



Cyber Assessment Framework

Introduction to Cyber Assessment Framework

One of the key objectives of the NIS Directive is to ensure that Operators of Essential Services (OES) take appropriate and proportionate technical and organisational measures to manage the risks to the security of network and information systems which support the delivery of essential services. As outlined below, OES will be required to meet a set of fourteen cyber security principles written in terms of *outcomes* i.e. specification of what needs to be achieved rather than exactly what needs to be done.

The requirements of the Directive were transposed into the Civil Contingencies Act 2007 and became effective on 10th May 2018. The Act designated the GRA as the Competent Authority and responsible for regulating, supervising and enforcing compliance with the conditions set on OES. The CAF was developed to provide guidance to OES and to provide the GRA with the capability to assess the extent to which OES are achieving the outcomes specified by the cyber security principles. The CAF is based on structured sets of Indicators of Good Practice (IGPs) and is described in more detail below.

While the current CAF is a document intended to be generic across all sectors, the GRA will engage with the different OES and will amend this document as and when required to encompass sector specific best practices.

Principles	Objectives
1. Governance	Managing Security Risk
2. Risk Management	
3. Asset Management	
4. Supply Chain	
5. Service Protection Policies and Processes	Defending systems against cyber attack
6. Identity and Access Control	
7. Data Security	
8. System Security	
9. Resilient Networks & Systems	
10. Staff Awareness & Training	Detecting cyber security events
11. Security Monitoring	
12. Proactive Security Event Discovery	Minimising the impact of cyber security incidents
13. Response and Recovery Planning	
14. Improvements	

CAF Requirements

The CAF has been developed to meet the following set of requirements:

1. maintain the outcome-focused approach of the principles and discourage assessments being carried out as tick-box exercises
2. be compatible with the use by OES of appropriate existing cyber security guidance and standards
3. enable the identification of effective cyber security improvement activities
4. be extensible to accommodate sector-specific elements as may be required
5. enable the setting of meaningful target security levels for OES to achieve
6. be as straightforward and cost-effective to apply as possible

CAF - Outline Approach

Each top-level NIS principle defines a fairly wide-ranging cyber security outcome. The precise approach organisations adopt to achieve each principle is not specified as this will vary according to organisational circumstances. However, each NIS principle can be broken down into a collection of lower-level contributing cyber security outcomes, all of which will normally need to be achieved to fully satisfy the NIS principle.

An assessment of the extent to which an organisation is meeting a cyber security principle is accomplished by assessing all the contributing outcomes for that principle. In order to assess the level of contributing outcomes:

1. each contributing outcome is associated with a set of IGPs and,
2. using the relevant IGPs, the circumstances under which the contributing outcome is judged 'achieved', 'not achieved' or (in some cases) 'partially achieved' are described.

For each contributing outcome the relevant IGPs have conveniently been arranged into table format. The resulting tables, referred to as *IGP tables*, constitute the basic building blocks of the CAF. In this way, each principle is associated with several IGP tables, one table per contributing outcome.

Using CAF IGP Tables

Assessment of contributing outcomes is primarily a matter of expert judgement and the IGP tables do not remove the requirement for the informed use of cyber security expertise and sector knowledge. Indicators in the IGP tables will usually provide good starting points for assessments but should be used flexibly. Conclusions about an organisation's cyber security should only be drawn after considering additional relevant factors and special circumstances.

The 'achieved' (GREEN) column of an IGP table defines the typical characteristics of an organisation **fully achieving** that outcome. It is intended that all the indicators would normally be present to support an assessment of 'achieved'.

The 'not achieved' (RED) column of an IGP table defines the typical characteristics of an organisation **not achieving** that outcome. It is intended that the presence of any one indicator would normally be sufficient to justify an assessment of 'not achieved'.

When present, the ‘partially achieved’ (AMBER) column of an IGP table defines the typical characteristics of an organisation **partially achieving** that outcome. It is also important that the partial achievement is delivering specific worthwhile cyber security benefits. An assessment of ‘partially achieved’ should represent more than giving credit for doing something vaguely relevant.

The following table summarises the key points relating to the purpose and nature of the indicators included in the CAF IGP tables

	Indicators in CAF IGP are...	Indicators in CAF IGP tables are not...
Purpose	...intended to help inform expert judgement.	...a checklist to be used in an inflexible assessment process.
Scope	...important examples of what an assessor will normally need to consider, which may need to be supplemented in some cases.	... an exhaustive list covering everything an assessor needs to consider.
Applicability	...designed to be widely applicable across different organisations, but applicability needs to be established.	...guaranteed to apply verbatim to all organisations.

Interpreting CAF Output

The result of applying the CAF is 39 individual assessments, each one derived from making a judgement on the extent to which a set of IGPs reflects the circumstances of the organisation being assessed. The CAF has been designed in such a way that a result in which all 39 contributing outcomes were assessed as ‘achieved’ would indicate a level of cyber security some way beyond the bare minimum ‘basic cyber hygiene’ level.

It is the responsibility of the GRA in collaboration with each sector to define what represents appropriate and proportionate cyber security for the purposes of the Act.

The GRA will carry out a consultation process to identify the contributing outcomes considered most important for an OES to achieve in order to manage security risks to a sector’s essential services. Those prioritised contributing outcomes would correspond to an initial view of appropriate and proportionate cyber security in their sector.

In practice a CAF profile would consist of a mixture of some contributing outcomes to be met at ‘achieved’, some at ‘partially achieved’ and perhaps some (representing cyber security capabilities not appropriate at the level of the profile) identified as ‘not applicable’.

CAF - Objective A - Managing Security Risk

A1 Governance

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

Principle

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 is true	All the following are true
<p>The security of network and information systems related to the delivery of essential services is not discussed or reported on regularly at board-level.</p> <p>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.</p> <p>The security of networks and information systems supporting your essential services is not driven effectively by the direction set at board level.</p> <p>Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.</p>	<p>Your organisation's approach and policy relating to the security of networks and information systems supporting the delivery of essential services are set and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.</p> <p>Regular board discussions on the security of network and information systems supporting the delivery of your essential service take place, based on timely and accurate information and informed by expert guidance.</p> <p>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.</p> <p>Direction set at board level is translated into effective organisational practices that direct and control the security of the networks and information systems supporting your essential service.</p>

A1.b Roles and responsibilities

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

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

A1.c Decision-making

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

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

A2 Risk Management

Principle

The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential 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 related to the delivery of essential services and communicating associated activities.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All the following are true	All the following are true
<p>Risk assessments are not based on a clearly defined set of threat assumptions.</p> <p>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.</p> <p>Risk assessments for critical systems are a "one-off" activity (or not done at all).</p> <p>The security element of project or programme milestones are solely dependent on completing the risk management process.</p> <p>One single approach to assessing risks is applied to every risk management problem within the organisation.</p> <p>Systems are assessed in isolation, without consideration of dependencies and interactions with other systems (including interactions between IT and OT environments).</p> <p>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 service.</p>	<p>Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed.</p> <p>Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential service.</p> <p>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.</p> <p>Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.</p> <p>You conduct risk assessments when significant events potentially affect the essential service, such as replacing a system or a change in the cyber security threat.</p> <p>You perform threat analysis and understand how generic threats apply to your organisation.</p>	<p>Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed.</p> <p>Your approach to risk is focused on the possibility of disruption to your essential service, leading to a detailed understanding how such disruption might arise as a consequence of possible attacker actions and the security properties of your networks and information systems.</p> <p>Your risk assessments are based on a clearly articulated set of threat assumptions, informed by an up-to-date understanding of security threats to your essential service.</p> <p>Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential service.</p> <p>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</p> <p>Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.</p>

<p>Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.</p>		<p>You conduct risk assessments when significant events potentially affect the essential service, such as replacing a system or a change in the cyber security threat</p> <p>Your risk assessments are dynamic, and are updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information.</p> <p>The effectiveness of your risk management process is reviewed periodically and improvements made as required.</p>
---	--	--

A2.b Assurance

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

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

A3 Asset Management

Principle

Everything required to deliver, maintain or support networks and information systems for essential 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 is true	All the following are true
<p>Inventories of assets relevant to the essential service are incomplete, non-existent, or inadequately detailed.</p> <p>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).</p> <p>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.</p> <p>Knowledge critical to the management, operation, or recovery of essential services is held by one or two key individuals with no succession plan.</p> <p>Asset inventories are neglected and out of date.</p>	<p>All assets relevant to the secure operation of essential services are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.</p> <p>Dependencies on supporting infrastructure (e.g. power, cooling etc) are recognised and recorded.</p> <p>You have prioritised your assets according to their importance to the delivery of the essential service.</p> <p>You have assigned responsibility for managing the physical assets.</p> <p>Assets relevant to essential services are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.</p>

A4 Supply Chain

Principle

The organisation understands and manages security risks to networks and information systems supporting the delivery of essential 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. Regardless of your outsourcing model the OES remains responsible for the security of the service and therefore all the requirements that come from the NIS Directive.

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
<p>You do not know what data belonging to you is held by suppliers, or how it is managed.</p> <p>Elements of the supply chain for essential services are subcontracted and you have little or no visibility of the sub-contractors.</p> <p>Relevant contracts do not have security requirements.</p> <p>Suppliers have access to systems that provide your essential service that is unrestricted, not monitored or bypasses your own security controls.</p>	<p>You understand the general risks suppliers may pose to your essential services.</p> <p>You know the extent of your supply chain for essential services, including sub-contractors.</p> <p>You engage with suppliers about security, and you set and communicate security requirements in contracts.</p> <p>You are aware of all third-party connections and have assurance that they meet your organisation's security requirements.</p> <p>Your approach to security incident management considers incidents that might arise in your supply chain.</p> <p>You have confidence that information shared with suppliers that is essential to the operation of your service is appropriately protected from well known attacks and known vulnerabilities.</p>	<p>You have a deeper understanding of your supply chain, including sub-contractors and the wider risks it faces. You take into account factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your risk assessment and procurement processes.</p> <p>Your approach to supply chain risk management considers the risks to your essential services arising from supply chain subversion by capable and well-resourced attackers.</p> <p>You have confidence that information shared with suppliers that might be essential to the service is well protected.</p> <p>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.</p> <p>All network connectivity and data sharing with third parties is managed effectively and proportionately.</p> <p>Where appropriate, your incident management process and that of your suppliers provide mutual support in the resolution of incidents.</p>

CAF - Objective B - Defending systems against cyber attack

B1 Service Protection Policies and Processes

Proportionate security measures in place to protect essential services and systems from cyber-attack.

Principle

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

B1.a Policy and process development

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

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>Your service protection policies and processes are absent or incomplete.</p> <p>Service protection policies and processes are not applied universally or consistently.</p> <p>People often or routinely circumvent service protection policies and processes to achieve business objectives.</p> <p>Your organisation's security governance and risk management approach has no bearing on your service protection policies and processes.</p> <p>System security is totally reliant on users' careful and consistent application of manual security processes.</p> <p>Service protection policies and processes have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period.</p> <p>Service protection policies and processes are not readily available to staff, too detailed to remember, or too hard to understand.</p>	<p>Your service protection policies and processes document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is often treated as a separate issue.</p> <p>You review and update service protection policies and processes in response to major cyber security incidents.</p>	<p>You fully document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is embedded throughout these policies and processes and key performance indicators are reported to your executive management.</p> <p>Your organisation's service protection policies and processes are developed to be practical, usable and appropriate for your essential service and your technologies.</p> <p>Essential service protection policies and processes that rely on user behaviour are practical, appropriate and achievable.</p> <p>You review and update protection policies and processes at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident.</p> <p>Any changes to essential service or the threat it faces triggers a review of service protection policies.</p> <p>Your systems are designed so that they remain secure even when user</p>

		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 is true	All of the following are true	All of the following are true
<p>Service protection policies and processes are ignored or only partially followed.</p> <p>The reliance on your service protection policies and processes is not well understood.</p> <p>Staff are unaware of their responsibilities under your service protection policies and processes.</p> <p>You do not attempt to detect breaches of service protection policies and processes.</p> <p>Service protection policies and processes lack integration with other organisational policies and processes.</p> <p>Your service protection policies and processes are not well communicated across your organisation.</p>	<p>Most of your service protection policies and processes are followed and their application is monitored.</p> <p>Your service protection policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.</p> <p>All staff are aware of their responsibilities under your service protection policies and processes.</p> <p>All breaches of service protection policies and processes with the potential to disrupt the essential service are fully investigated.</p> <p>Other breaches are tracked, assessed for trends and action is taken to understand and address.</p>	<p>All your service protection policies and processes are followed, their correct application and security effectiveness is evaluated.</p> <p>Your service protection policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.</p> <p>Your service protection policies and processes are effectively and appropriately communicated across all levels of the organisation resulting in good staff awareness of their responsibilities.</p> <p>Appropriate action is taken to address all breaches of service protection policies and processes with potential to disrupt the essential service including aggregated breaches.</p>

B2 Identity and Access Control

Principle

The organisation understands, documents and manages access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services 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 supporting your essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>Authorised users with access to networks or information systems on which your essential service depends cannot be individually identified.</p> <p>Unauthorised individuals or devices can access your networks or information systems on which your essential service depends.</p> <p>User access is not limited to the minimum necessary.</p>	<p>All authorised users with access to networks or information systems on which your essential service depends are individually identified and authenticated.</p> <p>User access to essential service networks and information systems is limited to the minimum necessary.</p> <p>You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for privileged access to sensitive systems such as operational technology.</p> <p>You individually authenticate and authorise all remote user access to all your networks and information systems that support your essential service.</p> <p>The list of users with access to essential service networks and systems is reviewed on a regular basis at least annually.</p>	<p>Only individually authenticated and authorised users can connect to or access your networks or information systems on which your essential service depends.</p> <p>User access to all your networks and information systems supporting the essential service is limited to the minimum necessary.</p> <p>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 service.</p> <p>You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, when you individually authenticate and authorise all remote access to all your networks and information systems that support your essential service.</p> <p>The list of individuals with access to all your networks and systems supporting the essential service is reviewed on a regular basis, at least every six months.</p> <p>The list of users with access to networks and systems supporting and delivering the essential service is reviewed on a regular basis, at least every six months.</p>

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 service.

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

B2.c Privileged user management

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

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>The identities of the individuals with privileged access to your essential service systems (infrastructure, platforms, software, configuration, etc) are not known or not managed.</p> <p>Privileged user access to your essential service systems is via weak authentication mechanisms. (e.g. only simple passwords.)</p> <p>The list of privileged users has not been reviewed recently. (e.g. within the last 12 months.)</p> <p>Privileged user access is granted on a system-wide basis rather than by role or function. Privilege user access to your essential services is via generic, shared or default name accounts.</p> <p>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.</p> <p>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.)</p>	<p>Privileged 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).</p> <p>The identities of the individuals with privileged access to your essential service systems (infrastructure, platforms, software, configuration, etc) are known and managed. This includes third parties.</p> <p>Activity by privileged users is routinely reviewed and validated. (e.g. at least annually.)</p> <p>Privileged users are only granted specific privileged permissions which are essential to their business role or function.</p>	<p>Privileged access to your essential service is carried out from dedicated separate accounts that are closely monitored and managed.</p> <p>The issuing of temporary, timebound 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.</p> <p>Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process.</p> <p>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.</p> <p>All Privileged user activity is routinely reviewed, validated and recorded for offline analysis and investigation.</p>

B2.d Identity and Access Management (IdAM)

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

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

B3 Data Security

Principle

Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause disruption to essential services. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the delivery of essential 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 delivery of the essential service, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to third parties storing or accessing data important to the delivery of essential services.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>You have incomplete knowledge of what data is used by and produced in the delivery of the essential service.</p> <p>You have not identified the important data on which your essential service relies.</p> <p>You cannot identify who has access to data important to the delivery of the essential service.</p> <p>You are not clearly articulated the impact of data compromise or inaccessibility.</p>	<p>You have identified and catalogued all the data important to the delivery of the essential service, or that would assist an attacker.</p> <p>You have identified and catalogued who has access to data important to the delivery of essential services.</p> <p>You periodically review location, transmission, quantity and quality of data important to the delivery of the essential service.</p> <p>You have identified all mobile devices and media that hold data important to the delivery of the essential service.</p> <p>You understand and document the impact on your essential service of all relevant scenarios, including unauthorised access, modification or deletion, or when authorised users are unable to appropriately access this data.</p> <p>You occasionally validate these impact statements.</p>	<p>You have identified and catalogued all the data important to the delivery of the essential service, or that would assist an attacker.</p> <p>You have identified and catalogued who has access to data important to the delivery of essential services.</p> <p>You maintain a current understanding of the location, quantity and quality of data important to the delivery of the essential service.</p> <p>You take steps to remove or minimise unnecessary copies or unneeded historic data.</p> <p>You have identified all mobile devices and media that may hold data important to the delivery of the essential service.</p> <p>You maintain a current understanding of the data links used to transmit data that is important to your essential service.</p> <p>You understand the context, limitations and dependencies of your important data.</p> <p>You understand and document the impact on your essential service of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data.</p> <p>You validate these impact statements regularly, e.g. annually.</p>

B3.b Data in transit

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

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>You do not know what all your data links are, or which carry data important to the delivery of the essential service.</p> <p>Data important to the delivery of the essential service travels without technical protection over untrusted or openly accessible carriers.</p> <p>Critical data paths that could fail, be jammed, be overloaded, etc. have no alternative path.</p>	<p>You have identified and suitably protected (effectively and proportionately) all the data links that carry data important to the delivery of the essential service.</p> <p>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.</p>	<p>You have identified and suitably protected (effectively and proportionately) all the data links that carry data important to the delivery of the essential service.</p> <p>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.</p> <p>Suitable alternative transmission paths are available where there is a significant risk of impact on the delivery of the essential service due to resource limitation (e.g. transmission equipment or service failure, or important data being blocked or jammed).</p>

B3.c Stored data

You have protected stored data important to the delivery of the essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All the following are true	All of the following are true
<p>You have no, or limited, knowledge of where data important to the delivery of the essential service is stored.</p> <p>You have not protected vulnerable stored data important to the delivery of the essential service in a suitable way.</p> <p>Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.</p>	<p>All copies of data important to the delivery of your essential service are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy.</p> <p>You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.</p> <p>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.</p> <p>You have suitable, secured backups of data to allow the essential service 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.</p>	<p>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.</p> <p>You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.</p> <p>If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied.</p> <p>You have suitable, secured backups of data to allow the essential service 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.</p> <p>Necessary historic or archive data is suitably secured in storage.</p>

B3.d Mobile data

You have protected data important to the delivery of the essential service on mobile devices.

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

B3.e Media / equipment sanitisation

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

Not Achieved	Achieved
At least one of the following is true	All of the following are true
Some or all devices, equipment or removable media that hold data important to the delivery of the essential service are disposed of without sanitisation of that data.	<p>You catalogue and track all devices that contain data important to the delivery of the essential service (whether a specific storage device or one with integral storage).</p> <p>All data important to the delivery of the essential service is sanitised from all devices, equipment or removable media before disposal.</p>

B4 System Security

Principle

Network and information systems and technology critical for the delivery of essential services are protected from cyber-attack. An organisational understanding of risk to essential 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 supports the delivery of essential services. You minimise their attack surface and ensure that the delivery of the essential service should not be impacted by the exploitation of any single vulnerability.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>Systems essential to the operation of the essential service are not appropriately segregated from other systems.</p> <p>Internet access is available from operational systems.</p> <p>Data flows between the essential service's operational systems and other systems are complex, making it hard to discriminate between legitimate and illegitimate/malicious traffic.</p> <p>Remote or third party accesses circumvent some network controls to gain more direct access to operational systems of the essential service.</p>	<p>You employ appropriate expertise to design network and information systems.</p> <p>You design strong boundary defences where your networks and information systems interface with other organisations or the world at large.</p> <p>You design simple data flows between your networks and information systems and any external interface to enable effective monitoring.</p> <p>You design to make network and information system recovery simple.</p> <p>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.</p>	<p>You employ appropriate expertise to design network and information systems.</p> <p>Your networks and information systems are segregated into appropriate security zones, e.g. operational systems for the essential service are segregated in a highly trusted, more secure zone.</p> <p>The networks and information systems supporting your essential service are designed to have simple data flows between components to support effective security monitoring.</p> <p>The networks and information systems supporting your essential service are designed to be easy to recover.</p> <p>Content-based attacks are mitigated for all inputs to operational systems that effect the essential service (e.g. via transformation and inspection).</p>

B4.b Secure configuration

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

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

B4.c Secure management

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

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>Essential service networks and systems are administered or maintained using non-dedicated devices.</p> <p>You do not have good or current technical documentation of your networks and information systems.</p>	<p>Your systems and devices supporting the delivery of the essential service are only administered or maintained by authorised privileged users from dedicated devices.</p> <p>Technical knowledge about networks and information systems, such as documentation and network diagrams, is regularly reviewed and updated.</p> <p>You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.</p>	<p>Your systems and devices supporting the delivery of the essential service 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.</p> <p>You regularly review and update technical knowledge about networks and information systems, such as documentation and network diagrams, and ensure they are securely stored.</p> <p>You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.</p>

B4.d. Vulnerability management

You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.

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

B5 Resilient Networks and Systems

Principle

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

B5.a Resilience preparation

You are prepared to restore your essential service following disruption.

Not Achieved	Partially Achieved	Achieved
Any of the following are true	All of the following are true	All of the following are true
<p>You have limited understanding of all the elements that are required to restore the essential service.</p> <p>You have not completed business continuity and/or disaster recovery plans for your essential service's networks, information systems and their dependencies.</p> <p>You have not fully assessed the practical implementation of these plans.</p>	<p>You know all networks, information systems and underlying technologies that are necessary to restore the essential service and understand their interdependencies.</p> <p>You know the order in which systems need to be recovered to efficiently and effectively restore the essential service.</p>	<p>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.</p> <p>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.</p>

B5.b Design for resilience

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

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>Operational networks and systems are not sufficiently segregated.</p> <p>Internet services, such as browsing and email, are accessible from essential service operational systems.</p> <p>You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential service.</p>	<p>Operational systems for your essential service are logically separated from your business systems, e.g. they reside on the same network as the rest of the organisation, but within a Demilitarised Zone (DMZ). Internet access is not available from operational systems.</p> <p>Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.</p>	<p>Your essential service's operational systems 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.</p> <p>You have identified and mitigated all resource limitations, i.e. bandwidth limitations and single network paths.</p>

		<p>You have identified and mitigated any geographical constraints or weaknesses. (e.g. systems that your essential service depends upon are replicated in another location, important network connectivity has alternative physical paths and service providers.)</p> <p>You review and update assessments of dependencies, resource and geographical limitation and mitigations when necessary.</p>
--	--	--

B5.c Backups

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

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>Backup coverage is incomplete in coverage and would be inadequate to restore your essential service.</p> <p>Backups are not frequent enough for your essential service to be restored within a suitable timeframe.</p>	<p>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.</p> <p>You routinely test backups to ensure that the backup process functions correctly, and the backups are usable.</p>	<p>Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event.</p> <p>Key roles are duplicated, and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential service.</p> <p>Backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.</p>

B6 Staff Awareness and Training

Principle

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 delivery of essential 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 is true	All of the following are true	All of the following are true
<p>People in your organisation don't understand what they contribute to the cyber security of the essential service.</p> <p>People in your organisation don't know how to raise a concern about cyber security.</p> <p>People believe that reporting issues may get them into trouble.</p> <p>Your organisation's approach to cyber security is perceived by staff as getting in the way of them delivering the essential service.</p>	<p>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.</p> <p>All people in your organisation understand the contribution they make to the essential service's cyber security.</p> <p>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.</p>	<p>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.</p> <p>People in your organisation raising potential cyber security incidents and issues are treated positively.</p> <p>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.</p> <p>Your management is seen to be committed to and actively involved in cyber security.</p> <p>Your organisation communicates openly about cyber security, with any concern being taken seriously.</p> <p>People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.</p>

B6.b Cyber security training

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

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

CAF - Objective C - Detecting Cyber Security Events

C1 Security Monitoring

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

Principle

The organisation monitors the security status of the networks and systems supporting the delivery of essential 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 delivery of your essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>Data relating to the security and operation of your essential services is not collected.</p> <p>You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential services, such as know malicious command and control signatures (e.g. because applying the indicator is difficult or your logging data is not sufficiently detailed).</p> <p>You are not able to audit the activities of users in relation to your essential service.</p> <p>You do not capture any traffic crossing your network boundary including as a minimum IP connections.</p>	<p>Data relating to the security and operation of some areas of your essential services is collected.</p> <p>You easily detect the presence or absence of IoCs on your essential services, such as know malicious command and control signatures.</p> <p>Some user monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour.</p> <p>You monitor traffic crossing your network boundary (including IP address connections as a minimum).</p>	<p>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 your essential service. (e.g. presence of malware, malicious emails, user policy violations).</p> <p>Your monitoring data provides enough detail to reliably detect security incidents that could affect your essential service.</p> <p>You easily detect the presence or absence of IoCs on your essential services, such as know malicious command and control signatures.</p> <p>Extensive monitoring of user activity in relation to essential services enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.</p> <p>You have extensive monitoring coverage that includes host-based monitoring and network gateways.</p> <p>All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.</p>

C1.b Securing logs

Logging data should be held securely and read access to it should be granted 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 is true	All of the following are true	All of the following are true
<p>It is possible for logging data to be edited or deleted.</p> <p>There is no controlled list of who can view and query logging information.</p> <p>There is no monitoring of the access to logging data.</p> <p>There is no policy for accessing logging data.</p> <p>Logging is not synchronised, using an accurate time source.</p>	<p>Only authorised staff can view logging data for investigations.</p> <p>Privileged users can view logging information.</p> <p>Some monitoring of access to logging data. (e.g. copying, deleting or modification, or even viewing.).</p>	<p>The integrity of logging data is protected, or any modification is detected and attributed.</p> <p>The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparative to those it is trying to identify. This includes protecting the service itself, and the data within it.</p> <p>Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered.</p> <p>Logging datasets are synchronised, using an accurate common time source, so separate datasets can be correlated in different ways.</p> <p>Access to logging data is limited to those with business need and no others.</p> <p>All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user.</p> <p>Legitimate reasons for accessing logging data are given in use policies.</p>

C1.c Generating alerts

Evidence of potential security incidents contained in your monitoring data is reliably identified and alerted upon.

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

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 is true	All of the following are true	All of the following are true
<p>Your organisation has no sources of threat intelligence.</p> <p>You do not apply updates in a timely way, after receiving them (e.g. AV signature updates, other threat signatures or IoCs).</p> <p>You do not receive signature updates for all protective technologies such as AV and IDS or other software in use.</p> <p>You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.</p>	<p>Your organisation uses some threat intelligence services, but you don't choose providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based infoshare, Integrated Control Systems (ICS) software vendors, antivirus providers, specialist threat intel firms).</p> <p>You receive signature updates for all your protective technologies (e.g. AV, IDS).</p> <p>You apply some updates, signatures and IoCs in a timely way.</p> <p>You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems).</p>	<p>You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong antivirus providers, sector and community-based infoshare).</p> <p>You are able to apply new signatures and IoCs within a reasonable (risk-based) time of receiving them.</p> <p>You receive signature updates for all your protective technologies (e.g. AV, IDS).</p> <p>You can 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).</p>

C1.e Monitoring tools and skills

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

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>There are no staff who perform a monitoring function.</p> <p>Monitoring staff do not have the correct specialist skills.</p> <p>Monitoring staff are not capable of reporting against governance requirements</p> <p>Monitoring staff lack the skills to successfully perform any part of the defined workflow.</p> <p>Monitoring tools are only able to make use of a fraction of logging data being collected.</p> <p>Monitoring tools cannot be configured to make use of new logging streams, as they come online.</p> <p>Monitoring staff have a lack of awareness of the essential services the organisation provides, what assets relate to those services and hence the importance of the logging data and security events.</p>	<p>Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.</p> <p>Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).</p> <p>Monitoring staff are capable of following most of the required workflows.</p> <p>Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types.</p> <p>Your monitoring tools can work with most logging data, with some configuration.</p> <p>Monitoring staff are aware of some essential services and can manage alerts relating to them.</p>	<p>You have monitoring staff, who are responsible for the analysis, investigation and reporting monitoring alerts covering both security and performance.</p> <p>Monitoring staff have defined roles and skills that covers all parts of the monitoring and investigation process.</p> <p>Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external.</p> <p>Monitoring staff are empowered to look beyond fixed processes to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.</p> <p>Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.</p> <p>Monitoring staff and tools drive and shape new log data collection and can make wide use of it.</p> <p>Monitoring staff are aware of essential services and related assets and can identify and prioritise alerts or investigations that relate to them.</p>

C2 Proactive Security Event Discovery

Principle

The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services, even when the activity evades standard signature based security prevent/detect solutions, or when it is not possible to use signature based detection, for some reason.

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 is true	All of the following are true
Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity. You have no established understanding of what abnormalities to look for that might signify malicious activities.	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.) 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 delivery of essential 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 is true	All of the following are true
You do not routinely search for system abnormalities indicative of malicious activity.	You routinely search for system abnormalities indicative of malicious activity with the potential to have an impact on networks and information systems supporting your essential service, and you generate 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.

CAF - Objective D - Minimising the impact of cyber security incidents

D1 Response and Recovery Planning

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

Principle

There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential 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 essential service and covers a range of incident scenarios.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
<p>Your incident response plan is not documented.</p> <p>Your incident response plan does not include your organisation's identified essential service.</p> <p>Your incident response plan is not well understood by relevant staff.</p>	<p>Your response plan covers your essential services.</p> <p>Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks only.</p> <p>Your response plan is understood by all staff who are involved with your organisation's response function</p> <p>Your response plan is documented and shared with all relevant stakeholders</p>	<p>Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential service.</p> <p>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.</p> <p>Your incident response plan is documented and integrated with wider organisational business and supply chain response plans.</p> <p>Your incident response plan is communicated and understood by the business areas involved with the supply or maintenance of your essential services.</p>

D1.b Response and recovery capability

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

Not Achieved	Achieved
At least one of the following is true	All of the following are true
<p>Inadequate arrangements have been made to make the right resources available to implement your response plan.</p> <p>Your response team members are not equipped to take good response decisions and put them into effect.</p> <p>Inadequate back-up mechanisms exist to allow the continued delivery of your essential service during an incident.</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Back-up mechanisms are available that can be readily activated to allow continued delivery of your essential service (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.</p> <p>Arrangements exist to augment your organisation's incident response capabilities with external support if necessary (e.g. specialist cyber incident responders).</p>

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

D2 Lessons Learned

Principle

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

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

Not Achieved	Achieved
At least one of the following is true	All of the following 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 is true	All of the following 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. Analysis is fed to senior management and incorporated into risk management and continuous improvement.