to the sector and essential function.
C1.f.PA.3	High-level documentation identifying the expected normal behaviour of key systems and user groups.

References and Further Guidance

- C.1 Security monitoring – NCSC.GOV.UK
- NCSC Building a SOC: Threat Intel: https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/threat-intelligence
- NCSC An Introduction to Threat Intel: https://www.ncsc.gov.uk/files/An-introduction-to-threat-intelligence.pdf
- MITRE ATT&CK : https://attack.mitre.org/

• NIST CSF 2.0 Subcategory:	ID.RA-03, DE.AE-07
• ISO 27001/27002:2022 Control:	5.7
• NIST SP 800-53 Rev. 5 Control:	RA-1, RA-5

11.4 Principle C2 Threat Hunting

11.4.1 Principle C2 Extended Guidance

Principle C2 represents the transition from reactive monitoring to proactive threat engagement. While Principle C1 focuses on identifying known threats through automated alerts, Principle C2 requires the organisation to actively search its systems for signs of compromise that have evaded standard signature-based controls. The scoping exercise is the necessary starting point for this principle, as it defines the technical environment and critical data paths where proactive searches should be prioritised.

A structured approach to proactive discovery is essential for managing the risk of sophisticated attacks designed to remain undetected for long periods, such as supply chain subversion or low-and-slow reconnaissance. For load control providers, the strategy should focus on the following areas:

- **Hypothesis-Driven Searches:** Formulating specific, intelligence-backed hypotheses based on threat information. This involves moving beyond passive waiting for alerts to actively searching logs and systems for evidence of specific adversary tactics, techniques, and procedures (TTPs) that are relevant to the load control technology stack.
- **Focus on TTPs over Indicators of Compromise:** Prioritising the identification of broader adversary behaviours rather than relying solely on short-lived technical indicators such as IP addresses or file hashes. This ensures that the discovery process remains effective even as attackers change their specific infrastructure or tools.
- **Continuous Improvement and Feedback Loops:** Ensuring that the results of proactive hunting activities are used to improve the wider security posture. Findings should be recorded and analysed to create new automated detection rules within the monitoring framework and to inform updated risk assessments.
- **Proportionate and Appropriate Capability:** The level of investment in proactive discovery should be appropriate to the complexity of the service and proportionate to the systemic risk. This does not necessarily require a large, dedicated internal team, but it does necessitate a defined and competent capability to look for abnormal behaviour within the specific technical environment.

By embedding proactive discovery into regular operations, the organisation moves from simple alerting to a state where it can actively hunt for unknown threats. This provides a critical safety net against sophisticated actors who aim to compromise the integrity of the load control service and the wider energy network.

11.4.2 C2.a Threat Hunting

C2.a Threat Hunting		
The organisation proactively seeks to detect, within networks and information systems, adverse activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard security prevent / detect solutions (or when standard solutions are not deployable).		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
C2.a.NA.1 You do not know the resources required for threat hunting.	**C2.a.PA.1** You have identified the *resources required to perform threat hunting* and are able to deploy these, in a timely manner, on an occasional basis.	**C2.a.A.1** You understand the *resources required to perform threat hunting* and these are deployed as part of business as usual.

C2.a.NA.2 You do not have access to an effective threat hunting capability.	**C2.a.PA.2** You deploy an effective threat hunting capability but not frequent enough to match the risks posed to network and information systems supporting your essential function(s) (e.g. you perform threat hunts in response to a tip off from a reputable source).	**C2.a.A.2** You deploy threat hunting resources at a frequency that matches the risks posed to network and information systems supporting your essential function(s).
C2.a.NA.3 Your threat hunts do not follow any structure and few if any records are created.	**C2.a.PA.3** Your threat hunts follow *pre-determined and documented methods* (e.g. hypothesis driven, data driven, entity driven) designed to identify adverse activity not detected by automated detections.	**C2.a.A.3** Your threat hunts follow *pre-determined and documented methods* (e.g. hypothesis driven, data driven, entity driven) designed to identify adverse activity not detected by automated detections.
	C2.a.PA.4 You document details of threat hunts and post hunt analysis.	**C2.a.A.4** You turn threat hunts into automated detections and alerting where appropriate.
		C2.a.A.5 You *routinely record details* of previous threat hunts and post hunt activities. You use these to drive improvements in your threat hunting and security posture.
		C2.a.A.6 You have *justified confidence in the effectiveness of your threat hunts* and the threat hunting process is reviewed and updated to match the risks posed to network and information systems supporting your essential function(s).
		C2.a.A.7 You leverage automation to improve threat hunts where appropriate (e.g. some stages of the threat hunting process are automated).
		C2.a.A.8 Your threat hunts *focus on the tactics, techniques and procedures (TTPs) of threats over atomic IoCs* (e.g. hashes, IP addresses, domain names etc).

IGP Ref	IGP Interpretation
C2.a.A.1 C2.a.PA.1	***[resources required to perform threat hunting]*** This includes: Dedicated personnel with forensic and behavioural analysis skills (C1.e); Access to all raw, unsampled log data (C1.a); and Specialised tooling (e.g., advanced SIEM query capability, data visualisation) to analyse large data sets efficiently.
C2.a.A.3 C2.a.PA.3	***[pre-determined and documented methods]*** This expects a formal methodology for hunts. The three primary methods are: Hypothesis-driven (starting with a TTP from A2.b), Data-driven (starting with an anomaly identified in the SIEM), or Entity-driven (starting with a high-risk asset like a privileged user or critical server). Documentation should record the methodology, scope, data sources, and the success/failure criteria.

C2.a.A.5	***[routinely record detail]*** This ensures the hunting process is formally integrated into the Lessons Learned (D2) framework. Records should be maintained detailing the hypotheses, findings, time spent, and, crucially, the resulting changes to detection rules, security controls (Objective B), or intelligence requirements (C1.f).
C2.a.A.6	***[justified confidence in the effectiveness of your threat hunts]*** Confidence should be demonstrated through assurance that is completed to a recognised standard, at least annually and on major system changes / updates. This is achieved by measuring the success rate of hypotheses and conducting "Purple Teaming" exercises. These exercises involve simulating specific TTPs (Red Team) while the hunting team (Blue Team) actively tracks and detects the activity to validate the hunting methodology and coverage.
C2.a.A.8	***[focus on the tactics, techniques and procedures (TTPs) of threats over atomic IoCs]*** This expects that Threat Hunting is primarily concerned with detecting how adversaries operate (their methods) rather than what they use (their indicators). Hunts should target behavioural chains that signal the adversary's intent, as TTPs are more resilient to change than ephemeral atomic IoCs (e.g., file hashes or IP addresses).

IGP Ref	Examples of Evidence to support IGPs
C2.a.A.1	A Threat Hunting Methodology Document or Policy outlining the principles, frequency, and formal structure of hunts.
C2.a.A.2	Threat Hunt Reports for routine exercises. These reports should document the hypothesis, the specific TTPs targeted (e.g., MITRE ATT&CK ID), the data sources queried, and the hunt's success or failure.
C2.a.A.2	Records demonstrating that threat hunting resources (personnel and tools) are deployed at a frequency that matches the risks posed to the essential service.
C2.a.A.3	Threat Hunt Reports for routine exercises. These reports should document the hypothesis, the specific TTPs targeted (e.g., MITRE ATT&CK ID), the data sources queried, and the hunt's success or failure.
C2.a.A.4	New Detection Rule Change Logs showing the conversion of a manual hunt finding into a new automated alert or a tuned rule in the SIEM.
C2.a.A.5	Post Hunt Activity Records demonstrating that results are used to drive improvements in the overall security posture and feed into the Lessons Learned process.

References and Further Guidance

- C.2 Threat Hunting – NCSC.GOV.UK
- NCSC Building a SOC: Threat Intel: https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/threat-intelligence
- NCSC An Introduction to Threat Intel: https://www.ncsc.gov.uk/files/An-introduction-to-threat-intelligence.pdf
- Home Office: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Detecting-the-Unknown-A-Guide-to-Threat-Hunting-v2.0.pdf
- MITRE ATT&CK : https://attack.mitre.org/

• NIST CSF 2.0 Subcategory:	DE.CM-03, DE.AE-02, ID.RA-03
• ISO 27001/27002:2022 Control:	5.7, 8.16
• NIST SP 800-53 Rev. 5 Control:	RA-3, SI-4, PM-15

12 Objective D: Minimising The Impact of Cyber Security Incidents

12.1 CAF Objective D Expected Outcome:

Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those function(s) where necessary.

12.2 Objective D Extended Guidance

Objective D represents the shift toward incident response and recovery, providing the primary mechanism to satisfy the statutory obligations under NIS Regulation 10(1) and 10(2), as well as Licence Conditions 9 and 10. These pillars require the implementation of appropriate and proportionate measures to manage the consequences of any incident and ensure the timely restoration of the essential service.

The scoping exercise is fundamental to this objective, as it identifies the critical systems, data, and external dependencies that must be prioritised during a recovery effort to maintain the load control function. While previous objectives focus on managing risk and building defences, Objective D is about ensuring the organisation can respond effectively to minimise harm.

For a load control provider, this means having the capability to contain an incident, manage its consequences, and recover control of its NIS in a timely manner. The effectiveness of this objective relies on the organisation's ability to demonstrate a mature and proven capability that is aligned with the overall risk profile of the service.

Meeting the expected outcomes requires a focus on proportionate and proven capability:

- **Proportionate and Appropriate:** The scale and depth of the response and recovery process should be appropriate to the organisation's risk profile and the complexity of the load control ecosystem. This includes managing external dependencies, such as third-party data feeds or grid signals, whose failure or compromise could impact the service. For example, a smaller provider may achieve the required confidence through well-structured tabletop exercises. A larger provider may require comprehensive practical tests, including live-system validation where appropriate. However, for industrial, commercial, or grid-scale assets where live-system testing is not feasible due to safety or grid stability risks, the provider should use high-fidelity offline environments or comprehensive exercises that involve all relevant operational stakeholders to prove the effectiveness of the response.
- **Proven:** The capability should be formally tested and validated (Principle D1.c). The outcome should be demonstrably effective in identifying the true causes of an incident and leading to clear, documented improvements (Principle D2). Testing must provide evidence that the response and recovery processes actually work in practice to restore the essential service within required timeframes.

Objective D provides the necessary feedback loop for the entire security programme. It ensures that insights gained from testing and actual incidents are used to refine risk assessments, strengthen protective measures, and improve detection capabilities. By ensuring that response plans are not just documented but are practically validated, the organisation can provide the necessary assurance to the Competent Authority that the load control service is resilient to disruption.

12.3 Principle D1 Response & Recovery Planning

12.3.1 Principle D1 Extended Guidance

Principle D1 is the cornerstone of effective incident management. It focuses on the preparation required to ensure that an organisation can respond effectively when a crisis occurs. This principle provides the

practical planning framework to meet the obligations set out in NIS Regulation 10(1) and 10(2), alongside Licence Conditions 9 and 10. The scoping exercise is the essential starting point for this preparation, as it identifies the critical systems, data, and external dependencies, such as third-party data feeds, that must be addressed within the response and recovery strategy.

Preparation involves defining clear roles, responsibilities, and procedures before an incident takes place. For load control providers, the strategy for planning should focus on the following core areas:

- **Response and Recovery Plans (D1.a):** The organisation must maintain documented plans that cover likely and well-understood attack scenarios. These plans should be accessible and clear, ensuring that all relevant staff are knowledgeable about the specific procedures required to contain an incident and restore the load control service. While plans should address common threats, they must also be flexible enough to provide a foundation for managing more complex or novel situations.
- **Response and Recovery Capability (D1.b):** Beyond the existence of a written plan, the organisation must have the actual capability to enact its procedures. This involves ensuring that the necessary technical tools, resources, and personnel with appropriate skills are available when required. This capability must be appropriate to the complexity of the service and the risks identified during the scoping and risk assessment processes.
- **Testing and Exercising (D1.c):** The effectiveness of response and recovery plans must be proven through a regular and formalised testing regime. This validation ensures that the plans are not merely theoretical but work in practice to restore the essential function within the required timeframes. The approach to testing should be proportionate to the risk profile of the service. While tabletop exercises may be sufficient for well-defined procedures, more complex scenarios may require practical validation. For industrial or grid-scale assets where live-system testing is not feasible due to safety or stability risks, the organisation should use high-fidelity offline environments or comprehensive stakeholder-led exercises to prove the plan's effectiveness.

The scale and complexity of these planning and testing activities are driven by the organisation's risk assessment. The goal is to move from a state of documented intention to a proven and demonstrable capability where response and recovery processes are appropriate, proportionate, and ready to be deployed to maintain service continuity.

12.3.2 D1.a Response Plan

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 network and information systems supporting the operation of your essential function(s) and covers a range of incident scenarios.		
Not achieved:	Partially Achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.
D1.a.NA.1 Your incident response plan is not documented.	**D1.a.PA.1** Your *incident response plan* covers your network and information systems supporting your essential function(s).	**D1.a.A.1** Your *incident response plan* is based on a *clear understanding* of the *security risks* to network and information systems supporting your essential function(s).
D1.a.NA.2 Your incident response plan does not include your organisations identified essential function(s).	**D1.a.PA.2** Your incident response plan *comprehensively* covers *scenarios* that are focused on *likely impacts* of *known and well understood attacks* only.	**D1.a.A.2** Your incident response plan is *comprehensive* (i.e. covers the complete *lifecycle* of an incident, roles and responsibilities, and reporting) and *covers likely impacts* of both known attack patterns and of possible attacks, previously unseen.

D1.a.NA.3 Your incident response plan is not well understood by relevant staff.	**D1.a.PA.3** Your incident response plan is *understood by all staff who are involved* with your organisation's response function.	**D1.a.A.3** Your incident response plan is documented and *integrated with wider organisational* business plans and *supply chain response plans,* as well as dependencies on supporting infrastructure (e.g. power, cooling etc).
	D1.a.PA.4 Your incident response plan is *documented* and *shared* with all *relevant stakeholders.*	**D1.a.A.4** Your incident response plan is *communicated* and *understood* by the business areas involved with the operation of your essential function(s).
	D1.a.PA.5 Your incident response plan is *readily accessible*, even when your organisations IT systems have been adversely affected by an incident.	
	D1.a.PA.6 Your incident response plan is regularly reviewed to ensure it remains effective.	

IGP Ref	IGP Interpretation
D1.a.A.1 D1.a.PA.1	***[incident response plan]*** This refers to the formal, documented plan that details the required actions, responsibilities, and practices that individuals across the organisation should follow to respond to a security incident. The plan should be grounded in the organisation's risk assessment. While the CAF's language is primarily aimed at cyber security, the plan should consider all credible causes of disruption to the licensed service, including non-cyber events such as cloud service provider outages, critical software bugs, or failures of key supporting infrastructure.
D1.a.A.1	***[clear understanding]*** This is a characteristic of an 'Achieved' plan. It means the plan is based on a clear understanding of the specific security risks to the network and information systems supporting the licensed service, as identified and documented in the risk management process (**A2**).
D1.a.A.1	***[security risks]*** This refers to the full spectrum of security risks identified in the organisation's risk register, not just those related to common attacks. An 'Achieved' plan is demonstrably linked to the organisation's specific risk register and considers the full range of threats, including novel and sophisticated ones.
D1.a.A.2 D1.a.PA.2	***[comprehensively]*** At the 'Partially Achieved' level, the plan comprehensively covers scenarios based on known and well-understood attacks. This means the plan should provide sufficient detail to guide responders through the likely stages of a common attack (e.g., a ransomware event or a denial-of-service attack against the CLF platform). This detail enables them to take pre-determined mitigation actions and understand post-breach responses, allowing for an effective and organised reaction even under pressure.
D1.a.A.2 D1.a.PA.3	***[likely impacts]*** The plan should be focused on the likely impacts of an incident on the licensed service. This requires a thorough understanding of how different attack scenarios could affect the confidentiality, integrity, and availability of the service. This impact analysis, which is a core component of the risk assessment process (**A2**), is what allows for the effective prioritisation of response activities and resources.

D1.a.A.2	***[comprehensive]*** In an 'Achieved' state, the plan is fully comprehensive. This means it covers the entire incident management lifecycle and includes detailed procedures and information to guide the response. A comprehensive plan would typically include: • **Activation Criteria**: How and when to initiate the plan. • **Triage and Classification**: Procedures to characterise events and classify them as reportable security incidents. • **Roles and Responsibilities**: A clear definition of the incident response team structure, its members, and their specific duties. • **Escalation Paths**: Defined procedures for escalating the response and engaging senior management or external support. • **Communication Plan**: Pre-defined communication methods and contact information for all internal and external stakeholders. • **Technical Procedures**: Playbooks for containing, eradicating, and recovering from specific types of incidents. • **Restoration Order**: A defined sequence for restoring systems and service components. • **Information Sources**: The location of supporting documentation needed for recovery (e.g., system configurations, network diagrams, vendor contact lists).
D1.a.A.2	***[lifecycle]*** This refers to the complete incident management lifecycle, which typically includes the following phases: Preparation; Identification; Containment; Eradication; Recovery; and Lessons Learned. An 'Achieved' plan should address all of these phases in detail.
D1.a.A.2	***[covers likely impacts]*** A mature, 'Achieved' plan goes beyond known attacks and also covers likely impacts of possible novel or previously unseen attack patterns. This requires a more abstract, impact-focused approach to planning (e.g., "what do we do if we lose control of the Load Control platform?") rather than relying solely on scenario-specific playbooks ("what do we do in case of X malware?")
D1.a.A.3	***[integrated]*** This means the incident response plan is not a standalone document but is formally integrated with other key business processes to ensure a coordinated response.
D1.a.A.3	***[wider organisational]*** and ***[supply chain response plans]*** The integration should extend to wider organisational plans such as emergency response, crisis management, business continuity, and safety management. It should also be integrated with the supply chain response plans of critical third-party suppliers (**A4**), ensuring that dependencies are managed, and communication channels are clear during a major incident.
D1.a.A.4	***[communicated]*** and ***[understood]*** In an 'Achieved' state, the plan is not just shared with direct responders but is effectively communicated to and understood by all business areas involved with the operation of the licensed service. This is achieved by incorporating incident response awareness into the organisation's overall security culture and training programmes (**B6**), ensuring wider organisational support and awareness during an incident.
D1.a.PA.2	***[scenarios]*** These are the plausible incident situations that the response plan is designed to address. The scenarios should be developed by analysing information from a range of sources, including open-source reporting, information provided by trusted security advisors (such as the NCSC), precedent cyber incidents (both internal and external), and, crucially, the organisation's own risk assessment. This ensures the plan is focused on credible threats and likely impacts rather than purely theoretical situations.
D1.a.PA.2	***[known and well understood attacks]*** This describes the scope of scenarios for a 'Partially Achieved' plan. It focuses on preparing for common attack types where the adversary's tactics, techniques, and procedures (TTPs) are generally known. This involves learning from precedent cyber-attacks and using frameworks like MITRE ATT&CK to understand the stages of an attack. This knowledge allows for the development of specific, targeted response playbooks that can be executed during an incident.

D1.a.PA.3	***[understood by all staff who are involved]*** The plan should be effectively communicated to and understood by all staff who are involved in the response function. This is not just about making a document available on a shared drive; it requires active communication and training to ensure that all stakeholders know their roles, responsibilities, and the actions they are expected to take during an incident. This understanding can be built and reinforced through a variety of methods, including formal training, information cascades, toolbox talks, workshops, and inclusion in the testing and exercising activities required in D1.c.
D1.a.PA.4	***[documented]*** The incident response plan cannot be an informal or ad-hoc process; it should be formally documented. This documentation should be controlled, versioned, and stored in a resilient manner so that it is accessible even if primary systems are unavailable during an incident. Good practice includes maintaining controlled paper copies or storing digital copies in a secure, segregated cloud location that is isolated from the primary production environment**.**
D1.a.PA.4	***[shared]*** The documented plan should be actively shared with all relevant internal and external stakeholders. This is achieved through the communication and training methods described above to ensure that everyone who needs the plan has access to it and understands how to use it.
D1.a.PA.4	***[relevant stakeholders]*** This includes all individuals and teams, both internal and external, who have a role to play in incident response. This extends beyond the core security team to include senior management, legal, communications, customer support, and key third-party suppliers or partners who may need to be engaged during an incident.
D1.a.PA.5	***[readily accessible]*** This expects that the plan's storage and distribution method should be resilient to the worst-case incident scenario (e.g., ransomware locking all systems). The plan should be stored out-of-band (e.g., in secure cloud storage segregated from the primary environment or as controlled, regularly updated hard copies), and that the correct individuals have access to it.

IGP Ref	Examples of Evidence to support IGPs
D1.a.A.1	The incident response plan is the primary piece of evidence. The document should be formally version-controlled, show clear ownership, and be stored in a resilient manner (e.g., Secure cloud storage separate from the core EIT environment, controlled hard copies) so it is accessible during an incident. The plan's scope should show consideration for non-cyber incidents like cloud provider outages.
D1.a.A.1	Link to Full Security Risks Register: Evidence showing the plan is based on a clear understanding of the full spectrum of security risks from the risk register, including novel and sophisticated threats, not just common ones.
D1.a.A.2	The plan itself should demonstrate its comprehensive nature by containing dedicated, detailed sections covering the full incident lifecycle. This would include documented procedures for: Activation, triage, and classification of incidents; Roles, responsibilities, and escalation paths; Internal and external communication plans; Technical playbooks for containment, eradication, and recovery; A defined restoration order for critical systems; A register of supporting information and where to find it (e.g., configs, diagrams, vendor contacts).
D1.a.A.3	Evidence of Integration: Explicit references within the incident response plan showing how it is integrated with wider organisational plans like Business Continuity, Disaster Recovery, and Crisis Management.
D1.a.A.3	Evidence from contracts or service agreements showing how the plan links to the supply chain response plans of critical third-party suppliers.
D1.a.A.4	Wider Communication and Understanding Records: Evidence that the plan has been communicated to, and is understood by, wider business areas beyond the core response team (e.g., through awareness briefings).
D1.a.A.4	Records showing that incident response awareness is part of the general security culture and training programme.
D1.a.PA.1	The incident response plan itself: This is the primary piece of evidence. The document should be formally version-controlled and show clear ownership.

D1.a.PA.3	Evidence for 'Partially Achieved' (Foundational Planning): Risk-Informed Scenarios: The plan should contain specific response playbooks for a range of credible scenarios based on known and well understood attacks.
D1.a.PA.3	There should be a clear link back to the organisation's risk assessment showing how these scenarios and their likely impacts were determined. Evidence could include minutes from risk workshops or references to specific threat intelligence reports that informed the scenarios.
D1.a.PA.4	Communication and Awareness Records: Evidence that the plan has been shared with and is understood by all staff who are involved. This could include: Email distribution lists and read-receipts; Attendance records and materials from training sessions, workshops, or toolbox talks; A clear, documented, and accessible process for any member of staff to report a security concern or incident to the response team.
D1.a.PA.5	Documentation of the resilient storage location (e.g., secure, segregated cloud storage or off-site hard copies) and the procedure to access the plan when primary systems fail.

References and Further Guidance	
• D.1 Response and recovery planning – NCSC.GOV.UK	
• NCSC Incident Management : https://www.ncsc.gov.uk/collection/incident-management	
• NIST CSF 2.0 Subcategory:	ID.IM-04, RS.MA-01
• ISO 27001/27002:2022 Control:	5.24, 5.26
• NIST SP 800-53 Rev. 5 Control:	IR-8, CP-2

12.3.3 D1.b Response & Recovery Capability

D1.b Response & Recovery Capability	
You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function(s). During an incident, you have access to timely information on which to base your response decisions.	
Not achieved:	Achieved
At least one of the following statements is true.	All the following statements are true.
D1.b.NA.1 Inadequate arrangements have been made to make the right resources available to implement your response plan.	**D1.b.A.1** You *understand the resources* that will likely be needed to carry out any *required response activities*, and *arrangements* are in place to make these resources available.
D1.b.NA.2 Your response team members are not equipped to make good response decisions and put them into effect.	**D1.b.A.2** You understand the *types of information* that will likely be needed *inform response decisions* and arrangements are in place to make this *information available.*
D1.b.NA.3 Inadequate back-up mechanisms exist to allow the continued operation of your essential function(s) during an incident.	**D1.b.A.3** Your *response team* members have the *skills and knowledge* required to decide on the response actions necessary to limit harm, and the *authority* to carry them out.
	D1.b.A.4 Key roles are *duplicated*, and operational *delivery knowledge is shared* with *all individuals* involved in the *operations and recovery* of the essential function(s).
	D1.b.A.5 *Back-up mechanisms* are available that can be readily activated to *allow continued operation* of your essential function(s), although possibly at a reduced level, if primary network and information systems *fail or are unavailable.*

	D1.b.A.6 Arrangements exist to *augment your organisation's incident response capabilities* with *external support* if necessary (e.g. specialist cyber incident responders).

IGP Ref	IGP Interpretation
D1.b.A.1	***[understand the resources]*** This requires that the organisation has formally identified and documented the resources needed to enact its incident response plan. This goes beyond just people; it includes pre-allocated funding and budgets for incident response, and the necessary technical tools (e.g., forensic software, secure out-of-band communication channels, access to sandboxed analysis environments). The organisation should have a designated incident response team or function (often called a Cyber Security Incident Response Team - CSIRT), with defined roles and responsibilities.
D1.b.A.1	***[required response activities]*** The resource planning should be based on the specific required response activities detailed in the incident response plan (**D1.a**). This means the organisation has analysed its response playbooks and determined, for each scenario, what specific skills, tools, and third-party support would be needed to successfully manage the incident from detection through to recovery.
D1.b.A.1	***[arrangements]*** This signifies that the organisation has moved beyond planning and has formal arrangements in place to make the identified resources available when an incident occurs. This includes having pre-approved emergency procurement processes, call-off contracts with specialist third parties, and clear procedures for mobilising internal staff, ensuring that resources can be deployed without delay.
D1.b.A.2	***[types of information]*** This requires the organisation to have pre-emptively identified the types of information that will be needed by the response team to make effective decisions during a crisis. This information is critical for establishing situational awareness and guiding the response. To be effective, this information should be identified and made available in advance. Examples of the types of information that are essential for an effective response include, but are not limited to: • The incident response plan itself and all supporting procedures and playbooks. • Real-time and historic data from monitoring and alerting systems (**C1**). • Detailed technical documentation, such as cloud architecture diagrams, network diagrams, system configurations, and API documentation. • A comprehensive asset inventory with a list of critical systems and their owners (**A3**). • Escalation paths and up-to-date contact information for all internal and external stakeholders, including third-party vendors and regulators. • Criteria for classifying and closing out incidents.
D1.b.A.2	***[inform response decisions]*** The information gathered should be sufficient to inform response decisions. This means designing processes that guide responders through a sequence of activities, controlling the flow of information to allow subject matter experts to focus on their tasks while keeping stakeholders informed. A documented triage process, often in the form of playbooks, is essential. This process should include decision trees and criteria for classifying incident severity, enabling responders to make consistent and effective decisions under pressure.
D1.b.A.2	***[information available]*** The organisation should have arrangements in place to make this critical information available to the response team during an incident. This means ensuring the information is stored in a resilient and accessible location, protected from the incident itself. For example, storing critical documentation and contact lists in a secure, segregated cloud repository or as controlled hard copies.
D1.b.A.3	***[response team]*** This refers to the designated group of individuals responsible for managing an incident. The response team should be formally constituted, with a clear structure and defined roles. It should include personnel familiar with the operation of the licensed service to provide essential context. While the core team may be internal, it can be augmented with third-party specialists as needed.

D1.b.A.3	***[skills and knowledge]*** This requires that the members of the response team collectively possess the necessary skills and knowledge to perform their assigned roles. This is achieved through a formal, role-based training and development programme (**B6**). This programme should cover not only the organisation's specific policies and procedures but also the technical skills required for incident handling, such as digital forensics, log analysis, and malware analysis. The organisation should have a process for identifying and addressing any skills gaps.
D1.b.A.3	***[authority]*** The response team members should have the necessary authority to carry out their duties effectively and in a timely manner. This means they are empowered to make critical decisions to contain an incident and limit harm, potentially including taking systems offline, blocking traffic, or engaging external support. This authority should be formally delegated and documented in the incident response plan.
D1.b.A.4	***[duplicated]*** To ensure resilience within the response team itself, key roles should be duplicated. This means having designated primary and alternate personnel for critical response functions, preventing a single point of failure if a key individual is unavailable. This should be part of a formal competency management and succession planning process.
D1.b.A.4	***[operational delivery knowledge is shared]*** This means that critical operational delivery knowledge is not held by a single individual (a "single point of knowledge"). This knowledge should be documented and shared with all individuals involved in the response and recovery process to ensure continuity. This is often achieved through cross-training, workshops, and maintaining a central, accessible knowledge base.
D1.b.A.4	***[all individuals]*** and ***[operations and recovery]*** The sharing of knowledge should extend to all individuals who have a role in the operations and recovery of the licensed service, ensuring a consistent and shared understanding of how to manage and restore systems.
D1.b.A.5	***[Back-up mechanisms]*** This refers to the technical and procedural solutions that allow continued operation of the licensed service during an incident. The specific Back-up mechanisms will depend on the criticality of the system and the organisation's risk assessment.
D1.b.A.5	***[allow continued operation]*** These mechanisms are designed to allow continued operation of the licensed service, although possibly at a reduced level, if primary systems fail or are unavailable. Examples include: • **Redundant Components:** Having duplicate, hot-standby systems for critical components like load control platforms or databases. • **Failover Sites**: Maintaining a secondary, geographically separate site (e.g., in a different cloud region) that can take over service delivery. • **Manual Processes:** Having defined and tested manual workarounds that can be used to deliver a reduced-capability service if automated systems are unavailable.
D1.b.A.5	***[fail or are unavailable]*** This covers a wide range of scenarios, from technical failures to systems being taken offline deliberately as part of an incident containment strategy. The back-up mechanisms should be designed to be activated in any situation where the primary systems are unavailable.
D1.b.A.6	***[augment your organisation's incident response capabilities]*** This acknowledges that an organisation may not have all the necessary specialist skills in-house. It should have arrangements in place to augment its internal capabilities with external support when needed.

D1.b.A.6	***[external support]*** This refers to specialist third parties who can be called upon during an incident. This external support could include: • Specialist cyber incident response and digital forensics firms. • The NCSC, as the national CSIRT. • Law enforcement. • Key technology vendors (e.g., cloud service providers, software developers). Crucially, clear terms of engagement should be drafted in advance, including pre-agreed contracts or retainers where appropriate. These arrangements should define priorities (e.g., service restoration vs. forensic evidence preservation) and service level agreements to ensure support is available when needed.

IGP Ref	Examples of Evidence to support IGPs
D1.b.A.1	Resource Management Plan: A document that details the resources (people, budget, tools) required to execute the incident response plan, based on an analysis of the required response activities.
D1.b.A.1 D1.b.A.3	Response Team Charter/Terms of Reference: A formal document constituting the response team (e.g., a CSIRT), defining its structure, and delegating the necessary authority to its members.
D1.b.A.2	Resilient Information Storage: Evidence of the secure and segregated location where critical types of information (plans, diagrams, contact lists) are stored to ensure they are available during an incident.
D1.b.A.2	Incident Response Playbooks: The documented playbooks and triage processes that guide the response team and ensure they have the right information to inform response decisions.
D1.b.A.3	Competency Framework and Training Plan: A framework defining the skills and knowledge required for each response role, along with a training plan and records to demonstrate how these competencies are developed and maintained. This should include evidence of succession planning to show key roles are duplicated.
D1.b.A.4	Knowledge Management System: Evidence of a system or process (e.g., a wiki, a shared document repository) where operational delivery knowledge is shared amongst all individuals involved in operations and recovery, preventing knowledge from being siloed.
D1.b.A.5	Resilient Architecture Diagrams: Architectural diagrams that illustrate the Back-up mechanisms in place, such as redundant components or failover sites in different cloud regions, designed to allow continued operation.
D1.b.A.5	Recovery Test Results: Reports from tests of Back-up mechanisms, such as failover drills or data restoration tests, proving they function correctly when primary systems fail or are unavailable.
D1.b.A.6	Third-Party Support Contracts: Formal arrangements and contracts for external support. This includes call-off retainers with incident response firms and specific support agreements with key technology vendors, detailing SLAs and terms of engagement.
D1.b.A.6	Call-out Test Records: Records of at least annual tests of the arrangements to augment capabilities with external support, ensuring contact details are correct and response procedures work as expected.

References and Further Guidance

• D.1 Response and recovery planning - NCSC.GOV.UK	
• NCSC Incident Management : https://www.ncsc.gov.uk/collection/incident-management	
• NIST CSF 2.0 Subcategory:	RS.MA-01
• ISO 27001/27002:2022 Control:	5.24, 5.26
• NIST SP 800-53 Rev. 5 Control:	IR-4, CP-2

12.3.4 D1.c Testing & Exercising

D1.c Testing & Exercising	
Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.	
Not achieved:	**Achieved**
At least one of the following statements is true.	All the following statements are true.
D1.c.NA.1 Exercises test only a discrete part of the process (e.g. that backups are working), but do not consider all areas.	**D1.c.A.1** *Exercise scenarios* are *based on* incidents experienced by your and other organisations or are composed using *experience* or *threat intelligence*.
D1.c.NA.2 Incident response exercises are not routinely carried out or are carried out in an ad-hoc way.	**D1.c.A.2** Exercise scenarios are *documented*, regularly *reviewed*, and *validated*.
D1.c.NA.3 Outputs from exercises are not fed into the organisation's lessons learned process.	**D1.c.A.3** Exercises are *routinely* run, with the *findings documented* and used to *refine* incident response *plans* and *protective security*, in line with the *lessons learned*.
D1.c.NA.4 Exercises do not test all parts of the response cycle.	**D1.c.A.4** Exercises *test all parts* of your *response cycle* relating to your essential function(s) (e.g. *restoration of normal function*(s) levels).

IGP Ref	IGP Interpretation
D1.c.A.1	***[Exercise scenarios]*** This refers to the documented narratives that form the basis of any test or exercise. These Exercise scenarios are used to simulate an incident and test the organisation's response plans and capabilities. They should be designed to provide a realistic challenge for the response team.
D1.c.A.1	***[based on]*** The scenarios cannot be arbitrary. To be effective, they should be based on credible and relevant sources of information. This ensures that the testing programme is focused on preparing the organisation for the threats it is most likely to face.
D1.c.A.1	***[experience]*** One of the key sources for scenarios is experience. This includes learning from past incidents that have affected your own organisation, as well as analysing public reports of incidents that have affected other organisations, particularly within the energy or IoT sectors. Using real-world experience makes the exercises more realistic and impactful.
D1.c.A.1	***[threat intelligence]*** Scenarios should also be informed by threat intelligence (as gathered in **C1.d**). This means using your understanding of the current threat landscape, including the specific TTPs used by adversaries, to create scenarios that test your defences against relevant and emerging threats.
D1.c.A.2	***[documented]*** All exercise scenarios should be formally documented. This includes detailing the narrative, objectives of the exercise, expected participant actions, and success criteria. This documentation allows for consistency, review, and reuse of scenarios.
D1.c.A.2	***[reviewed]*** The documented scenarios should be periodically reviewed, at least annually, to ensure they remain relevant and effective. This review should happen as part of a scheduled process and be triggered by events such as a significant change to the licensed service or the receipt of new threat intelligence.
D1.c.A.2	***[validated]*** The scenarios themselves need to be validated to ensure they are credible, realistic, and provide a meaningful test of the response plans. This validation might involve a peer review process or a walkthrough with key stakeholders before the exercise is conducted.

D1.c.A.3	***[routinely]*** Exercises are not a one-off event; they should be run routinely as part of a scheduled programme. The frequency and type of exercise should be appropriate and proportionate. For example, a less mature organisation might conduct tabletop exercises quarterly and a more in-depth functional test annually. The key is that the testing is part of a regular, planned cycle of assurance. The testing schedule should be documented in a formal policy.
D1.c.A.3	***[findings documented]*** The outputs of every exercise should be formally documented. These documented findings should capture what went well, what went poorly, any identified gaps in plans or capabilities, and recommendations for improvement.
D1.c.A.3	***[refine]*** The primary purpose of documenting findings is to use them to refine and improve the organisation's resilience.
D1.c.A.3	***[plans]*** The documented findings should be used to refine the incident response plans (**D1.a**), ensuring they are updated to address any weaknesses identified during the exercise.
D1.c.A.3	***[protective security]*** A key insight from testing is that it can reveal weaknesses in existing protective security controls (**Objective B**). Findings should also be used to identify and prioritise improvements to these preventative measures.
D1.c.A.3	***[lessons learned]*** This links directly to **Principle D2**. The documented findings from exercises should be fed into a formal lessons learned process to ensure they are assigned owners, tracked, and actioned through to completion.
D1.c.A.4	***[test all parts]*** A mature testing programme should, over time, test all parts of the response. This does not mean every exercise should be a full-scale simulation. The programme should use a variety of methods to ensure all components are tested, including: • **Orientation/walkthroughs:** To familiarise new staff with plans. • **Tabletop exercises:** To test decision-making and communication. • **Functional testing:** To test specific technical capabilities, like failing over a service or restoring data from backups. • **Full-scale simulations:** To test the entire response capability in a realistic scenario.
D1.c.A.3	***[response cycle]*** This indicator requires that an organisation's testing programme, over time, exercises all phases of the incident management response cycle. This typically includes Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. The goal is to build justified confidence in the ability to execute each phase. However, it is understood that the methods used to test each phase will differ, and a full, live technical test of every phase may not be appropriate or proportionate for all organisations. While phases like Identification (e.g., did our monitoring tools generate an alert?) and Recovery (e.g., can we restore from backup?) can often be tested with functional, hands-on exercises, phases like Containment and Eradication present a different challenge. • Containment: Testing the active containment of a threat (e.g., isolating a cloud environment, blocking IP addresses) can carry a risk of operational impact if not performed in a dedicated, segregated test environment. • Eradication: Testing the eradication of malware would require a live infection, which is not a safe or practical expectation. Therefore, for these more challenging phases, it is perfectly acceptable and appropriate to use realistic simulations to test the organisation's capability. This involves exercising the procedural and decision-making aspects of the plan. Examples of effective simulation include: • Advanced Tabletop Exercises: A scenario-based discussion where the response team is presented with technical injects (e.g., "The malware is now spreading to the following systems. What are your specific containment actions? Who

	authorises them? How are they communicated?") to test their decision-making process under pressure. • Cyber Range Exercises: For more mature organisations, using a dedicated cyber range (either internal or third-party) to safely simulate an attack and allow the response team to practice containment and eradication techniques using their actual tools, but on a replica of their environment. The key is that the organisation can demonstrate it has a credible and tested plan for every phase of the response cycle, even if the testing methods are adapted to be proportionate to the risk and maturity of the organisation.
D1.c.A.4	***[restoration of normal function(s) levels]*** The testing should go beyond just containing a simulated incident. It should validate the ability to fully recover systems and achieve restoration of normal function(s) levels. For some organisations, particularly those with complex or legacy systems, full technical restoration testing might be high-risk. In such cases, confidence can be built through alternate means, such as testing the recovery of individual components, validating the capability to re-engineer or rebuild systems, and thoroughly exercising the manual processes that would be used during a real restoration.

IGP Ref	Examples of Evidence to support IGPs
D1.c.A.1	Planning and Preparation Evidence: The documented plans for specific exercises. These documents should show that the scenarios are based on credible sources, such as specific threat intelligence reports, analysis of past incidents (experience), or outputs from the organisation's risk assessment.
D1.c.A.1	Evidence from the risk register or related workshops showing how identified risks have been used to develop and prioritise exercise scenarios.
D1.c.A.2	A formal document that defines the organisation's approach to testing its incident response capability. This should include the process for ensuring scenarios are formally documented, reviewed, and validated.
D1.c.A.2	The Exercise scenarios themselves: The documented plans for specific exercises, demonstrating they have been reviewed and validated prior to execution.
D1.c.A.3	A formal document that defines the organisation's approach to testing its incident response capability. This should include: The schedule or frequency for when exercises will be routinely run; and the different types of exercises to be used to test all parts of the response cycle (e.g., tabletops, functional tests).
D1.c.A.3	Operational and Assurance Records (Execution and Findings): Evidence that exercises have taken place as scheduled. This could include meeting invitations, attendance lists, and photos or screenshots from the exercise itself.
D1.c.A.3	Post-Exercise Reports: each exercise, there should be a formal report where the findings are documented. This report should detail what went well, what did not, and provide specific, actionable recommendations to refine both the response plans and underlying protective security controls.
D1.c.A.3	A formal log or register that tracks the findings and recommendations from all exercises. This register should show that each finding has been assigned an owner and is being tracked through to resolution, demonstrating a closed-loop process.
D1.c.A.4	Specific records from exercises that tested the restoration of normal function(s) levels. This could be: Results from a technical test of a data backup restoration; A report from a functional test of a service failover to a secondary site; or, for organisations where full technical testing is high-risk, evidence from a detailed walkthrough that validates the manual processes for rebuilding or re-engineering a critical system.

References and Further Guidance

• D.1 Response and recovery planning - NCSC.GOV.UK	
• NCSC Incident Management : https://www.ncsc.gov.uk/collection/incident-management	
• NIST CSF 2.0 Subcategory:	ID.IM-02
• ISO 27001/27002:2022 Control:	5.29, 5.30

• NIST SP 800-53 Rev. 5 Control:	IR-3, CP-4

12.4 Principle D2 Lessons Learned

12.4.1 Principle D2 Extended Guidance

Principle D2 ensures that the incident management lifecycle is completed by using every event as an opportunity for organisational learning and improvement. This principle provides the final mechanism for satisfying the statutory requirements of NIS Regulation 10(1) and 10(2), as well as the obligations in Licence Conditions 9 and 10, by ensuring that the measures taken to manage risks are continuously refined based on real-world evidence.

The scoping exercise remains relevant here, as it defines the technical and operational boundaries that must be investigated following an incident. Effective implementation of this principle ensures that the root causes of a disruption, whether technical, procedural, or organisational, are fully understood and addressed.

To ensure that incidents drive meaningful change, the organisation should focus on the following core areas:

- **Post-Incident Analysis (D2.a):** The organisation must maintain a formal and documented process for reviewing incidents. The scale and depth of this analysis should be appropriate to the incident's severity and the complexity of the service. For some scenarios, this might involve a structured debrief to identify contributing factors, while more significant events may require deep digital forensic analysis, particularly when external dependencies or third-party data feeds are involved. The objective is to move beyond superficial fixes to identify the fundamental reasons why a control failed or a vulnerability existed.
- **Driving Improvements (D2.b):** Insights gained from post-incident reviews must be used to strengthen the overall security posture. This requires a defined process to ensure that lessons learned are fed back into all other security objectives. This includes updating risk assessments in Objective A, refining protective technical controls in Objective B, and improving the sensitivity of detection capabilities in Objective C.

The effectiveness of this principle is demonstrated when the organisation can show that it has implemented documented and effective improvements to prevent the recurrence of similar incidents. By maintaining this rigorous feedback loop, the organisation provides the necessary assurance to the Competent Authority that the load control service is being managed through a process of continuous refinement and that all security measures remain appropriate and proportionate to the evolving threat landscape.

12.4.2 D2.a Post Incident Analysis

D2.a Post Incident Analysis	
When an incident occurs, your organisation takes steps to understand its causes, informing appropriate remediating action.	
Not achieved:	Achieved
At least one of the following statements is true.	All the following statements are true.
D2.a.NA.1 You are not usually able to resolve incidents to a root cause or identify the contributing factors within a broader systems context.	**D2.a.A.1** Root cause analysis is conducted routinely as a key part of your *lessons learned* activities following an incident.

D2.a.NA.2 You do not have a formal process for investigating causes.	**D2.a.A.2** Your post incident analysis is *comprehensive*, considering *organisational factors* (e.g. policies, processes and procedures), technical factors (e.g. system design, vulnerabilities), *human factors* (e.g. training, security culture) and any changes to threat.
D2.a.NA.3 Investigators form theories early in the process and only seek evidence that affirms their belief.	**D2.a.A.3** All *relevant incident data* is made *available* to the analysis team to *perform post incident analysis.*
D2.a.NA.4 Investigations are solely focused on identifying the person(s) who can be held responsible for the incident.	**D2.a.A.4** Your analysis considers what could have happened *under plausible, alternative circumstances* (e.g. 'what if' / 'if only' scenarios).

IGP Ref	IGP Interpretation
D2.a.A.1	***[lessons learned]*** This refers to the formal process of analysing an incident to identify opportunities for improvement. The root cause analysis is a key input into the wider lessons learned activities (covered in D2.b). It ensures that the organisation moves beyond just resolving the immediate incident to understanding why it happened, which is essential for preventing recurrence.
D2.a.A.2	***[comprehensive]*** This requires that the root cause analysis is thorough and holistic. A comprehensive analysis should not stop at the immediate technical cause (e.g., "a vulnerability was exploited"). It should dig deeper to understand the full context of the incident lifecycle. The analysis should aim to: • Establish the full timeline of events, including how long an attacker may have been present in the environment before detection. • Identify all the weaknesses, technical and non-technical, that were exploited or contributed to the incident's success. • Assess the effectiveness (or failure) of existing security controls and processes. • Determine any human factors that contributed to the incident. • Produce a clear action plan with recommendations to increase resilience.
D2.a.A.2	***[organisational factors]*** The analysis should cover organisational process issues. This means looking beyond technology to identify failures or weaknesses in procedures. For example, the root cause of an incident might not be a missing patch, but a breakdown in the change management process that allowed an insecure system to be deployed, or a failure in the user access review process that left a dormant, privileged account active.
D2.a.A.2	***[human factors]*** The investigation assesses the role of people and culture in the incident. This includes reviewing if training was adequate (B6), if security policy was circumvented due to resource pressures, or if reporting systems failed due to a perceived blame culture (D2.a.NA.4).
D2.a.A.3	***[relevant incident data]*** This refers to all the information and forensic artefacts required by the analysis team to conduct their investigation. The process should ensure that all relevant incident data is made available to the analysis team.
D2.a.A.3	***[available]*** To be made available, this data should be collected and preserved in a way that maintains its integrity. This data includes, but is not limited to: • All logs from affected systems, monitoring tools, and security appliances. • Forensic data, such as disk images of servers, memory dumps, or network packet captures. • The incident response plan itself and all logs from the incident handling team. • Physical and logical access records. • Any specialist investigation technologies or tools required by the analysis team.

D2.a.A.3	• ***[perform post incident analysis.]*** This is the active process of conducting the investigation. The team assigned to perform post incident analysis should be able to operate effectively. The purpose of the analysis, to learn lessons, should be clear to all stakeholders. Where necessary, the analysis team may need to be independent from the operational team that was managing the incident, and the organisation should have arrangements in place (e.g., call-off contracts) to bring in external specialists to lead or augment the analysis if required.
D2.a.A.4	• ***[under plausible, alternative circumstances]*** This encourages learning beyond the immediate incident by performing counterfactual analysis ('what if'). It requires using the incident data to identify potential systemic weaknesses that did not directly contribute this time but could have led to a worse outcome (e.g., "if only the firewall rule had worked, what would the attacker have done next?").

IGP Ref	Examples of Evidence to support IGPs
D2.a.A.1	Post-Incident Review / Root Cause Analysis Policy: A formal, documented process that outlines how the organisation investigates the root causes of incidents. This policy should define: • The triggers for initiating a root cause analysis (e.g., all incidents classified above a certain severity). • The structure and responsibilities of the analysis team. • The requirement for the analysis to be comprehensive, covering organisational process issues as well as technical vulnerabilities. • The process for making all relevant incident data available to the analysis team.
D2.a.A.1	Operational and Assurance Records: Root Cause Analysis Reports: This is the primary piece of evidence. For each significant incident, a formal report should be produced that documents: • The full incident timeline. • The identified root cause(s), including any contributing organisational process issues or human factors. • The specific technical vulnerabilities in networks, systems or software that were exploited. • An assessment of the effectiveness of existing security controls.
D2.a.A.2	Formal Post Incident Analysis Reports that explicitly identify and document causal and contributing factors from the technical, organisational, and human factors domains.
D2.a.A.3	Data Preservation Records: Evidence demonstrating that relevant incident data was successfully collected and preserved for the analysis team. This could include chain-of-custody forms for forensic images or logs from archival systems.
D2.a.A.3	Third-Party Engagement Records: If external specialists are used to perform root cause analysis, evidence of their engagement would include the statement of work, call-off contract details, and the final report delivered by the third party.
D2.a.A.4	Interview or debrief records demonstrating that the analysis team considered plausible, alternative circumstances (D2.a.A.4) beyond the immediate technical failure.

References and Further Guidance

• D.2 Lessons learned - NCSC.GOV.UK	
• NCSC Learn from the incident : https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery/step-5--learn-from-the-incident	
• NIST CSF 2.0 Subcategory:	RS.AN-03
• ISO 27001/27002:2022 Control:	5.27
• NIST SP 800-53 Rev. 5 Control:	IR-8, SI-4

12.4.3 D2.b Using Incidents to Drive Improvements

D2.b Using Incidents to Drive Improvements	
Your organisation uses lessons learned from incidents to improve your security measures.	
Not achieved:	**Achieved**
At least one of the following statements is true.	All the following statements are true.
D2.b.NA.1 Following incidents, lessons learned are not captured or are limited in scope.	**D2.b.A.1** You have a *documented incident review process/policy* which ensures that lessons learned from each incident, *including near misses*, are identified, captured, and acted upon.
D2.b.NA.2 Improvements arising from lessons learned following an incident are not implemented or not given sufficient organisational priority.	**D2.b.A.2** *Lessons learned* cover issues with reporting, roles, governance, skills and organisational policies, processes and procedures as well as technical aspects of network and information systems.
D2.b.NA.3 Changes are made as a 'knee jerk' reaction to an incident without proper analysis and testing to ensure the change is appropriate.	**D2.b.A.3** You use lessons learned to *improve* security measures, including updating and retesting response plans when necessary.
D2.b.NA.4 You wait until a severe or high-profile incident has occurred before you take steps to improve.	**D2.b.A.4** *Security improvements* identified as a result of lessons learned are *prioritised*, with the highest priority improvements completed *promptly*.
	D2.b.A.5 *Analysis* is fed to *senior management* and incorporated into *risk management* and *continuous improvement.*
	D2.b.A.6 Your organisation maximises the lessons learned by *using the analysis into 'what if' / 'if only' scenarios.*
	D2.b.A.7 Your organisation learns from reported incidents in your sector and the wider national infrastructure.

IGP Ref	IGP Interpretation
D2.b.A.1	***[documented incident review process/policy]*** This requires a formal, documented process or policy that ensures that after a security incident, a review is conducted to identify, capture, and act upon the lessons learned. This process is the formal mechanism that transforms the findings from a root cause analysis (**D2.a**) into tangible improvements. The policy should define the triggers for the review, the roles and responsibilities of those involved, and the expected outputs.
D2.b.A.1	***[including near misses]*** Potential security events that were detected and contained without resulting in adverse impact should still be formally reviewed. This proactive learning prevents failures from recurring and validates the effectiveness of detection and containment controls.
D2.b.A.2	***[Lessons learned]*** This term refers to the full spectrum of insights gained from analysing an incident. A comprehensive Lessons learned process should cover not only the technical aspects of the incident but also any issues with reporting, roles, governance, skills, and organisational processes. The goal is to identify weaknesses across people, processes, and technology to prevent a recurrence of the incident and to improve the overall response capability.
D2.b.A.3	***[improve]*** The organisation should use the lessons learned to actively improve its security measures. This is the practical application of the analysis. It means taking the recommendations from the post-incident review and turning them into concrete actions.

D2.b.A.4	***[Security improvements]*** This refers to the specific, tangible actions taken as a result of the lessons learned process. These Security improvements should be formally captured and managed, for example in a dedicated improvement plan or the organisation's risk register.
D2.b.A.4	***[prioritised]*** The identified security improvements should be prioritised for implementation. This prioritisation should be risk-based, taking into account the severity of the incident that occurred and the potential impact of a similar incident happening again.
D2.b.A.4	***[promptly]*** The highest priority improvements should be completed promptly. The timeframe for implementing improvements should be defined and tracked, ensuring that critical weaknesses are addressed without undue delay.
D2.b.A.5	***[Analysis]*** This refers to the formal output of the post-incident review and lessons learned process. This Analysis should not just be a technical report; it should be synthesised into a format that is meaningful for different audiences, including senior management. The analysis should include trends over time, looking at the type, frequency, and nature of incidents to highlight systemic areas of weakness.
D2.b.A.5	***[senior management]*** The analysis and key findings from the lessons learned process should be fed to senior management. This ensures that the organisation's leadership has visibility of the security issues and can provide the necessary resources and strategic direction to address them.
D2.b.A.5	***[risk management]*** The outputs of the lessons learned process should be incorporated back into the organisation's formal risk management framework (**A2**). This means that new risks may be identified, the assessment of existing risks may change, and the effectiveness of security controls can be re-evaluated based on real-world performance during an incident.
D2.b.A.5	***[continuous improvement]*** This is the ultimate goal of the lessons learned process. It is the engine that drives continuous improvement across the entire security programme. By systematically analysing incidents and implementing improvements, the organisation demonstrates a mature approach to security, ensuring its defences and response capabilities evolve in step with the changing threat landscape.
D2.b.A.6	***[using the analysis into 'what if' / 'if only' scenarios.]*** The Post Incident Analysis (D2.a) findings to be used to identify latent systemic weaknesses. The analysis should explore how slightly different circumstances could have led to failure, ensuring resources are focused on eliminating broader vulnerabilities, not just the single exploited factor.

IGP Ref	Examples of Evidence to support IGPs
D2.b.A.1	Governance and Policy Evidence: A documented incident review process/policy: This is the core policy document that governs the lessons learned process. It should define the formal process for identifying, capturing, and acting upon findings from any security incident.
D2.b.A.2	Operational Records and Outputs: The formal outputs from the post-incident review process. These reports should be comprehensive, covering not just technical root causes but also issues with reporting, roles, governance, and organisational processes.
D2.b.A.3	Change Management Records: Evidence from a change management system showing that the identified improvements have been implemented. This could include records of security control reconfigurations, updates to response plans, or enhancements to monitoring systems.
D2.b.A.4	Improvement Plan / Risk Register: It should contain entries for the specific Security improvements identified as a result of the lessons learned process. Each entry should be prioritised based on risk and have a defined timeline for completion, demonstrating that high-priority items are being actioned quickly.
D2.b.A.5	Management and Reporting Evidence: Analysis Reports for Senior Management: Examples of reports or presentations delivered to senior management. This Analysis should synthesise the findings from incidents, identify trends over time, and provide an assessment of the overall effectiveness of the incident response capability.

D2.b.A.5	Risk Management Committee Minutes: Records from risk committee meetings showing that the outputs of the lessons learned process are being formally incorporated into the organisation's risk management framework. This demonstrates that incident data is being used to update risk assessments and control effectiveness ratings.
D2.b.A.5	Continuous Improvement Tracking: Evidence of a continuous improvement cycle. This could be in the form of regular management reports, dashboards with Key Performance Indicators (KPIs) related to incident response (e.g., mean time to detect, mean time to recover), or a register of all improvement actions and their status.
D2.b.A.6	Records demonstrating that the "what if" or counterfactual analysis from the D2.a report was used to justify and fund broader systemic security improvements.
D2.b.A.7	Evidence of the process for assimilating and applying external threat intelligence and sector incident reports to update internal controls and policies.

References and Further Guidance

• D.2 Lessons learned - NCSC.GOV.UK	
• NCSC Learn from the incident : https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery/step-5--learn-from-the-incident	
• NIST CSF 2.0 Subcategory:	RS.IM-01, RS.IM-02
• ISO 27001/27002:2022 Control:	5.27
• NIST SP 800-53 Rev. 5 Control:	CA-5, IR-8

13 Objective E: Physical Security, Principles and Guidance.

13.1 Ofgem Objective E: Expected Outcome

The risks of physical events leading to adverse effects on network and information systems are understood and systematically managed.

13.2 Objective E: Extended Guidance

DSIT's interpretation of OES NIS security duties includes taking non-cyber measures to manage the risk of "physical events that might have an adverse effect on networks and information systems[16]". DESNZ's NIS Policy Guidance re-iterates DSIT's interpretation and requires an OES to "identify and manage other[17]" security issues in an appropriate and proportionate manner[18]".

The NCSC have produced the CAF collection to assist organisations improve the security of network and information systems. The CAF collection focuses on cyber-based threats to networks and covers supply chain and personnel risks. However, the CAF's treatment of risks arising through physical events is limited[19].

The aim of this supplementary security objective is to detail Ofgem's expectations regarding the management of physical events that might have an adverse network and information systems that are in an OES' NIS scope. Ofgem have produced this security objective in the same format as NCSC's CAF security objectives, the intent is that this will lead to a consistent approach in the self-assessment of cyber and physical security objectives.

Ofgem intend that their physical security objective is used as a supplement to the CAF and refer to it as Objective E. Objective E specifies security outcomes relating to 2 distinct categories of physical risk. Principle E1 relates to the risks presented by malicious threat actors gaining physical access to the components of network and information systems. Principle E2 relates to non-malicious risks such as those caused by environmental hazards and accidents.

13.3 Principle E1: Physical security of network and information systems

Appropriate and proportionate physical security measures are in place to protect network and information systems from unauthorised physical access and tampering.

13.3.1 Principle E1: Extended Guidance

Effective security of network and information systems requires that components of the networks are protected against the threat of unauthorised physical access. The risks associated with unauthorised physical access are numerous and include, but are not limited to, attackers directly connecting to device ports for the purpose of downloading malware or extracting data, and attackers using plant HMIs to change system parameters.

Holistic cyber security requires an integrated approach. Physical and cyber security management systems must complement each other, and security teams must work together closely to manage those elements of the security systems that overlap. Examples of these overlaps include the cyber security of the security systems used to enforce physical security (such as access control systems and video management systems) and the identification of zones within facilities that contain critical network components that require enhanced physical security.

[16] https://assets.publishing.service.gov.uk/media/5ad87a14ed915d32a65dbe9b/NIS_-_Guidance_for_Competent_Authorities.pdf.
[17] Where 'other' refers to other than cyber security.
[18] https://assets.publishing.service.gov.uk/media/6530f1459274590000df959e3/implementation-of-the-network-and-information-systems-regulations-guidance.pdf
[19] This was intentional, as the provision of this advice is outside of the remit of NCSC. Responsibility for the provision of this advice rests with the Competent Authority (CA).

Objective E relates only to the physical security of the components of the network and information systems on which the essential function relies.

13.3.2 E1.a Governance and risk management processes relating to physical security risks.

E1.a Governance and risk management processes relating to physical security risks.	
You manage your physical and cyber security risks in an integrated manner and your physical and cyber-security risk management processes are mutually supporting.	
Not achieved: At least one of the following statements is true	Achieved: All the following statements are true
E1.a.NA.1 Your organisation does not have a board-level individual who has overall accountability for physical security of sites hosting network and information systems.	**E1.a.A.1** The physical security of your network and information systems is delivered via appropriate organisational structures, well-defined responsibilities and accountabilities and suitably qualified and experienced personnel. These structures are designed to ensure that physical and cyber security policies and plans are mutually supporting/complimentary.
E1.a.NA.2 Your organisation has not conducted a risk assessment that takes account of the risks of unauthorised physical access to network and information system components across your sites.	**E1.a.A.2** Your management systems (cyber or physical or both) include security objectives relating to the physical security of your network and information systems.
E1.a.NA.3 Your organisation does not have a security management system with an explicit objective of reducing the risk of unauthorised access to network and information systems.	**E1.a.A.3** You have identified and registered all facilities, and specific zones within those facilities, that require physical security control measures for the purpose of securing network and information systems.
	E1.a.A.4 Your physical security risk assessments take account of the potential impacts resulting from unauthorised physical access to network and information system components. Your investment in physical security measures reflects these potential impacts.
	E1.a.A.5 Your organisation has made use of NPSA guidance to help inform its view of appropriate and proportionate physical security measures for its sites.

IGP Ref	Ofgem intended IGP Interpretation
E1.a.A.1	Ofgem intends that this IGP will: • Guide OES to develop the structures and teams to ensure that the physical security of network and information systems is comprehensively managed. This IGP aims to avoid the tendency for physical security of network and information systems to be managed on an ad-hoc basis by IT/OT staff, it encourages OES to use the expertise of their existing physical security staff to manage physical aspects of NIS security. Mutually supporting/complimentary physical and cyber security policies and plans describes a situation in which OES have considered how physical security controls can be used to augment cyber controls, or to provide compensating controls, where required. • Avoid situations in which the physical security of network and information systems is not considered due to gaps between physical and cyber security teams.

E1.a.A.2	Ofgem intends that this IGP will avoid situations in which the physical security of network and information systems are not considered due to gaps between physical and cyber security teams.
E1.a.A.3	Ofgem intends that this IGP will guide OES toward identifying and recording all those facilities that contain network and information systems that are in their NIS scopes. These facilities may include manned and unmanned sites. The register should also identify any zones/areas within these facilities that require enhanced physical access control measures (such as control rooms and equipment rooms).
E1.a.A.4	Ofgem intend that this IGP will guide OES to take account of the risk posed by physical security breaches and to provide network and information systems with a level of physical protection that is proportionate to the risk.
E1.a.A.5	Ofgem intends this IGP to guide OES to make use of NPSA guidance where appropriate and to liaise with NPSA security advisors. In the case of OES with designated CNI sites, OES should ensure that they have established and maintain contact with a NPSA security advisor. In the case of OES who do not have designated CNI sites, liaison should be achieved through involvement with the relevant NPSA sector forum. OES should request access to NPSA's extranet to provide them with access to detailed guidance on physical security measures.

IGP Ref	Examples of Evidence to support IGPs
E1.a.A.1	A master list of security roles and responsibilities that is maintained as part of the security management system (this is often achieved in a RACI table format).
E1.a.A.2	References to the physical security of network and information systems within one, or both, of the cyber and physical security management systems.
E1.a.A.3	Demonstration that the OES is aware of all the facilities that contain network and information systems that are in NIS scope.
E1.a.A.3	Demonstration that the OES is aware of the zones/areas within its facilities that require enhanced physical access control measures (examples may include control rooms and equipment/server rooms).
E1.a.A.4	risk assessments that document physical security risks against network and information systems and NIS improvement plan actions that respond to those risks that require treatment. Ofgem accepts that many OES will conduct these risk assessments by facility type/group, rather than by individual facility. This is because of the number of remote facilities involved and that risks are may be common between facilities within the same type/group. OES are reminded that the protective security needs of different types of sites will vary significantly and that it may be appropriate and proportionate to afford a lower level of physical security to less critical sites.
E1.a.A.5	Evidence of liaison with NPSA advisors.

References and Further Guidance
• www.npsa.gov.uk

13.3.3 E1.b – Designing and implementing physical security controls

E1.b – Designing and implementing physical security controls	
You have referenced relevant NPSA physical security guidance when designing and implementing controls.	
Not achieved: At least one of the following statements is true	Achieved: All the following statements are true

E1.b.NA.1 You have not referred to any NPSA physical security guidance when implementing controls..	**E1.b.A.1** You reference relevant NPSA guidance when designing and implementing new physical security controls.
	E1.b.A.2 You have identified any IT networked physical security systems that your cyber security management system relies on and have included these systems as part of your NIS scope.
	E1.b.A.3 Projects to implement new IT networked physical security systems employ devices that are assured under the Cyber Assurance of Physical Security Systems (CAPSS) scheme[20] or recognised equivalent.

IGP Ref	Ofgem intended IGP Interpretation
E1.b.A.1	Ofgem intends this IGP to guide OES toward making full use of NPSA physical security advice and guidance. Doing so will assist in the implementation of appropriate and proportionate security controls. NPSA's physical security guidance can be found on the NPSA internet and extranet sites at the 'Advice' tab.
E1.b.A.2	Ofgem intends this IGP to ensure that an OES' NIS scope is comprehensive and takes account of the essential service's reliance on the networked physical security systems that are used to protect it.
E1.b.A.3	Ofgem does not have any additional interpretation for this security outcome.

IGP Ref	Examples of Evidence to support IGPs
E1.b.A.1	Confirmation that the OES is aware of, and making use of, relevant NPSA advice and guidance.
E1.b.A.1	Inclusion of any network and information systems that provide physical security functionality that the essential service relies upon.

References and Further Guidance
• www.npsa.gov.uk

13.4 Principle E2: Broader network and information systems resilience risks

Managing the broader risks to network and information system security. In this context, 'broader risks' refers to those risks arising from non-malicious hazards.

13.4.1 Principle E2 Extended Guidance

The security of network and information systems relies on the control of risks arising from both malicious and non-malicious hazards.

Non malicious hazards, such as fire and accidental damage, can have significant impacts on the delivery of the essential function and must be controlled. Risk assessments are required to identify and prioritise the potential for accidents, failures and environmental factors to adversely impact the operation of network and information systems. Adequate controls are then required to reduce these risks to a level that is appropriate and proportionate.

[20] CAPSS is a joint NPSA and NCSC scheme.

13.4.2 E2.a – Broader resilience risks

E2.a – Broader resilience risks	
Proportionate and appropriate control measures are in place to manage the risks to network and information system security arising from non-malicious hazards.	
Not achieved: At least one of the following statements is true	Achieved: All the following statements are true
E2.a.NA.1 Your network and information system resilience risk assessments are limited to cyber and physical security risks and do not consider broader resilience risks.	**E2.a.A.1** Your risks assessment take account of the risks to NIS system that are associated with accidents, failures and environmental factors. You are actively and effectively controlling all risks.

IGP Ref	IGP Interpretation

E2.a.A.1	Ofgem intends this IGP to:
	• Direct OES to identify risks to the network and information systems other than just cyber and physical tampering. These could include, but are not limited to the following operational risks:
	  • loss of power.
	  • hardware failure and long lead-times for replacements.
	  • software failures.
	  • hardware failure and inability to procure replacements due to obsolescence.
	  • accidental physical damage, e.g. severed network cables.
	  • environmental hazards such as fire and flooding. In this context, flooding refers to the risk of flooding caused by malfunction of plant and services on the site (e.g.inadvertent activation of fire suppression system), it does not take account flooding of the site.
	• Direct OES to apply appropriate and proportionate controls.

IGP Ref	Examples of Evidence to support IGPs
E2.a.A.1	Risk assessments that document broader resilience risks to network and information systems and NIS improvement plan actions that respond to those risks that require treatment.

References and Further Guidance
• www.npsa.gov.uk

14 Glossary of Terms

Term / Acronym	Definition/ Meaning
Anomaly Detection	Anomaly Detection is the technique of establishing a statistical or machine learning baseline of normal user and system behaviour within an environment. It functions by continuously monitoring real-time data and generating alerts when activity significantly deviates from that baseline.
Application Programming Interface (API)	Application Programming Interface: A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.
Artificial intelligence (AI)	Artificial intelligence (AI) describes computer systems which can perform tasks usually requiring human intelligence.
CAF Assessment	A Cyber Assessment Framework (CAF) Assessment is either a self-assessment, or a third-party audited assessment as directed by the Authority, of the Load Control Organisation's security posture against a relevant CAF Profile.
CAF Contributing Outcome (CO)	A Contributing Outcome is a specific requirement in CAF that supports the achievement of a broader security outcome.
CAF Indicators of Good Practice (IGPs)	CAF Indicators of Good Practice are associated with each CAF Contributing Outcome. They provide examples of effective security measures but are not an exhaustive, prescriptive checklist.
Consumer Led Flexibility (CLF)	Consumer Led Flexibility means an arrangement between a Flexibility Service Provider and a Customer in relation to activities undertaken as defined by 4(3)(3J)(b) of the Electricity Act 1989).
Critical National Infrastructure (CNI)	Critical National Infrastructure are assets that are essential for the functioning of society, such as those associated with energy supply, water supply, transportation, health and telecommunications.
Crypto Agility	Crypto agility describes the capabilities needed to replace and adapt cryptographic algorithms for protocols, applications, software, hardware, and infrastructures without interrupting the flow of a running system to achieve resiliency. Crypto agility should be considered for each specific implementation environment.
Cyber Assessment Framework (CAF)	The CAF is a collection of cyber security guidance for organisations that play a vital role in the day-to-day life of the UK, with a focus on essential functions. It is aimed at helping an organisation achieve and demonstrate an appropriate level of cyber resilience in relation to certain specified vitally important functions performed by that organisation, functions that are at risk of disruption as a result of a serious cyber incident.
Cyber Resilience Audit (CRA)	The Cyber Resilience Audit scheme gives consumers confidence in companies that have been assessed as meeting the NCSC standard for delivering independent cyber audits. The Cyber Resilience Audit scheme members will undertake independent cyber audits on behalf of a Cyber Oversight Body.
Cyber Security and Resilience Bill (CSRB)	The Cyber Security and Resilience Bill will reform and add to the existing Network and Information Systems (NIS) Regulations 2018, to increase UK defences against cyber-attacks.
Cyber Security Management System (CSMS).	A Cyber Security Management System is the comprehensive set of policies, processes, governance structures, and controls established by an organisation to manage and reduce cyber security risks to its critical systems and services.
Demand Side Response (DSR)	The intentional alteration of electricity consumption patterns by end users from their normal consumption levels in response to external signals. These signals, such as pricing incentives or direct control instructions, are

	used to manage demand, improve network resilience, and support the integration of renewable energy sources into the grid.
Department for Energy Security and Net Zero. (DESNZ)	Department for Energy Security and Net Zero (DESNZ) leads on the government's mission to make the UK a clean energy superpower.
Domestic Consumer / Customer	Domestic Consumer / Customer is a consumer provided with or seeking to be provided with a Consumer-Led Flexibility service located at a Domestic Premises but excludes such Customer insofar as they are provided with or seeking to be provided with a Consumer-Led Flexibility service at a premises other than Domestic Premises.
Domestic Premises	Domestic Premises means premises at which a supply of electricity is taken wholly or mainly for domestic purposes.
Downstream Gas and Electricity (DGE)	Downstream Gas and Electricity (DGE) refers to the essential services within the gas and electricity sectors in Great Britain, focusing on transmission, distribution, and supply to consumers, excluding upstream production.
Energy Smart Appliance (ESA)	ESA has the meaning given to this term in section 238 of the Energy Act 2023, where it relates to an electric vehicle, electric vehicle charge point, hydronic heat pump, storage heater, heat battery, hot water heat pumps, standalone direct electrical hot water cylinders, hybrid heat pump, or battery energy storage system.
Enterprise IT (EIT)	"IT" is a general term for information technology, while "Enterprise IT" refers specifically to the large-scale systems and services used by major organisations to support their daily operations. The key differences are scale, complexity, and purpose: IT is the broad field of using computers and networks, whereas Enterprise IT is the application of this field to meet the complex, high-demand, and security-critical needs of a large business, focusing on reliability and strategic goals. This may include messaging, collaboration, service delivery platforms like Microsoft 365.
ESA Manager (ESAM)	An ESA Manager (ESAM) is a logical entity that provides an interface to Load Controllers and that represents one or more ESAs.
Essential services	Under the Network and Information Systems (NIS) regulations, an essential service is one that is critical for maintaining societal or economic activities, where its provision relies on network and information systems, and any incident would have significant disruptive effects. Throughout this guidance, where the term "essential" is used, it should be interpreted as meaning "essential for the provision of the Licensed Load Control service/activity". See 2.2.3
Flexibility Service Provider (FSP)	Flexibility Service Provider: organisations entering into flex arrangements directly with a consumer. Any person undertaking activity as defined by 6BAA(1)(b) of the Electricity Act 1989.
Internet of Things (IoT)	Internet of Things (IoT) is the technology describing everyday objects (rather than computers and smartphones) that can connect to the internet. Examples include speakers, televisions, security cameras and consumer ESAs.
Joint Competent Authority	The Department for Energy Security and Net Zero and Ofgem are the designated Joint Competent Authority under the Network and Information Systems Regulations 2018.
Licensed Load Control organisations	The Load Control Licence is the formal statutory instrument, granted by Ofgem, that permits an organisation to undertake Licensed Load Control activities within the Demand Side Response sector covering both Domestic and Small Non-Domestic CLF and the Industrial and Commercial (I&C) DSR sector.
Load Control System (or Load Control Platform)	Load Control System (or Load Control Platform) means any systems which are operated by or on behalf of a Load Controller and used in whole or in part for: (a) constructing load control communications to Energy Smart Appliances;

	(b) sending load control communications to Energy Smart Appliances; (c) receiving, sending, storing, using or otherwise carrying out any processing in respect of load control communications with Energy Smart Appliances; (d) receiving responses or alerts from Energy Smart Appliances, intended for the Load Controller.
Load Controller	A Load Controller means any persons undertaking activity under 6BAA(1)(a) of the Electricity Act 1989.
Load-Altering Attack (LAA)	A Load-Altering Attack (LAA) is a cyber-physical attack where an adversary compromises a large number of OT or IoT enabled, high-wattage appliances (e.g. EV Charge points) to maliciously manipulate the aggregate power consumption in a power grid. The primary goal is to disrupt the balance between electricity supply and demand, which can lead to severe consequences such as frequency deviations, voltage fluctuations, line failures, cascading outages, and even blackouts.
National Cyber Security Centre (NCSC)	The NCSC is a part of GCHQ that helps businesses, the public sector and individuals protect the online services and devices that the UK depend on, and act as the National Technical Authority for cyber security.
National Energy System Operator (NESO)	The National Energy System Operator (NESO) was created as a result of the UK's 2023 Energy Act. NESO is at the centre of the UK's energy system and act as a neutral voice and look at the whole picture to suggest fair solutions for energy that work for everyone across the country.
NCSC Assured Service Providers (ASPs)	NCSC Assured Service Providers (ASPs) are companies that have met the stringent standards of the NCSC to provide professional cybersecurity services.
network and Information system (lower case)	"network and information system" means: (a) an electronic communications network; (b) any device or group of interconnected or related devices which performs automatic processing of digital data; and (c) digital data stored, processed, retrieved or transmitted by elements covered under (a) or (b) for the purposes of their operation, use, protection and maintenance. See 2.2.4
Network & Information Systems (NIS) (upper case)	Network & Information Systems Regulations (NIS Regulations) 2018. The Security of Network & Information Systems Regulations provide legal measures to boost the level of security (both cyber & physical resilience) of network and information systems for the provision of essential services and digital services.
Operational Technology (OT)	OT is defined as technology that interfaces with the physical world and includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.
Operator of Essential Services (OES)	"Operator of Essential Services" means an entity designated or deemed to be designated under Regulation 8 of the Network and Information Systems Regulations 2018 as an operator of essential services in relation to its activities, being an organisation that provides a service which is essential for the maintenance of critical societal or economic activities, where the provision of that service depends on network and information systems, and an incident affecting those systems would have significant disruptive effects on the provision of that service.
Post-Quantum Cryptography	The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks.
Smart Secure Electricity Systems (SSES)	The DESNZ Smart Secure Electricity Systems (SSES) Programme is designed to create the technical and regulatory frameworks to enable the untapped flexibility from small scale devices, such as domestic electric vehicle charge points and heat pumps.

Threat Hunting	Threat hunting is an active, iterative process of proactively searching through network and system data (logs, telemetry) to detect adversaries who have evaded existing security controls. It is typically hypothesis-driven, focusing on detecting novel TTPs rather than reacting to known signatures.
TTPs	TTP stands for Tactics, Techniques, and Procedures, which are the methods and behaviours used by threat actors to carry out cyberattacks. Analysing TTPs helps security teams understand how adversaries operate, allowing them to detect, mitigate, and predict attacks more effectively.