National Cyber Security Centre
a part of GCHQ

Cyber Assessment Framework V4.0 – Record of Changes

Version as of 4th August 2025

How the CAF indexing system is used:

In the Record of Changes table below amendments to the CAF are referenced by CAF version, Objective, Principle, Contributing Outcome (CO) and Indicator of Good Practice (IGP) numbering. For example, taking the reference '[3.2]A1.a.A.4' means CAF v3.2, Objective 'A', Principle '1', Contributing Outcome 'a', Column 'A' for Achieved with the final number '4' referring to the fourth IGP in the Achieved column. Similarly, for other Column references 'PA' in other table rows means 'Partially Achieved' and 'NA' means 'Not Achieved'.

A second example using '[4.0]A1.c.NA.5' means CAF v4.0, Objective 'A', Principle '1', Contributing Outcome 'c', Column 'NA' for 'Not Achieved' with the final number '5' referring to the fifth IGP in the 'Not Achieved' column.

Principle headings and explanatory text have been included even if unchanged to aid use and navigation through the document.

CAF v3.2 Contributing Outcome Reference	Changed From / Removed	CAF v4.0 Contributing Outcome Reference	Changed To / Added
[3.2]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.**		
[3.2]A1.a	**Board Direction** You have effective organisational security management led at board level and articulated clearly in corresponding policies.		
[3.2]A1.a.A.4	Direction set at board-level is translated into effective organisational practices that direct and control the security of the network and information systems supporting your essential function(s).	**[4.0]A1.a.A.4**	Direction set at board-level is translated into effective organisational practices that direct and control the security of network and information systems supporting your essential function(s).
		[4.0]A1.a.A.5 (New)	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.

		[4.0]A1.a.A.6 (New)	Security is recognised as an important enabler for the resilience of your essential function(s) and considered in all relevant discussions.
[3.2]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.		
[3.2]A1.c.NA.4	Organisational structure causes risk decisions to be made in isolation. (e.g. engineering and IT don't talk to each other about risk).	**[4.0]A1.c.NA.5**	Organisational structure causes risk decisions to be made in isolation. (e.g. engineering and IT do not talk to each other about risk).
		[4.0]A1.c.NA.4 (New)	Decision-makers are unable to justify their risk management decisions.
[3.2]A1.c.NA.5	Risk priorities are too vague to make meaningful distinctions between them. (e.g. almost all risks are rated 'medium' or 'amber').	**[4.0]A1.c.NA.6**	Risk priorities are too vague to make meaningful distinctions between them. (e.g. almost all risks are rated 'medium' or 'amber').
[3.2]A2	**Risk Management** **The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.**	**[4.0]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.**
[3.2]A2.a	**Risk Management Process** Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of your essential function(s) and communicating associated activities.	**[4.0]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.
[3.2]A2.a.NA.7	Security requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of the essential function(s).	**[4.0]A2.a.NA.7**	Security requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of network and information systems supporting your essential function(s).
[3.2]A2.a.PA.2	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).	**[4.0]A2.a.PA.2**	Your risk assessments are informed by an understanding of known and well understood threats and vulnerabilities in network and information systems supporting your essential function(s).

[3.2]A2.a.PA.5	You conduct risk assessments when significant events potentially affect the essential function(s), such as replacing a system or a change in the cyber security threat.	**[4.0]A2.a.PA.5**	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.
[3.2]A2.a.PA.6	You perform threat analysis and understand how generic threats apply to your organisation.	**[4.0]A2.b.PA.1**	You perform threat analysis and understand how common threats apply to network and information systems supporting your essential function(s).
[3.2]A2.a.A.2	Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of network and information systems.	**[4.0]A2.a.A.2**	Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible threat actor actions and the security properties of network and information systems supporting your essential function(s).
[3.2]A2.a.A.3	Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function(s) and your sector.	**[4.0]A2.a.A.3**	Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of threats to network and information systems supporting your essential function(s), your sector and wider national infrastructure**.**
[3.2]A2.a.A.5	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.	**[4.0]A2.a.A.5**	The output from your risk management process is a clear set of traceable and prioritised security requirements that will address the risks in line with your organisational approach to security.
[3.2]A2.a.A.7	Your risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to network and information systems, change of use and new threat information.	**[4.0]A2.a.A.7**	Your risk assessments are dynamic and readily updated in the light of relevant changes which may include technical changes to network and information systems supporting your essential function(s), change of use, the introduction of new or emergent technologies or new threat information.
[3.2]A2.a.A.9	You perform detailed threat analysis and understand how this applies to your organisation in the context of the threat to your sector and the wider CNI.	**[4.0]A2.b.A.1**	You perform detailed threat analysis and understand how this applies to network and information systems supporting your essential function(s), in the context of your sector and wider national infrastructure.
		[4.0]A2.a.A.9 (New)	You anticipate technological developments that could be used to adversely impact network and information systems supporting your essential function(s).
[3.2]A2.b	**Assurance** You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to your essential function(s).	**[4.0]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).

[3.2]A2.b.NA.1	A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value.	**[4.0]A2.c.NA.1**	A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value.
[3.2]A2.b.NA.2	Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments.	**[4.0]A2.c.NA.2**	Assurance methods are applied without appreciation of their strengths and limitations.
[3.2]A2.b.NA.3	Assurance is assumed because there have been no known problems to date.	**[4.0]A2.c.NA.3**	Assurance is assumed because there have been no known problems to date.
[3.2]A2.b.A.1	You validate that the security measures in place to protect the network and information systems are effective and remain effective for the lifetime over which they are needed.	**[4.0]A2.c.A.1**	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.
[3.2]A2.b.A.2	You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential function(s).	**[4.0]A2.c.A.2**	You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of network and information systems supporting your essential function(s).
[3.2]A2.b.A.3	Your confidence in the security as it relates to your technology, people, and processes can be justified to, and verified by, a third party.	**[4.0]A2.c.A.3**	Your confidence in the security as it relates to your technology, people, and processes can be justified to, and verified by, a third party.
[3.2]A2.b.A.4	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.	**[4.0]A2.c.A.4**	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.
[3.2]A2.b.A.5	The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.	**[4.0]A2.c.A.5**	The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.
		[4.0]A2.b (New)	**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.
		[4.0]A2.b.NA.1 (New)	You are unable to perform threat analysis.
		[4.0]A2.b.NA.2 (New)	You do not understand the threat to network and information systems supporting your essential function(s).

		[4.0]A2.b.NA.3 (New)	You do not have a clearly defined set of threat assumptions.
		[4.0]A2.b.NA.4 (New)	You do not use your understanding of threat to inform your risk management decisions.
		From [3.2]A2.a.PA.6 to [4.0]A2.b.PA.1	You perform threat analysis and understand how common threats apply to network and information systems supporting your essential functions(s).
		[4.0]A2.b.PA.2 (New)	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.
		[4.0]A2.b.PA.3 (New)	You anticipate what threat actors might target in network and information systems to cause an adverse impact to your essential function(s).
		[4.0]A2.b.PA.4 (New)	Your understanding of threat is informed by common incidents.
		[4.0]A2.b.PA.5 (New)	You apply your understanding of threat to inform your risk management decision-making.
		From [3.2]A2.a.A.9 to [4.0]A2.b.A.1	You perform detailed threat analysis and understand how this applies to network and information systems supporting your essential function(s), in the context of your sector and wider national infrastructure.
		[4.0]A2.b.A.2 (New)	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).
		[4.0]A2.b.A.3 (New)	You use appropriate techniques to develop an understanding of network and information systems supporting your essential function(s) from a threat actor's perspective. You anticipate probable attack methods and techniques, targets and objectives, and develop plausible scenarios.
		[4.0]A2.b.A.4 (New)	You understand the different steps a capable and well-resourced threat actor would need to take to reach the probable target(s).

		[4.0]A2.b.A.5 (New)	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).
		[4.0]A2.b.A.6 (New)	You maintain a detailed understanding of current threats (e.g. by threat intelligence and proactive research).
		[4.0]A2.b.A.7 (New)	You apply your detailed understanding of threat to inform your risk management decision-making.
		[4.0]A2.b.A.8 (New)	You have documented the steps required to undertake detailed threat analysis.
[3.2]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).**		
[3.2]A3.a	**Asset Management**		
[3.2]A3.a.NA.1	Inventories of assets relevant to the essential function(s) are incomplete, non-existent, or inadequately detailed.	**[4.0]A3.a.NA.1**	Inventories of assets relevant to network and information systems supporting your essential function(s) are incomplete, non-existent or inadequately detailed.
[3.2]A3.a.NA.4	Knowledge critical to the management, operation, or recovery of the essential function(s) is held by one or two key individuals with no succession plan.	**[4.0]A3.a.NA.4**	Knowledge critical to the management, operation, or recovery of network and information systems supporting your essential function(s) is held by one or two key individuals with no succession plan.
[3.2]A3.a.A.1	All assets relevant to the secure operation of essential function(s) are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.	**[4.0]A3.a.A.1**	All assets relevant to the secure operation of network and information systems supporting your essential function(s) are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.
[3.2]A3.a.A.3	You have prioritised your assets according to their importance to the operation of the essential function(s).	**[4.0]A3.a.A.3**	You have prioritised your assets according to their importance to the operation network and information systems supporting your essential function(s).
[3.2]A3.a.A.4	You have assigned responsibility for managing all assets, including physical assets, relevant to the operation of the essential function(s).	**[4.0]A3.a.A.4**	You have assigned responsibility for managing all assets, including physical assets, relevant to the operation of network and information systems supporting your essential function(s).

[3.2]A3.a.A.5	Assets relevant to the essential function(s) are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.	**[4.0]A3.a.A.5**	Assets relevant to network and information systems supporting your essential function(s) are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.
[3.2]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 external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.**	**[4.0]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.**
[3.2]A4.a	**Supply Chain**	**[4.0]A4.a (New)**	**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).
[3.2]A4.a.NA.2	Elements of the supply chain for essential function(s) are subcontracted and you have little or no visibility of the sub-contractors.	**[4.0]A4.a.NA.2**	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.
[3.2]A4.a.NA.4	Suppliers have access to systems that provide your essential function(s) that is unrestricted, not monitored or bypasses your own security controls.	**[4.0]A4.a.NA.4**	Suppliers have access to network and information systems that support your essential function(s) that is unrestricted, not monitored or bypasses your own security controls.
[3.2]A4.a.PA.1	You understand the general risks suppliers may pose to your essential function(s).	**[4.0]A4.a.PA.1**	You understand the general risks suppliers may pose to network and information systems supporting your essential function(s).
[3.2]A4.a.PA.2	You know the extent of your supply chain that supports your essential function(s), including sub-contractors.	**[4.0]A4.a.PA.2**	You know the extent of your supply chain that supports network and information systems supporting your essential function(s), including sub-contractors.
[3.2]A4.a.PA.3	You understand which contracts are relevant and you include appropriate security obligations, in relevant contracts.	**[4.0]A4.a.PA.4**	You understand which contracts are relevant and you include appropriate security obligations, in relevant contracts.
		[4.0]A4.a.PA.3 (New)	Suppliers to network and information systems supporting your essential function(s) can demonstrate appropriate and proportionate levels of cyber security within the context of common threats.
[3.2]A4.a.PA.4	You are aware of all third-party connections and have assurance that they meet your organisation's security requirements.	**[4.0]A4.a.PA.5**	You are aware of all third-party connections and have assurance that they meet your organisation's security requirements.

[3.2]A4.a.PA.5	Your approach to security incident management considers incidents that might arise in your supply chain.	**[4.0]A4.a.PA.6**	Your approach to security incident management considers incidents that might arise in your supply chain.
[3.2]A4.a.PA.6	You have confidence that information shared with suppliers that is necessary for the operation of your essential function(s) is appropriately protected from well-known attacks and known vulnerabilities.	**[4.0]A4.a.PA.7**	You have confidence that information held by suppliers that is necessary for the operation of network and information systems supporting your essential function(s) is appropriately protected from common threats.
[3.2]A4.a.A.1	You have a deep understanding of your supply chain, including sub-contractors and the wider risks it faces. You consider factors such as supplier's partnerships, competitors, nationality and other organisations with which they subcontract. This informs your risk assessment and procurement processes.	**[4.0]A4.a.A.1**	You have a deep understanding of your supply chain, including sub-contractors, and the wider risks it faces.
		[4.0]A4.a.A.2 (divided from) [3.2]A4.a.A.1	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.
[3.2]A4.a.A.2	Your approach to supply chain risk management considers the risks to your essential function(s) arising from supply chain subversion by capable and well-resourced attackers.	**[4.0]A4.a.A.3**	Your approach to supply chain risk management considers the risks to network and information systems supporting your essential function(s) arising from supply chain subversion by capable and well-resourced threat actors.
		[4.0]A4.a.A.4 (New)	Critical suppliers to network and information systems supporting your essential function(s) can demonstrate appropriate and proportionate levels of cyber security within the context of capable and well-resourced threat actors.
[3.2]A4.a.A.3	You have confidence that information shared with suppliers that is essential to the operation of your function(s) is appropriately protected from sophisticated attacks.	**[4.0]A4.a.A.5**	You have confidence that information held by suppliers that is essential to the operation of network and information systems supporting your essential function(s) is appropriately protected from capable and well-resourced threat actors.
[3.2]A4.a.A.4	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.	**[4.0]A4.a.A.6**	You understand which contracts are relevant and you include appropriate security obligations in relevant contracts.
		[4.0]A4.a.A.7 (divided from) [3.2]A4.a.A.4	You have a proactive approach to contract management which may include a contract management plan for relevant contracts.

[3.2]A4.a.A.5	Customer / supplier ownership of responsibilities is laid out in contracts.	**[4.0]A4.a.A.8**	Customer / supplier ownership of responsibilities is defined in contracts.
[3.2]A4.a.A.6	All network connections and data sharing with third parties are managed effectively and proportionately.	**[4.0]A4.a.A.9**	All network connections and data sharing with third parties are managed effectively and proportionately.
[3.2]A4.a.A.7	When appropriate, your incident management process and that of your suppliers provide mutual support in the resolution of incidents.	**[4.0]A4.a.A.10**	When appropriate, your incident management process and that of your suppliers provide mutual support in the resolution of incidents.
		[4.0]A4.b (New)	**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).
		[4.0]A4.b.NA.1 (New)	Your software supplier(s) is unaware of the composition and provenance of software provided to you.
		[4.0]A4.b.NA.2 (New)	Software, including updates and patches, undergoes little to no testing.
		[4.0]A4.b.NA.3 (New)	Updates and patches often introduce new problems or fail to address existing issues.
		[4.0]A4.b.NA.4 (New)	Vulnerabilities are discovered in software despite the negligible difficulty of implementing mitigations.
		[4.0]A4.b.PA.1 (New)	Your software supplier leverages secure development principles and practices.
		[4.0]A4.b.PA.2 (New)	Your software supplier(s) can demonstrate a limited understanding of the composition and provenance of software provided to you.
		[4.0]A4.b.PA.3 (New)	You consider the security of environments (e.g. development, test and production), including source code and repositories, used in the production of software to be appropriate and proportionate within the context of common threats.
		[4.0]A4.b.PA.4 (New)	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.
		[4.0]A4.b.PA.5 (New)	You have arrangements in place with your software supplier to receive timely security updates, patches and notifications.
		[4.0]A4.b.PA.6 (New)	Software, including updates and patches, is obtained from your supplier(s) via secure channels.
		[4.0]A4.b.PA.7 (New)	Your software supplier(s) has processes in place to identify, report and mitigate security vulnerabilities.
		[4.0]A4.b.PA.8 (New)	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).
		[4.0]A4.b.PA.9 (New)	If open-source software is used, you have taken appropriate and proportionate steps to establish and maintain sufficient confidence in its security for its use.
		[4.0]A4.b.PA.10 (New)	You have appropriate support and maintenance arrangements in place.
		[4.0]A4.b.A.1 (New)	Your software supplier(s) leverages an established secure software development framework (e.g. NIST Secure Software Development Framework (SSDF), Microsoft Secure Development Lifecycle (SDL)).
		[4.0]A4.b.A.2 (New)	Your software supplier can demonstrate a thorough understanding of the composition and provenance of software provided to you, including any third-party components used in the development of that software, and those components are being monitored for new vulnerabilities throughout the lifespan of the product.
		[4.0]A4.b.A.3 (New)	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.
		[4.0]A4.b.A.4 (New)	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.

		[4.0]A4.b.A.5 (New)	You can attest the authenticity and integrity of software, including updates and patches.
[3.2]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.**		
[3.2]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 on your essential function(s).	**[4.0]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).
[3.2]B1.a.A.1	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.	**[4.0]B1.a.A.1**	You fully document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance.
		[4.0]B1.a.A.2 (divided from) [3.2]B1.a.A.1	Cyber security is integrated and embedded throughout policies, processes and procedures and key performance indicators are reported to your executive management.
[3.2]B1.a.A.2	Your organisation's policies, processes and procedures are developed to be practical, usable and appropriate for your essential function(s) and your technologies.	**[4.0]B1.a.A.3**	Your organisation's policies, processes and procedures are developed to be practical, usable and appropriate to mitigate the risk of adverse impact to network and information systems supporting your essential function(s).
[3.2]B1.a.A.3	Policies, processes and procedures that rely on user behaviour are practical, appropriate and achievable.	**[4.0]B1.a.A.4**	Policies, processes and procedures that rely on user behaviour are practical, appropriate and achievable.
[3.2]B1.a.A.4	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.	**[4.0]B1.a.A.5**	You review and update policies, processes and procedures at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident.
[3.2]B1.a.A.5	Any changes to the essential function(s) or the threat it faces triggers a review of policies, processes and procedures.	**[4.0]B1.a.A.6**	Any changes to the essential function(s) or the threat it faces triggers a review of policies, processes and procedures.

[3.2]B1.a.A.6	Your systems are designed so that they remain secure even when user security policies, processes and procedures are not always followed.	**[4.0]B1.a.A.7**	Your systems are designed so that they remain secure even when user security policies, processes and procedures are not always followed.
[3.2]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.**		
[3.2]B2.a	**Identity Verification, Authentication and Authorisation** You robustly verify, authenticate and authorise access to the network and information systems supporting your essential function(s).	**[4.0]B2.a**	**Identity Verification, Authentication and Authorisation** You robustly verify, authenticate and authorise access to network and information systems supporting your essential function(s).
[3.2]B2.a.NA.4	The number of authorised users and systems that have access to network and information systems are not limited to the minimum necessary.	**[4.0]B2.a.NA.4**	The number of authorised users and systems that have access to network and information systems is not limited to the minimum necessary to support your essential function(s).
[3.2]B2.a.PA.2	All authorised users and systems with access to network or information systems on which your essential function(s) depends are individually identified and authenticated.	**[4.0]B2.a.PA.2**	All authorised users and systems with access to network and information systems supporting your essential function(s) are individually identified and authenticated.
[3.2]B2.a.PA.3	The number of authorised users and systems that have access to essential function(s) network and information systems is limited to the minimum necessary.	**[4.0]B2.a.PA.3**	The number of authorised users and systems that have access to network and information systems is limited to the minimum necessary to support your essential function(s).
[3.2]B2.a.PA.4	You use additional authentication mechanisms, such as multi-factor (MFA), for privileged access to all network and information systems that operate or support your essential function(s).	**[4.0]B2.a.PA.4**	You use additional strong authentication mechanisms, such as multi-factor authentication (MFA), for privileged access to all network and information systems that operate or support your essential function(s).
[3.2]B2.a.A.3	The number of authorised users and systems that have access to all network and information systems supporting the essential function(s) is limited to the minimum necessary.	**[4.0]B2.a.A.3**	The number of authorised users and systems that have access to network and information systems is limited to the minimum necessary to support your essential function(s).
[3.2]B2.a.A.4	You use additional authentication mechanisms, such as multi-factor (MFA), for all user access, including remote access, to all network and information systems that operate or support your essential function(s).	**[4.0]B2.a.A.4**	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).
[3.2]B2.c	**Privileged User Management** You closely manage privileged user access to network and information systems supporting your essential function(s).		

[3.2]B2.c.NA.5	Privileged user access to your essential function(s) is via generic, shared or default name accounts.	**[4.0]B2.c.NA.5**	Privileged user access to network and information systems supporting your essential function(s) is via generic, shared or default name accounts.
[3.2]B2.c.PA.1	All privileged user access to network and information systems supporting your essential function(s) requires strong authentication, such as multi-factor (MFA).	**[4.0]B2.c.PA.1**	All privileged user access to network and information systems supporting your essential function(s) requires strong authentication, such as multi-factor authentication (MFA).
[3.2]B2.d	**Identity and Access Management (IdAM)** You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting your essential function(s).	**[4.0]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).
[3.2]B2.d.A.3	All user, device and systems access to the systems supporting the essential function(s) is logged and monitored.	**[4.0]B2.d.A.3**	All user, device and systems access to network and information systems supporting your essential function(s) is logged and monitored.
[3.2]B2.d.A.5	Attempts by unauthorised users, devices or systems to connect to the systems supporting the essential function(s) are alerted, promptly assessed and investigated.	**[4.0]B2.d.A.5**	Attempts by unauthorised users, devices or systems to connect to network and information systems supporting your essential function(s) are alerted, promptly assessed and investigated.
[3.2]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 an attacker, such as design details of network and information systems.**	**[4.0]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.**
[3.2]B3.a	**Understanding Data** You have a good understanding of data important to the operation of your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, 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).	**[4.0]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).
[3.2]B3.a.NA.1	You have incomplete knowledge of what data is used by and produced in the operation of the essential function(s).	**[4.0]B3.a.NA.1**	You have incomplete knowledge of what data is used by and produced in the operation of network and information systems supporting your essential function(s).

[3.2]B3.a.NA.2	You have not identified the important data on which your essential function(s) relies.	**[4.0]B3.a.NA.2**	You have not identified the important data on which network and information systems supporting your essential function(s) relies.
[3.2]B3.a.NA.3	You have not identified who has access to data important to the operation of the essential function(s).	**[4.0]B3.a.NA.3**	You have not identified who has access to data important to the operation of network and information systems supporting your essential function(s).
[3.2]B3.a.PA.1	You have identified and catalogued all the data important to the operation of the essential function(s), or that would assist an attacker	**[4.0]B3.a.PA.1**	You have identified and catalogued all the data important to the operation of network and information systems supporting your essential function(s), or that would assist a threat actor.
[3.2]B3.a.PA.2	You have identified and catalogued who has access to the data important to the operation of the essential function(s)	**[4.0]B3.a.PA.2**	You have identified and catalogued who has access to the data important to the operation of network and information systems supporting your essential function(s).
[3.2]B3.a.PA.3	You regularly review location, transmission, quantity and quality of data important to the operation of the essential function(s).	**[4.0]B3.a.PA.3**	You regularly review location, transmission, quantity and quality of data important to the operation of network and information systems supporting your essential function(s).
[3.2]B3.a.PA.4	You have identified all mobile devices and media that hold data important to the operation of the essential function(s).	**[4.0]B3.a.PA.4**	You have identified all mobile devices and media that hold data important to the operation of network and information systems supporting your essential function(s).
[3.2]B3.a.PA.5	You understand and document the impact on your essential function(s) of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data.	**[4.0]B3.a.PA.5**	You understand and document the impact on your essential function(s) of all relevant scenarios, including unauthorised data access, uncontrolled release, modification or deletion, or when authorised users are unable to appropriately access this data.
[3.2]B3.a.A.1	You have identified and catalogued all the data important to the operation of the essential function(s), or that would assist an attacker.	**[4.0]B3.a.A.1**	You have identified and catalogued all the data important to the operation of network and information systems supporting your essential function(s), or that would assist a threat actor.
[3.2]B3.a.A.2	You have identified and catalogued who has access to the data important to the operation of the essential function(s).	**[4.0]B3.a.A.2**	You have identified and catalogued who has access to the data important to the operation of network and information systems supporting your essential function(s).
[3.2]B3.a.A.3	You maintain a current understanding of the location, quantity and quality of data important to the operation of the essential function(s).	**[4.0]B3.a.A.3**	You maintain a current understanding of the location, quantity and quality of data important to the operation of network and information systems supporting your essential function(s).
[3.2]B3.a.A.5	You have identified all mobile devices and media that may hold data important to the operation of the essential function(s).	**[4.0]B3.a.A.5**	You have identified all mobile devices and media that may hold data important to the operation of network and information systems supporting your essential function(s).

[3.2]B3.a.A.6	You maintain a current understanding of the data links used to transmit data that is important to your essential function(s).	**[4.0]B3.a.A.6**	You maintain a current understanding of the data links used to transmit data that is important to network and information systems supporting your essential function(s).
[3.2]B3.a.A.8	You understand and document the impact on your essential function(s) of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data.	**[4.0]B3.a.A.8**	You understand and document the impact on your essential function(s) of all relevant scenarios, including unauthorised data access, uncontrolled release, modification or deletion, or when authorised users are unable to appropriately access this data.
[3.2]B3.b	**Data in Transit** You have protected the transit of data important to the operation of your essential function(s). This includes the transfer of data to third parties.	**[4.0]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.
[3.2]B3.b.PA.2	You apply appropriate technical means (e.g. cryptography) to protect data that travels over non-trusted or openly accessible carriers, but you have limited or no confidence in the robustness of the protection applied.	**[4.0]B3.b.PA.2**	You apply appropriate physical and / or technical means (e.g. cryptography) to protect data that travels over non-trusted or openly accessible carriers, but you have limited or no confidence in the robustness of the protection applied.
[3.2]B3.b.A.2	You apply appropriate physical and / or technical means to protect data that travels over non-trusted or openly accessible carriers, with justified confidence in the robustness of the protection applied.	**[4.0]B3.b.A.2**	You apply appropriate physical and / or technical means (e.g. cryptography) to protect data that travels over non-trusted or openly accessible carriers, with justified confidence in the robustness of the protection applied.
[3.2]B3.c	**Stored Data** You have protected stored soft and hard copy data important to the operation of your essential function(s).	**[4.0]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).
[3.2]B3.c.NA.1	You have no, or limited, knowledge of where data important to the operation of the essential function(s) is stored.	**[4.0]B3.c.NA.1**	You have no, or limited, knowledge of where data important to the operation of network and information systems supporting your essential function(s) is stored.
[3.2]B3.c.NA.2	You have not protected vulnerable stored data important to the operation of the essential function(s) in a suitable way.	**[4.0]B3.c.NA.2**	You have not protected vulnerable stored data important to the operation of network and information systems supporting your essential function(s) in a suitable way.
[3.2]B3.c.PA.1	All copies of data important to the operation of 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.	**[4.0]B3.c.PA.1**	All copies of data important to the operation of network and information systems supporting your essential function(s) are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy.

[3.2]B3.c.PA.4	You have suitable, secured backups of data to allow the operation of the essential function(s) to continue should the original data not be available. This may include offline or segregated backups, or appropriate alternative forms such as paper copies.	**[4.0]B3.c.PA.4**	You have suitable, secured backups of data to allow the operation of network and information systems supporting your essential function(s) to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.
[3.2]B3.c.A.1	All copies of data important to the operation of 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.	**[4.0]B3.c.A.1**	All copies of data important to the operation of network and information systems supporting your essential function(s) are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy.
[3.2]B3.c.A.4	You have suitable, secured backups of data to allow the operation of the essential function(s) to continue should the original data not be available. This may include offline or segregated backups, or appropriate alternative forms such as paper copies.	**[4.0]B3.c.A.4**	You have suitable, secured backups of data to allow the operation of network and information systems supporting your essential function(s) to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.
[3.2]B3.d	**Mobile Data** You have protected data important to the operation of your essential function(s) on mobile devices.	**[4.0]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).
[3.2]B3.d.NA.1	You don't know which mobile devices may hold data important to the operation of the essential function(s).	**[4.0]B3.d.NA.1**	You do not know which mobile devices may hold data important to the operation of network and information systems supporting your essential function(s).
[3.2]B3.d.NA.2	You allow data important to the operation of the essential function(s) to be stored on devices not managed by your organisation, or to at least equivalent standard.	**[4.0]B3.d.NA.2**	You allow data important to the operation of network and information systems supporting your essential function(s) to be stored on devices not managed by your organisation, or to at least equivalent standard.
[3.2]B3.d.PA.1	You know which mobile devices hold data important to the operation of the essential function(s).	**[4.0]B3.d.PA.1**	You know which mobile devices hold data important to the operation of network and information systems supporting your essential function(s).
[3.2]B3.d.PA.2	Data important to the operation of the essential function(s) is stored on mobile devices only when they have at least the security standard aligned to your overarching security policies.	**[4.0]B3.d.PA.2**	Data important to the operation of network and information systems supporting your essential function(s) is stored on mobile devices only when they have at least the security standard aligned to your overarching security policies.
[3.2]B3.d.A.1	Mobile devices that hold data that is important to the operation of the 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.	**[4.0]B3.d.A.1**	Mobile devices that hold data that is important to the operation of network and information systems supporting your essential function(s) are catalogued, are under your organisation's control and configured

			according to best practice for the platform, with appropriate technical and procedural policies in place.
[3.2]B3.d.A.2	Your organisation can remotely wipe all mobile devices holding data important to the operation of the essential function(s).	**[4.0]B3.d.A.2**	Your organisation can remotely wipe all mobile devices holding data important to the operation of network and information systems supporting your essential function(s).
[3.2]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 your essential function(s).	**[4.0]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).
[3.2]B3.e.NA.1	Some or all devices, equipment or removable media that hold data important to the operation of the essential function(s) are reused or disposed of without sanitisation of that data.	**[4.0]B3.e.NA.1**	Some or all devices, equipment or removable media that hold data important to the operation of network and information systems supporting your essential function(s) are reused or disposed of without sanitisation of that data.
[3.2]B3.e.PA.1	Data important to the operations of the essential function(s) is removed from all devices, equipment and removable media before reuse and / or disposal.	**[4.0]B3.e.PA.1**	Data important to the operations of network and information systems supporting your essential function(s) is removed from all devices, equipment and removable media before reuse and / or disposal.
[3.2]B3.e.A.1	You catalogue and track all devices that contain data important to the operation of the essential function(s) (whether a specific storage device or one with integral storage).	**[4.0]B3.e.A.1**	You catalogue and track all devices that contain data important to the operation of network and information systems supporting your essential function(s) (whether a specific storage device or one with integral storage).
[3.2]B3.e.A.2	Data important to the operation of the essential function(s) is removed from all devices, equipment and removable media before reuse and / or disposal using an assured product or service.	**[4.0]B3.e.A.2**	Data important to the operation of network and information systems supporting your essential function(s) is removed from all devices, equipment and removable media before reuse and / or disposal using an assured product or service.
[3.2]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 attackers to compromise networks and systems.**	**[4.0]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.**

[3.2]B4.a	**Secure by Design** You design security into the network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential function(s) should not be impacted by the exploitation of any single vulnerability.		
[3.2]B4.a.NA.1	Systems essential to the operation of the essential function(s) are not appropriately segregated from other systems.	**[4.0]B4.a.NA.1**	Network and information systems supporting the operation of the essential function(s) are not appropriately segregated from other systems.
[3.2]B4.a.NA.2	Internet access is available from network and information systems supporting your essential function(s).	**[4.0]B4.a.NA.2**	Internet services, such as browsing and email, are accessible from network and information systems supporting your essential function(s).
[3.2]B4.a.PA.1	You employ appropriate expertise to design network and information systems.	**[4.0]B4.a.PA.1**	You employ appropriate expertise to design network and information systems supporting your essential function(s).
[3.2]B4.a.A.1	You employ appropriate expertise to design network and information systems.	**[4.0]B4.a.A.1**	You employ appropriate expertise to design network and information systems supporting your essential function(s).
[3.2]B4.a.A.5	Content-based attacks are mitigated for all inputs to network and information systems that affect the essential function(s) (e.g. via transformation and inspection).	**[4.0]B4.a.A.5**	Content-based attacks are mitigated for all inputs to network and information systems that affect the essential function(s) (e.g. via transformation and inspection / sanitisation and validation).
		[4.0]B4.a.A.6 (New)	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).
[3.2]B4.b	**Secure Configuration** You securely configure the network and information systems that support the operation of your essential function(s).	**[4.0]B4.b**	**Secure Configuration** You securely configure network and information systems that support the operation of your essential function(s).
[3.2]B4.b.NA.1	You haven't identified the assets that need to be carefully configured to maintain the security of the essential function(s).	**[4.0]B4.b.NA.1**	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).
		[4.0]B4.b.NA.6 (New)	Standard users are able to change settings that would adversely impact the security of network and information systems supporting your essential function(s).

[3.2]B4.b.PA.1	You have identified and documented the assets that need to be carefully configured to maintain the security of the essential function(s).	**[4.0]B4.b.PA.1**	You have identified and documented the assets that need to be carefully configured to maintain the security of network and information systems supporting your essential function(s).
[3.2]B4.b.PA.4	Changes and adjustments to security configuration at security boundaries with the network and information systems supporting your essential function(s) are approved and documented.	**[4.0]B4.b.PA.4**	Changes and adjustments to security configurations at security boundaries of network and information systems supporting your essential function(s) are approved and documented.
[3.2]B4.b.PA.6	Generic, shared, default name and built-in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed.	**[4.0]B4.b.PA.6**	Generic, shared, default name and built-in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed. Service accounts are appropriately protected.
[3.2]B4.b.A.1	You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of the essential function(s).	**[4.0]B4.b.A.1**	You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of network and information systems supporting your essential function(s).
[3.2]B4.b.A.3	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.	**[4.0]B4.b.A.3**	You closely and effectively manage changes in your environment, ensuring that network and information systems configurations are secure and documented.
[3.2]B4.b.A.6	Standard users are not able to change settings that would impact security or the business operation.	**[4.0]B4.b.PA.7**	Standard users are not able to change settings that would adversely impact the security of network and information systems supporting your essential function(s).
[3.2]B4.b.A.7	If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated.	**[4.0]B4.b.A.6**	If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated.
[3.2]B4.b.A.8	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.	**[4.0]B4.b.A.7**	Generic, shared, default name and built-in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed. Service accounts are appropriately protected.
[3.2]B4.d	**Vulnerability Management** You manage known vulnerabilities in network and information systems to prevent adverse impact on your essential function(s).		
[3.2]B4.d.NA.1	You do not understand the exposure of your essential function(s) to publicly-known vulnerabilities.	**[4.0]B4.d.NA.1**	You do not understand the exposure of network and information systems supporting your essential function(s) to publicly-known vulnerabilities.

[3.2]B4.d.NA.3	You have not recently tested to verify your understanding of the vulnerabilities of the network and information systems that support your essential function(s).	**[4.0]B4.d.NA.3**	You have not recently tested to verify your understanding of the vulnerabilities of network and information systems that support your essential function(s).
[3.2]B4.d.PA.1	You maintain a current understanding of the exposure of your essential function(s) to publicly-known vulnerabilities.	**[4.0]B4.d.PA.1**	You maintain a current understanding of the exposure of network and information systems supporting your essential function(s) to publicly-known vulnerabilities.
[3.2]B4.d.PA.2	Announced vulnerabilities for all software packages, network and information systems used to support your essential function(s) are tracked, prioritised and externally exposed vulnerabilities are mitigated (e.g. by patching) promptly.	**[4.0]B4.d.PA.2**	Announced vulnerabilities for all software packages used in network and information systems supporting your essential function(s) are tracked, prioritised and externally exposed vulnerabilities are mitigated (e.g. by patching) promptly.
[3.2]B4.d.PA.5	You regularly test to fully understand the vulnerabilities of the network and information systems that support the operation of your essential function(s).	**[4.0]B4.d.PA.5**	You regularly test to fully understand the vulnerabilities of network and information systems that support the operation of your essential function(s).
[3.2]B4.d.A.1	You maintain a current understanding of the exposure of your essential function(s) to publicly-known vulnerabilities.	**[4.0]B4.d.A.1**	You maintain a current understanding of the exposure of network and information systems supporting your essential function(s) to publicly-known vulnerabilities.
[3.2]B4.d.A.2	Announced vulnerabilities for all software packages, network and information systems used to support your essential function(s) are tracked, prioritised and mitigated (e.g. by patching) promptly.	**[4.0]B4.d.A.2**	Announced vulnerabilities for all software packages used in network and information systems supporting your essential function(s) are tracked, prioritised and mitigated (e.g. by patching) promptly.
[3.2]B4.d.A.3	You regularly test to fully understand the vulnerabilities of the network and information systems that support the operation of your essential function(s) and verify this understanding with third-party testing.	**[4.0]B4.d.A.3**	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.
[3.2]B4.d.A.4	You maximise the use of supported software, firmware and hardware in network and information systems supporting your essential function(s).	**[4.0]B4.d.A.4**	You actively maximise the use of supported software, firmware and hardware in network and information systems supporting your essential function(s).
[3.2]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 essential functions.**	**[4.0]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).**
[3.2]B5.a	**Resilience Preparation** You are prepared to restore the operation of your essential function(s) following adverse impact.	**[4.0]B5.a**	**Resilience Preparation** You are prepared to restore the operation of your essential function(s) following adverse impact to network and information systems.

[3.2]B5.a.NA.1	You have limited understanding of all the elements that are required to restore operation of the essential function(s).	**[4.0]B5.a.NA.1**	You have limited understanding of all the elements that are required to restore operation of network and information systems supporting your essential function(s).
[3.2]B5.a.PA.1	You know all network and information systems, and underlying technologies, that are necessary to restore the operation of the essential function(s) and understand their interdependence.	**[4.0]B5.a.PA.1**	You know all network and information systems, and underlying technologies, that are necessary to restore the operation of your essential function(s) and understand their interdependence.
[3.2]B5.b	**Design for Resilience** You design the 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.	**[4.0]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.
[3.2]B5.b.NA.2	Internet services, such as browsing and email, are accessible from network and information systems supporting the essential function(s).	**[4.0]B5.b.NA.2**	Internet services, such as browsing and email, are accessible from network and information systems supporting your essential function(s).
[3.2]B5.b.PA.1	Network and information systems supporting the operation of your essential function(s) are logically separated from your business systems (e.g. they reside on the same network as the rest of the organisation but within a DMZ). Internet services are not accessible from network and information systems supporting the essential function(s).	**[4.0]B5.b.PA.1**	Network and information systems supporting the operation of your essential function(s) are logically separated from your business systems (e.g. they reside on the same network as the rest of the organisation but within a DMZ).
		[4.0]B5.b.PA.2 (divided from) [3.2]B5.b.PA.1	Internet services, such as browsing and email are not accessible from network and information systems supporting your essential function(s).
[3.2]B5.b.PA.2	Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.	**[4.0]B5.b.PA.3**	Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.
[3.2]B5.b.A.1	Network and information systems supporting the operation of your essential function(s) are segregated from other business and external systems by appropriate technical and physical means (e.g. separate network and system infrastructure with independent user administration). Internet services are not accessible from network and information systems supporting the essential function(s).	**[4.0]B5.b.A.1**	Network and information systems supporting the operation of your essential function(s) are segregated from other business and external systems by appropriate technical and physical means (e.g. separate network and system infrastructure with independent user administration).
		[4.0]B5.b.A.2 (divided from) [3.2]B5.b.A.1	Internet services, such as browsing and email, are not accessible from network and information systems supporting your essential function(s).
[3.2]B5.b.A.2	You have identified and mitigated all resource limitations (e.g. bandwidth limitations and single network paths).	**[4.0]B5.b.A.3**	You have identified and mitigated all resource limitations (e.g. bandwidth limitations and single network paths).

[3.2]B5.b.A.3	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).	**[4.0]B5.b.A.4**	You have identified and mitigated any geographical constraints or weaknesses. (e.g. systems that your essential function(s) depends upon are replicated in another location, important network connectivity has alternative physical paths and service providers).
[3.2]B5.b.A.4	You review and update assessments of dependencies, resource and geographical limitations and mitigations when necessary.	**[4.0]B5.b.A.5**	You review and update assessments of dependencies, resource and geographical limitations and mitigations when necessary.
[3.2]B5.c	**Backups** You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).	**[4.0]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.
[3.2]B5.c.PA.1	You have appropriately secured backups (including data, configuration information, software, equipment, processes and knowledge). These backups will be accessible to recover from an extreme event.	**[4.0]B5.c.PA.1**	You have appropriately secured backups (including data, configuration information, software, equipment, processes and knowledge). These backups will be accessible to recover from an extreme event including ransomware attack.
[3.2]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 essential functions.**	**[4.0]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).**
[3.2]B6.a	**Cyber Security Culture** You develop and maintain a positive cyber security culture.	**[4.0]B6.a**	**Cyber Security Culture** You develop and maintain a positive cyber security culture and a shared sense of responsibility.
[3.2]B6.a.NA.1	People in your organisation don't understand what they contribute to the cyber security of the essential function(s).	**[4.0]B6.a.NA.1**	People in your organisation do not understand what they contribute to the cyber security of network and information systems supporting your essential function(s).
[3.2]B6.a.NA.2	People in your organisation don’t know how to raise a concern about cyber security.	**[4.0]B6.a.NA.2**	People in your organisation do not know how to raise a concern about cyber security.
[3.2]B6.a.NA.4	Your organisation's approach to cyber security is perceived by staff as hindering the business of the organisation.	**[4.0]B6.a.NA.4**	Your organisation's approach to cyber security is perceived by staff as hindering the business of the organisation and may encourage poor security behaviours.
		[4.0]B6.a.NA.5 (New)	Formal or informal incentives and rewards conflict with the promotion of positive security outcomes.

[3.2]B6.a.PA.2	All people in your organisation understand the contribution they make to the essential function(s) cyber security.	**[4.0]B6.a.PA.2**	All people in your organisation understand the contribution they make to the cyber security of network and information systems supporting your essential functions(s).
		[4.0]B6.a.PA.4 (New)	You identify and address issues that inhibit people from behaving in a manner that supports your intended cyber security outcomes.
[3.2]B6.a.A.6	People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.	**[4.0]B6.a.A.6**	People across your organisation collaborate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.
[3.2]B6.b	**Cyber Security Training** The people who support the operation of your essential function(s) are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed.	**[4.0]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.
		[4.0]B6.b.NA.4 (New)	Training is used as a “silver bullet” for all user security behaviours.
		[4.0]B6.b.NA.5 (New)	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.
		[4.0]B6.b.NA.6 (New)	Training materials contain out of date or contradictory information, or information that conflicts with other policies, processes or procedures.
[3.2]C	**Detecting Cyber Security Events** **Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential function(s).**	**[4.0]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).**
[3.2]C1	**Security Monitoring** The organisation monitors the security status of the network and information systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.	**[4.0]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.
[3.2]C1.a	**Monitoring Coverage**	**[4.0]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

	The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).		adversely affect the security or resiliency of network and information system(s) supporting the operation of your essential function(s).
[3.2]C1.a.NA.1	Data relating to the security and operation of your essential function(s) is not collected.	**[4.0]C1.a.NA.1**	Data relating to the security and operation of network and information systems supporting your essential function(s) is not collected.
[3.2]C1.a.NA.2	You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on 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).	**[4.0]C1.c.NA.4**	You do not confidently detect the presence of IoCs on network and information systems supporting your essential function(s), such as known malicious command and control signatures (e.g. because applying the indicator is difficult or your log data is not sufficiently detailed).
[3.2]C1.a.NA.3	You are not able to audit the activities of users in relation to your essential function(s).	**[4.0]C1.a.NA.2**	You are not able to audit the activities of users and systems in relation to network and information systems supporting your essential function(s).
[3.2]C1.a.NA.4	You do not capture any traffic crossing your network boundary including as a minimum IP connections.	**[4.0]C1.a.NA.3**	You do not monitor traffic crossing your network boundary.
		[4.0]C1.a.NA.8 (New)	You do not understand where log data is stored or how long it should be stored for.
		[4.0]C1.a.NA.9 (New)	You have no way of ensuring log data is being captured as expected and available when needed.
[3.2]C1.a.PA.1	Data relating to the security and operation of some areas of your essential function(s) is collected but coverage is not comprehensive.	**[4.0]C1.a.PA.1**	Data relating to the security and operation of some areas of network and information systems supporting your essential function(s) is collected but coverage is not comprehensive.
[3.2]C1.a.PA.2	You easily detect the presence or absence of IoCs on your essential function(s), such as known malicious command and control signatures.	**[4.0]C1.c.PA.1**	You easily detect the presence of Indicators of Compromise (IoCs) on network and information systems supporting your essential function(s), such as known malicious command and control signatures.
[3.2]C1.a.PA.3	Some user monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour.	**[4.0]C1.a.PA.2**	Some user and system monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour.
[3.2]C1.a.PA.4	You monitor traffic crossing your network boundary (including IP address connections as a minimum).	**[4.0]C1.a.PA.3**	You monitor traffic crossing your network boundary (including IP address connections as a minimum).
		[4.0]C1.a.PA.7 (New)	You ensure log data is available for analysis when needed.

[3.2]C1.a.A.1	Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents that could affect the operation of your essential function(s) (e.g. presence of malware, malicious emails, user policy violations).	**[4.0]C1.a.A.1**	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).
[3.2]C1.a.A.2	Your monitoring data provides enough detail to reliably detect security incidents that could affect the operation of your essential function(s).	**[4.0]C1.a.A.2**	Your monitoring data provides enough detail to promptly and reliably detect security events, incidents and support investigations. This is reviewed regularly and after a significant security event.
[3.2]C1.a.A.3	You easily detect the presence or absence of IoCs on your essential function(s), such as known malicious command and control signatures.	**[4.0]C1.c.A.1**	You easily detect the presence of Indicators of Compromise (IoCs) on network and information systems supporting your essential function(s), such as known malicious command and control signatures, as well as abnormalities or behaviours indicative of adverse activity.
[3.2]C1.a.A.4	Extensive monitoring of user activity in relation to the operation of your essential function(s) enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.	**[4.0]C1.a.A.3**	Extensive monitoring of user and system activity in relation to network and information systems that support your essential function(s) enables you to promptly detect policy violations, suspicious or undesirable user and system behaviour, deviations from normal / routine behaviour or abnormalities indicative of adverse activity.
[3.2]C1.a.A.5	You have extensive monitoring coverage that includes host-based monitoring and network gateways.	**[4.0]C1.a.A.4**	Your logging and monitoring capability includes host-based and network monitoring.
[3.2]C1.a.A.6	All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.	**[4.0]C1.a.A.5**	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.
		[4.0]C1.a.A.9 (New)	You regularly review the data sources and tools included in your logging and monitoring strategy to ensure it remains effective.
[3.2]C1.b	**Securing Logs** You hold log data securely and grant appropriate access only to accounts with business a need. No system or user should ever need to modify or delete master copies of log data within an agreed retention period, after which it should be deleted.	**[4.0]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.
[3.2]C1.b.NA.1	It is possible for log data to be easily edited or deleted by unauthorised users or malicious attackers.	**[4.0]C1.b.NA.1**	It is possible for log data to be easily edited or deleted by unauthorised users / systems or attackers.

[3.2]C1.b.NA.2	There is no controlled list of the users and systems that can view and query log data.	**[4.0]C1.b.NA.2**	There is no control of the users and systems that can access log data.
[3.2]C1.b.NA.4	There is no policy for accessing log data.	**[4.0]C1.b.NA.4**	There are no policies covering access to log data.
[3.2]C1.b.NA.5	Log data is not synchronised, using an accurate common time source.	**[4.0]C1.a.NA.4**	Log data cannot be synchronised using an accurate common time source.
[3.2]C1.b.PA.1	Only authorised staff can view log data for investigations.	**[4.0]C1.b.PA.1**	Only authorised users and systems can access log data.
[3.2]C1.b.PA.2 (Merged with [3.2]C1.b.A.5)	Authorised users and systems can appropriately access log data.	**[4.0]C1.b.A.1**	Appropriate access to log data is limited to those users and systems with a business need.
[3.2]C1.b.PA.3	There is some monitoring of access to log data (e.g. copying, deleting, modifying or viewing).	**[4.0]C1.b.PA.2**	There is some monitoring of access to log data (e.g. copying, deleting or modification, or even viewing).
		[4.0]C1.b.PA.3 (New)	You have defined and implemented retention periods for log data.
[3.2]C1.b.A.1	The integrity of log data is protected, or any modification is detected and attributed.	**[4.0]C1.b.A.5**	The integrity of log data is protected, verified and any modification, including deletion is detected and attributed.
[3.2]C1.b.A.2	The logging architecture has mechanisms, policies, processes and procedures to ensure that it can protect itself from threats comparable to those it is trying to identify. This includes protecting the essential function(s) itself, and the data within it.	**[4.0]C1.b.A.2**	The logging architecture has mechanisms, policies, processes and procedures to ensure that it can protect itself from threats comparable to those that it is trying to identify. This includes protecting the function itself and the data within it.
[3.2]C1.b.A.4	Log data is synchronised, using an accurate common time source, so that separate datasets can be correlated in different ways.	**[4.0]C1.a.A.6**	Log datasets are synchronised including using an accurate common time source so that separate datasets can be correlated in appropriate ways.
[3.2]C1.b.A.5 (Merged with [3.2]C1.b.PA.2)	Access to log data is limited to those with business need and no others.	**[4.0]C1.b.A.1**	Appropriate access to log data is limited to those users and systems with a business need.
[3.2]C1.b.A.6	All actions involving all log data (e.g. copying, deleting, modifying or viewing) can be traced back to a unique user.	**[4.0]C1.b.A.4**	All actions involving log data (e.g. copying, deleting, modification, or even viewing) can be traced back to a unique user or system.
[3.2]C1.b.A.7	Legitimate reasons for accessing log data are given in use policies.	**[4.0]C1.b.PA.4**	You have given legitimate reasons for accessing log data in your policies.

[3.2]C1.c	**Generating Alerts** Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.	[4.0]C1.c	**Generating Alerts** Evidence of potential security incidents contained in your monitoring data is reliably identified and where appropriate triggers alerts.
[3.2]C1.c.NA.1	Alerts from third party security software are not investigated (e.g. Anti-Virus (AV) providers).	**[4.0]C1.d.NA.1**	You do not triage alerts from your detection security technologies (e.g. AV, IDS).
[3.2]C1.c.NA.2	Logs are distributed across devices with no easy way to access them other than manual login or physical action	**[4.0]C1.a.NA.5**	Logs are stored in locations where they are not readily available to authorised users and systems.
[3.2]C1.c.NA.3	The resolution of alerts to a network asset or system is not performed.	**[4.0]C1.c.NA.3**	The enrichment of security alerts within network and information systems supporting your essential function(s) cannot be performed.
[3.2]C1.c.NA.4	Security alerts relating to essential function(s) are not prioritised.	**[4.0]C1.c.NA.2**	Security alerts relating to network and information systems supporting your essential function(s) are not prioritised.
[3.2]C1.c.NA.5	Logs are reviewed infrequently.	**[4.0]C1.c.NA.6**	Logs are monitored infrequently.
[3.2]C1.c.PA.1	Alerts from third party security software are investigated, and action taken.	**[4.0]C1.d.PA.1**	You investigate and triage alerts from some security tools and take action.
[3.2]C1.c.PA.2	Some, but not all, log data can be easily queried with search tools to aid investigations.	**[4.0]C1.a.PA.4**	Some but not all log datasets can be easily queried with search tools to aid in investigations.
[3.2]C1.c.PA.3	The resolution of alerts to a network asset or system is performed regularly.	**[4.0]C1.c.PA.4**	The enrichment of alerts within network and information systems supporting your essential function(s) is performed but not as part of the original alert.
[3.2]C1.c.PA.4	Security alerts relating to some essential function(s) are prioritised.	**[4.0]C1.c.PA.3**	Security alerts relating to network and information systems that support your essential function(s) are prioritised.
[3.2]C1.c.PA.5	Logs are reviewed at regular intervals.	**[4.0]C1.c.PA.9**	Logs are monitored at regular intervals.
		[4.0]C1.c.PA.5 (New)	Detections and alerting rely on off the shelf tooling without customisation or users reporting events and potential incidents.

		[4.0]C1.c.PA.6 (New)	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.
		[4.0]C1.c.PA.7 (New)	Where appropriate, detections and alerting result in automated actions being taken. (e.g. malware identified by AV is quarantined).
		[4.0]C1.c.PA.8 (New)	You monitor on an irregular basis for user or system abnormalities indicative of adverse activity.
[3.2]C1.c.A.1	Log data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.	**[4.0]C1.a.A.7**	You enrich log data with other network and information systems data to provide a more comprehensive picture of actions and behaviours.
[3.2]C1.c.A.2 (Removed)	A wide range of signatures and indicators of compromise is used for investigations of suspicious activity and alerts.		
[3.2]C1.c.A.3	Alerts can be easily resolved to network assets using knowledge of networks and systems. The resolution of these alerts is performed in almost real time.	**[4.0]C1.c.A.4**	Alerts are routinely enriched within network and information systems supporting your essential function(s). The enrichment of these alerts is performed in almost real time and as part of the original alert.
[3.2]C1.c.A.4	Security alerts relating to all essential function(s) are prioritised and this information is used to support incident management.	**[4.0]C1.c.A.3**	Security alerts relating to all network and information systems supporting your essential function(s) are prioritised and this information is used to support incident management.
[3.2]C1.c.A.5	Logs are reviewed almost continuously, in real time.	**[4.0]C1.c.A.9**	Logs are monitored continuously in near real time.
[3.2]C1.c.A.6	Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.	**[4.0]C1.c.A.5**	Alerts and the underlying detections are regularly reviewed and tested to ensure they are generated promptly and reliably, and it is possible to distinguish genuine security incidents from false alarms.
		[4.0]C1.c.A.6 (New)	Alerts and the underlying detection rules are customisable and tuned to reduce false positives as well as optimising responses.
		[4.0]C1.c.A.7 (New)	Detections and alerting may use off the shelf tooling and rules as well as custom tooling and / or rules.
[3.2]C1.d	**Identifying Security Incidents** You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.	**[4.0]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.

[3.2]C1.d.NA.1	Your organisation has no sources of threat intelligence.	**[4.0]C1.f.NA.1**	Your organisation has no sources of threat intelligence.
[3.2]C1.d.NA.2	You do not apply updates in a timely way, after receiving them (e.g. AV signature updates, other threat signatures or Indicators of Compromise (IoCs)).	**[4.0]C1.c.NA.1**	You do not apply updates to your detection security technologies in a timely way, after receiving them (e.g. AV signature updates, other threat signatures or Indicators of Compromise (IoCs)).
[3.2]C1.d.NA.3	You do not receive signature updates for all protective technologies such as AV and IDS or other software in use.	**[4.0]C1.f.NA.6**	You do not receive updates for all your detection security technologies (e.g. AV, IDS).
[3.2]C1.d.NA.4	You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	**[4.0]C1.f.NA.2**	You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.
		[4.0]C1.d.NA.2 (New)	You do not categorise alerts and incidents by type and priority / severity level.
		[4.0]C1.d.NA.3 (New)	You do not have Standard Operating Procedures (SOPs) / Playbooks / Runbooks available for use during triage.
		[4.0]C1.d.NA.4 (New)	You do not keep records of triage performed.
		[4.0]C1.d.NA.5 (New)	You do not have a sufficient understanding of normal user or system behaviour to make effective decisions within triage.
[3.2]C1.d.PA.1	Your organisation uses some threat intelligence services, but you don't necessarily choose sources or providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based infoshare, ICS software vendors, anti-virus providers, specialist threat intel firms, special interest groups).	**[4.0]C1.f.PA.2**	Your organisation may use threat intelligence services, but you do not necessarily choose sources or providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based infoshare, software vendors, anti-virus providers, specialist threat intel firms, special interest groups).
[3.2]C1.d.PA.2 (Merged with [3.2]C1.d.A.3)	You receive updates for all your signature based protective technologies (e.g. AV, IDS).	**[4.0]C1.f.PA.4**	You receive regular updates for all your detection security technologies (e.g. AV, IDS).
[3.2]C1.d.PA.3	You apply some updates, signatures and IoCs in a timely way.	**[4.0]C1.c.PA.2**	You apply some updates, new signatures and IoCs in a timely way.
[3.2]C1.d.PA.4	You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems).	**[4.0]C1.f.PA.1**	You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security incidents).

		C1.d.PA.2 (New)	You have created, made available and use when appropriate Standard Operating Procedures (SOPs) / Playbooks / Runbooks covering the most common use cases. These are regularly reviewed to ensure they remain effective.
		C1.d.PA.3 (New)	You perform some triage and actions taken by monitoring and detection personnel are recorded.
		C1.d.PA.4 (New)	You categorise alerts and incidents by type and priority / severity level.
		C1.d.PA.5 (New)	Your understanding of normal user or system behaviour informs your decision making within triage.
[3.2]C1.d.A.1	You have selected threat intelligence sources or services using risk-based and threat informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong anti-virus providers, sector and community-based infoshare, special interest groups).	**[4.0]C1.f.A.2**	When using threat intelligence feeds, these have been selected using risk-based and threat-informed decisions based on your business needs and sector.
[3.2]C1.d.A.2	You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.	**[4.0]C1.c.A.2**	You apply all updates, new signatures and IoCs promptly.
[3.2]C1.d.A.3 (Merged with [3.2]C1.d.PA.2)	You receive signature updates for all your protective technologies (e.g. AV, IDS).	**[4.0]C1.f.PA.4**	You receive regular updates for all your detection security technologies (e.g. AV, IDS).
[3.2]C1.d.A.4	You track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, government agencies).	**[4.0]C1.f.A.1**	You track the effectiveness of your threat intelligence and actively share feedback on the usefulness of Indicators of Compromise (IoCs) and other intelligence with the threat community (e.g. sector partners, threat intelligence providers, government agencies).
		[4.0]C1.d.A.1 (New)	You investigate and triage alerts from all security tools and take action.
		[4.0]C1.d.A.2 (New)	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.
		[4.0]C1.d.A.3 (New)	You categorise alerts and incidents by type and priority / severity level.

		[4.0]C1.d.A.4 (New)	You document all triage related activities performed by monitoring and detection personnel and these are used to drive improvements.
		[4.0]C1.d.A.5 (New)	Triage provides enough information for subsequent activities to be prioritised (e.g. the containment of damaging malware).
		[4.0]C1.d.A.6 (New)	Your understanding of normal user and system behaviour, and threats, is sufficient for effective decision making within triage.
[3.2]C1.e	**Monitoring Tools and Skills** Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential function(s) they need to protect.	**[4.0]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.
[3.2]C1.e.NA.1	There are no staff who perform a monitoring function.	**[4.0]C1.e.NA.1**	There are no personnel who perform a monitoring and detection function.
[3.2]C1.e.NA.2	Monitoring staff do not have the correct specialist skills.	**[4.0]C1.e.NA.2**	Monitoring and detection personnel do not have the correct specialist skills.
[3.2]C1.e.NA.3	Monitoring staff are not capable of reporting against governance requirements.	**[4.0]C1.e.NA.3**	Monitoring and detection personnel are not capable of reporting against governance requirements.
[3.2]C1.e.NA.4 (Removed)	Monitoring staff lack the skills to successfully perform some significant parts of the defined workflow.		
[3.2]C1.e.NA.5	Monitoring tools are only able to make use of a fraction of log data being collected.	**[4.0]C1.a.NA.7**	Your monitoring tools are only able to make use of a fraction of the log data being collected.
[3.2]C1.e.NA.6	Monitoring tools cannot be configured to make use of new logging streams, as they come online.	**[4.0]C1.a.NA.6**	Your monitoring tools cannot be configured to make use of new log streams as they come online.
[3.2]C1.e.NA.7	Monitoring staff 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.	**[4.0]C1.e.NA.4**	Monitoring and detection personnel have a lack of awareness of the essential function(s) the organisation provides, what assets relate to those functions and hence the importance of the log data and security events.

		[4.0]C1.e.NA.5 (New)	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).
		[4.0]C1.e.NA.6 (New)	Monitoring and detection personnel are overwhelmed with the amount of data and alerts they have to work with. Alert / triage fatigue is present.
[3.2]C1.e.PA.1	Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.	**[4.0]C1.e.PA.1**	Monitoring and detection personnel have some investigative skills and a basic understanding of the data they need to work with.
[3.2]C1.e.PA.2	Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).	**[4.0]C1.e.PA.2**	Monitoring and detection personnel can report to other parts of the organisation (e.g. security directors, resilience managers).
[3.2]C1.e.PA.3	Monitoring staff are capable of following most of the required workflows.	**[4.0]C1.e.PA.3**	Monitoring and detection personnel are capable of following most of the required workflow(s).
[3.2]C1.e.PA.4	Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types.	**[4.0]C1.a.PA.6**	Your monitoring tools can make use of log data that would capture all common threats.
[3.2]C1.e.PA.5	Your monitoring tools work with most log data, with some configuration.	**[4.0]C1.a.PA.5**	Your monitoring tools work with most log data, with some configuration.
[3.2]C1.e.PA.6	Monitoring staff are aware of some essential function(s) and can manage alerts relating to them.	**[4.0]C1.e.PA.4**	Monitoring and detection personnel are aware of some of the network and information systems and your essential function(s), and can manage alerts relating to them.
		[4.0]C1.e.PA.5 (New)	Monitoring and detection personnel have some understanding of the operational context (e.g. people, processes, network and information systems that support your essential function(s)) to enhance the security monitoring function.
		[4.0]C1.e.PA.6 (New)	Monitoring and detection personnel deal with their workload and cases effectively.
[3.2]C1.e.A.1	You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.	**[4.0]C1.e.A.1**	You have monitoring and detection personnel who are responsible for the proactive and reactive analysis, investigation and reporting of monitoring alerts covering both security and performance.
[3.2]C1.e.A.2	Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.	**[4.0]C1.e.A.2**	Monitoring and detection personnel have defined roles and skills that cover all parts of the monitoring and investigation process.

[3.2]C1.e.A.3	Monitoring staff follow policies, processes and procedures that address all governance reporting requirements, internal and external.	**[4.0]C1.e.A.3**	Monitoring and detection personnel follow policies, processes and procedures that address all governance reporting requirements, internal and external.
[3.2]C1.e.A.4	Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.	**[4.0]C1.e.A.4**	Monitoring and detection personnel are empowered to look beyond the fixed process to investigate and understand non-standard threats.
[3.2]C1.e.A.5	Your monitoring tools make use of all log data collected to pinpoint activity within an incident.	**[4.0]C1.a.A.8**	Your monitoring tools make use of log data to pinpoint activity.
[3.2]C1.e.A.6	Monitoring staff and tools drive and shape new log data collection and can make wide use of it.	**[4.0]C1.e.A.6**	Monitoring and detection personnel drive and shape new log data collection and can make effective use of it.
[3.2]C1.e.A.7	Monitoring staff are aware of the operation of essential function(s) and related assets and can identify and prioritise alerts or investigations that relate to them.	**[4.0]C1.e.A.5**	Monitoring and detection personnel are aware of the network and information systems and your essential function(s), related assets and can identify and prioritise alerts and investigations that relate to them.
		[4.0]C1.e.A.7 (New)	Monitoring and detection personnel are capable of following all of the required workflow(s).
		[4.0]C1.e.A.8 (New)	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.
		[4.0]C1.e.A.9 (New)	Monitoring and detection personnel deal with their workload and cases effectively as well as identifying areas for improvement.
		[4.0]C1.f (New)	**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.
		From [3.2]C1.d.NA.1 To [4.0]C1.f.NA.1	Your organisation has no sources of threat intelligence.
		From [3.2]C1.d.NA.4 To	You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.

		[4.0]C1.f.NA.2	
		[4.0]C1.f.NA.3 (New)	You have no awareness of the steps necessary to make best use of threat intelligence for security monitoring.
		[4.0]C1.f.NA.4 (New)	Threat intelligence is unreliable and / or is not actioned by the appropriate users or systems in a timely manner.
		From [3.2]C2.a.NA.2 To [4.0]C1.f.NA.5	You have no established understanding of what abnormalities to look for that might signify adverse activities.
		From [3.2]C1.d.NA.3 To [4.0]C1.f.NA.6	You do not receive updates for all your detection security technologies (e.g. AV, IDS).
		[4.0]C1.f.NA.7 (New)	You do not understand normal user and system behaviour sufficiently to be able to use abnormalities to detect adverse activity.
		From [3.2]C1.d.PA.4 To [4.0]C1.f.PA.1	You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security incidents).
		From [3.2]C1.d.PA.1 to [4.0]C1.f.PA.2	Your organisation may use threat intelligence services, but you do not necessarily choose sources or providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based infoshare, software vendors, anti-virus providers, specialist threat intel firms, special interest groups).
		From [3.2]C2.a.A.2 to [4.0]C1.f.PA.3	The user and system abnormalities from past attacks and threat intelligence, on your and other network and information systems, are used to signify adverse activity.
		From [3.2]C1.d.PA.2 & [3.2]C1.d.A.3 to [4.0]C1.f.PA.4	You receive regular updates for all your detection security technologies (e.g. AV, IDS).

		From [3.2]C1.d.A.4 To [4.0]C1.f.A.1	You track the effectiveness of your threat intelligence and actively share feedback on the usefulness of Indicators of Compromise (IoCs) and other intelligence with the threat community (e.g. sector partners, threat intelligence providers, government agencies).
		From [3.2]C1.d.A.1 To [4.0]C1.f.A.2	When using threat intelligence feeds, these have been selected using risk-based and threat-informed decisions based on your business needs and sector.
		[4.0]C1.f.A.3 (New)	You make relevant, reliable and actionable threat intelligence available to the necessary users and systems promptly.
		[4.0]C1.f.A.4 (New)	You contextualise threat intelligence and link it to the why and / or how attacks take place for security monitoring.
		From [3.2]C2.a.A.1 to [4.0]C1.f.A.5	You understand normal user and system abnormalities fully, to such an extent that searching for system abnormalities is an effective way of detecting adverse activity (e.g. you fully understand which systems should and should not communicate and when).
		From [3.2]C2.a.A.3 to [4.0]C1.f.A.6	The user and system abnormalities you monitor for are based on the nature of adverse activities likely to impact network and information systems supporting the operation of your essential function(s).
		From [3.2]C2.a.A.4 to [4.0]C1.f.A.7	The user and system abnormalities indicative of adverse activity you use are regularly updated to reflect changes in network and information systems supporting your essential function(s) and current threat intelligence.
		[4.0]C1.f.A.8 (New)	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.
[3.2]C2 (Removed)	**Proactive Security Event Discovery** **The organisation detects, within network and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades**		

	standard signature based security prevent/detect solutions (or when standard solutions are not deployable).		
[3.2]C2.a (Removed)	**System Abnormalities for Attack Detection** You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.		
[3.2]C2.a.NA.1	Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity.	**[4.0]C1.f.NA.7**	You do not understand normal user and system behaviour sufficiently to be able to use abnormalities to detect adverse activity.
[3.2]C2.a.NA.2	You have no established understanding of what abnormalities to look for that might signify malicious activities.	**[4.0]C1.f.NA.5**	You have no established understanding of what abnormalities to look for that might signify adverse activities.
[3.2]C2.a.A.1	Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity (e.g. You fully understand which systems should and should not communicate and when).	**[4.0]C1.f.A.5**	You understand normal user and system abnormalities fully, to such an extent that searching for system abnormalities is an effective way of detecting adverse activity (e.g. you fully understand which systems should and should not communicate and when).
[3.2]C2.a.A.2	System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.	**[4.0]C1.f.PA.3**	The user and system abnormalities from past attacks and threat intelligence, on your and other network and information systems, are used to signify adverse activity.
[3.2]C2.a.A.3	The system abnormalities you search for consider the nature of attacks likely to impact on the network and information systems supporting the operation of your essential function(s).	**[4.0]C1.f.A.6**	The user and system abnormalities you monitor for consider the nature of adverse activities likely to impact network and information systems supporting the operation of your essential function(s).
[3.2]C2.a.A.4	The system abnormality descriptions you use are updated to reflect changes in network and information systems and current threat intelligence.	**[4.0]C1.f.A.7**	The user and system abnormalities indicative of adverse activity you use are regularly updated to reflect changes in network and information systems supporting your essential function(s) and current threat intelligence.
[3.2]C2.b (Removed)	**Proactive Attack Discovery** You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.		
[3.2]C2.b.NA.1	You do not routinely search for system abnormalities indicative of malicious activity.	**[4.0]C1.c.NA.5**	You do not monitor for user or system abnormalities indicative of adverse activity.

[3.2]C2.b.A.1	You routinely search for system abnormalities indicative of malicious activity on the network and information systems supporting the operation of your essential function(s), generating alerts based on the results of such searches.	**[4.0]C1.c.A.8**	You continuously monitor for user and system abnormalities indicative of adverse activity generating alerts based on the results of such monitoring.
[3.2]C2.b.A.2	You have justified confidence in the effectiveness of your searches for system abnormalities indicative of malicious activity.	**[4.0]C2.a.A.6**	You have justified confidence in the effectiveness of your threat hunts and the threat hunting process is reviewed and updated to match the risks posed to network and information systems supporting your essential function(s).
		[4.0]C2 (New)	**Threat Hunting** **The organisation proactively seeks to detect, within network 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).**
		[4.0]C2.a (New)	**Threat Hunting**
		[4.0]C2.a.NA.1 (New)	You do not know the resources required for threat hunting.
		[4.0]C2.a.NA.2 (New)	You do not have access to an effective threat hunting capability.
		[4.0]C2.a.NA.3 (New)	Your threat hunts do not follow any structure and few if any records are created.
		[4.0]C2.a.PA.1 (New)	You have identified the resources required to perform threat hunting and are able to deploy these, in a timely manner, on an occasional basis.
		[4.0]C2.a.PA.2 (New)	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).
		[4.0]C2.a.PA.3 (New)	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.

		[4.0]C2.a.PA.4 (New)	You document details of threat hunts and post hunt analysis.
		[4.0]C2.a.A.1 (New)	You understand the resources required to perform threat hunting and these are deployed as part of business as usual.
		[4.0]C2.a.A.2 (New)	You deploy threat hunting resources at a frequency that matches the risks posed to network and information systems supporting your essential function(s).
		[4.0]C2.a.A.3 (New)	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.
		[4.0]C2.a.A.4 (New)	You turn threat hunts into automated detections and alerting where appropriate.
		[4.0]C2.a.A.5 (New)	You routinely record details of previous threat hunts and post hunt activities. You use these to drive improvements in your threat hunting and security posture.
		From [3.2]C2.b.A.2 To [4.0]C2.a.A.6	You have justified confidence in the effectiveness of your threat hunts and the threat hunting process is reviewed and updated to match the risks posed to network and information systems supporting your essential function(s).
		[4.0]C2.a.A.7 (New)	You leverage automation to improve threat hunts where appropriate (e.g. some stages of the threat hunting process are automated).
		[4.0]C2.a.A.8 (New)	Your threat hunts focus on the tactics, techniques and procedures (TTPs) of threats over atomic IoCs (e.g. hashes, IP addresses, domain names etc).
[3.2]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.**		
[3.2]D1.a	**Response Plan**	**[4.0]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

	You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function(s) and covers a range of incident scenarios.		systems supporting the operation of your essential function(s) and covers a range of incident scenarios.
[3.2]D1.a.PA.1	Your incident response plan covers your essential function(s).	**[4.0]D1.a.PA.1**	Your incident response plan covers network and information systems supporting your essential function(s).
		[4.0]D1.a.PA.5 (New)	Your incident response plan is readily accessible, even when your organisations IT systems have been adversely affected by an incident.
		[4.0]D1.a.PA.6 (New)	Your incident response plan is regularly reviewed to ensure it remains effective.
[3.2]D1.a.A.1	Your incident response plan is based on a clear and understanding of the security risks to the network and information systems supporting your essential function(s).	**[4.0]D1.a.A.1**	Your incident response plan is based on a clear understanding of the security risks to network and information systems supporting your essential function(s).
[3.2]D2	**Lessons Learned** **When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.**	**[4.0]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.**
[3.2]D2.a	**Incident Root Cause Analysis** When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.	**[4.0]D2.a**	**Post Incident Analysis** When an incident occurs, your organisation takes steps to understand its causes, informing appropriate remediating action.
[3.2]D2.a.NA.1	You are not usually able to resolve incidents to a root cause.	**[4.0]D2.a.NA.1**	You are not usually able to resolve incidents to a root cause or identify the contributing factors within a broader systems context.
		[4.0]D2.a.NA.3 (New)	Investigators form theories early in the process and only seek evidence that affirms their belief.
		[4.0]D2.a.NA.4 (New)	Investigations are solely focused on identifying the person(s) who can be held responsible for the incident.
[3.2]D2.a.A.1	Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident.	**[4.0]D2.a.A.1**	Post incident analysis is conducted routinely as a key part of your lessons learned activities following an incident.
[3.2]D2.a.A.2	Your root cause analysis is comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software.	**[4.0]D2.a.A.2**	Your post incident analysis is comprehensive, considering organisational factors (e.g. policies, processes and procedures), technical factors (e.g.

			system design, vulnerabilities), human factors (e.g. training, security culture) and any changes to threat.
[3.2]D2.a.A.3	All relevant incident data is made available to the analysis team to perform root cause analysis.	**[4.0]D2.a.A.3**	All relevant incident data is made available to the analysis team to perform post incident analysis.
		[4.0]D2.a.A.4 (New)	Your analysis considers what could have happened under plausible, alternative circumstances (e.g. 'what if' / 'if only' scenarios).
[3.2]D2.b	**Using Incidents to Drive Improvements** Your organisation uses lessons learned from incidents to improve your security measures.		
		[4.0]D2.b.NA.3 (New)	Changes are made as a 'knee jerk' reaction to an incident without proper analysis and testing to ensure the change is appropriate.
		[4.0]D2.b.NA.4 (New)	You wait until a severe or high-profile incident has occurred before you take steps to improve.
[3.2]D2.b.A.1	You have a documented incident review process/policy which ensures that lessons learned from each incident are identified, captured, and acted upon.	**[4.0]D2.b.A.1**	You have a documented incident review process / policy which ensures that lessons learned from each incident, including near misses, are identified, captured, and acted upon.
[3.2]D2.b.A.2	Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of network and information systems.	**[4.0]D2.b.A.2**	Lessons learned cover issues with reporting, roles, governance, skills and organisational policies, processes and procedures as well as technical aspects of network and information systems.
[3.2]D2.b.A.4	Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.	**[4.0]D2.b.A.4**	Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed promptly.
		[4.0]D2.b.A.6 (New)	Your organisation maximises the lessons learned by using the analysis into 'what if' / 'if only' scenarios.
		[4.0]D2.b.A.7 (New)	Your organisation learns from reported incidents in your sector and the wider national infrastructure.