Telecommunications (Jersey) Law 2002

Case T-046: Fixed Line Voice and 4G Outage of network of JT (Jersey) Limited on 28 July 2021: Directions to JT (Jersey) Limited

Document No: JCRA 22/30

Date: 6 May 2022

Jersey Competition Regulatory Authority
2nd Floor Salisbury House, 1-9 Union Street
St Helier
Jersey, JE2 3RF
Tel 01534 514990

Web: www.jcra.je

Contents

Section

1. Executive Summary

1.1 On 20 September 2021 the Authority published an Information Note announcing that it was investigating the outage on 28 July 2021 (***2021 Outage***) of:

(a) the voice service on fixed lines, SIP Trunk and ISDN30; and

(b) the 4G service

in relation to certain subscribers on the telecommunications network operated by JT under a licence (***Licence***) issued to it by the Authority under the Telecommunications (Jersey) Law 2002 (***Telecoms Law***).

1.2 Following such investigation, with which JT cooperated, the Authority informed JT on 8 November 2021 that the Authority had determined that, in relation to the 2021 Outage, JT was in contravention of two conditions of its licence:

(a) Condition 9: *the obligation to take 'all reasonable steps to ensure the integrity of its network';* and

(b) Condition 14.1: *the obligation to provide 'a public emergency call service'*.

1.3 JT has accepted this determination. The Telecoms Law provides that in the event of a contravention of a licence condition:

(a) Article 19(1) – 'the Authority shall give a direction to the licensee to take steps, or specific steps, to ensure compliance with that condition'; and

(b) Article 19A – 'the Authority may, in addition to, or in place of … giving a direction under Article 19(1) …make an order imposing a financial penalty on the licensee for the contravention.

1.4 The Authority issued its Notification of Proposed Directions to JT on 16 February 2022, setting out the text of two Directions (Direction 1 and Direction 2). The deadline for JT to make representations in relation to the proposed Directions was 17:00 on 16 March 2022. JT made, but has subsequently withdrawn, certain representations.

1.5 Direction 1 and Direction 2 come into effect on 6 May 2022 in the form set out below.

2. The scope of Direction 1 and Direction 2

Summary

2.1 This section sets out the Authority's decision in respect of the directions to be issued to JT.

2.2 The Authority considers that it is appropriate to issue directions to JT pursuant to Article 19(1) of the Telecommunications (Jersey) Law 2002.

Directions

2.3 **Direction 1** imposes obligations on JT to ensure that Conditions 9 and 14.1 are met and specifically incorporates and gives effect to certain undertakings given by JT to the Authority; and

2.4 **Direction 2** sets out a self-reporting framework in relation to fulfilling the obligations set out in Direction 1**.**

Directions issued to JT (Jersey) Limited

DIRECTION 1

The Authority directs JT (Jersey) Limited (***JT***) to comply with its obligations under Conditions 9 and 14 of its licence under the Telecommunications (Jersey) Law 2002 (the ***Telecoms Law***) and to take all actions necessary to ensure that its network is resilient, reliable and secure for the benefit of the people of Jersey and to ensure that its network provides a public emergency call service at all times.

In relation to Direction 1, JT shall achieve all of the following by the stated dates, which shall be indicative of JT's compliance with the Direction:

Subject	**JT action**	**Date/recurrence etc**
Service Incident Reporting	JT shall report to the Authority within 24 hours of the occurrence of any significant outage affecting its network or the provision of the public emergency call service and, without prejudice to such obligation, shall report to the Authority any occurrence of: • 100 fixed lines and/or 5 Enterprise (ISDN 30 or SIPTrunk) lines being out of service for 30 minutes or more; or • any 2G or 3G mobile based band unit being out of service for 30 minutes or more	From date of these Directions
	Comply with the Authority's Guidance on the Provision of a Public Emergency Calls Service	The date of adoption by the Authority
Advance notice of planned works	Provide: • the Authority; and • each Other Licensed Operator which may be affected or which is dependent on JT's network for the provision of a public emergency call service with not less than 7 days' written notice of any planned works that have the possibility of causing an outage or impacting the ability of a user to contact the emergency services	From the date of these Directions
Network Performance/Reliability KPIs (to be agreed with the Authority)	Report to the Authority on network performance/reliability KPIs within one month of the end of each quarter	Quarterly with the Q1 2022 report by 20 April 2022; KPIs to be agreed in advance of that date
Resolution of ZTE RFO items (as annexed to JT's SI report of 12 August 2021)	Confirm and action any outstanding items from the ZTE RFO and report to the Authority	30 June 2022

Subject	**JT action**	**Date/recurrence etc**
Change Management	Make all necessary improvements to its change management approval process to ensure that risks are identified and addressed and, without prejudice to such obligation, in compliance with the Further Directions of the Authority in relation to Case T-027[1] in relation to change management policies	From the date of these Directions
	Complete the deployment of an Asset Management System and Change Management Database and confirm to the Authority	31 December 2022 for deployment; confirmation by 13 January 2023

[1] JCRA Document 22/19 dated 17 March 2022

DIRECTION 2

The Authority directs JT to ensure that it has in place robust processes for ensuring that it complies with Direction 1 and to enable it to demonstrate to the Authority that this is so.

In relation to Direction 2 and indicative of compliance with it, JT shall adopt, and completely, accurately and diligently carry out reviews under, the Security Assurance Framework (***SAF***), being the SAF in the form annexed to these Directions as updated from time to time by agreement with the Authority and subject to the final paragraph below. JT shall:

1.1 Complete its first SAF review by 31 March 2022 and shall provide the Authority a report on the outcome of such review within 10 days of completion.

1.2 In such report set out in respect of each of the headings/subheadings in the SAF:

(a) Whether the outcome is 'Achieved' or 'Not Achieved' or, where permitted, 'Partially Achieved';

(b) Evidence of the basis for determining such outcome such as to enable the Authority to understand the process followed and criteria applied and the justification for the conclusion;

(c) In respect of 'Not Achieved' or 'Partially Achieved' outcomes, JT's action plan for ensuring that the outcome will merit 'Achieved' status by the time of the next SAF review;

1.3 Take all due account of any comments or recommendations of the Authority in respect of such report.

1.4 Without prejudice to Conditions 4.1, 4.3 and 4.4 of its licence under the Telecoms Law, provide the Authority and its advisors with all such information relating to compliance with the SAF as the Authority shall reasonably specify and shall give the Authority and its advisors access to all relevant records, documents and JT staff and systems.

1.5 Without prejudice to Condition 4.5 of such licence, be responsible for meeting the Authority's reasonable costs (including the costs of external advisors) in connection with considering such report. Where so directed by the Authority, JT shall lodge with the Authority a sum on account of some or all of such costs.

1.6 Carry out additional SAF reviews on the same basis as set out in paragraph 1.2 on a not less than a 6 monthly basis, additionally setting out and justifying any changes in any outcome from the immediately prior report, including (with explanation and action plan) any failures to improve any previous 'Partially Achieved' or 'Not Achieved' outcome.

This Direction 2 shall remain in effect until 31 December 2027 save that the Authority shall have the discretion to reduce the frequency or detail required in relation to the reporting of the reviews if it is satisfied that JT is complying with the relevant part of Direction 2 or if the Authority determines that such reviews are in whole or in part rendered unnecessary by reason of a change in the Telecoms Law or JT's licence.

Direction 1 and Direction 2 shall come into effect on 6 May 2022.

BY ORDER OF THE AUTHORITY

JCRA/JT Security Assurance Framework

1. Introduction

The Security Assurance Framework (SAF) is intended to help JT to achieve and demonstrate an appropriate level of security resilience in relation to JT's provision of essential network services.

In this context, the term security resilience refers to JT's ability to maintain the correct operation of its essential network services, even in the presence of adverse security events, which could be caused by equipment or operational failures or by malicious attacks.

The SAF is intended to be used by JT to help to manage the risk of a loss or degradation of JT's essential network services as a result of an adverse security event, and to provide assurance to the JCRA that JT is successfully managing that risk.

The SAF is based on industry best practice and international standards on security, extended as required for this purpose, and is presented as a set of high-level principles to guide decision-making, and in terms of outcomes to be achieved, rather than a detailed set of prescriptive actions to be carried-out against a compliance checklist. This approach allows JT to develop its own ways of achieving the specified SAF outcomes, while the inclusion of good practice indicators within the SAF provide both JT and the JCRA with a benchmark for understanding the extent to which the measures put in place by JT are sufficient to achieve SAF outcomes. This approach is also consistent with the JCRA's general approach to goal-based regulation.

The 14 SAF security principles define a set of top-level outcomes that collectively describe good practice for security resilience, and each is accompanied by more detail on the factors JT may need to take into account in deciding how to achieve each outcome, including sets of indicators of good practice (IGPs). The IGP tables for each SAF outcome indicate whether JT is assessed as achieving (green), not achieving (red) or partially achieving (amber) the outcome, leading to an overall assessment of achievement against the (currently) 39 indicators.

The JCRA intends the SAF principles and guidance to be used by JT as follows:

- Understand the principles and why they are important. Interpret the principles for JT.
- Compare the outcomes described in the principles to JT's current practices. Use the guidance to inform the comparison.
- Identify shortcomings. Understand the seriousness of shortcomings using organisational context and prioritise.
- Implement prioritised remediation. Use the guidance to inform remediation activities.

The SAF is intended to be used by the JCRA to periodically review JT’s security resilience, and JT’s plans to further improve their achievement of SAF outcomes (initially, annually). The SAF may be refined over time to take account of experience of use, or due to the emergence of new risks or threats.

2. SAF Foundations

The SAF is derived from the UK National Cyber Security Centre's (NCSC) Cyber Assurance Framework (CAF)[1]. The CAF provides a systematic and comprehensive approach to assessing the extent to which security and resilience risks to essential services are being managed by the organisation responsible. The CAF may be used by the responsible organisation itself (self-assessment) and/or by a regulator to gain assurance in the regulated organisation's capability to successfully manage security and resilience risks.

The SAF is a CAF Profile, ie the use of an adaptation/extension of the CAF as a basis for a regulator (JCRA) setting a target for a regulated organisation (JT) to achieve. As a CAF Profile, the SAF may place a sector-specific regulatory interpretation on the CAF generic outcomes and/or Indicators of Good Practice (IGPs), and/or may include some additional sector-specific outcomes and/or IGPs.

The CAF and SAF are compatible with the use of existing generic and sector-specific security and resilience guidance and standards, and applicable legislation (see section 4 for a list of principal references). While compliance with, and certification against, existing security and resilience standards may help CAF/SAF outcomes to be achieved, they may not be necessary or sufficient.

[1] Contains public sector information licensed under the Open Government Licence v3.0. http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/

3. SAF Principles, Outcomes and Indicators of Good Practice

Objective A – Managing Security Risk[2]

Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting the provision of essential network services[3].

Principle A1 Governance

The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.

A1.a Board Direction

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

Not achieved	Achieved
At least one of the following statements is true	All the following statements are true
The security of network and information systems related to the provision of essential network services is not discussed or reported on regularly at board-level.	Your organisation's approach and policy relating to the security of networks and information systems supporting the provision of essential network services are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.
Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance.	Regular board discussions on the security of network and information systems supporting the provision of essential network services take place, based on timely and accurate information and informed by expert guidance.
The security of networks and information systems supporting the provision of	There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level.

[2] https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-a-managing-security-risk

[3] In the SAF, we use the term 'the provision of essential network services' in place of the generic term 'essential function' in the NCSC's CAF.

Not achieved	Achieved
essential network servces are not driven effectively by the direction set at board level. Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.	Direction set at board level is translated into effective organisational practices that direct and control the security of the networks and information systems providing your essential network services.

A1.b Roles & Responsibilities

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

Not achieved	Achieved
At least one of the following statements is true	All the following statements are true
Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis.	Necessary roles and responsibilities for the security of networks and information systems providing your essential network services have been identified. These are reviewed periodically to ensure they remain fit for purpose.
Staff are assigned security responsibilities but without adequate authority or resources to fulfil them.	Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties.
Staff are unsure what their responsibilities are for the security of the provision of essential network services.	There is clarity on who in your organisation has overall accountability for the security of the networks and information systems providing your essential network services.

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 provision of essential network services are considered in the context of other organisational risks.

Not achieved	Achieved
At least one of the following statements is true	All the following statements are true
What should be relatively straightforward risk decisions are constantly referred up the chain, or not made.	Senior management have visibility of key risk decisions made throughout the organisation.
Risks are resolved informally (or ignored) at a local level without a formal reporting mechanism when it is not appropriate.	Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the provision of essential network services, as set by senior management.
Decision-makers are unsure of what senior management's risk appetite is, or only understand it in vague terms such as "averse" or "cautious".	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.
Organisational structure causes risk decisions to be made in isolation. (e.g. engineering and IT don't talk to each other about risk).	Risk management decisions are periodically reviewed to ensure their continued relevance and validity.
Risk priorities are too vague to make meaningful distinctions between them (e.g. almost all risks are rated 'medium' or 'amber').	

Principle A2 Risk Management

The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the provision of essential network services. This includes an overall organisational approach to risk management.

A2.a Risk Management Process

Your organisation has effective internal processes for managing risks to the security of network and information systems providing essential network services and communicating associated activities.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Risk assessments are not based on a clearly defined set of threat assumptions. 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. Risk assessments for critical systems are a "one-off" activity (or not done at all). The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes. There is no systematic process in place to ensure that identified security risks are managed effectively. Systems are assessed in isolation, without consideration of dependencies and interactions with other systems (e.g. interactions between IT and OT environments).	Your organisational process ensures that security risks to networks and information systems relevant to the provision of essential network services are identified, analysed, prioritised, and managed. Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems providing your essential network services. 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. Significant conclusions reached in the course of your risk management process are communicated to	Your organisational process ensures that security risks to networks and information systems relevant to the provision of essential network services are identified, analysed, prioritised, and managed. Your approach to risk is focused on the possibility of adverse impact to your essential network services, leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your networks and information systems. Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential network services and your sector. Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information

Not achieved	Partially achieved	Achieved
Security requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of the essential network services. Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.	key security decision-makers and accountable individuals. You conduct risk assessments when significant events potentially affect essential network services, such as replacing a system or a change in the cyber security threat. You perform threat analysis and understand how generic threats apply to your organisation.	systems providing your essential network services. 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. Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals. You conduct risk assessments when significant events potentially affect essential network services, such as replacing a system or a change in the cyber security threat. Your risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information. The effectiveness of your risk management process is reviewed periodically, and improvements made as required. You perform detailed threat analysis and understand how

Not achieved	Partially achieved	Achieved
		this applies to your organisation in the context of the threat to your sector and the wider CNI.

A2.b Assurance

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

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

Principle A3 Asset Management

Everything required to deliver, maintain or support networks and information systems necessary for the provision of essential network services is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).

A3.a Asset Management

Not achieved	Achieved
At least one of the following statements is true	All the following statements are true
Inventories of assets relevant to provision of essential network services are incomplete, non-existent, or inadequately detailed. Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT). 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. Knowledge critical to the management, operation, or recovery of essential network services is held by one or two key individuals with no succession plan. Asset inventories are neglected and out of date.	All assets relevant to the secure provision of essential network services are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date. Dependencies on supporting infrastructure (e.g. power, cooling etc) are recognised and recorded. You have prioritised your assets according to their importance to the provision of essential network services. You have assigned responsibility for managing physical assets. Assets relevant to essential network services are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.

Principle A4 Supply Chain

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

A4.a Supply Chain

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
You do not know what data belonging to you is held by suppliers, or how it is managed. Elements of the supply chain for essential network services are subcontracted and you have little or no visibility of the sub-contractors. Relevant contracts do not have security requirements. Suppliers have access to systems that provide your essential network services that is unrestricted, not monitored or bypasses your own security controls.	You understand the general risks suppliers may pose to your essential network services. You know the extent of your supply chain for essential network services, including sub-contractors. You engage with suppliers about security, and you set and communicate security requirements in contracts. You are aware of all third-party connections and have assurance that they meet your organisation's security requirements. Your approach to security incident management considers incidents that might arise in your supply chain.	You have a deep understanding of your supply chain, including sub-contractors and the wider risks it faces. You consider factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your risk assessment and procurement processes. Your approach to supply chain risk management considers the risks to your essential network services arising from supply chain subversion by capable and well-resourced attackers. You have confidence that information shared with suppliers that is essential to the provision of your essential network services is appropriately protected from sophisticated attacks. You can clearly express the security needs you place on suppliers in ways that are mutually understood and are laid in contracts. There is a clear and documented shared-responsibility model.

Not achieved	Partially achieved	Achieved
	You have confidence that information shared with suppliers that is necessary for the provision of your essential network services is appropriately protected from well-known attacks and known vulnerabilities.	All network connections and data sharing with third parties is managed effectively and proportionately. When appropriate, your incident management process and that of your suppliers provide mutual support in the resolution of incidents.

Objective B – Protecting against cyber attack[4]

Proportionate security measures are in place to protect the networks and information systems providing essential network services from cyber attack.

Principle B1 Service Protection Policies and Processes

The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support provision of essential network services.

B1.a Policy and Process Development

You have developed and continue to improve a set of cyber security and resilience policies and processes that manage and mitigate the risk of adverse impact on the provision of essential network services.

Not achieved	**Partially achieved**	**Achieved**
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Your policies and processes are absent or incomplete. Policies and processes are not applied universally or consistently. People often or routinely circumvent policies and processes to achieve business objectives. Your organisation's security governance and risk management approach has no bearing on your policies and processes.	Your policies and processes document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. You review and update policies and processes in response to major cyber security incidents.	You fully document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is integrated and embedded throughout these policies and processes and key performance indicators are reported to your executive management. Your organisation's policies and processes are developed to be practical, usable and appropriate for your provision of essential network services and your technologies. Policies and processes that rely on

[4] https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-b-protecting-against-cyber-attack

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

B1.b Policy and Process Implementation

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

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Policies and processes are ignored or only partially followed. The reliance on your policies and processes is not well understood. Staff are unaware of their responsibilities	Most of your policies and processes are followed and their application is monitored. Your policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.	All your policies and processes are followed, their correct application and security effectiveness is evaluated. Your policies and processes are integrated with other organisational policies and processes, including HR

Not achieved	Partially achieved	Achieved
under your policies and processes. You do not attempt to detect breaches of policies and processes. Policies and processes lack integration with other organisational policies and processes. Your policies and processes are not well communicated across your organisation.	All staff are aware of their responsibilities under your policies and processes. All breaches of policies and processes with the potential to adversely impact essential network servcies are fully investigated. Other breaches are tracked, assessed for trends and action is taken to understand and address.	assessments of individuals' trustworthiness. Your policies and processes are effectively and appropriately communicated across all levels of the organisation resulting in good staff awareness of their responsibilities. Appropriate action is taken to address all breaches of policies and processes with potential to adversely impact the provision of essential network services including aggregated breaches.

Principle B2 Identity and Access Control

The organisation understands, documents and manages access to networks and information systems supporting the provision of essential network services. Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.

B2.a Identity Verification, Authentication and Authorisation

You robustly verify, authenticate and authorise access to the networks and information systems providing your essential network services.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Authorised users with access to networks or	All authorised users with access to networks or information systems on which	Only authorised and individually authenticated users can physically access and logically connect to

Not achieved	Partially achieved	Achieved
information systems on which your essential network services depend cannot be individually identified. Unauthorised individuals or devices can access your networks or information systems on which your essential network services depend. User access is not limited to the minimum necessary.	your essential network servcies depend are individually identified and authenticated. User access to essential function networks and information systems is limited to the minimum necessary. You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for privileged access to sensitive systems such as operational technology. You individually authenticate and authorise all remote user access to all your networks and information systems that support your essential network services. The list of users with access to networks and systems providing essential network services is reviewed on a regular basis, at least annually.	your networks or information systems on which your essential network services depend. User access to all your networks and information systems supporting the essential function is limited to the minimum necessary. You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for privileged access to all systems that operate or support your essential network services. You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, when you individually authenticate and authorise all remote user access to all your networks and information systems that support your essential network services. The list of users with access to networks and systems supporting and delivering essential network services is reviewed on a regular basis, at least every six months.

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 network services..

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Users can connect to your networks and systems supporting your essential network services using devices that are not corporately managed. Privileged users can perform administrative functions from devices that are not corporately managed. You have not gained assurance in the security of any third-party devices or networks connected to your systems. Physically connecting a device to your network gives that device access without device or user authentication	Only corporately owned and managed devices can access your networks and information systems supporting your essential network services. All privileged access occurs from corporately management devices dedicated to management functions. 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. The act of connecting to a network port or cable does not grant access to any systems. You are able to detect unknown devices being connected to your network and investigate such incidents.	Dedicated devices are used for privileged actions (such as administration or accessing network and information systems supporting your essential network services). These devices are not used for directly browsing the web or accessing email. You either obtain independent and professional assurance of the security of third-party devices or networks before they connect to your systems, or you only allow third-party devices or networks dedicated to supporting your systems to connect. You perform certificate-based device identity management and only allow known devices to access systems necessary for the provision of your essential network services. You perform regular scans to detect unknown devices and investigate any findings.

B2.c Privileged User Management

You closely manage privileged user access to networks and information systems supporting essential network services.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
The identities of the individuals with privileged access to your systems (infrastructure, platforms, software, configuration, etc) are not known or not managed. Privileged user access to your systems is via weak authentication mechanisms (e.g. only simple passwords). The list of privileged users has not been reviewed recently (e.g. within the last 12 months). Privileged user access is granted on a system-wide basis rather than by role or function. Privileged user access to your systems is via generic, shared or default name accounts. 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.	Privileged user access requires additional validation, but this does not use a strong form of authentication (e.g. two-factor, hardware authentication or additional real-time security monitoring). The identities of the individuals with privileged access to your systems (infrastructure, platforms, software, configuration, etc) are known and managed. This includes third parties. Activity by privileged users is routinely reviewed and validated. (e.g. at least annually). Privileged users are only granted specific privileged permissions which are essential to their business role or function.	Privileged user access to your systems is carried out from dedicated separate accounts that are closely monitored and managed. The issuing of temporary, time-bound rights for privileged user access and external third-party support access is either in place or you are migrating to an access control solution that supports this functionality. Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process. All privileged user access to your networks and information systems requires strong authentication, such as two-factor, hardware authentication, or additional real-time security monitoring. All privileged user activity is routinely reviewed, validated and recorded for offline analysis and investigation.

Not achieved	Partially achieved	Achieved
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).		

B2.d Identity and Access Managemeny (IdaM)

You assure good management and maintenance *of identity and access control for your networks and information systems providing essential network services.*

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Greater rights are granted to users than necessary. User rights are granted without validation of their identity and requirement for access. User rights are not reviewed when they move jobs. User rights remain active when people leave your organisation.	You follow a robust procedure to verify each user and issue the minimum required access rights. You regularly review access rights and those no longer needed are revoked. User permissions are reviewed when people change roles via your joiners, leavers and movers process. All user access is logged and monitored.	Your procedure to verify each user and issue the minimum required access rights is robust and regularly audited. User permissions are reviewed both when people change roles via your joiners, leavers and movers process and at regular intervals - at least annually. All user access is logged and monitored. You regularly review access logs and correlate this data with other access records and expected activity. Attempts by unauthorised users to connect to your systems are alerted, promptly assessed and investigated.

Principle B3 Data Security

Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on essential network services. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the provision of essential network services. It also covers information that would assist an attacker, such as design details of networks and information systems.

B3.a Understanding Data

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

Not achieved	**Partially achieved**	**Achieved**
At least one of the following statements is true	All of the following statements are true	All the following statements are true
You have incomplete knowledge of what data is used by and produced in the provision of essential network services. You have not identified the important data on which your essential network services rely. You have not identified who has access to data important to the provision of essential network services.	You have identified and catalogued all the data important to the provision of essential network services, or that would assist an attacker. You have identified and catalogued who has access to the data important to the provision of essential network services. You periodically review location, transmission, quantity and quality of data important to the provision of essential network services.	You have identified and catalogued all the data important to the provision of essential network services, or that would assist an attacker. You have identified and catalogued who has access to the data important to the provision of essential network services. You maintain a current understanding of the location, quantity and quality of data important to the provision of essential network services. You take steps to remove or minimise unnecessary copies or unneeded historic data. You have identified all mobile devices and media that may hold

Not achieved	Partially achieved	Achieved
You have not clearly articulated the impact of data compromise or inaccessibility.	You have identified all mobile devices and media that hold data important to the provision of essential network services. You understand and document the impact on your essential network services of all relevant scenarios, including unauthorised access, modification or deletion, or when authorised users are unable to appropriately access this data. You occasionally validate these documented impact statements.	data important to the provision of essential network services. You maintain a current understanding of the data links used to transmit data that is important to your essential function. You understand the context, limitations and dependencies of your important data. You understand and document the impact on your essential network services of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data. You validate these documented impact statements regularly, at least annually.

B3.b Data in Transit

You have protected the transit of data important to the provision of essential network services. This includes the transfer of data to third parties.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
You do not know what all your data links are, or which carry data	You have identified and protected (effectively and proportionately) all the data links that carry data important	You have identified and protected (effectively and proportionately) all the data links that carry data important

Not achieved	Partially achieved	Achieved
important to the provision of your essential network services. Data important to the provision of essential network services travels without technical protection over non-trusted or openly accessible carriers. Critical data paths that could fail, be jammed, be overloaded, etc. have no alternative path.	to the provision of your essential network services. You apply appropriate 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.	to the provision of your essential network services. You apply appropriate physical or technical means to protect data that travels over non-trusted or openly accessible carriers, with justified confidence in the robustness of the protection applied. Suitable alternative transmission paths are available where there is a significant risk of impact on the provision of essential network services due to resource limitation (e.g. transmission equipment or function failure, or important data being blocked or jammed).

B3.c Stored Data

You have protected stored data important to the provision of the essential network services.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
You have no, or limited, knowledge of where data important to the provision of essential network services is stored. You have not protected vulnerable stored data important to the provision of	All copies of data important to the provision of your essential network services are necessary. Where this important data is transferred to less secure systems, the data is provided with limited	You have only necessary copies of this data. Where data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy.

Not achieved	Partially achieved	Achieved
essential network services in a suitable way. Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.	detail and/or as a read-only copy. You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion. 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. You have suitable, secured backups of data to allow the provision of essential network services 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.	You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion. If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied. You have suitable, secured backups of data to allow the provision of essential network services 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. Necessary historic or archive data is suitably secured in storage.

B3.d Mobile Data

You have protected data important to the provision of essential network services on mobile devices.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
You don’t know which mobile devices may hold data important to the provision of essential network services. You allow data important to the provision of essential network services to be stored on devices not managed by your organisation, or to at least equivalent standard. Data on mobile devices is not technically secured, or only some is secured.	You know which mobile devices hold data important to the provision of essential network servcies. Data important to the provision of essential network servces is only stored on mobile devices with at least equivalent security standard to your organisation. Data on mobile devices is technically secured.	Mobile devices that hold data that is important to the provision of essential network services 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. Your organisation can remotely wipe all mobile devices holding data important to the provision of essential network services. You have minimised this data on these mobile devices. Some data may be automatically deleted off mobile devices after a certain period.

B3.e Media/Equipment Sanitisation

You appropriately sanitise media and equipment holding data important to the provision of essential network services.

Not achieved	Achieved
At least one of the following statements is true	All the following statements are true
Some or all devices, equipment or removable media that hold data important to the provision of essential network	You catalogue and track all devices that contain data important to the provision of essential network services (whether a

Not achieved	Achieved
services are disposed of without sanitisation of that data.	specific storage device or one with integral storage). All data important to the provision of essential network services is sanitised from all devices, equipment or removable media before disposal.

Principle B4 System Security

Network and information systems and technology critical for the provision of essential network services are protected from cyber attack. An organisational understanding of risk to the provision of essential network services informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.

B4.a Secure by Design

You design security into the network and information systems that support the provision of essential network services. You minimise their attack surface and ensure that the provision of essential network servuces 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 of the following statements are true	All the following statements are true
Systems essential to the provision of essential network services are not appropriately segregated from other systems. Internet access is available from operational systems. Data flows between the operational systems and other systems are complex, making it hard to discriminate between	You employ appropriate expertise to design network and information systems. You design strong boundary defences where your networks and information systems interface with other	You employ appropriate expertise to design network and information systems. Your networks and information systems are segregated into appropriate security zones, e.g. operational systems for essential network services are segregated in a highly trusted, more secure zone. The networks and information

Not achieved	Partially achieved	Achieved
legitimate and illegitimate/malicious traffic. Remote or third party accesses circumvent some network controls to gain more direct access to operational systems of essential network services.	organisations or the world at large. You design simple data flows between your networks and information systems and any external interface to enable effective monitoring. You design to make network and information system recovery simple. All inputs to operational systems are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.	systems providing your essential network services are designed to have simple data flows between components to support effective security monitoring. The networks and information systems providing your essential neteork services are designed to be easy to recover. Content-based attacks are mitigated for all inputs to operational systems that affect the essential network services (e.g. via transformation and inspection).

B4.b Secure Configuration

You securely configure the network and information systems that support the provision of essential network services.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
You haven't identified the assets that need to be carefully configured	You have identified and documented the assets that need to be carefully	You have identified, documented and actively manage (e.g. maintain security

Not achieved	Partially achieved	Achieved
to maintain the security of essential network services. 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 network services. Configuration details are not recorded or lack enough information to be able to rebuild the system or device. The recording of security changes or adjustments that effect your essential network services is lacking or inconsistent.	configured to maintain the security of essential network services. Secure platform and device builds are used across the estate. Consistent, secure and minimal system and device configurations are applied across the same types of environment. Changes and adjustments to security configuration at security boundaries with the networks and information systems supporting your essential network services are approved and documented. You verify software before installation is permitted.	configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of essential network services. All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment. You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented. You regularly review and validate that your network and information systems have the expected, secured settings and configuration. Only permitted software can be installed and standard users cannot change settings that would impact security or business operation. If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated.

B4.c Secure Management

You manage your organisation's network and information systems that support the provision of essential network services to enable and maintain security.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Networks and systems providing essential network services are administered or maintained using non-dedicated devices. You do not have good or current technical documentation of your networks and information systems.	Your systems and devices supporting the provision of essential network services are only administered or maintained by authorised privileged users from dedicated devices. Technical knowledge about networks and information systems, such as documentation and network diagrams, is regularly reviewed and updated. You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.	Your systems and devices supporting the provision of essential network services are only administered or maintained by authorised privileged users from dedicated devices that are technically segregated and secured to the same level as the networks and systems being maintained. You regularly review and update technical knowledge about networks and information systems, such as documentation and network diagrams, and ensure they are securely stored. You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.

B4.d Vulnerability Management

You manage known vulnerabilities in your network and information systems to prevent adverse impact on essential network services.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
You do not understand the exposure of your provision essential network services to publicly-known vulnerabilities. You do not mitigate externally-exposed vulnerabilities promptly. There are no means to check data or software imports for malware. You have not recently tested to verify your understanding of the vulnerabilities of the networks and information systems that support your essential function. You have not suitably mitigated systems or software that is no longer supported. You are not pursuing replacement for unsupported systems or software.	You maintain a current understanding of the exposure of your provision of essential network services to publicly-known vulnerabilities. Announced vulnerabilities for all software packages, network equipment and operating systems used to support your provision of essential network servcies are tracked, prioritised and externally-exposed vulnerabilities are mitigated (e.g. by patching) promptly. Some vulnerabilities that are not externally exposed have temporary mitigations for an extended period. You have temporary mitigations for unsupported systems and software while pursuing migration to supported technology. You regularly test to fully understand the vulnerabilities of the networks and information systems that support the provision of your essential network services.	You maintain a current understanding of the exposure of your provision of essential network services to publicly-known vulnerabilities. Announced vulnerabilities for all software packages, network equipment and operating systems used to support the provision of your essential network services are tracked, prioritised and mitigated (e.g. by patching) promptly. You regularly test to fully understand the vulnerabilities of the networks and information systems that support the provision of your essential network services and verify this understanding with third-party testing. You maximise the use of supported software, firmware and hardware in your networks and information systems supporting your provision of essential network services.

Principle B5 Resilient Networks and Systems

The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of systems that support the provision of essential network services.

B5.a Resilience Preparation

You are prepared to restore the provision of your essential network services following adverse impact.

Not achieved	Partially achieved	Achieved
Any of the following statements are true	All of the following statements are true	All the following statements are true
You have limited understanding of all the elements that are required to restore the provision of essential network services. You have not completed business continuity and/or disaster recovery plans for your networks, information systems and their dependencies. You have not fully assessed the practical implementation of your disaster recovery plans.	You know all networks, information systems and underlying technologies that are necessary to restore the provision of essential network services and understand their interdependence. You know the order in which systems need to be recovered to efficiently and effectively restore the provision of essential network services.	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. You use your security awareness and threat intelligence sources, to make immediate and potentially temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.

B5.b Design for Resilience

You design the network and information systems providing your essential network services 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 of the following statements are true	All the following statements are true
Operational networks and systems are not appropriately segregated. Internet services, such as browsing and email, are accessible from essential operational systems supporting the provision of essential network services. You do not understand or lack plans to mitigate all resource limitations that could adversely affect your provision of essential network services.	Operational systems that support the provision of essential network servces 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. Internet access is not available from operational systems. Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.	Operational systems that support the provision of essential network services 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. Internet services are not accessible from operational systems. You have identified and mitigated all resource limitations, e.g. bandwidth limitations and single network paths. You have identified and mitigated any geographical constraints or weaknesses (e.g. systems that your provision of essential network services depend upon are replicated in another location, important network connectivity has alternative physical paths and service providers). You review and update assessments of dependencies, resource and geographical

Not achieved	Partially achieved	Achieved
		limitations and mitigation's when necessary.

B5.c Backups

You hold accessible and secured current backups of data and information needed to recover provision of your essential network services**.**

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Backup coverage is incomplete in coverage and would be inadequate to restore operation of your provision of essential network services. Backups are not frequent enough for the provision of your essential network services to be restored within a suitable time-frame.	You have appropriately secured backups (including data, configuration information, software, equipment, processes and key roles or knowledge). These backups will be accessible to recover from an extreme event. You routinely test backups to ensure that the backup process functions correctly and the backups are usable.	Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event. Key roles are duplicated, and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the provision of essential network services. Backups of all important data and information needed to recover the provision of essential network services are made, tested, documented and routinely reviewed.

Principle B6 Staff Awareness and Training

Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the provision of essential network services.

B6.a Cyber Security Culture

You develop and pursue a positive cyber security culture.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
People in your organisation don't understand what they contribute to the cyber security of the provision of essential network services. People in your organisation don't know how to raise a concern about cyber security. People believe that reporting issues may get them into trouble. Your organisation's approach to cyber security is perceived by staff as hindering the business of the organisation.	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. All people in your organisation understand the contribution they make to the cyber security of the provision of essential network services. 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.	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. People in your organisation raising potential cyber security incidents and issues are treated positively. 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. Your management is seen to be committed to and actively involved in cyber security. Your organisation communicates openly about

Not achieved	Partially achieved	Achieved
		cyber security, with any concern being taken seriously. People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.

B6.b Cyber Security Training

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

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
There are teams who operate and support your essential network services that lack any cyber security training. Cyber security training is restricted to specific roles in your organisation. Cyber security training records for your organisation are lacking or incomplete.	You have defined appropriate cyber security training and awareness activities for all roles in your organisation, from executives to the most junior roles. You use a range of teaching and communication techniques for cyber security training and awareness to reach the widest audience effectively. Cyber security information is easily available.	All people in your organisation, from the most senior to the most junior, follow appropriate cyber security training paths. Each individual's cyber security training is tracked and refreshed at suitable intervals. You routinely evaluate your cyber security training and awareness activities to ensure they reach the widest audience and are effective. You make cyber security information and good practice

Not achieved	Partially achieved	Achieved
		guidance easily accessible, widely available and you know it is referenced and used within your organisation.

Objective C – Detecting cyber security events[5]

Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, the provision of essential network services.

Principle C1 Security Monitoring

The organisation monitors the security status of the networks and systems supporting the provision of essential network services in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

C1.a Monitoring Coverage

The data sources that you include in your monitoring allow for timely identification of security events which might affect the provision of your essential network services.

Not achieved	**Partially achieved**	**Achieved**
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Data relating to the security and provision of your essential network services is not collected. You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential network services, such as known malicious command and control signatures (e.g. because applying the indicator is difficult or your logging data is not sufficiently detailed). You are not able to audit the activities of users in	Data relating to the security and provision of some areas of your essential network services is collected. You easily detect the presence or absence of IoCs on your essential network services, such as known malicious command and control signatures. Some user monitoring is done, but not covering a fully agreed list of suspicious or	Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents that could affect the provision of your essential network services (e.g. presence of malware, malicious emails, user policy violations). Your monitoring data provides enough detail to reliably detect security incidents that could affect the provision of your essential network services. You easily detect the presence or absence of IoCs on your essential network services, such as

[5] https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-c-detecting-cyber-security-events

Not achieved	Partially achieved	Achieved
relation to your provision of essential network services. You do not capture any traffic crossing your network boundary including as a minimum IP connections.	undesirable behaviour. You monitor traffic crossing your network boundary (including IP address connections as a minimum).	known malicious command and control signatures. Extensive monitoring of user activity in relation to the provision of essential network services enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour. You have extensive monitoring coverage that includes host-based monitoring and network gateways. All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.

C1.b Securing Logs

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

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
It is possible for logging data to be easily edited or deleted by unauthorised users or malicious attackers. There is no controlled list of who can view and query logging information. There is no	Only authorised staff can view logging data for investigations. Privileged users can view logging information. There is some monitoring of access to logging data (e.g. copying,	The integrity of logging data is protected, or any modification is detected and attributed. The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparable to those it is trying to identify. This

Not achieved	Partially achieved	Achieved
monitoring of the access to logging data. There is no policy for accessing logging data. Logging is not synchronised, using an accurate common time source.	deleting or modification, or even viewing).	includes protecting the function itself, and the data within it. Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered. Logging datasets are synchronised, using an accurate common time source, so separate datasets can be correlated in different ways. Access to logging data is limited to those with business need and no others. All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user. Legitimate reasons for accessing logging data are given in use policies.

C1.c Generating Logs

Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.

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

Not achieved	Partially achieved	Achieved
Alerts from third party security software is not investigated e.g. Anti-Virus (AV) providers.	Alerts from third party security software are investigated, and action taken.	Logging data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.
Logs are distributed across devices with no easy way to access them other than manual login or physical action.	Some logging datasets can be easily queried with search tools to aid investigations.	A wide range of signatures and indicators of compromise are used for investigations of suspicious activity and alerts.
The resolution of alerts to a network asset or system is not performed.	The resolution of alerts to a network asset or system is performed regularly.	Alerts can be easily resolved to network assets using knowledge of networks and systems.
Security alerts relating to essential functions are not prioritised.	Security alerts relating to some essential network services are prioritised.	Security alerts relating to all essential network services are prioritised and this information is used to support incident management.
Logs are reviewed infrequently.	Logs are reviewed at regular intervals.	Logs are reviewed almost continuously, in real time. Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.

C1.d Identifying Security Incidents

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

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Your organisation has no sources of threat intelligence.	Your organisation uses some threat intelligence services, but you don't choose providers specifically because of your	You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your

Not achieved	Partially achieved	Achieved
You do not apply updates in a timely way, after receiving them (e.g. AV signature updates, other threat signatures or Indicators of Compromise (IoCs)).	business needs, or specific threats in your sector (e.g. sector-based infoshare, ICS software vendors, anti-virus providers, specialist threat intel firms).	business needs and sector (e.g. vendor reporting and patching, strong anti-virus providers, sector and community-based infoshare).
You do not receive signature updates for all protective technologies such as AV and IDS or other software in use.	You receive updates for all your signature based protective technologies (e.g. AV, IDS).	You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.
You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	You apply some updates, signatures and IoCs in a timely way.	You receive signature updates for all your protective technologies (e.g. AV, IDS).
	You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems).	You track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, government agencies).

C1.e Monitoring Tools and Skills

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

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
There are no staff who perform a monitoring function.	Monitoring staff have some investigative	You have monitoring staff, who are responsible for

Not achieved	Partially achieved	Achieved
Monitoring staff do not have the correct specialist skills. Monitoring staff are not capable of reporting against governance requirements. Monitoring staff lack the skills to successfully perform any part of the defined workflow. Monitoring tools are only able to make use of a fraction of logging data being collected. Monitoring tools cannot be configured to make use of new logging streams, as they come online. Monitoring staff have a lack of awareness of the essential network services the organisation provides, what assets relate to those servicess and hence the importance of the logging data and security events.	skills and a basic understanding of the data they need to work with. Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers). Monitoring staff are capable of following most of the required workflows. Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types. Your monitoring tools work with most logging data, with some configuration. Monitoring staff are aware of some essential network services and can manage alerts relating to them.	the analysis, investigation and reporting of monitoring alerts covering both security and performance. Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process. Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external. Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data. Your monitoring tools make use of all logging data collected to pinpoint activity within an incident. Monitoring staff and tools drive and shape new log data collection and can make wide use of it. Monitoring staff are aware of the provision of essential network services and related assets and can identify and prioritise alerts or

Not achieved	Partially achieved	Achieved
		investigations that relate to them.

Principle C2 Proactive Security Event Discovery

The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the provision of essential network services even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployable).

C2.a System Abnormalities for Attack Detection

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

Not achieved	Achieved
At least one of the following statements is true	All the following statements are true
Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity.	Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity (e.g. you fully understand which systems should and should not communicate and when).
You have no established understanding of what abnormalities to look for that might signify malicious activities.	System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.
	The system abnormalities you search for consider the nature of attacks likely to impact on the networks and information systems supporting the provision of essential network services.
	The system abnormality descriptions you use are updated to reflect changes in your networks and information systems and current threat intelligence.

C2.b Proactive Attack Discovery

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

Not achieved	Achieved
At least one of the following statements is true	All the following statements are true
You do not routinely search for system abnormalities indicative of malicious activity.	You routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting the provision of your essential network services, generating alerts based on the results of such searches. You have justified confidence in the effectiveness of your searches for system abnormalities indicative of malicious activity.

Objective D – Minimising the impact of cyber security incidents[6]

Capabilities exist to minimise the adverse impact of a cyber security incident on the provision of essential network services, including the restoration of those services where necessary.

Principle D1 Response and Recovery Planning

There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential network services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

D1.a Response Plan

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

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Your incident response plan is not documented. Your incident response plan does not include your organisation's identified essential function. Your incident response plan is not well understood by relevant staff.	Your response plan covers your provision of essential network services. Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks only. Your response plan is understood by all staff who are involved with your organisation's response function.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your provision of essential network services. 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. Your incident response plan is documented and integrated with

[6] https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-d-minimising-the-impact-of-cyber-security-incidentshttps://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-d-minimising-the-impact-of-cyber-security-incidents

Not achieved	Partially achieved	Achieved
	Your response plan is documented and shared with all relevant stakeholders.	wider organisational business and supply chain response plans. Your incident response plan is communicated and understood by the business areas involved with the provision of your essential network services.

D1.b Response and Recovery Capability

You have the capability to enact your incident response plan, including effective limitation of impact on the provision of your essential network services. 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
Inadequate arrangements have been made to make the right resources available to implement your response plan. Your response team members are not equipped to make good response decisions and put them into effect. Inadequate back-up mechanisms exist to allow the continued provision of your essential network services during an incident.	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. You understand the types of information that will likely be needed to inform response decisions and arrangements are in place to make this information available. 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. Back-up mechanisms are available that can be readily activated to allow continued provision of your essential network srvices (although possibly at a reduced level) if primary networks and information systems fail or are unavailable. Arrangements exist to augment your organisation’s

Not achieved	Achieved
	incident response capabilities with external support if necessary (e.g. specialist cyber incident responders).

D1.c Testing and 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
Exercises test only a discrete part of the process (e.g. that backups are working), but do not consider all areas. Incident response exercises are not routinely carried out or are carried out in an ad-hoc way. Outputs from exercises are not fed into the organisation's lessons learned process. Exercises do not test all parts of the response cycle.	Exercise scenarios are based on incidents experienced by your and other organisations or are composed using experience or threat intelligence. Exercise scenarios are documented, regularly reviewed, and validated. Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned. Exercises test all parts of your response cycle relating to your provision of essential network services (e.g. restoration of normal function levels).

Principle D2 Lessons Learned

When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.

D2.a Incident Root Cause Analysis

When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.

Not achieved	Achieved
At least one of the following statements is true	All the following statements are true
You are not usually able to resolve incidents to a root cause. You do not have a formal process for investigating causes.	Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident. Your root cause analysis is comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software. All relevant incident data is made available to the analysis team to perform root cause analysis.

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
Following incidents, lessons learned are not captured or are limited in scope. Improvements arising from lessons learned following an incident are not implemented or not given sufficient organisational priority.	You have a documented incident review process/policy which ensures that lessons learned from each incident are identified, captured, and acted upon. Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems. You use lessons learned to improve security measures, including updating and retesting response plans when necessary. Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.

Not achieved	Achieved
	Analysis is fed to senior management and incorporated into risk management and continuous improvement.

4. References

Guidance

- ENISA Technical Guideline on Security Measures

https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures

- NCSC/CPNI Guidance

https://www.ncsc.gov.uk/

- Ofcom Guidance on Security Requirements

https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf

- NICC/EC-RRG ND 1643 – Industry/vendor best practice recommendations on Network Interconnect

http://www.niccstandards.org.uk/publications/index.cfm

Standards

- ISO/IEC 27001:2013 – Information Security

https://www.iso.org/isoiec-27001-information-security.html

- ISO/IEC 22301 – Business Continuity Management

https://www.iso.org/standard/75106.html

Legislation

- The EU Security of Networks & Information Systems (NIS) Directive, https://digital-strategy.ec.europa.eu/en/policies/nis-directive which aims to raise levels of cyber security and resilience of key systems across the EU, which was implemented into UK law in May 2018 via the NIS Regulations, https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

- The UK Telecommunications (Security) Bill, https://bills.parliament.uk/bills/2806 amends the Communications Act 2003 by placing strengthened telecoms security duties on public telecoms providers, providing new powers for the government to set out specific security requirements and issue codes of practice, and giving Ofcom new tools and responsibilities to ensure industry compliance, and includes Draft Electronic Communications (Security Measures) Regulations https://www.gov.uk/government/publications/draft-electronic-communications-security-measures-regulations to be taken by public telecoms providers.

  The Bill is expected to complete its passage through the UK Parliament in October

2021, to be followed by consultations on the Draft Regulations, and Codes of Practice to provide guidance on how, and to what timescale, certain telecoms providers should comply with their legal obligations.