National Cyber
Security Centre
a part of GCHQ

Cyber Assessment Framework 4.0

The CAF is a collection of cyber security guidance for organisations that play a vital role in the day-to-day life of the UK, with a focus on essential functions.

Contents

Please Note: A list of all changes made between CAF V3.2 and V4.0, and all previous versions of the CAF are available on the NCSC website.

The CAF - A tool for assessing cyber resilience

The Cyber Assessment Framework (CAF) provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential function(s) are being managed by the organisation responsible. CAF-based assessments can be carried out either by the responsible organisation itself (self-assessment) or by an independent external entity, possibly a regulator / cyber oversight body or a suitably qualified organisation acting on behalf of a regulator, such as an NCSC assured commercial service provider.

The NCSC CAF cyber security and resilience objective and principles provide the foundations of the CAF. The 4 high-level objectives and the 14 principles are written in terms of outcomes, i.e. specification of what needs to be achieved rather than a checklist of what needs to be done. The CAF adds additional levels of detail to the top-level principles, including a collection of structured sets of Indicators of Good Practice (IGPs) as described in more detail below.

It should be noted that NCSC developed the CAF in its role as national technical authority for cyber security, with an expectation that it would be used, amongst other things, as a tool to support effective cyber regulation. NCSC itself has no regulatory responsibilities, and organisations subject to cyber regulation should consult with their regulators to learn whether they should use the CAF in the context of meeting regulatory requirements.

CAF Requirements

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

1. provide a suitable framework to assist in carrying out cyber resilience assessments.
2. maintain the outcome-focused approach of the NCSC cyber security and resilience principles and discourage assessments being carried out as tick-box exercises.
3. be compatible with the use of appropriate existing cyber security guidance and standards.
4. enable the identification of effective cyber security and resilience improvement activities.
5. exist in a common core version which is sector-agnostic.
6. be extensible to accommodate sector-specific elements as may be required.
7. enable the setting of meaningful target security levels for organisations to achieve, possibly reflecting a regulator view of appropriate and proportionate security.
8. be as straightforward and cost-effective to apply as possible.

CAF Principles and contributing outcomes

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

An assessment of the extent to which an organisation is meeting a particular principle is accomplished by assessing all the contributing outcomes for that principle. In order to inform assessments at the level of contributing outcomes:

1. each contributing outcome is associated with a set of indicators of good practice (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 tables of IGPs, one table per contributing outcome.

Using IGPs

Assessment of contributing outcomes is primarily a matter of expert judgement and the IGPs do not remove the requirement for the informed use of cyber security expertise and sector knowledge. IGPs will usually provide good starting points for assessments but should be used flexibly and in conjunction with the NCSC guidance associated with the top-level cyber security and resilience principles. Conclusions about an organisation's cyber security and resilience 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 exception would be when an IGP may not be applicable if there are compensating measures that would meet the requirements of the relevant objective.

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 and resilience 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 IGPs.

	IGPs are...	IGPs 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.

Setting target levels of cyber security and resilience

The result of applying the CAF is 41 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 41 contributing outcomes were assessed as 'achieved' would indicate a level of cyber security some way beyond the bare minimum 'basic cyber hygiene' level.

A cyber oversight body will need to set target levels of cyber resilience for organisations within their sector. One way of setting these target levels is in relation to the *ability to withstand specified categories of cyber attacks* (e.g. resilience to basic capability attacks, moderate capability attacks etc.) and the CAF has been designed to support this approach via the idea of CAF profiles.

The NCSC has worked with regulators and other organisations with a cyber resilience oversight role on an approach to interpreting CAF output based on identifying those contributing outcomes considered most important to achieve in order to manage security risks to that organisation's essential functions. Those prioritised contributing outcomes would correspond to an initial view of appropriate and proportionate cyber security for that organisation. The subset of contributing outcomes identified as the most important in this way would represent an example of a CAF profile – something that could be used as the basis for setting a target for organisations to achieve.

In practice a CAF profile consists 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'.

It is not the responsibility of the NCSC to mandate what represents appropriate and proportionate cyber security and resilience. Any target set for organisations to achieve in terms of CAF results is for the relevant cyber oversight body to define.

Making the CAF sector specific

The common core of the CAF (consisting of objectives, principles, contributing outcomes and indicators of good practice) is sector agnostic in the sense that it is designed to be generally applicable to all organisations responsible for essential functions across all key sectors. It is possible that there will be a need for some sector specific aspects of the CAF, which could include the following:

i) Sector-specific CAF Profiles

Some target profiles may well be sector specific. As mentioned in the section on setting target levels, it will be a decision for the relevant cyber oversight body to put an interpretation on CAF results, which may be from a regulatory perspective.

ii) Sector-specific Interpretations of Contributing Outcomes/IGPs

It may be necessary in some cases for a sector-specific interpretation of contributing outcomes and/or IGPs to better clarify meaning within the sector.

iii) Sector-specific Additional Contributing Outcomes/IGPs

There may be circumstances in which sector-specific cyber security requirements cannot be adequately covered by an interpretation of a generic contributing outcome or IGP. In these cases, an additional sector-specific contributing outcome or IGP may need to be defined.

The NCSC will continue to work with the full range of CAF stakeholders to determine if sector-specific aspects of the CAF are required, and to assist in introducing changes as necessary.

The Cyber Assessment Framework

CAF - Objective A - Managing security risk

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

Principle A1 Governance

The organisation has appropriate management policies, processes and procedures 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 operation of essential function(s) is not discussed or reported on regularly at board-level. Board-level discussions on the security of network and information systems are based on partial or out-of-date information, without the benefit of expert guidance. The security of network and information systems supporting your essential function(s) 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.	Your organisation's approach and policy relating to the security of network and information systems supporting the operation of your essential function(s) are owned and managed at board-level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation. Regular board-level discussions on the security of network and information systems supporting the operation of your essential function(s) take place, based on timely and accurate information and informed by expert guidance. There is a board-level individual who has overall accountability for the security of

	network and information systems and drives regular discussion at board-level. Direction set at board-level is translated into effective organisational practices that direct and control the security of network and information systems supporting your essential function(s). The board has the information and understanding needed in order to effectively discuss how the security and resilience of network and information systems contributes to the delivery of essential function(s) and what the potential impact from compromise of those systems would be. Security is recognised as an important enabler for the resilience of your essential function(s) and considered in all relevant discussions.

A1.b Roles and Responsibilities

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

Not Achieved	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. Staff are assigned security responsibilities but without adequate authority or resources to fulfil them. Staff are unsure what their responsibilities are for the security of the essential function(s).	Key roles and responsibilities for the security of network and information systems supporting your essential function(s) have been identified. These are reviewed regularly to ensure they remain fit for purpose. Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties. There is clarity on who in your organisation has overall accountability for the security of network and information systems supporting your essential function(s).

A1.c Decision-making

You have senior-level accountability for the security of network and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the operation of your essential function(s) 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. Risks are resolved informally (or ignored) at a local level when the use of a more formal risk reporting mechanism would be more appropriate. Decision-makers are unsure of what senior management's risk appetite is, or only understand it in vague terms such as "averse" or "cautious". Decision-makers are unable to justify their risk management decisions. Organisational structure causes risk decisions to be made in isolation. (e.g. engineering and IT do not talk to each other about risk). Risk priorities are too vague to make meaningful distinctions between them. (e.g. almost all risks are rated 'medium' or 'amber').	Senior management have visibility of key risk decisions made throughout the organisation. Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the essential function(s), as set by senior management. 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. Risk management decisions are regularly reviewed to ensure their continued relevance and validity.

Principle A2 Risk Management

The organisation takes appropriate steps to identify, assess and understand security risks to network and information systems supporting the operation of essential functions. 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 and resilience of network and information systems related to the operation of your essential function(s) and communicating associated activities.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
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 network and information systems supporting your essential function(s) 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.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed. Your risk assessments are informed by an understanding of known and well understood threats and vulnerabilities in network and information systems supporting your essential function(s). 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 organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed. Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible threat actor actions and the security properties of network and information systems supporting your essential function(s). Your risk assessments are based on a clearly understood set of threat assumptions, informed by

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). Security requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of network and information systems supporting your essential function(s). Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.	your risk management process are communicated to key security decision-makers and accountable individuals. You conduct risk assessments when significant events potentially affect the essential function(s), such as replacing a system, introducing new or emergent technologies or a change in the cyber security threat.	an up-to-date understanding of threats to network and information systems supporting your essential function(s), your sector and wider national infrastructure**.** Your risk assessments are informed by an understanding of the vulnerabilities in network and information systems supporting your essential function(s). The output from your risk management process is a clear set of traceable and prioritised security requirements that will address the risks in line with your organisational approach to security. Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals. Your risk assessments are dynamic and readily updated in the light of relevant changes which may include technical changes to network and information systems supporting your essential function(s), change of use, the introduction of new or

		emergent technologies or new threat information. The effectiveness of your risk management process is reviewed regularly, and improvements made as required. You anticipate technological developments that could be used to adversely impact network and information systems supporting your essential function(s).

A2.b Understanding Threat

You understand the capabilities, methods and techniques of threat actors and what network and information systems they may compromise to adversely impact your essential function(s).

This information is used to inform security and resilience risk management decisions, adjusting, enhancing or adding security measures to better defend against threats.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You are unable to perform threat analysis. You do not understand the threats to network and information systems supporting your essential function(s). You do not have a clearly defined set of threat assumptions. You do not use your understanding of threat to inform your risk management decisions.	You perform threat analysis and understand how common threats apply to network and information systems supporting your essential function(s). You understand common types of cyber attacks, including the methods and techniques, and how these might apply to network and information systems supporting your essential function(s). This understanding is kept up to date. You anticipate what threat actors might target in network and information systems to cause an adverse impact to your essential function(s). Your understanding of threat is informed by common incidents. You apply your understanding of threat to	You perform detailed threat analysis and understand how this applies to network and information systems supporting your essential function(s), in the context of your sector and wider national infrastructure. Your detailed understanding of threat includes the methods and techniques available to capable and well-resourced threat actors and how they could be used systematically against network and information systems supporting your essential function(s). You use appropriate techniques to develop an understanding of network and information systems supporting your essential function(s) from a threat actor's perspective. You anticipate probable attack methods and techniques,

	inform your risk management decision-making.	targets and objectives, and develop plausible scenarios. You understand the different steps a capable and well-resourced threat actor would need to take to reach the probable target(s). You identify and justify what measures can be used at each step to reduce the likelihood of the threat actor reaching the probable target(s) or achieving their objective(s). You maintain a detailed understanding of current threats (e.g. by threat intelligence and proactive research). You apply your detailed understanding of threat to inform your risk management decision-making. You have documented the steps required to undertake detailed threat analysis.

A2.c Assurance

You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to the operation of network and information systems supporting your essential function(s).

Not Achieved	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. Assurance is assumed because there have been no known problems to date.	You validate that the security measures in place to protect network and information systems supporting your essential function(s) 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 network and information systems supporting your essential function(s). 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 network and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).

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 network and information systems supporting your essential function(s) 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 and / or important / critical data, are stored for long periods of time with no clear business need or retention policy. Knowledge critical to the management, operation, or recovery of network and information systems supporting your essential function(s) is held by one or two key individuals with no succession plan. Asset inventories are neglected and out of date.	All assets relevant to the secure operation of network and information systems supporting your essential function(s) are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date. Dependencies on supporting infrastructure (e.g. power, cooling etc) are recognised and recorded. You have prioritised your assets according to their importance to the operation of network and information systems supporting your essential function(s). You have assigned responsibility for managing all assets, including physical assets, relevant to the operation of network and information systems supporting your essential function(s). Assets relevant to network and information systems supporting your essential function(s) are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.

Principle A4 Supply Chain

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

A4.a Supply Chain

You understand and effectively manage the risks associated with suppliers to the security of network and information systems supporting the operation of your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You do not know what data belonging to you is held by suppliers, or how it is managed. Elements of the supply chain for network and information systems supporting your essential function(s) are subcontracted and you have little or no visibility of the sub-contractors. You have no understanding of which contracts are relevant and / or relevant contracts do not specify appropriate security obligations. Suppliers have access to network and information systems that support your essential function(s) that is unrestricted, not monitored	You understand the general risks suppliers may pose to network and information systems supporting your essential function(s). You know the extent of your supply chain that supports network and information systems supporting your essential function(s), including sub-contractors. Suppliers to network and information systems that support your essential function(s) can demonstrate appropriate and proportionate levels of cyber security within the context of common threats. You understand which contracts are relevant and you include appropriate	You have a deep understanding of your supply chain, including sub-contractors, and the wider risks it faces. You consider factors such as your supplier's ownership, nationality, partnerships, competitors, other organisations with which they sub-contract and their approach to cyber security. These factors inform your risk assessment and are fully considered in your procurement lifecycle processes and purchasing decisions. Your approach to supply chain risk management considers the risks to network and information systems

or bypasses your own security controls.	security obligations, in relevant 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 confidence that information held by suppliers that is necessary for the operation of network and information systems supporting your essential function(s) is appropriately protected from common threats.	supporting your essential function(s) arising from supply chain subversion by capable and well-resourced threat actors. Critical suppliers to network and information systems supporting your essential functions(s) can demonstrate appropriate and proportionate levels of cyber security within the context of capable and well-resourced threat actors. You have confidence that information held by suppliers that is essential to the operation of network and information systems supporting your essential function(s) is appropriately protected from capable and well-resourced threat actors. You understand which contracts are relevant and you include appropriate security obligations, in relevant contracts. You have a proactive approach to contract management which may include a contract management plan for relevant contracts. Customer / supplier ownership of responsibilities is defined in contracts.

		All network connections and data sharing with third parties are managed effectively and proportionately. When appropriate, your incident management process and that of your suppliers provide mutual support in the resolution of incidents.

A4.b Secure Software Development and Support

You actively maximise the use of secure and supported software, whether developed internally or sourced externally, within network and information systems supporting the operation of your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Your software supplier(s) is unaware of the composition and provenance of software provided to you. Software, including updates and patches, undergoes little to no testing. Updates and patches often introduce new problems or fail to address existing issues. Vulnerabilities are discovered in software despite the negligible difficulty of implementing mitigations.	Your software supplier leverages secure development principles and practices. Your software supplier(s) can demonstrate a limited understanding of the composition and provenance of software provided to you. You consider the security of environments (e.g. development, test and production), including source code and repositories, used in the production of software to	Your software supplier(s) leverages an established secure software development framework (e.g. NIST Secure Software Development Framework (SSDF), Microsoft Secure Development Lifecycle (SDL)). Your software supplier can demonstrate a thorough understanding of the composition and provenance of software provided to you, including any third-party components used in the development of that

	be appropriate and proportionate within the context of common threats. The testing regime uses a range of different approaches (e.g. static and dynamic analysis, unit and integration testing and point in time assessments) that verify all aspects of the development lifecycle covering both functional and non-functional testing. You have arrangements in place with your software supplier to receive timely security updates, patches and notifications. Software, including updates and patches, is obtained from your supplier(s) via secure channels. Your software supplier(s) has processes in place to identify, report and mitigate security vulnerabilities. You have arrangements in place with your software supplier to be notified of any significant events that may adversely impact network and information systems supporting your essential function(s). If open-source software is used, you have taken appropriate and proportionate steps to establish and maintain	software, and those components are being monitored for new vulnerabilities throughout the lifespan of the product. You consider the security of environments (e.g. development, test, and production), including source code and repositories, used in the production of software to be appropriate and proportionate within the context of capable and well-resourced threat actors. The software development lifecycle is informed by a detailed and up to date understanding of threat and applies appropriate techniques, such as threat modelling, to identify and assess potential vulnerabilities and attack vectors. You can attest to the authenticity and integrity of software, including updates and patches.

	sufficient confidence in its security for its use. You have appropriate support and maintenance arrangements in place.	

CAF - Objective B - Protecting against cyber attack

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

Principle B1 Service Protection Policies, Processes and Procedures

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

B1.a Policy, Process and Procedure Development

You have developed and continue to improve a set of cyber security and resilience policies, processes and procedures that manage and mitigate the risk of adverse impact to network and information systems supporting your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Your policies, processes and procedures are absent or incomplete. Policies, processes and procedures are not applied universally or consistently. People often or routinely circumvent policies, processes and procedures to achieve business objectives. Your organisation's security governance and risk management approach has no bearing on your policies, processes and procedures.	Your policies, processes and procedures document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. You review and update policies, processes and procedures 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 policies, processes and procedures and key performance indicators are reported to your executive management. Your organisation's policies, processes and procedures are developed to be practical, usable and

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

B1.b Policy, Process and Procedure Implementation

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

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Policies, processes and procedures are ignored or only partially followed. How your policies, processes and procedures support the resilience of your essential function(s) is not well understood. Staff are unaware of their responsibilities under your policies, processes and procedures. You do not attempt to detect breaches of policies, processes and procedures. Policies, processes and procedures lack integration with other organisational policies, processes and procedures. Your policies, processes and procedures are not well communicated across your organisation.	Most of your policies, processes and procedures are followed and their application is monitored. Your policies, processes and procedures are integrated with other organisational policies, processes and procedures, including HR assessments of individuals' trustworthiness. All staff are aware of their responsibilities under your policies, processes and procedures. All breaches of policies, processes and procedures with the potential to adversely impact the essential function(s) are fully investigated. Other breaches are tracked, assessed for trends and action is taken to understand and address.	All your policies, processes and procedures are followed, their correct application and security effectiveness is evaluated. Your policies, processes and procedures are integrated with other organisational policies, processes and procedures, including HR assessments of individuals' trustworthiness. Your policies, processes and procedures 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, processes and procedures with potential to adversely impact the essential function(s) including aggregated breaches.

Principle B2 Identity and Access Control

The organisation understands, documents and manages access to network and information systems supporting the operation of essential functions. 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 network and information systems supporting your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Initial identity verification is not robust enough to provide an acceptable level of confidence of a user's identity profile. Authorised users and systems with access to networks or information systems on which your essential function(s) depends cannot be individually identified. Unauthorised individuals or devices can access your network or information systems on which your essential function(s) depends. The number of authorised users and systems that have access to network and information systems is not limited to the minimum	Your process of initial identity verification is robust enough to provide a reasonable level of confidence of a user's identity profile before allowing an authorised user access to network and information systems that support your essential function(s). All authorised users and systems with access to network and information systems supporting your essential function(s) are individually identified and authenticated. The number of authorised users and systems that have access to network and information systems is limited to the minimum	Your process of initial identity verification is robust enough to provide a high level of confidence of a user's identity profile before allowing an authorised user access to network and information systems that support your essential function(s). Only authorised and individually authenticated users can physically access and logically connect to your network or information systems on which your essential function(s) depends. The number of authorised users and systems that have access to network and information systems is limited to the minimum

necessary to support your essential function(s). Your approach to authenticating users, devices and systems does not follow up to date best practice.	necessary to support your essential function(s). You use additional strong authentication mechanisms, such as multi-factor authentication (MFA), for privileged access to all network and information systems that operate or support your essential function(s). You individually authenticate and authorise all remote access to all network and information systems that support your essential function(s). The list of users and systems with access to network and information systems supporting and delivering the essential function(s) is reviewed on a regular basis, at least annually. Your approach to authenticating users, devices and systems follows up to date best practice.	necessary to support your essential function(s). You use additional strong authentication mechanisms, such as multi-factor authentication (MFA), for all user access, including remote access, to all network and information systems that operate or support your essential function(s). The list of users and systems with access to network and information systems supporting and delivering the essential function(s) is reviewed on a regular basis, at least every six months. Your approach to authenticating users, devices and systems follows up to date best practice.

B2.b Device Management

You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Users can connect to network and information systems supporting your essential function(s) using devices that are not corporately owned and managed. Privileged users can perform privileged operations from devices that are not corporately owned and 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 network and information systems gives that device access without device or user authentication.	Only corporately owned and managed devices can access your essential function(s) network and information systems. All privileged operations are performed from corporately owned and managed devices. These devices provide sufficient separation, using a risk-based approach, from the activities of standard users. 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 network and information systems and investigate such incidents.	All privileged operations performed on network and information systems supporting your essential function(s) are conducted from highly trusted devices, such as Privileged Access Workstations, dedicated solely to those operations. You either obtain independent and professional assurance of the security of third-party devices or networks before they connect to network and information systems, or you only allow third-party devices or networks that are dedicated to supporting network and information systems to connect. You perform certificate-based device identity management and only allow known devices to access systems necessary for the operation of your essential function(s). You perform regular scans to detect unknown devices and investigate any findings.

B2.c Privileged User Management

You closely manage privileged user access to network and information systems supporting your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
The identities of the individuals with privileged access to network and information systems (infrastructure, platforms, software, configuration etc) supporting your essential function(s) are not known or not managed. Privileged user access to network and information systems supporting your essential function(s) 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(s). Privileged user access to network and information systems supporting your essential function(s) is via generic, shared or default name accounts.	All privileged user access to network and information systems supporting your essential function(s) requires strong authentication, such as multi-factor authentication (MFA). The identities of the individuals with privileged access to network and information systems (infrastructure, platforms, software, configuration etc) supporting your essential function(s) are known and managed. This includes third parties. Activity by privileged users is routinely reviewed and validated (e.g. at least annually). Privileged users are only granted specific privileged user access rights which are essential to their business role or function.	Privileged user access to network and information systems supporting your essential function(s) is carried out from dedicated separate accounts that are closely monitored and managed. The issuing of temporary, time-bound rights for privileged user access and / or external third-party support access is in place. Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process. All privileged user activity is routinely reviewed, validated and recorded for offline analysis and investigation.

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. 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 Management (IdAM)

You closely manage and maintain identity and access control for users, devices and systems accessing network and information systems supporting your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Greater access rights are granted than necessary. Identity validation and requirement for access of a user, device or systems is not carried out. User access rights are not reviewed when users change roles. User access rights remain active when users leave your organisation. Access rights granted to devices or systems to access other devices and systems are not reviewed on a regular basis (at least annually).	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 access rights are reviewed when users change roles via your joiners, leavers and movers process. All user, device and system access to the systems supporting the essential function(s) is logged and monitored, but it is not compared to other log data or access records.	You follow a robust procedure to verify each user and issue the minimum required access rights, and the application of the procedure is regularly audited. User access rights are reviewed both when people change roles via your joiners, leavers and movers process and at regular intervals - at least annually. All user, device and systems access to network and information systems supporting your essential function(s) is logged and monitored. You regularly review access logs and correlate this data with other access records and expected activity. Attempts by unauthorised users, devices or systems to connect to network and information systems supporting your essential function(s) are alerted, promptly assessed and investigated.

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 functions. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of essential functions. It also covers information that would assist a threat actor, such as design details of network and information systems.

B3.a Understanding Data

You have a good understanding of data important to the operation of network and information systems supporting your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, uncontrolled release, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You have incomplete knowledge of what data is used by and produced in the operation of network and information systems supporting your essential function(s). You have not identified the important data on which network and information systems supporting your essential function(s) relies. You have not identified who has access to data important to the operation of network and information systems supporting your essential function(s).	You have identified and catalogued all the data important to the operation of network and information systems supporting your essential function(s), or that would assist a threat actor. You have identified and catalogued who has access to the data important to the operation of network and information systems supporting your essential function(s). You regularly review location, transmission, quantity and quality of data important to the operation	You have identified and catalogued all the data important to the operation of network and information systems supporting your essential function(s), or that would assist a threat actor. You have identified and catalogued who has access to the data important to the operation of network and information systems supporting your essential function(s). You maintain a current understanding of the location, quantity and quality of data important to the

You have not clearly articulated the impact of data compromise or lack of availability.	of network and information systems supporting your essential function(s). You have identified all mobile devices and media that hold data important to the operation of network and information systems supporting your essential function(s). You understand and document the impact on your essential function(s) of all relevant scenarios, including unauthorised data access, uncontrolled release, modification or deletion, or when authorised users are unable to appropriately access this data. You occasionally validate these documented impact statements.	operation of network and information systems supporting your essential function(s). You take steps to remove or minimise unnecessary copies or unneeded historic data. You have identified all mobile devices and media that may hold data important to the operation of network and information systems supporting your essential function(s). You maintain a current understanding of the data links used to transmit data that is important to network and information systems supporting your essential function(s). You understand the context, limitations and dependencies of your important data. You understand and document the impact on your essential function(s) of all relevant scenarios, including unauthorised data access, uncontrolled release, modification or deletion, or when authorised users are unable to appropriately access this data. 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 operation of network and information systems supporting your essential function(s). This includes the transfer of data to third parties.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You do not know what all your data links are, or which carry data important to the operation of the essential function(s). Data important to the operation of the essential function(s) 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.	You have identified and protected (effectively and proportionately) all the data links that carry data important to the operation of your essential function(s). You apply appropriate physical and / or technical means (e.g. cryptography) to protect data that travels over non-trusted or openly accessible carriers, but you have limited or no confidence in the robustness of the protection applied.	You have identified and protected (effectively and proportionately) all the data links that carry data important to the operation of your essential function(s). You apply appropriate physical and / or technical means (e.g. cryptography) to protect data that travels over non-trusted or openly accessible carriers, with justified confidence in the robustness of the protection applied. Suitable alternative transmission paths are available where there is a significant risk of impact on the operation of the essential function(s) due to resource limitation (e.g. transmission equipment or function failure, or important data being blocked or jammed).

B3.c Stored Data

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

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You have no, or limited, knowledge of where data important to the operation of network and information systems supporting your essential function(s) is stored. You have not protected vulnerable stored data important to the operation of network and information systems supporting your essential function(s) in a suitable way. Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.	All copies of data important to the operation of network and information systems supporting your essential function(s) are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy. You have applied suitable physical and / 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 operation of network and information systems supporting your essential function(s) to continue	All copies of data important to the operation of network and information systems supporting your essential function(s) are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy. You have applied suitable physical and / 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 operation of network and information systems supporting your essential function(s) to continue

	should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.	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 operation of network and information systems supporting your essential function(s) on mobile devices (e.g. smartphones, tablets and laptops).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You do not know which mobile devices may hold data important to the operation of network and information systems supporting your essential function(s). You allow data important to the operation of network and information systems supporting your essential function(s) to be stored on devices not managed by your organisation, or to at least equivalent standard. Data on mobile devices is not technically secured, or only some is secured.	You know which mobile devices hold data important to the operation of network and information systems supporting your essential function(s). Data important to the operation of network and information systems supporting your essential function(s) is stored on mobile devices only when they have at least the security standard aligned to your overarching security policies. Data on mobile devices is technically secured.	Mobile devices that hold data that is important to the operation of network and information systems supporting your essential function(s) are catalogued, are under your organisation's control and configured according to best practice for the platform, with appropriate technical and procedural policies in place. Your organisation can remotely wipe all mobile devices holding data important to the operation of network and information systems supporting your essential function(s). 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

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

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

Principle B4 System Security

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

B4.a Secure by Design

You design security into network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential function(s) should not be impacted by the exploitation of any single vulnerability.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Network and information systems supporting the operation of the essential function(s) are not appropriately segregated from other systems. Internet services, such as browsing and email are accessible from network and information systems supporting your essential function(s). Data flows between network and information systems supporting your essential function(s) and other systems are complex, making it hard to discriminate between legitimate and illegitimate / malicious traffic.	You employ appropriate expertise to design network and information systems supporting your essential function(s). You design strong boundary defences where network and information systems interface with other organisations or the world at large. You design simple data flows between network and information systems and any external interface to enable effective monitoring. You design to make network and information system recovery simple. All inputs to network and information systems	You employ appropriate expertise to design network and information systems supporting your essential function(s). Network and information systems are segregated into appropriate security zones (e.g. systems supporting the essential function(s) are segregated in a highly trusted, more secure zone). The network and information systems supporting your essential function(s) are designed to have simple data flows between components to support effective security monitoring.

Remote or third-party accesses circumvent some network controls to gain more direct access to network and information systems supporting the essential function(s).	supporting your essential function(s) are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.	The network and information systems supporting your essential function(s) are designed to be easy to recover. Content-based attacks are mitigated for all inputs to network and information systems that affect the essential function(s) (e.g. via transformation and inspection / sanitisation and validation). If automated decision-making technologies are in use, you design and apply appropriate restrictions to prevent actions that could have an adverse impact on network and information systems supporting your essential function(s).

B4.b Secure Configuration

You securely configure network and information systems that support the operation of your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You have not identified the assets that need to be carefully configured to maintain the security of network and information systems supporting your essential function(s). Policies relating to the security of operating system builds or configuration are not applied consistently across network and information systems relating to your essential function(s). 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 affect your essential function(s) is lacking or inconsistent. Generic, shared, default name and built-in accounts have not been removed or disabled.	You have identified and documented the assets that need to be carefully configured to maintain the security of network and information systems supporting your essential function(s). 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 configurations at security boundaries of network and information systems supporting your essential function(s) are approved and documented. You verify software before installation is permitted. Generic, shared, default name and built-in accounts have been removed or disabled. Where this is not possible, credentials to	You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of network and information systems supporting your essential function(s). 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 information systems configurations are secure and documented. You regularly review and validate that network and information systems have the expected, secure settings and configuration.

Standard users are able to change settings that would adversely impact the security of network and information systems supporting your essential function(s).	these accounts have been changed. Service accounts are appropriately protected. Standard users are not able to change settings that would adversely impact the security of network and information systems supporting your essential function(s).	Only permitted software can be installed. If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated. Generic, shared, default name and built-in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed. Service accounts are appropriately protected.

B4.c Secure Management

You manage your organisation's network and information systems that support the operation of your essential function(s) to enable and maintain security.

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

B4.d. Vulnerability Management

You manage known vulnerabilities in network and information systems to prevent adverse impact on your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements below are true	All the following statements are true
You do not understand the exposure of network and information systems supporting your essential function(s) to publicly-known vulnerabilities. You do not mitigate externally exposed vulnerabilities promptly. You have not recently tested to verify your understanding of the vulnerabilities of network and information systems that support your essential function(s). 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 network and information systems supporting your essential function(s) to publicly-known vulnerabilities. Announced vulnerabilities for all software packages used in network and information systems supporting your essential function(s) are tracked, prioritised and externally exposed vulnerabilities are mitigated (e.g. by patching) promptly. 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 network and information systems that support the operation of your essential function(s).	You maintain a current understanding of the exposure of network and information systems supporting your essential function(s) to publicly-known vulnerabilities. Announced vulnerabilities for all software packages used in network and information systems supporting your essential function(s) are tracked, prioritised and mitigated (e.g. by patching) promptly. You regularly test to fully understand the vulnerabilities of network and information systems that support the operation of your essential function(s) and verify this understanding with third-party testing. You actively maximise the use of supported software, firmware and hardware in network and information systems supporting your essential function(s).

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 operation of your essential function(s).

B5.a Resilience Preparation

You are prepared to restore the operation of your essential function(s) following adverse impact to network and information systems.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All the following statements are true	All the following statements are true
You have limited understanding of all the elements that are required to restore operation of network and information systems supporting your essential function(s). You have not completed business continuity and disaster recovery plans for network and information systems, including their dependencies, supporting the operation of the essential function(s). You have not fully assessed the practical implementation of your business continuity and disaster recovery plans.	You know all network and information systems, and underlying technologies, that are necessary to restore the operation of your essential function(s) and understand their interdependence. You know the order in which systems need to be recovered to efficiently and effectively restore the operation of the essential function(s).	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 identify new or heightened levels of risk, which result in immediate and potentially temporary security measures to enhance the security of network and information systems supporting your essential function(s), (e.g. in response to a widespread outbreak of very damaging malware).

B5.b Design for Resilience

You design network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Network and information systems supporting the operation of your essential function(s) are not appropriately segregated. Internet services, such as browsing and email, are accessible from network and information systems supporting your essential function(s). You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential function(s).	Network and information systems supporting the operation of your essential function(s) are logically separated from your business systems (e.g. they reside on the same network as the rest of the organisation but within a DMZ). Internet services, such as browsing and email, are not accessible from network and information systems supporting your essential function(s). Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.	Network and information systems supporting the operation of your essential function(s) are segregated from other business and external systems by appropriate technical and physical means (e.g. separate network and system infrastructure with independent user administration). Internet services, such as browsing and email, are not accessible from network and information systems supporting your essential function(s). 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 essential function(s) depends 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 limitations and mitigations when necessary.

B5.c Backups

You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s) following an adverse impact to network and information systems.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Backup coverage is incomplete and does not include all relevant data and information needed to restore the operation of your essential function(s). Backups are not frequent enough for the operation of your essential function(s) to be restored effectively. Your restoration process does not restore your essential function(s) in a suitable time frame.	You have appropriately secured backups (including data, configuration information, software, equipment, processes and knowledge). These backups will be accessible to recover from an extreme event including ransomware attack. You routinely test backups to ensure that the backup process function(s) 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. Backups of all important data and information needed to recover the essential function(s) 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 operation of your essential function(s).

B6.a Cyber Security Culture

You develop and maintain a positive cyber security culture and a shared sense of responsibility.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
People in your organisation do not understand what they contribute to the cyber security of network and information systems supporting your essential function(s). People in your organisation do not 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 and may encourage poor security behaviours. Formal or informal incentives and rewards conflict with the promotion	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 network and information systems supporting your essential functions(s). 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. You identify and address issues that inhibit people	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, 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

of positive security outcomes.	from behaving in a manner that supports your intended cyber security outcomes.	actively involved in cyber security. Your organisation communicates openly about cyber security, with any concern being taken seriously. People across your organisation collaborate 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 operation of network and information systems supporting your essential function(s) are appropriately trained in cyber security.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
There are teams who operate and support your essential function(s) 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.	All people in your organisation, from the most senior to the most junior, follow appropriate cyber security training paths. Each individuals 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

Training is used as a “silver bullet” for all user security behaviours. The success of training is only measured by the number of people reached, rather than assessing whether it has a positive impact on security behaviours. Training materials contain out of date or contradictory information, or information that conflicts with other policies, processes or procedures.	Cyber security information is easily available.	widest audience and are effective. You make cyber security information and good practice guidance easily accessible, widely available and you know it is referenced and used within your organisation.

CAF - Objective C – Detecting Cyber Security Events

Capabilities exist to ensure security defences remain effective and to detect cyber security events and incidents adversely affecting, or with the potential to adversely affect, essential function(s).

Principle C1 Security Monitoring

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

C1.a Sources and Tools for Logging and Monitoring

The data sources and tools that you include in your logging and monitoring allow for timely identification of events which might adversely affect the security or resiliency of network and information system(s) supporting the operation of your essential function(s).

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Data relating to the security and operation of network and information systems supporting your essential function(s) is not collected. You are not able to audit the activities of users and systems in relation to network and information systems supporting your essential function(s). You do not monitor traffic crossing your network boundary. Log data cannot be synchronised using an	Data relating to the security and operation of some areas of network and information systems supporting your essential function(s) is collected but coverage is not comprehensive. Some user and system monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour. You monitor traffic crossing your network boundary (including IP address	Monitoring is based on a thorough understanding of network and information systems supporting your essential function(s), techniques used by threat actors, and awareness of what logging and monitoring is required to detect events and incidents that could affect the operation of your essential function(s). Your monitoring data provides enough detail to promptly and reliably detect security events,

accurate common time source. Logs are stored in locations where they are not readily available to authorised users and systems. Your monitoring tools cannot be configured to make use of new log streams as they come online. Your monitoring tools are only able to make use of a fraction of the log data being collected. You do not understand where log data is stored or how long it should be stored for. You have no way of ensuring log data is being captured as expected and available when needed.	connections as a minimum). Some but not all log datasets can be easily queried with search tools to aid in investigations. Your monitoring tools work with most log data, with some configuration. Your monitoring tools can make use of log data that would capture all common threats. You ensure log data is available for analysis when needed.	incidents and support investigations. This is reviewed regularly and after a significant security event. Extensive monitoring of user and system activity in relation to network and information systems that support your essential function(s) enables you to promptly detect policy violations, suspicious or undesirable user and system behaviour, deviations from normal / routine behaviour or abnormalities indicative of adverse activity. Your logging and monitoring capability includes host-based and network monitoring. All new network and information systems supporting your essential function(s) are considered as potential logging and monitoring data sources to maintain a comprehensive monitoring capability. Log datasets are synchronised including using an accurate common time source so that separate datasets can be correlated in appropriate ways. You enrich log data with other network and information systems data to

		provide a more comprehensive picture of actions and behaviours. Your monitoring tools make use of log data to pinpoint activity. You regularly review the data sources and tools included in your logging and monitoring strategy to ensure it remains effective.

C1.b Securing Logs

You hold log data securely and grant appropriate user and system access only to accounts with a business need. Log data is held for a suitable retention period, after which it is deleted.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
It is possible for log data to be easily edited or deleted by unauthorised users / systems or attackers. There is no control of the users and systems that can access log data. There is no monitoring of the access to log data. There are no policies covering access to log data.	Only authorised users and systems can access log data. There is some monitoring of access to log data (e.g. copying, deleting or modification, or even viewing). You have defined and implemented retention periods for log data. You have given legitimate reasons for accessing log data in your policies.	Appropriate access to log data is limited to those users and systems with a business need. The logging architecture has mechanisms, policies, processes and procedures to ensure that it can protect itself from threats comparable to those that it is trying to identify. This includes protecting the function itself and the data within it. Log data analysis and normalisation is only performed on copies of the

		log data keeping the master copy unaltered. All actions involving log data (e.g. copying, deleting, modification, or even viewing) can be traced back to a unique user or system. The integrity of log data is protected, verified and any modification, including deletion, is detected and attributed.

C1.c Generating Alerts

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

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You do not apply updates to your detection security technologies in a timely way, after receiving them (e.g. AV signature updates, other threat signatures or Indicators of Compromise (IoCs)). Security alerts relating to network and information systems supporting your essential function(s) are not prioritised. The enrichment of security alerts within network and information systems	You easily detect the presence of Indicators of Compromise (IoCs) on network and information systems supporting your essential function(s), such as known malicious command and control signatures. You apply some updates, new signatures and IoCs in a timely way. Security alerts relating to network and information systems that support your	You easily detect the presence of Indicators of Compromise (IoCs) on network and information systems supporting your essential function(s), such as known malicious command and control signatures, as well as abnormalities or behaviours indicative of adverse activity. You apply all updates, new signatures and IoCs promptly. Security alerts relating to all network and information systems supporting your

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

C1.d Triage of Security Alerts

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

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

C1.e Personnel Skills for Monitoring and Detection

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

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
There are no personnel who perform a monitoring and detection function. Monitoring and detection personnel do not have the correct specialist skills. Monitoring and detection personnel are not capable of reporting against governance requirements. Monitoring and detection personnel have a lack of awareness of the essential function(s) the organisation provides, what assets relate to those functions and hence the importance of the log data and security events. Monitoring and detection personnel have no awareness of other roles or tasks outside of security monitoring and detection that are relevant to the operation of your essential function(s).	Monitoring and detection personnel have some investigative skills and a basic understanding of the data they need to work with. Monitoring and detection personnel can report to other parts of the organisation (e.g. security directors, resilience managers). Monitoring and detection personnel are capable of following most of the required workflow(s). Monitoring and detection personnel are aware of some of the network and information systems and your essential function(s), and can manage alerts relating to them. Monitoring and detection personnel have some understanding of the operational context (e.g. people, processes, network and information systems	You have monitoring and detection personnel who are responsible for the proactive and reactive analysis, investigation and reporting of monitoring alerts including both security and performance. Monitoring and detection personnel have defined roles and skills that cover all parts of the monitoring and investigation process. Monitoring and detection personnel follow policies, processes and procedures that address all governance reporting requirements, internal and external. Monitoring and detection personnel are empowered to look beyond the fixed process to investigate and understand non-standard threats. Monitoring and detection personnel are aware of the network and information

Monitoring and detection personnel are overwhelmed with the amount of data and alerts they have to work with. Alert / triage fatigue is present.	that support your essential function(s)) to enhance the security monitoring function. Monitoring and detection personnel deal with their workload and cases effectively.	systems and your essential function(s), related assets and can identify and prioritise alerts and investigations that relate to them. Monitoring and detection personnel drive and shape new log data collection and can make effective use of it. Monitoring and detection personnel are capable of following all of the required workflow(s). Monitoring and detection personnel have a sufficient understanding of the operational context (e.g. people, processes, network and information systems that support your essential function) to enhance the security monitoring function. Monitoring and detection personnel deal with their workload and cases effectively as well as identifying areas for improvement.

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

Threats to the operation of network and information systems, and corresponding user and system behaviour, are sufficiently understood. These are used to detect cyber security incidents.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Your organisation has no sources of threat intelligence. You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users. You have no awareness of the steps necessary to make best use of threat intelligence for security monitoring. Threat intelligence is unreliable and / or is not actioned by the appropriate users or systems in a timely manner. You have no established understanding of what abnormalities to look for that might signify adverse activities. You do not receive updates for all your detection security technologies (e.g. AV, IDS).	You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security incidents). Your organisation may use threat intelligence services, but you do not necessarily choose sources or providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based infoshare, software vendors, anti-virus providers, specialist threat intel firms, special interest groups). The user and system abnormalities from past attacks and threat intelligence, on your and other network and information systems, are used to signify adverse activity. You receive regular updates for all of your detection security technologies (e.g. AV, IDS).	You track the effectiveness of your threat intelligence and actively share feedback on the usefulness of Indicators of Compromise (IoCs) and other intelligence with the threat community (e.g. sector partners, threat intelligence providers, government agencies). When using threat intelligence feeds, these have been selected using risk-based and threat-informed decisions based on your business needs and sector. You make relevant, reliable and actionable threat intelligence available to the necessary users and systems promptly. You contextualise threat intelligence and link it to the why and / or how attacks take place for security monitoring.

You do not understand normal user and system behaviour sufficiently to be able to use abnormalities to detect adverse activity.		You understand normal user and system abnormalities fully, to such an extent that searching for system abnormalities is an effective way of detecting adverse activity (e.g. you fully understand which systems should and should not communicate and when). The user and system abnormalities you monitor for are based on the nature of adverse activities likely to impact network and information systems supporting the operation of your essential function(s). The user and system abnormalities indicative of adverse activity you use are regularly updated to reflect changes in network and information systems supporting your essential function(s) and current threat intelligence. You possess the capability to share threat intelligence (e.g. ways to effectively detect adversaries) with the threat community / defender community (sector partners, threat intelligence providers, government agencies) when required.

Principle C2 Threat Hunting

The organisation proactively seeks to detect, within networks and information systems, adverse activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard security prevent / detect solutions (or when standard solutions are not deployable).

C2.a Threat Hunting

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
You do not know the resources required for threat hunting. You do not have access to an effective threat hunting capability. Your threat hunts do not follow any structure and few if any records are created.	You have identified the resources required to perform threat hunting and are able to deploy these, in a timely manner, on an occasional basis. You deploy an effective threat hunting capability but not frequent enough to match the risks posed to network and information systems supporting your essential function(s) (e.g. you perform threat hunts in response to a tip off from a reputable source). Your threat hunts follow pre-determined and documented methods (e.g. hypothesis driven, data driven, entity driven) designed to identify adverse activity not detected by automated detections.	You understand the resources required to perform threat hunting and these are deployed as part of business as usual. You deploy threat hunting resources at a frequency that matches the risks posed to network and information systems supporting your essential function(s). Your threat hunts follow pre-determined and documented methods (e.g. hypothesis driven, data driven, entity driven) designed to identify adverse activity not detected by automated detections. You turn threat hunts into automated detections and alerting where appropriate. You routinely record details of previous threat hunts and

	You document details of threat hunts and post hunt analysis.	post hunt activities. You use these to drive improvements in your threat hunting and security posture. You have justified confidence in the effectiveness of your threat hunts and the threat hunting process is reviewed and updated to match the risks posed to network and information systems supporting your essential function(s). You leverage automation to improve threat hunts where appropriate (e.g. some stages of the threat hunting process are automated). Your threat hunts focus on the tactics, techniques and procedures (TTPs) of threats over atomic IoCs (e.g. hashes, IP addresses, domain names etc).

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

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

Principle D1 Response and Recovery Planning

There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential function(s) 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 network and information systems supporting the operation of your essential function(s) and covers a range of incident scenarios.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Your incident response plan is not documented. Your incident response plan does not include your organisations identified essential function(s). Your incident response plan is not well understood by relevant staff.	Your incident response plan covers network and information systems supporting your essential function(s). Your incident response plan comprehensively covers scenarios that are focused on likely impacts of known and well understood attacks only. Your incident 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 and understanding of the security risks to network and information systems supporting your essential function(s). 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

	Your incident response plan is documented and shared with all relevant stakeholders. Your incident response plan is readily accessible, even when your organisations IT systems have been adversely affected by an incident. Your incident response plan is regularly reviewed to ensure it remains effective.	possible attacks, previously unseen. Your incident response plan is documented and integrated with wider organisational business plans and supply chain response plans, as well as dependencies on supporting infrastructure (e.g. power, cooling etc). Your incident response plan is communicated and understood by the business areas involved with the operation of your essential function(s).

D1.b Response and Recovery Capability

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

Not Achieved	Achieved
At least one of the following statements is true	All the following statements are true
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 operation of your essential function(s) 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. Key roles are duplicated, and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential function(s). Back-up mechanisms are available that can be readily activated to allow continued operation of your essential function(s), although possibly at a reduced level, if primary network and information systems fail or are unavailable. Arrangements exist to augment your organisation's 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.	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

Exercises do not test all parts of the response cycle.	response plans and protective security, in line with the lessons learned. Exercises test all parts of your response cycle relating to your essential function(s) (e.g. restoration of normal function(s) levels).

Principle D2 Lessons Learned

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

D2.a Post Incident Analysis

When an incident occurs, your organisation takes steps to understand its causes, informing appropriate remediating action.

Not Achieved	Achieved
At least one of the following statements is true	All the following statements are true
You are not usually able to resolve incidents to a root cause or identify the contributing factors within a broader systems context. You do not have a formal process for investigating causes. Investigators form theories early in the process and only seek evidence that affirms their belief. Investigations are solely focused on identifying the person(s) who can be held responsible for the incident.	Post incident analysis is conducted routinely as a key part of your lessons learned activities following an incident. Your post incident analysis is comprehensive, considering organisational factors (e.g. policies, processes and procedures), technical factors (e.g. system design, vulnerabilities), human factors (e.g. training, security culture) and any changes to threat. All relevant incident data is made available to the analysis team to perform post incident analysis. Your analysis considers what could have happened under plausible, alternative circumstances (e.g. 'what if' / 'if only' scenarios).

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. Changes are made as a 'knee jerk' reaction to an incident without proper analysis and testing to ensure the change is appropriate. You wait until a severe or high-profile incident has occurred before you take steps to improve.	You have a documented incident review process / policy which ensures that lessons learned from each incident, including near misses, are identified, captured, and acted upon. Lessons learned cover issues with reporting, roles, governance, skills and organisational policies, processes and procedures as well as technical aspects of network and information systems. 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 promptly. Analysis is fed to senior management and incorporated into risk management and continuous improvement. Your organisation maximises the lessons learned by using the analysis into 'what if' / 'if only' scenarios. Your organisation learns from reported incidents in your sector and the wider national infrastructure.