Data Security and Protection Toolkit 2024-25

CAF aligned DSPT - Objective B – Protecting against cyber-attack and data breaches

This session is being recorded and will be uploaded to the CAN workspace

NHS England
18 July 2024

Welcome and agenda for today

Housekeeping

- The session is being recorded and is a one-way broadcast, please use the Q&A function to ask any questions
- The slides and recording will be uploaded to the CAN workspace after there will be a link to the recording for non-CAN members
- The first two webinars have now been uploaded to YouTube (unlisted) and can be accessed here:

  Webinar 1 Background and overview session: https://www.youtube.com/watch?v=BG6YE1h4W40
  Webinar 2 Section A - managing risk: https://www.youtube.com/watch?v=2aZ6TyEkUgc

- If you experience any technical issues, please leave and re-join the call

Agenda for today

1. Overview and background session
2. Demonstration of the new user interface
3. Question and answer session

Webinar content

Session 3 – Objective B – Protecting against cyber attack and data breaches

- Overview – what is in the Objective and which teams need to be involved in responding to it?
- Contributing outcomes – A step through B1 to B3
- Half Time Quiz
- Contributing outcomes – A step through B4 to B6
- Q&A session

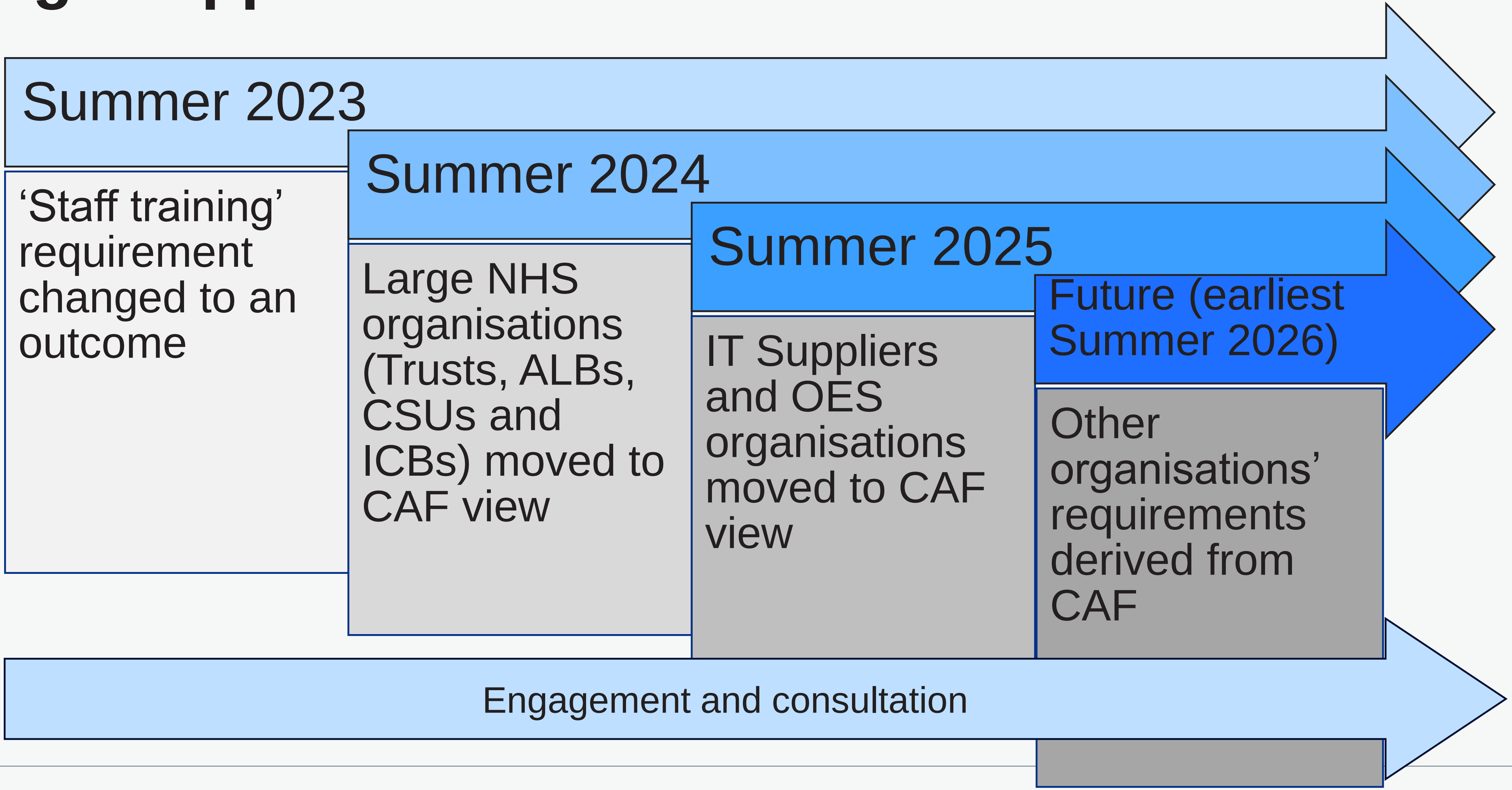
What is happening and why?

What you need to know

- In September 2024 the DSPT will be changing to adopt the National Cyber Security Centre’s Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance.

- This change will lead to NHS Trusts, CSUs, ALBs and ICBs seeing a different interface when they log in, which sets out CAF-aligned requirements in terms of Objectives, Principles and Outcomes.

Staged approach for DSPT



Summer 2023

'Staff training' requirement changed to an outcome

Summer 2024

Large NHS organisations (Trusts, ALBs, CSUs and ICBs) moved to CAF view

Summer 2025

IT Suppliers and OES organisations moved to CAF view

Future (earliest Summer 2026)

Other organisations' requirements derived from CAF

Engagement and consultation

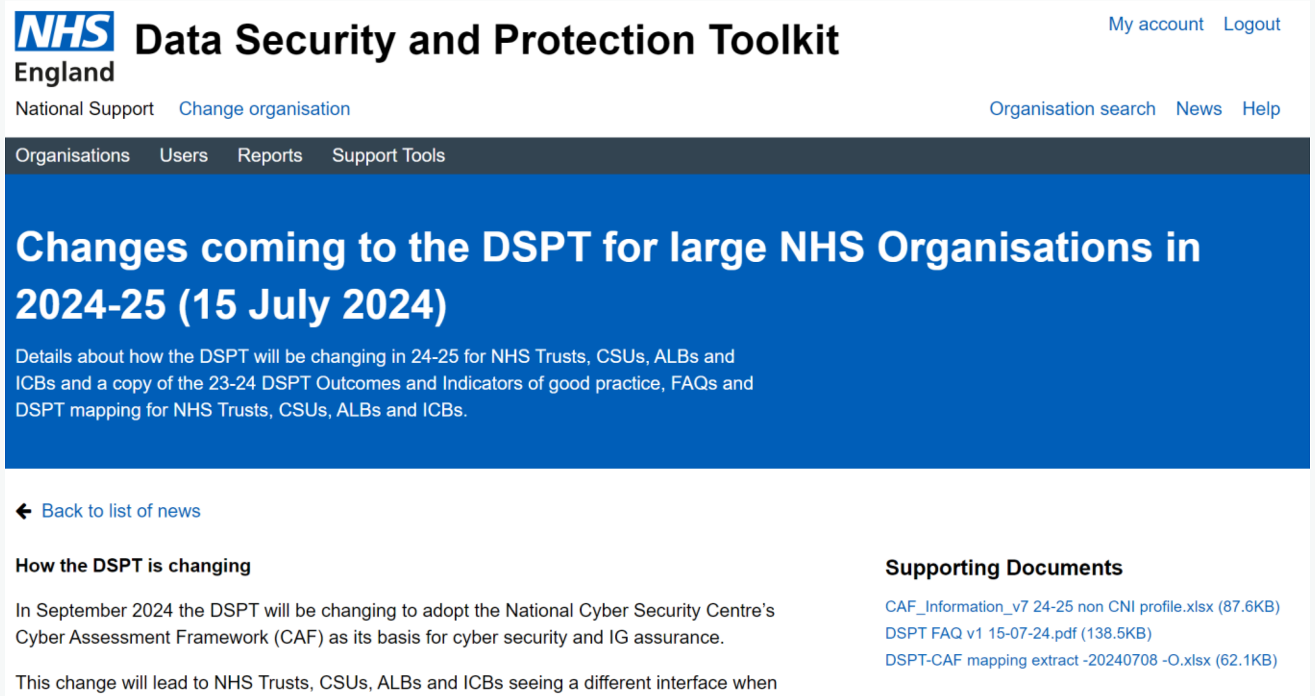
Useful documents

News item explaining the changes

DSPT for 24-25 in spreadsheet form

Mapping to 23-24 DSPT

FAQs from the webinar



Changes coming to the DSPT for large NHS Organisations in 2024-25 (15 July 2024)

Details about how the DSPT will be changing in 24-25 for NHS Trusts, CSUs, ALBs and ICBs and a copy of the 23-24 DSPT Outcomes and Indicators of good practice, FAQs and DSPT mapping for NHS Trusts, CSUs, ALBs and ICBs.

Back to list of news

How the DSPT is changing

In September 2024 the DSPT will be changing to adopt the National Cyber Security Centre's Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance.

This change will lead to NHS Trusts, CSUs, ALBs and ICBs seeing a different interface when

Supporting Documents

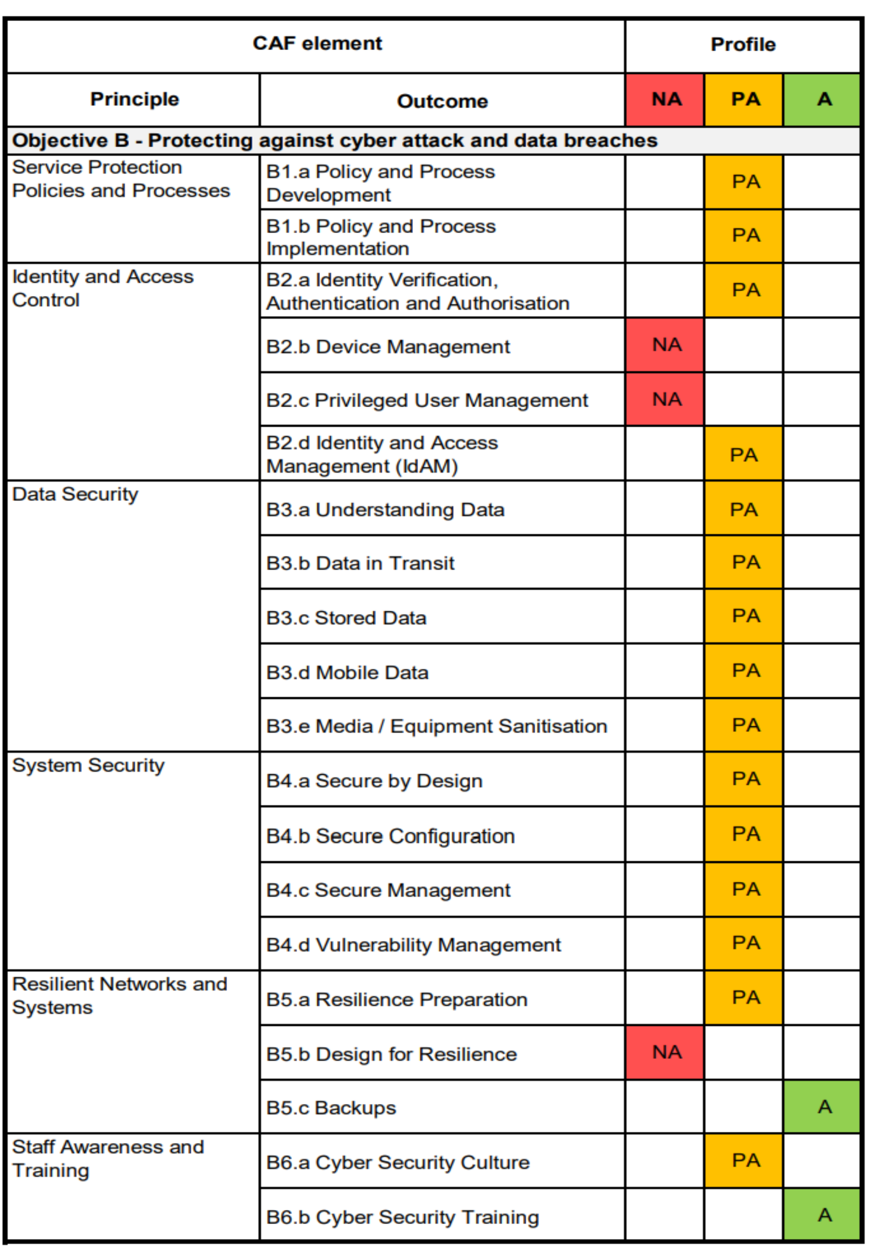
CAF_Information_v7 24-25 non CNI profile.xlsx (87.6KB)
DSPT FAQ v1 15-07-24.pdf (138.5KB)
DSPT-CAF mapping extract -20240708 -O.xlsx (62.1KB)

https://www.dsptoolkit.nhs.uk/News/DSPT-Changes-in-24-25

Objective B - Protecting against cyber attack and data breaches

Expectations for Standards met:

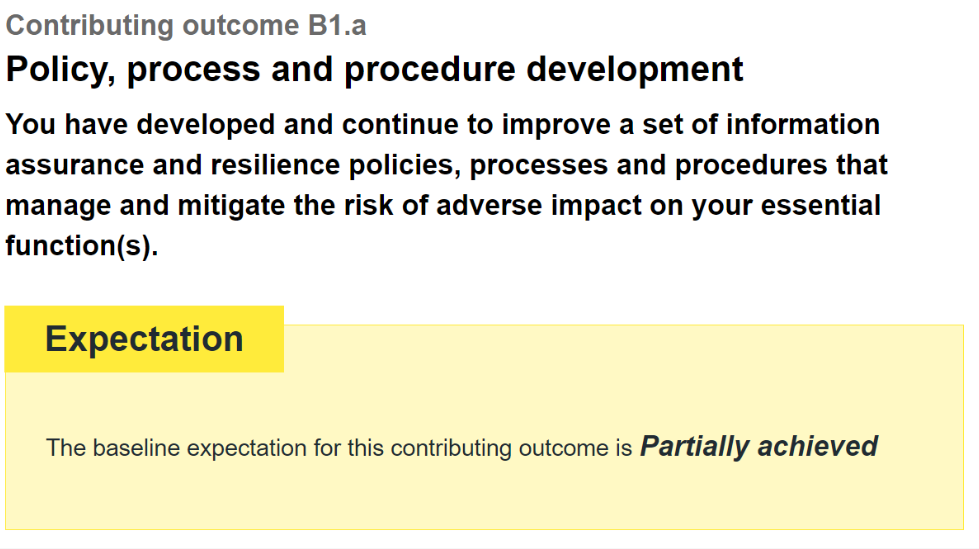
Objective B - Protecting against cyber attack and data breaches



CAF element		Profile		
Principle	**Outcome**	**NA**	**PA**	**A**
Objective B - Protecting against cyber attack and data breaches				
Service Protection Policies and Processes	B1.a Policy and Process Development		PA	
	B1.b Policy and Process Implementation		PA	
Identity and Access Control	B2.a Identity Verification, Authentication and Authorisation		PA	
	B2.b Device Management	NA		
	B2.c Privileged User Management	NA		
	B2.d Identity and Access Management (IdAM)		PA	
Data Security	B3.a Understanding Data		PA	
	B3.b Data in Transit		PA	
	B3.c Stored Data		PA	
	B3.d Mobile Data		PA	
	B3.e Media / Equipment Sanitisation		PA	
System Security	B4.a Secure by Design		PA	
	B4.b Secure Configuration		PA	
	B4.c Secure Management		PA	
	B4.d Vulnerability Management		PA	
Resilient Networks and Systems	B5.a Resilience Preparation		PA	
	B5.b Design for Resilience	NA		
	B5.c Backups			A
Staff Awareness and Training	B6.a Cyber Security Culture		PA	
	B6.b Cyber Security Training			A

Principle: B1 Policies, processes and procedures

Contributing outcome:
B1.a Policy, process and procedure development



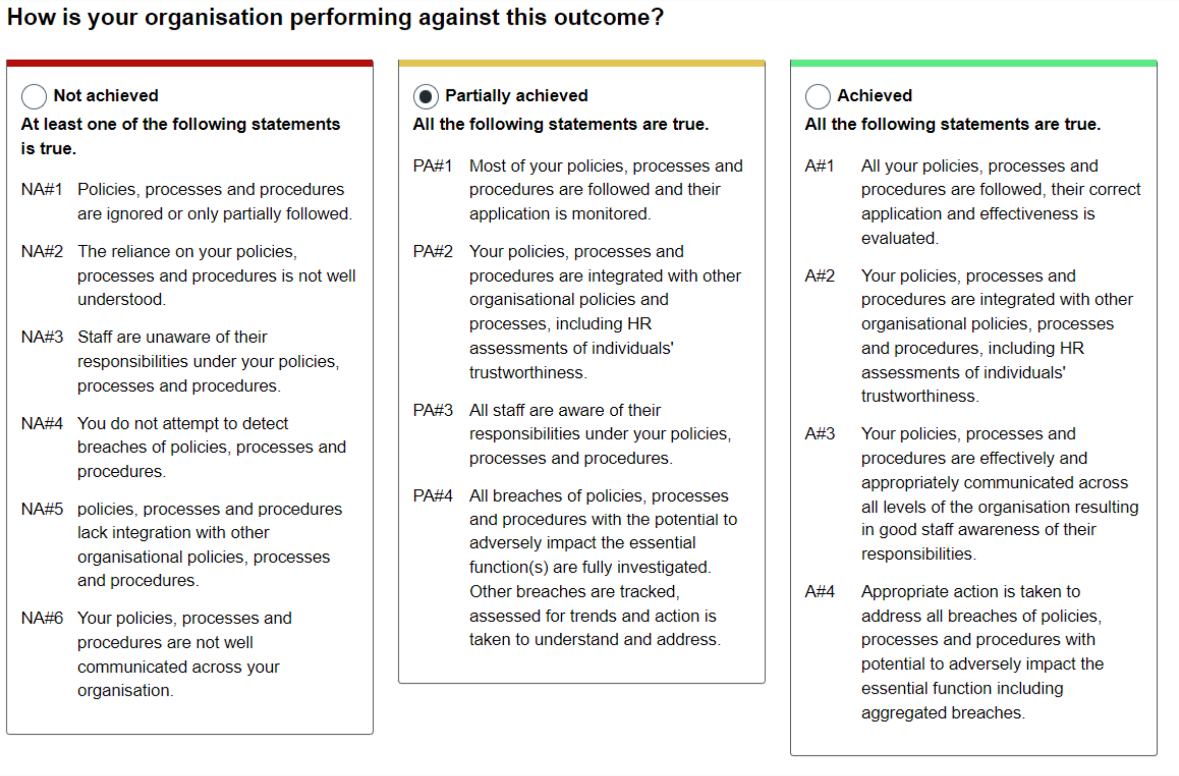
Contributing outcome B1.a

Policy, process and procedure development

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

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Policies, processes and procedures are ignored or only partially followed.

NA#2 The reliance on your policies, processes and procedures is not well understood.

NA#3 Staff are unaware of their responsibilities under your policies, processes and procedures.

NA#4 You do not attempt to detect breaches of policies, processes and procedures.

NA#5 policies, processes and procedures lack integration with other organisational policies, processes and procedures.

NA#6 Your policies, processes and procedures are not well communicated across your organisation.

● **Partially achieved**

All the following statements are true.

PA#1 Most of your policies, processes and procedures are followed and their application is monitored.

PA#2 Your policies, processes and procedures are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.

PA#3 All staff are aware of their responsibilities under your policies, processes and procedures.

PA#4 All breaches of policies, processes and procedures with the potential to adversely impact the essential function(s) are fully investigated. Other breaches are tracked, assessed for trends and action is taken to understand and address.

○ **Achieved**

All the following statements are true.

A#1 All your policies, processes and procedures are followed, their correct application and effectiveness is evaluated.

A#2 Your policies, processes and procedures are integrated with other organisational policies, processes and procedures, including HR assessments of individuals' trustworthiness.

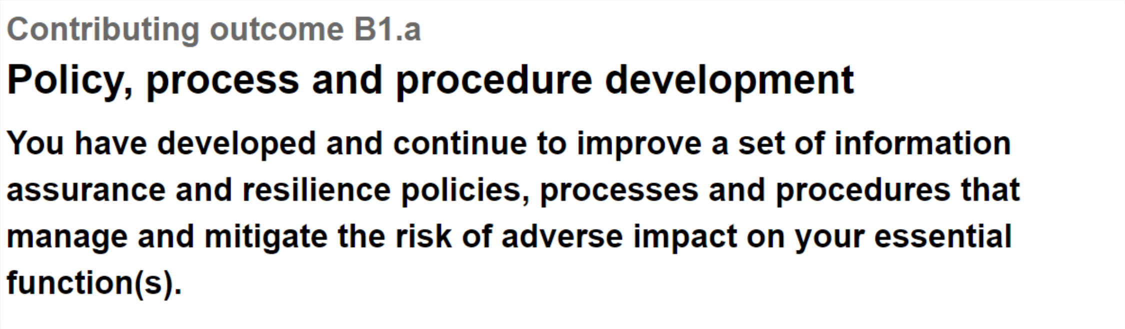
A#3 Your policies, processes and procedures are effectively and appropriately communicated across all levels of the organisation resulting in good staff awareness of their responsibilities.

A#4 Appropriate action is taken to address all breaches of policies, processes and procedures with potential to adversely impact the essential function including aggregated breaches.

Principle: B1 Policies, processes and procedures

Contributing outcome:
B1.a Policy, process and procedure development

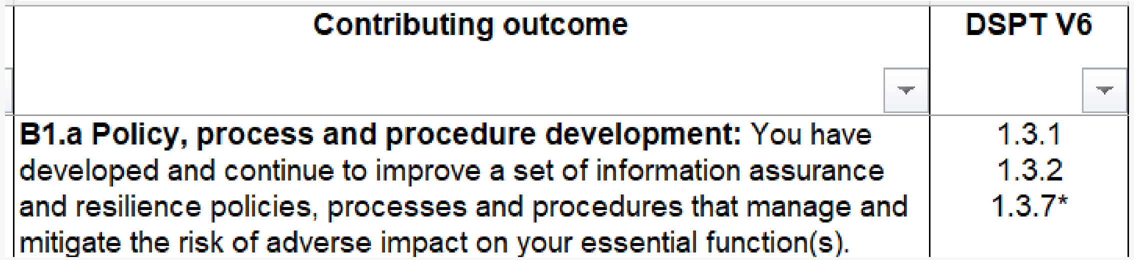
DSPT Mapping and Guidance



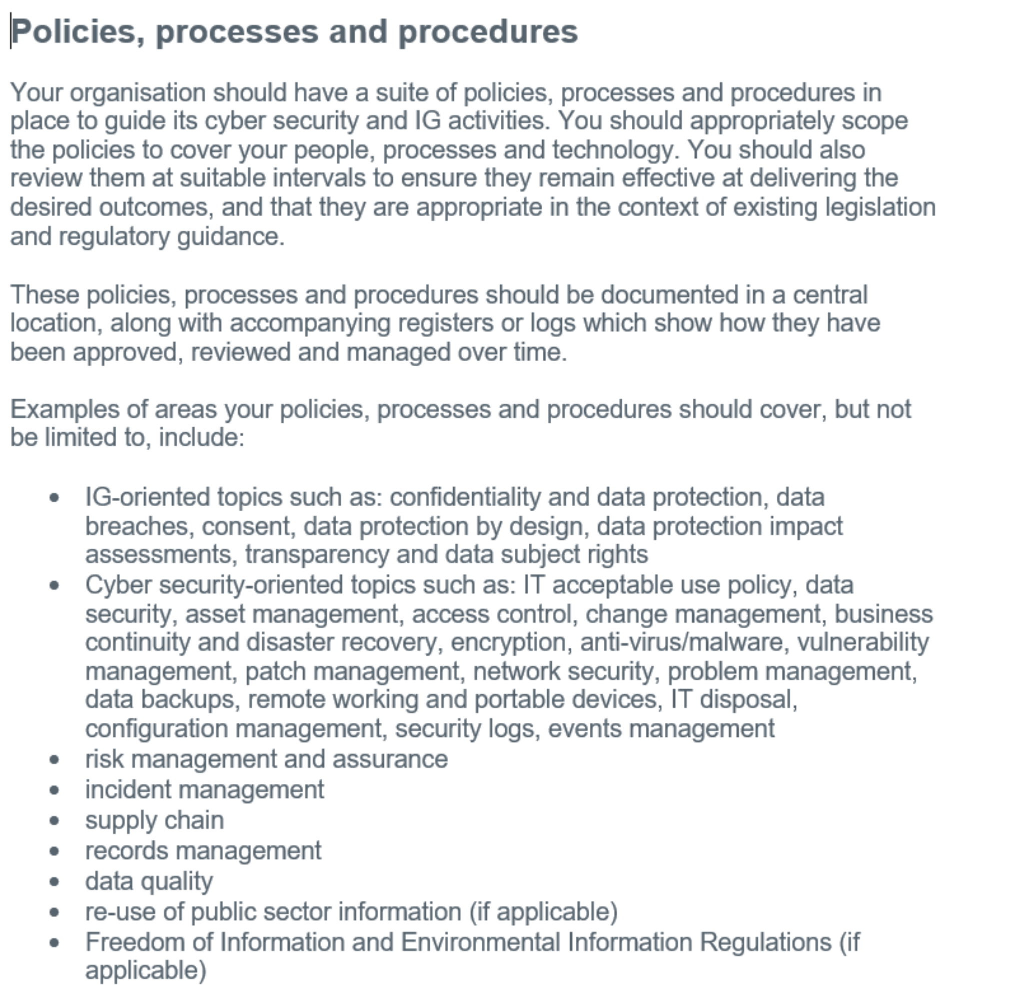
Contributing outcome B1.a

Policy, process and procedure development

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



Contributing outcome	DSPT V6
B1.a Policy, process and procedure development: You have developed and continue to improve a set of information assurance and resilience policies, processes and procedures that manage and mitigate the risk of adverse impact on your essential function(s).	1.3.1 1.3.2 1.3.7*



Policies, processes and procedures

Your organisation should have a suite of policies, processes and procedures in place to guide its cyber security and IG activities. You should appropriately scope the policies to cover your people, processes and technology. You should also review them at suitable intervals to ensure they remain effective at delivering the desired outcomes, and that they are appropriate in the context of existing legislation and regulatory guidance.

These policies, processes and procedures should be documented in a central location, along with accompanying registers or logs which show how they have been approved, reviewed and managed over time.

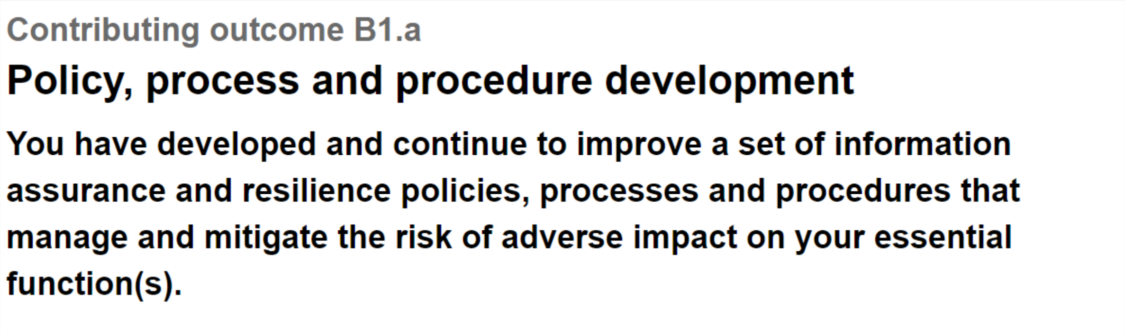
Examples of areas your policies, processes and procedures should cover, but not be limited to, include:

- IG-oriented topics such as: confidentiality and data protection, data breaches, consent, data protection by design, data protection impact assessments, transparency and data subject rights
- Cyber security-oriented topics such as: IT acceptable use policy, data security, asset management, access control, change management, business continuity and disaster recovery, encryption, anti-virus/malware, vulnerability management, patch management, network security, problem management, data backups, remote working and portable devices, IT disposal, configuration management, security logs, events management
- risk management and assurance
- incident management
- supply chain
- records management
- data quality
- re-use of public sector information (if applicable)
- Freedom of Information and Environmental Information Regulations (if applicable)

Principle: B1 Policies, processes and procedures

Contributing outcome:
B1.a Policy, process and procedure development

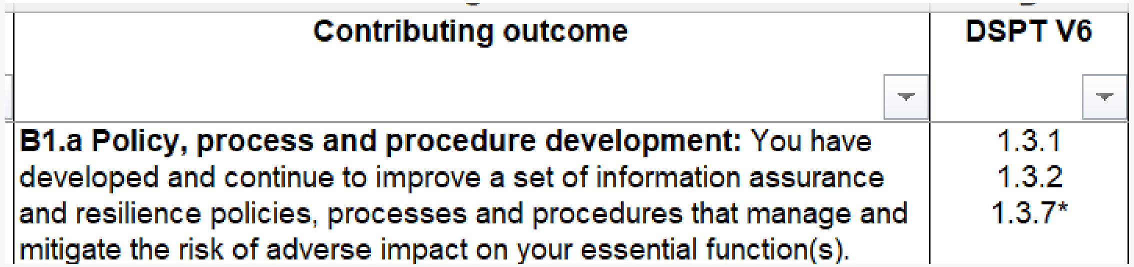
DSPT Mapping and Guidance



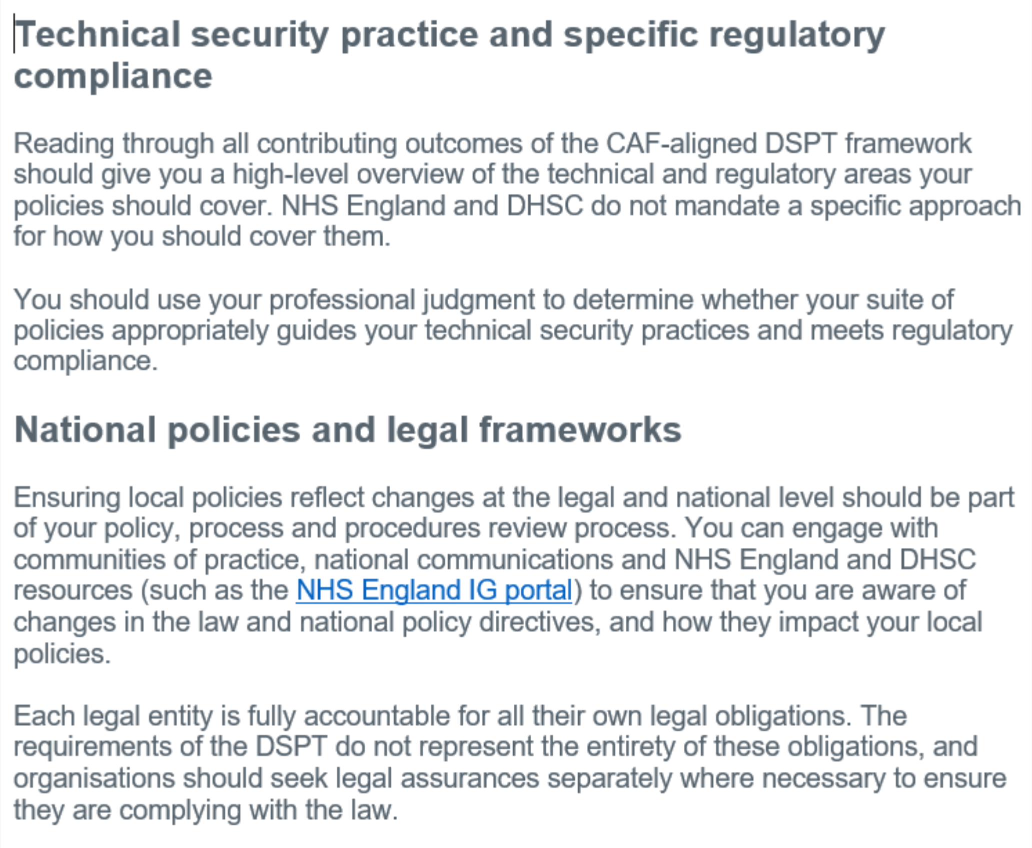
Contributing outcome B1.a

Policy, process and procedure development

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



Contributing outcome	DSPT V6
B1.a Policy, process and procedure development: You have developed and continue to improve a set of information assurance and resilience policies, processes and procedures that manage and mitigate the risk of adverse impact on your essential function(s).	1.3.1 1.3.2 1.3.7*



Technical security practice and specific regulatory compliance

Reading through all contributing outcomes of the CAF-aligned DSPT framework should give you a high-level overview of the technical and regulatory areas your policies should cover. NHS England and DHSC do not mandate a specific approach for how you should cover them.

You should use your professional judgment to determine whether your suite of policies appropriately guides your technical security practices and meets regulatory compliance.

National policies and legal frameworks

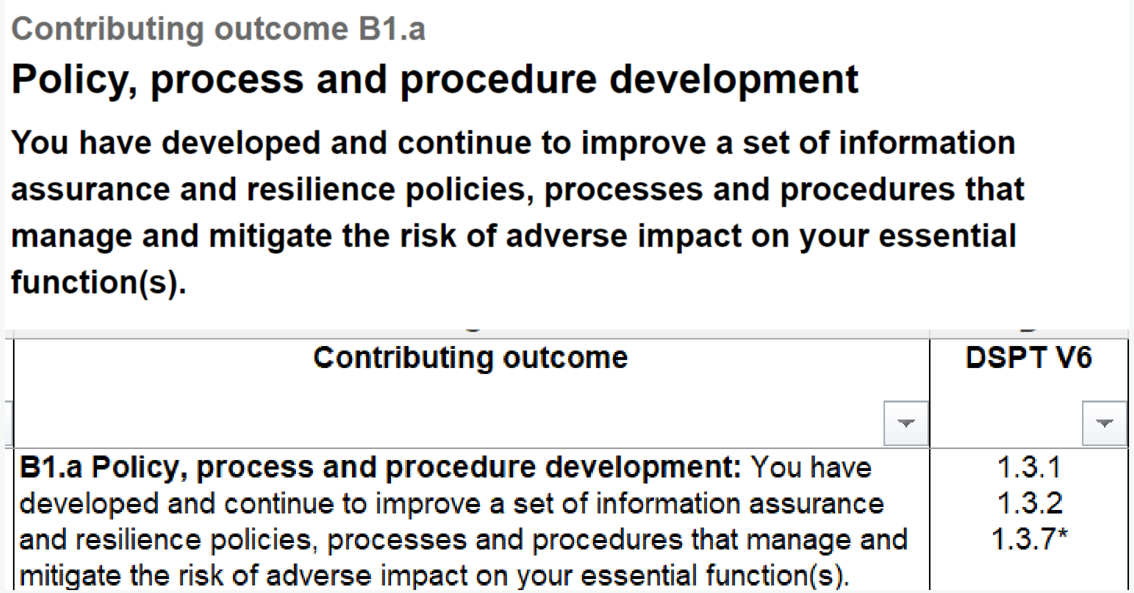
Ensuring local policies reflect changes at the legal and national level should be part of your policy, process and procedures review process. You can engage with communities of practice, national communications and NHS England and DHSC resources (such as the NHS England IG portal) to ensure that you are aware of changes in the law and national policy directives, and how they impact your local policies.

Each legal entity is fully accountable for all their own legal obligations. The requirements of the DSPT do not represent the entirety of these obligations, and organisations should seek legal assurances separately where necessary to ensure they are complying with the law.

Principle: B1 Policies, processes and procedures

Contributing outcome:
B1.a Policy, process and procedure development

DSPT Supporting evidence

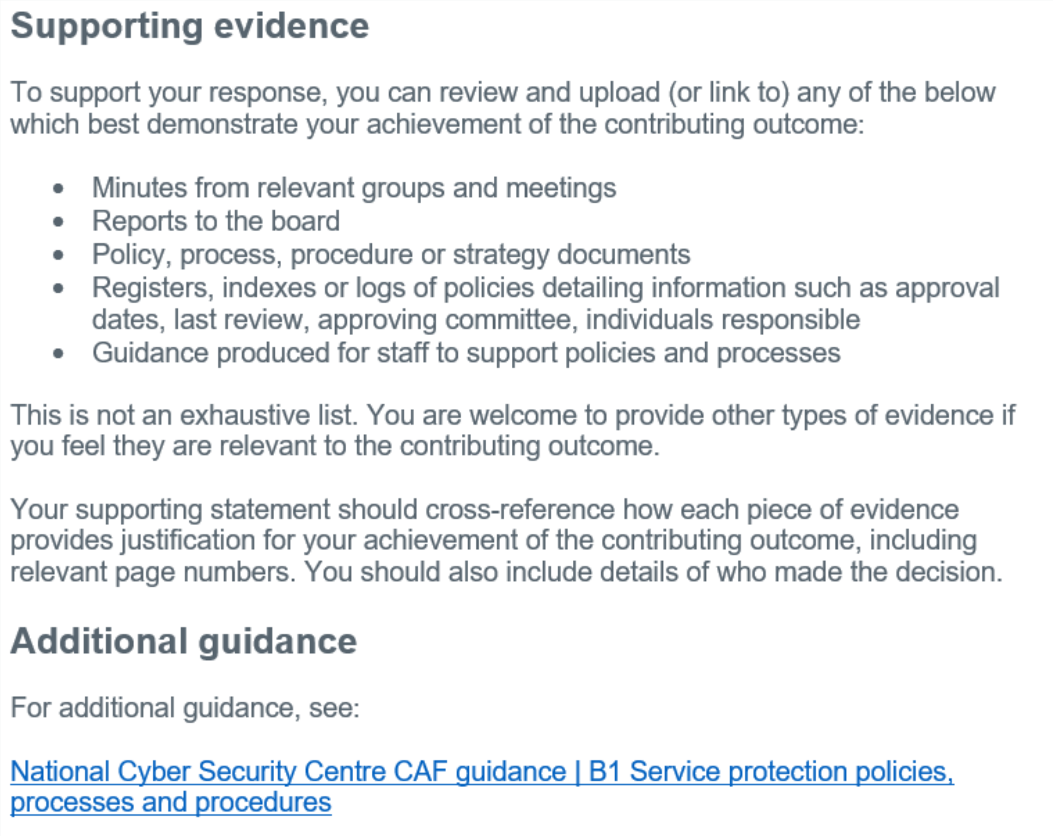


Contributing outcome B1.a

Policy, process and procedure development

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

Contributing outcome	DSPT V6
B1.a Policy, process and procedure development: You have developed and continue to improve a set of information assurance and resilience policies, processes and procedures that manage and mitigate the risk of adverse impact on your essential function(s).	1.3.1 1.3.2 1.3.7*



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Minutes from relevant groups and meetings
- Reports to the board
- Policy, process, procedure or strategy documents
- Registers, indexes or logs of policies detailing information such as approval dates, last review, approving committee, individuals responsible
- Guidance produced for staff to support policies and processes

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B1 Service protection policies, processes and procedures

Principle: B1 Policies, processes and procedures

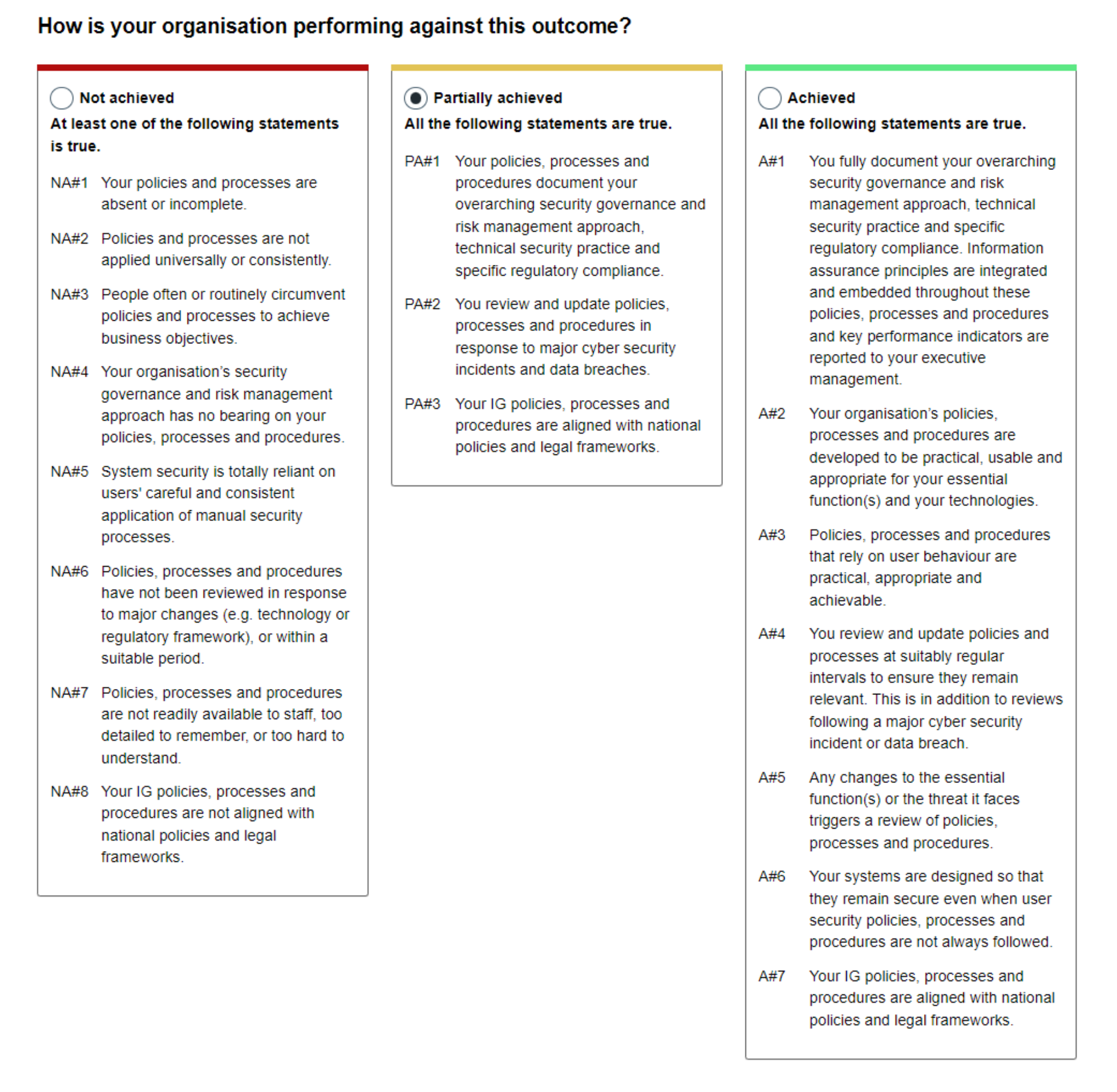
Contributing outcome:
B1.b Policy, process and procedure implementation

Contributing outcome: B1.b
Policy, process and procedure implementation

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

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Your policies and processes are absent or incomplete.

NA#2 Policies and processes are not applied universally or consistently.

NA#3 People often or routinely circumvent policies and processes to achieve business objectives.

NA#4 Your organisation's security governance and risk management approach has no bearing on your policies, processes and procedures.

NA#5 System security is totally reliant on users' careful and consistent application of manual security processes.

NA#6 Policies, processes and procedures have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period.

NA#7 Policies, processes and procedures are not readily available to staff, too detailed to remember, or too hard to understand.

NA#8 Your IG policies, processes and procedures are not aligned with national policies and legal frameworks.

● **Partially achieved**

All the following statements are true.

PA#1 Your policies, processes and procedures document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance.

PA#2 You review and update policies, processes and procedures in response to major cyber security incidents and data breaches.

PA#3 Your IG policies, processes and procedures are aligned with national policies and legal frameworks.

○ **Achieved**

All the following statements are true.

A#1 You fully document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Information assurance principles are integrated and embedded throughout these policies, processes and procedures and key performance indicators are reported to your executive management.

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.

A#3 Policies, processes and procedures that rely on user behaviour are practical, appropriate and achievable.

A#4 You review and update policies and processes at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident or data breach.

A#5 Any changes to the essential function(s) or the threat it faces triggers a review of policies, processes and procedures.

A#6 Your systems are designed so that they remain secure even when user security policies, processes and procedures are not always followed.

A#7 Your IG policies, processes and procedures are aligned with national policies and legal frameworks.

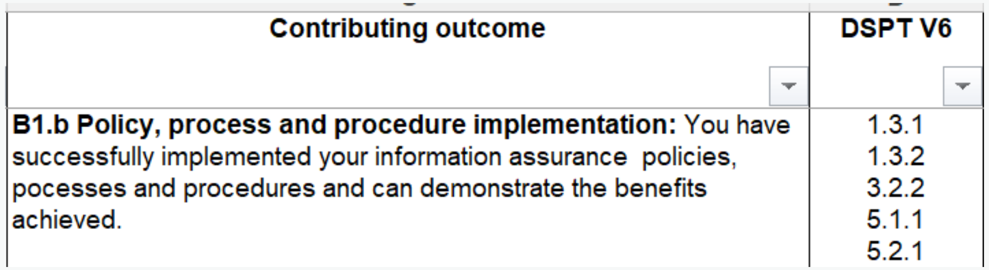
Principle: B1 Policies, processes and procedures

Contributing outcome:
B1.b Policy, process and procedure implementation

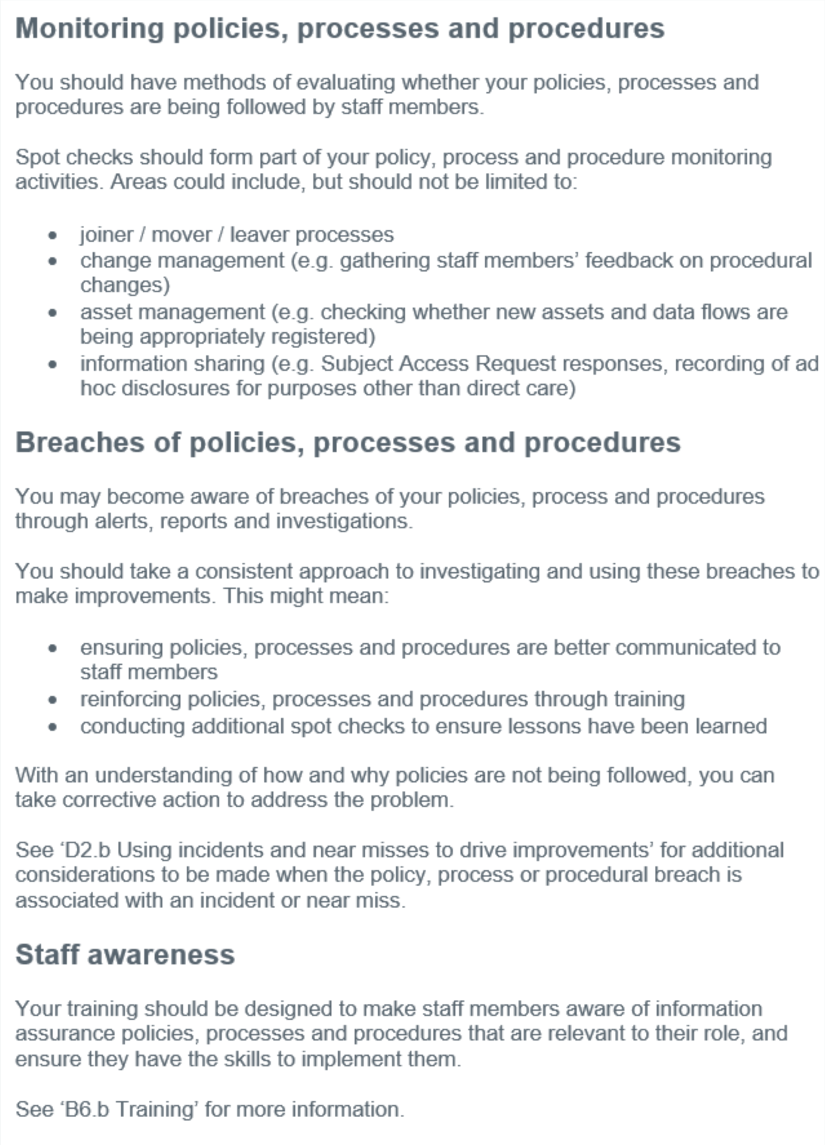
DSPT Mapping and Guidance

Contributing outcome: B1.b
Policy, process and procedure implementation

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



Contributing outcome	DSPT V6
B1.b Policy, process and procedure implementation: You have successfully implemented your information assurance policies, pocesses and procedures and can demonstrate the benefits achieved.	1.3.1 1.3.2 3.2.2 5.1.1 5.2.1



Monitoring policies, processes and procedures

You should have methods of evaluating whether your policies, processes and procedures are being followed by staff members.

Spot checks should form part of your policy, process and procedure monitoring activities. Areas could include, but should not be limited to:

- joiner / mover / leaver processes
- change management (e.g. gathering staff members' feedback on procedural changes)
- asset management (e.g. checking whether new assets and data flows are being appropriately registered)
- information sharing (e.g. Subject Access Request responses, recording of ad hoc disclosures for purposes other than direct care)

Breaches of policies, processes and procedures

You may become aware of breaches of your policies, process and procedures through alerts, reports and investigations.

You should take a consistent approach to investigating and using these breaches to make improvements. This might mean:

- ensuring policies, processes and procedures are better communicated to staff members
- reinforcing policies, processes and procedures through training
- conducting additional spot checks to ensure lessons have been learned

With an understanding of how and why policies are not being followed, you can take corrective action to address the problem.

See 'D2.b Using incidents and near misses to drive improvements' for additional considerations to be made when the policy, process or procedural breach is associated with an incident or near miss.

Staff awareness

Your training should be designed to make staff members aware of information assurance policies, processes and procedures that are relevant to their role, and ensure they have the skills to implement them.

See 'B6.b Training' for more information.

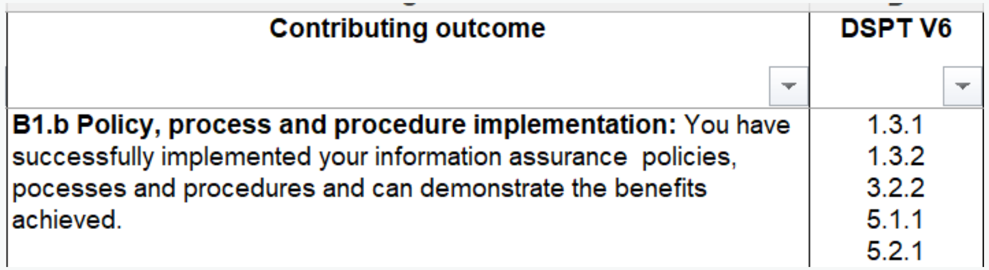
Principle: B1 Policies, processes and procedures

Contributing outcome:
B1.b Policy, process and procedure implementation

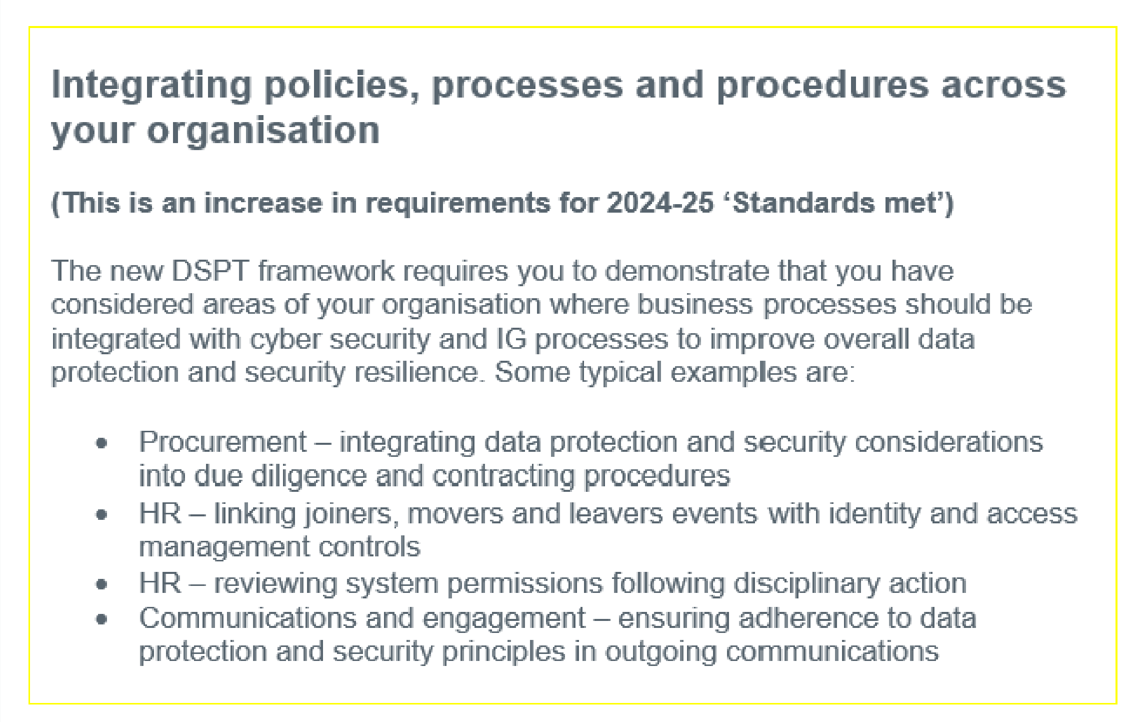
DSPT Mapping and Guidance

Contributing outcome: B1.b
Policy, process and procedure implementation

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



Contributing outcome	DSPT V6
B1.b Policy, process and procedure implementation: You have successfully implemented your information assurance policies, pocesses and procedures and can demonstrate the benefits achieved.	1.3.1 1.3.2 3.2.2 5.1.1 5.2.1



Integrating policies, processes and procedures across your organisation

(This is an increase in requirements for 2024-25 'Standards met')

The new DSPT framework requires you to demonstrate that you have considered areas of your organisation where business processes should be integrated with cyber security and IG processes to improve overall data protection and security resilience. Some typical examples are:

- Procurement – integrating data protection and security considerations into due diligence and contracting procedures
- HR – linking joiners, movers and leavers events with identity and access management controls
- HR – reviewing system permissions following disciplinary action
- Communications and engagement – ensuring adherence to data protection and security principles in outgoing communications

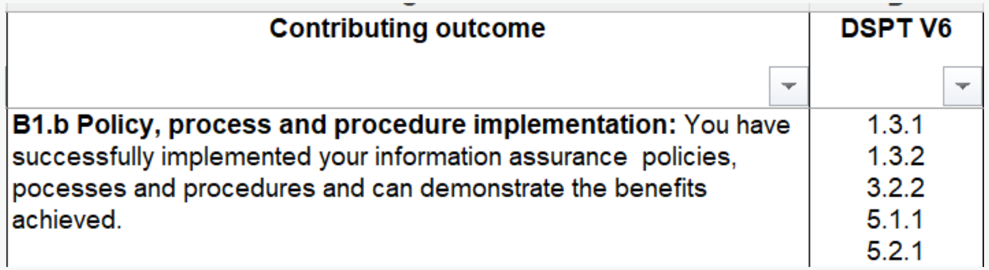
Principle: B1 Policies, processes and procedures

Contributing outcome:
B1.b Policy, process and procedure implementation

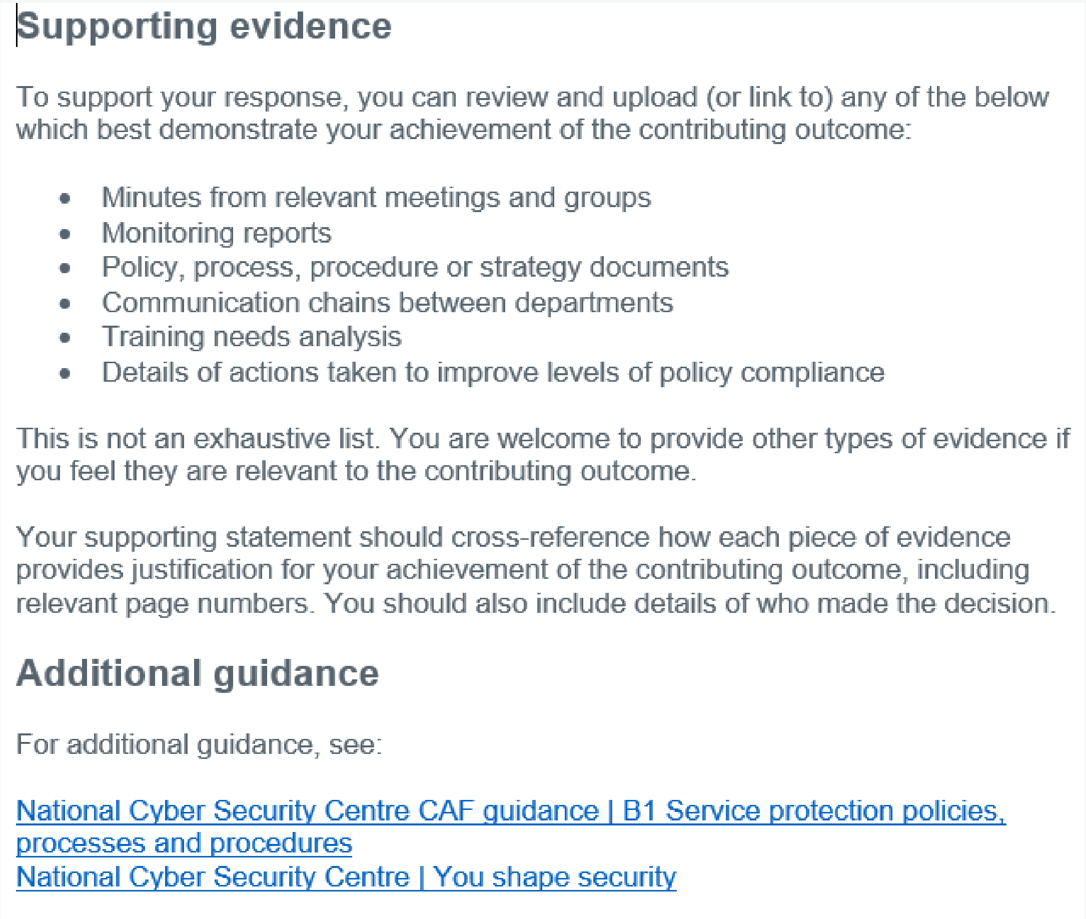
DSPT Supporting evidence

Contributing outcome: B1.b
Policy, process and procedure implementation

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



Contributing outcome	DSPT V6
B1.b Policy, process and procedure implementation: You have successfully implemented your information assurance policies, pocesses and procedures and can demonstrate the benefits achieved.	1.3.1 1.3.2 3.2.2 5.1.1 5.2.1



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Minutes from relevant meetings and groups
- Monitoring reports
- Policy, process, procedure or strategy documents
- Communication chains between departments
- Training needs analysis
- Details of actions taken to improve levels of policy compliance

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

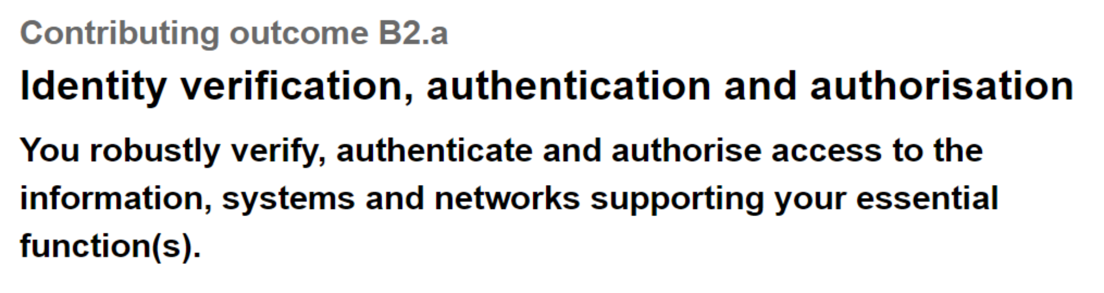
Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B1 Service protection policies, processes and procedures
National Cyber Security Centre | You shape security

Principle: B2 Identity and access control

Contributing outcome:
B2.a Identity verification, authentication and authorisation



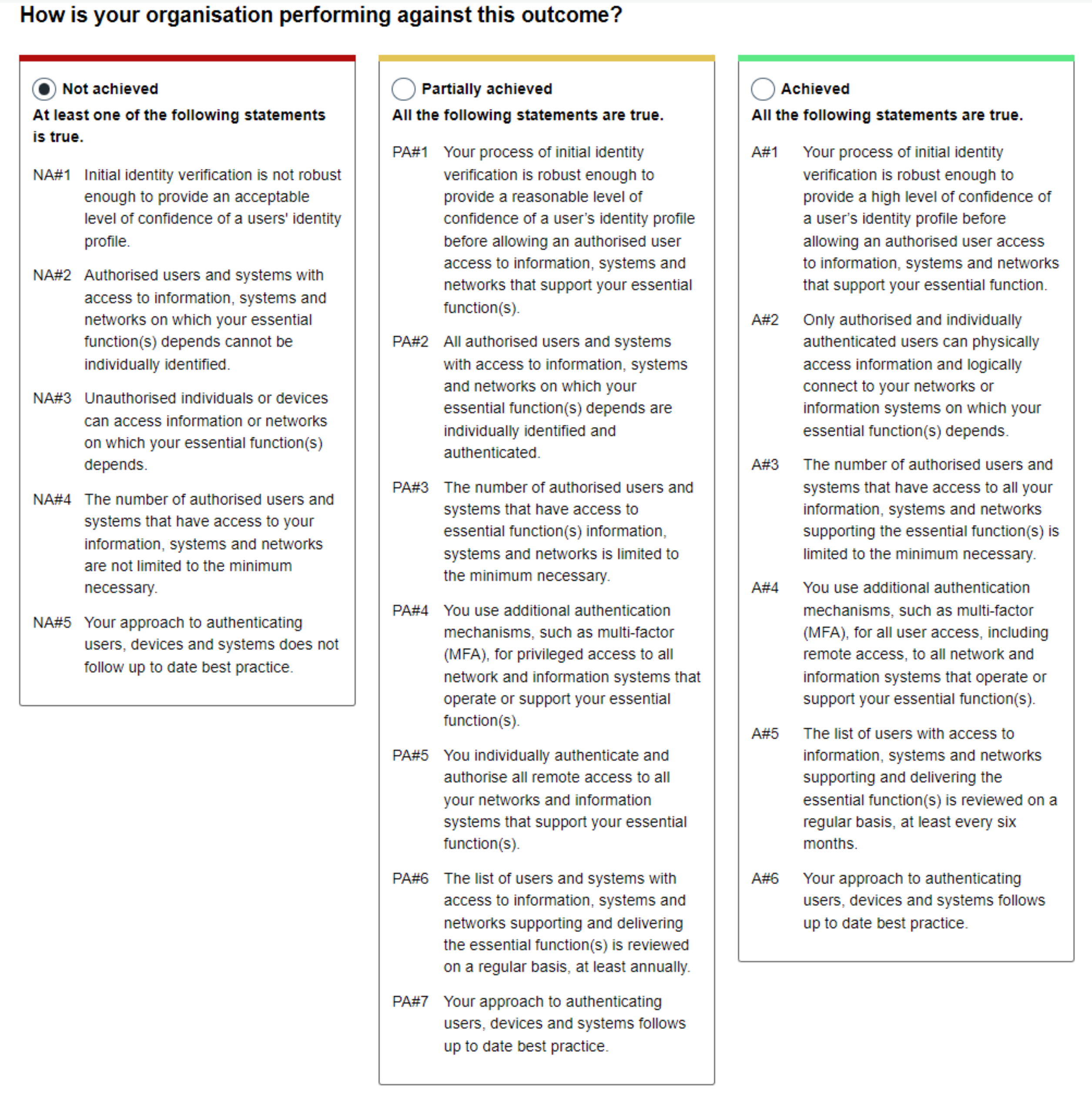
Contributing outcome B2.a

Identity verification, authentication and authorisation

You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s).

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

● **Not achieved**

At least one of the following statements is true.

NA#1 Initial identity verification is not robust enough to provide an acceptable level of confidence of a users' identity profile.

NA#2 Authorised users and systems with access to information, systems and networks on which your essential function(s) depends cannot be individually identified.

NA#3 Unauthorised individuals or devices can access information or networks on which your essential function(s) depends.

NA#4 The number of authorised users and systems that have access to your information, systems and networks are not limited to the minimum necessary.

NA#5 Your approach to authenticating users, devices and systems does not follow up to date best practice.

○ **Partially achieved**

All the following statements are true.

PA#1 Your process of initial identity verification is robust enough to provide a reasonable level of confidence of a user's identity profile before allowing an authorised user access to information, systems and networks that support your essential function(s).

PA#2 All authorised users and systems with access to information, systems and networks on which your essential function(s) depends are individually identified and authenticated.

PA#3 The number of authorised users and systems that have access to essential function(s) information, systems and networks is limited to the minimum necessary.

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).

PA#5 You individually authenticate and authorise all remote access to all your networks and information systems that support your essential function(s).

PA#6 The list of users and systems with access to information, systems and networks supporting and delivering the essential function(s) is reviewed on a regular basis, at least annually.

PA#7 Your approach to authenticating users, devices and systems follows up to date best practice.

○ **Achieved**

All the following statements are true.

A#1 Your process of initial identity verification is robust enough to provide a high level of confidence of a user's identity profile before allowing an authorised user access to information, systems and networks that support your essential function.

A#2 Only authorised and individually authenticated users can physically access information and logically connect to your networks or information systems on which your essential function(s) depends.

A#3 The number of authorised users and systems that have access to all your information, systems and networks supporting the essential function(s) is limited to the minimum necessary.

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).

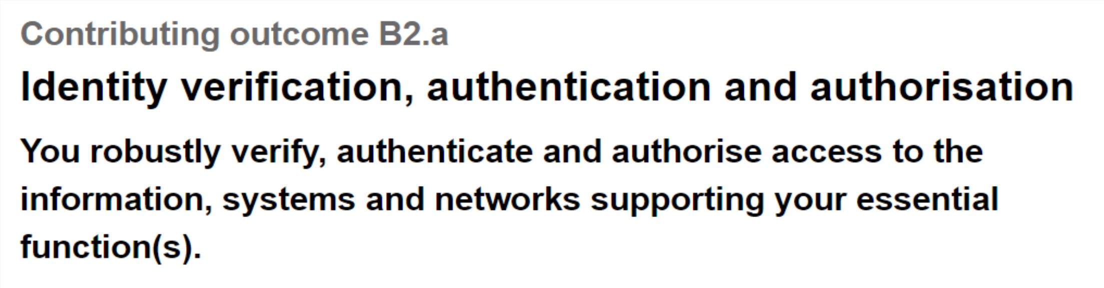
A#5 The list of users with access to information, systems and networks supporting and delivering the essential function(s) is reviewed on a regular basis, at least every six months.

A#6 Your approach to authenticating users, devices and systems follows up to date best practice.

Principle: B2 Identity and access control

Contributing outcome:
B2.a Identity verification, authentication and authorisation

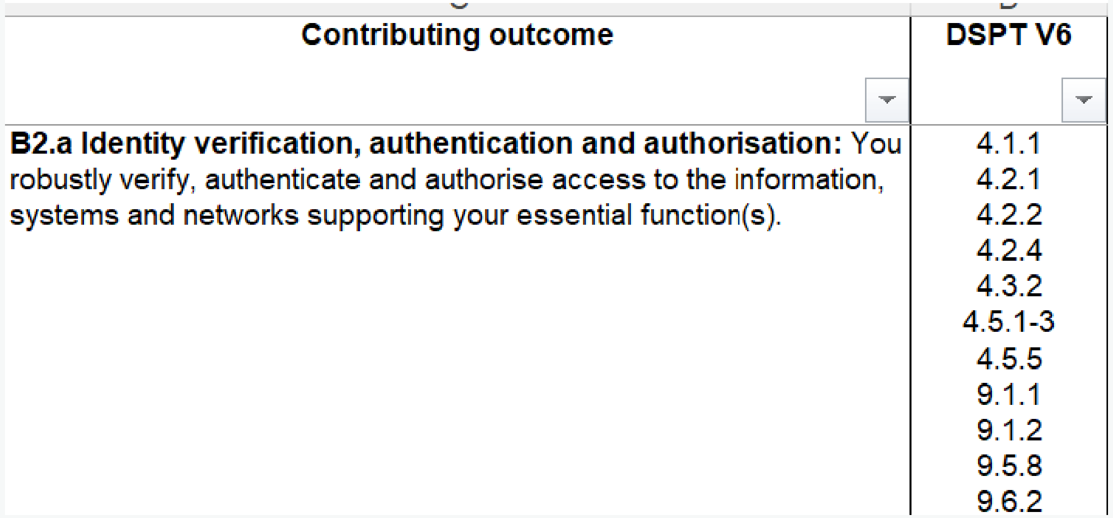
DSPT Mapping and Guidance



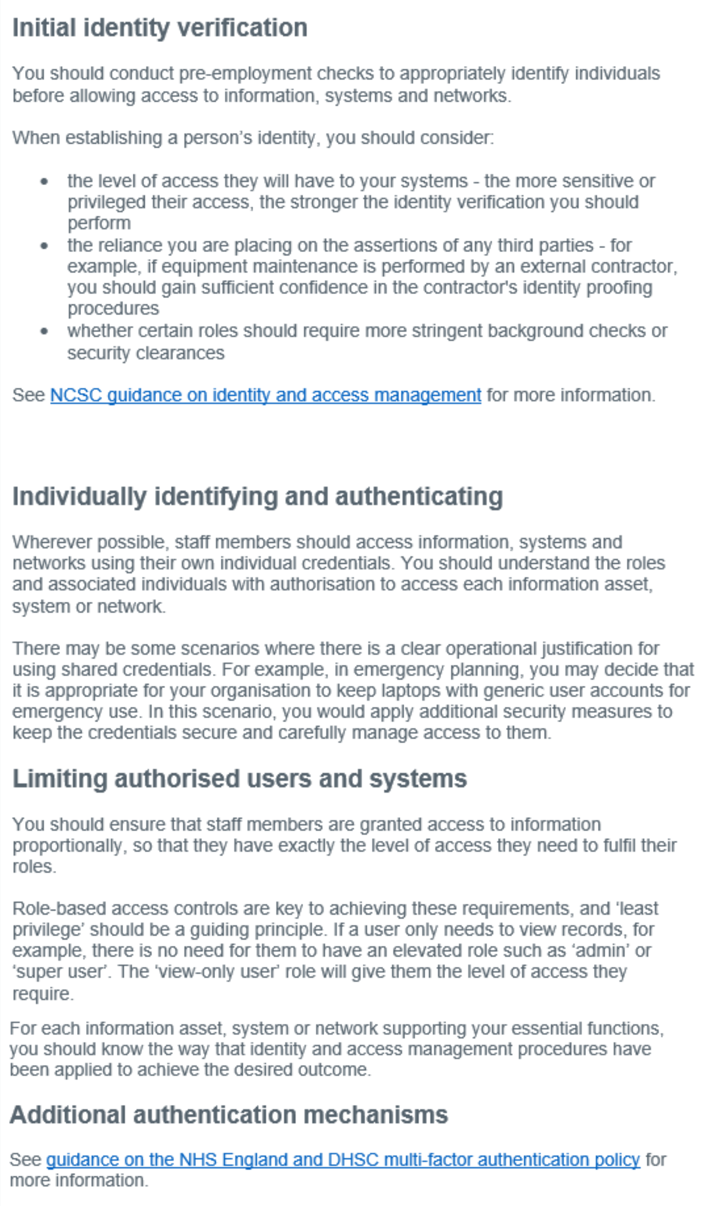
Contributing outcome B2.a

Identity verification, authentication and authorisation

You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s).



Contributing outcome	DSPT V6
B2.a Identity verification, authentication and authorisation: You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s).	4.1.1 4.2.1 4.2.2 4.2.4 4.3.2 4.5.1-3 4.5.5 9.1.1 9.1.2 9.5.8 9.6.2



Initial identity verification

You should conduct pre-employment checks to appropriately identify individuals before allowing access to information, systems and networks.

When establishing a person's identity, you should consider:

- the level of access they will have to your systems - the more sensitive or privileged their access, the stronger the identity verification you should perform
- the reliance you are placing on the assertions of any third parties - for example, if equipment maintenance is performed by an external contractor, you should gain sufficient confidence in the contractor's identity proofing procedures
- whether certain roles should require more stringent background checks or security clearances

See NCSC guidance on identity and access management for more information.

Individually identifying and authenticating

Wherever possible, staff members should access information, systems and networks using their own individual credentials. You should understand the roles and associated individuals with authorisation to access each information asset, system or network.

There may be some scenarios where there is a clear operational justification for using shared credentials. For example, in emergency planning, you may decide that it is appropriate for your organisation to keep laptops with generic user accounts for emergency use. In this scenario, you would apply additional security measures to keep the credentials secure and carefully manage access to them.

Limiting authorised users and systems

You should ensure that staff members are granted access to information proportionally, so that they have exactly the level of access they need to fulfil their roles.

Role-based access controls are key to achieving these requirements, and 'least privilege' should be a guiding principle. If a user only needs to view records, for example, there is no need for them to have an elevated role such as 'admin' or 'super user'. The 'view-only user' role will give them the level of access they require.

For each information asset, system or network supporting your essential functions, you should know the way that identity and access management procedures have been applied to achieve the desired outcome.

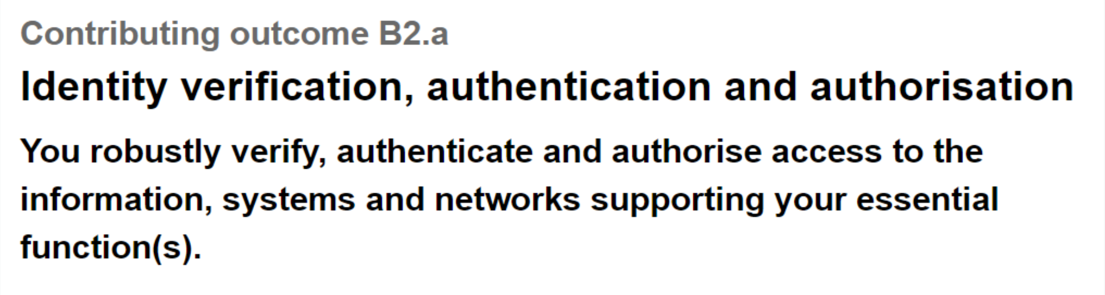
Additional authentication mechanisms

See guidance on the NHS England and DHSC multi-factor authentication policy for more information.

Principle: B2 Identity and access control

Contributing outcome:
B2.a Identity verification, authentication and authorisation

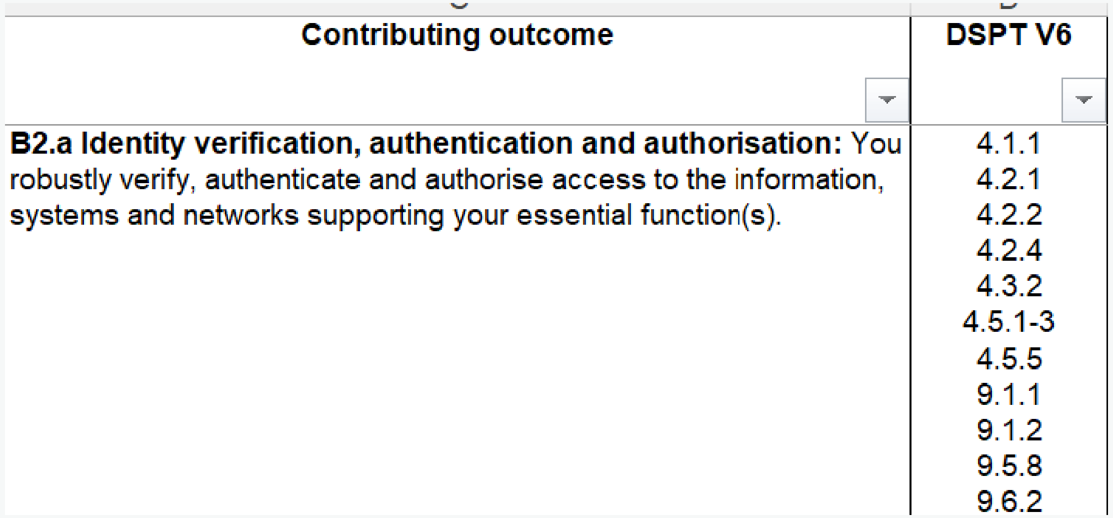
Supporting evidence



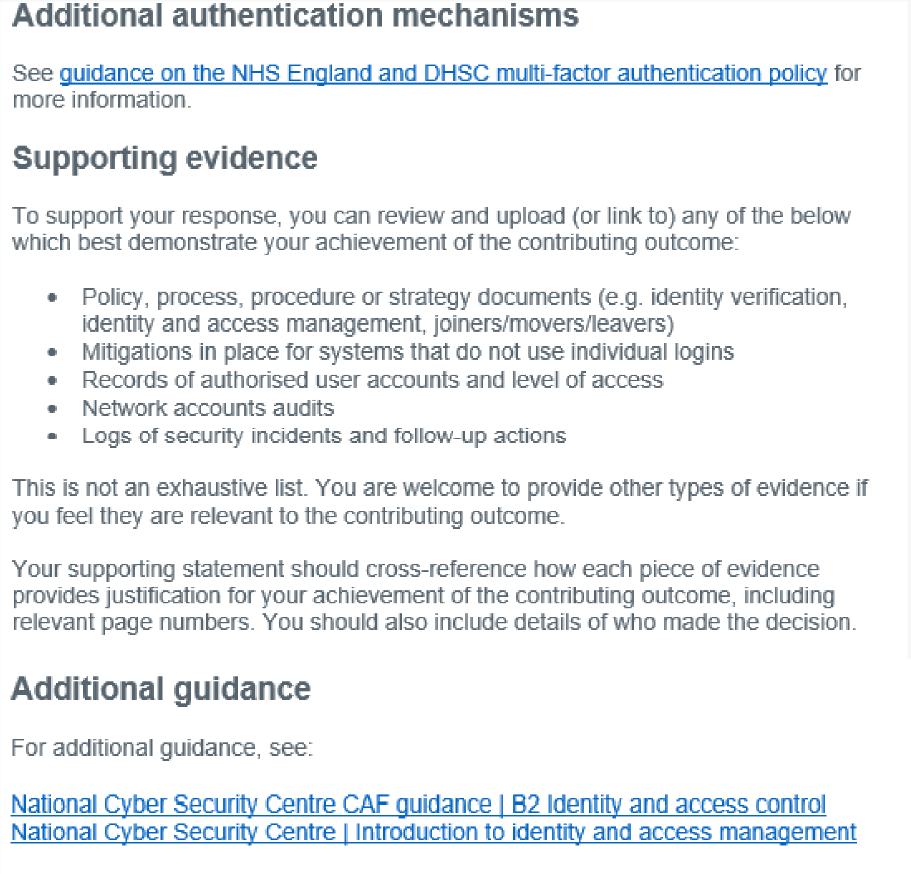
Contributing outcome B2.a

Identity verification, authentication and authorisation

You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s).



Contributing outcome	DSPT V6
B2.a Identity verification, authentication and authorisation: You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s).	4.1.1 4.2.1 4.2.2 4.2.4 4.3.2 4.5.1-3 4.5.5 9.1.1 9.1.2 9.5.8 9.6.2



Additional authentication mechanisms

See guidance on the NHS England and DHSC multi-factor authentication policy for more information.

Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Policy, process, procedure or strategy documents (e.g. identity verification, identity and access management, joiners/movers/leavers)
- Mitigations in place for systems that do not use individual logins
- Records of authorised user accounts and level of access
- Network accounts audits
- Logs of security incidents and follow-up actions

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

Additional guidance

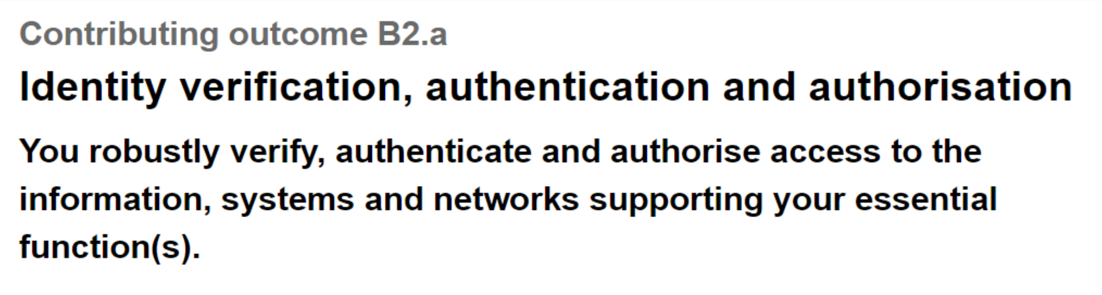
For additional guidance, see:

National Cyber Security Centre CAF guidance | B2 Identity and access control
National Cyber Security Centre | Introduction to identity and access management

Principle: B2 Identity and access control

Contributing outcome:
B2.a Identity verification, authentication and authorisation

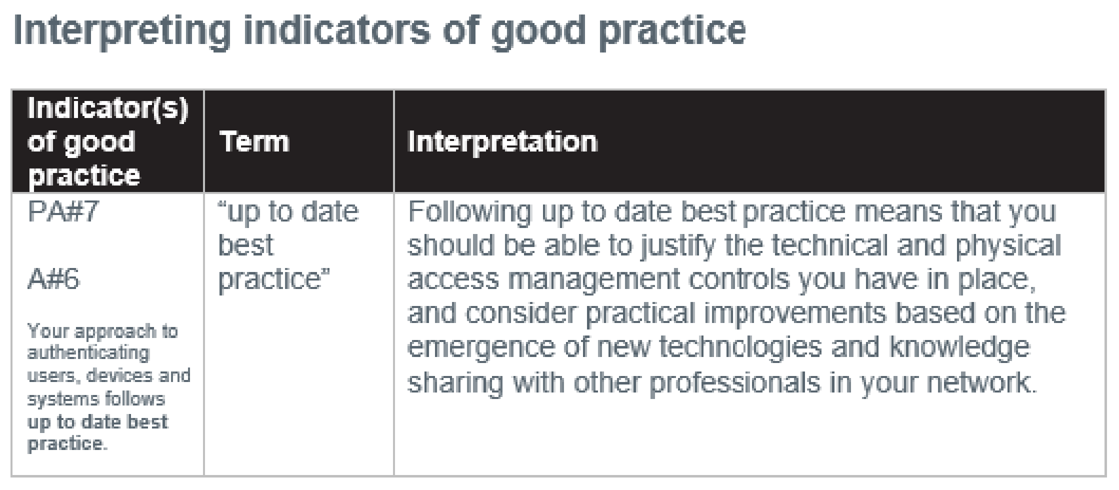
Interpretations



Contributing outcome B2.a

Identity verification, authentication and authorisation

You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s).



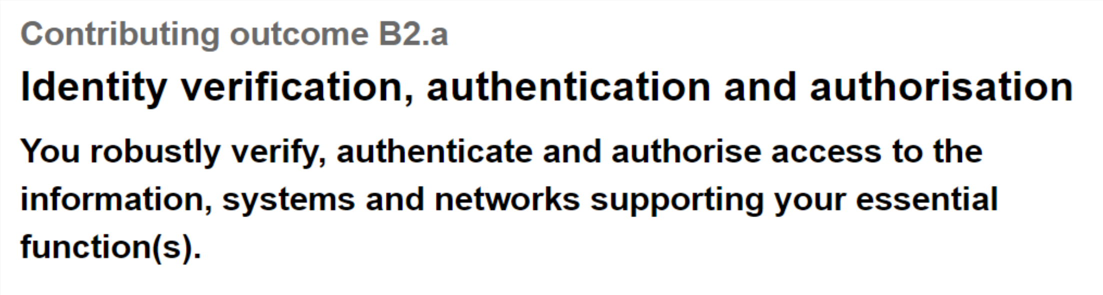
Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#7 A#6 Your approach to authenticating users, devices and systems follows **up to date best practice.**	"up to date best practice"	Following up to date best practice means that you should be able to justify the technical and physical access management controls you have in place, and consider practical improvements based on the emergence of new technologies and knowledge sharing with other professionals in your network.

Principle: B2 Identity and access control

Contributing outcome:
B2.a Identity verification, authentication and authorisation

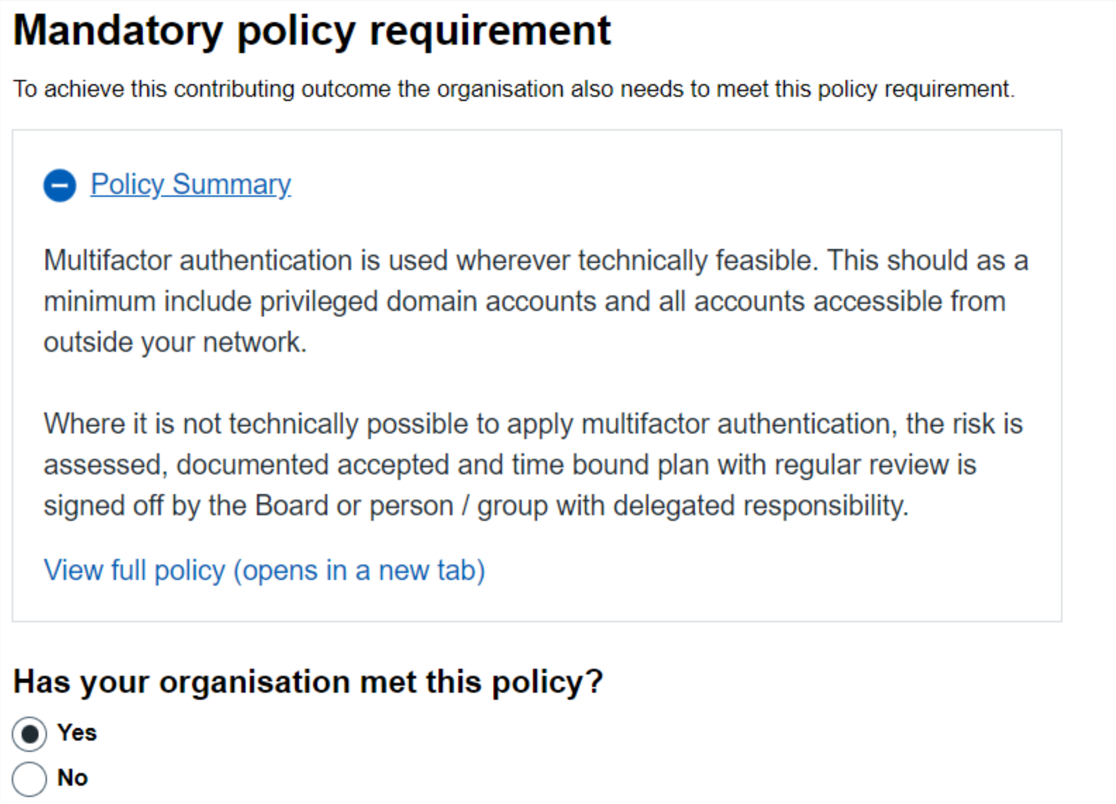
Mandatory Policy Requirement



Contributing outcome B2.a

Identity verification, authentication and authorisation

You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s).



Mandatory policy requirement

To achieve this contributing outcome the organisation also needs to meet this policy requirement.

Policy Summary

Multifactor authentication is used wherever technically feasible. This should as a minimum include privileged domain accounts and all accounts accessible from outside your network.

Where it is not technically possible to apply multifactor authentication, the risk is assessed, documented accepted and time bound plan with regular review is signed off by the Board or person / group with delegated responsibility.

View full policy (opens in a new tab)

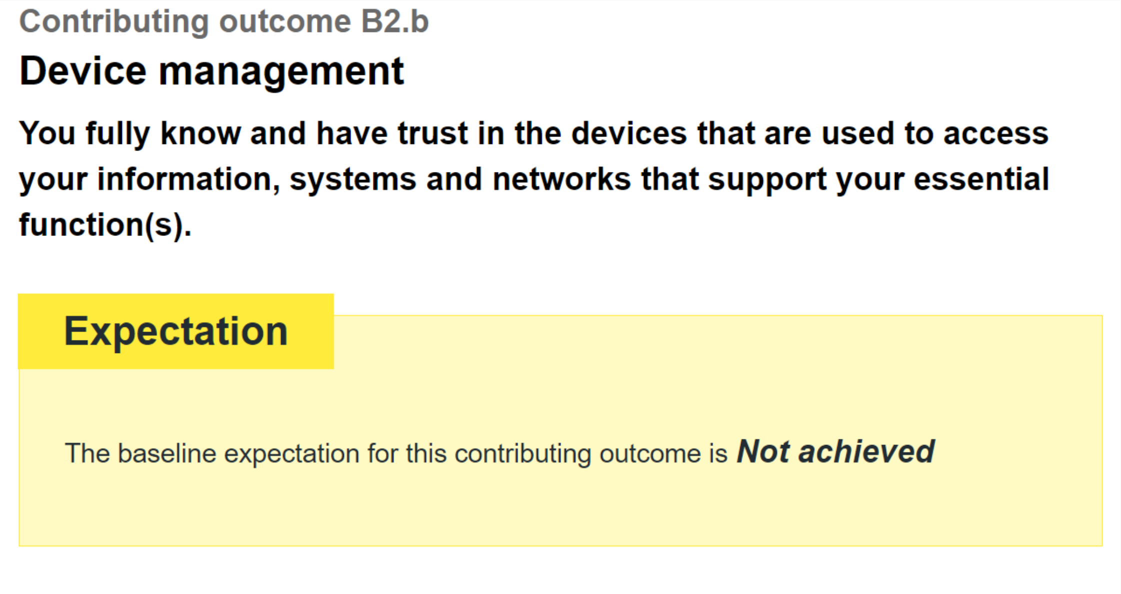
Has your organisation met this policy?

● Yes

○ No

Principle: B2 Identity and access control

Contributing outcome: B2.b Device Management



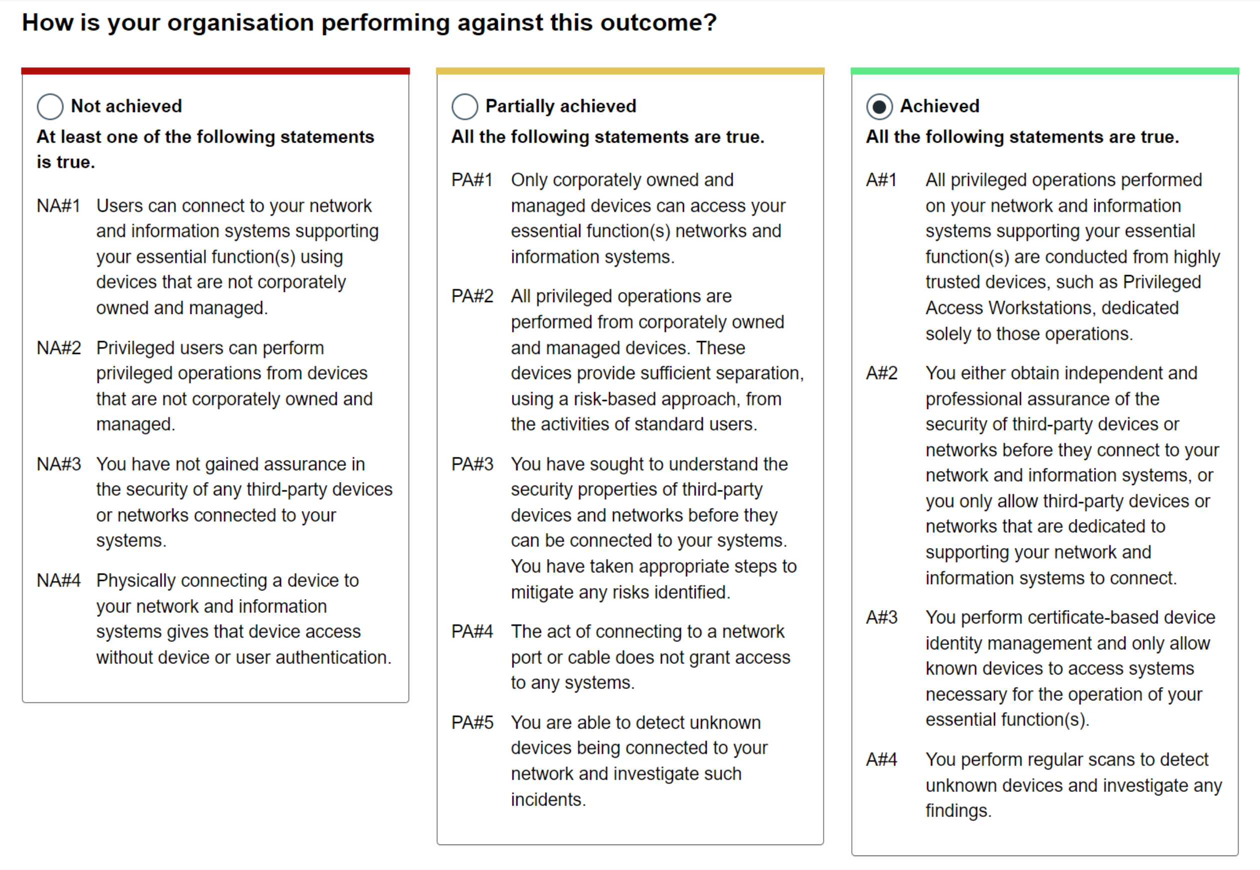
Contributing outcome B2.b

Device management

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

Expectation

The baseline expectation for this contributing outcome is ***Not achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Users can connect to your network and information systems supporting your essential function(s) using devices that are not corporately owned and managed.

NA#2 Privileged users can perform privileged operations from devices that are not corporately owned and managed.

NA#3 You have not gained assurance in the security of any third-party devices or networks connected to your systems.

NA#4 Physically connecting a device to your network and information systems gives that device access without device or user authentication.

○ **Partially achieved**

All the following statements are true.

PA#1 Only corporately owned and managed devices can access your essential function(s) networks and information systems.

PA#2 All privileged operations are performed from corporately owned and managed devices. These devices provide sufficient separation, using a risk-based approach, from the activities of standard users.

PA#3 You have sought to understand the security properties of third-party devices and networks before they can be connected to your systems. You have taken appropriate steps to mitigate any risks identified.

PA#4 The act of connecting to a network port or cable does not grant access to any systems.

PA#5 You are able to detect unknown devices being connected to your network and investigate such incidents.

● **Achieved**

All the following statements are true.

A#1 All privileged operations performed on your network and information systems supporting your essential function(s) are conducted from highly trusted devices, such as Privileged Access Workstations, dedicated solely to those operations.

A#2 You either obtain independent and professional assurance of the security of third-party devices or networks before they connect to your network and information systems, or you only allow third-party devices or networks that are dedicated to supporting your network and information systems to connect.

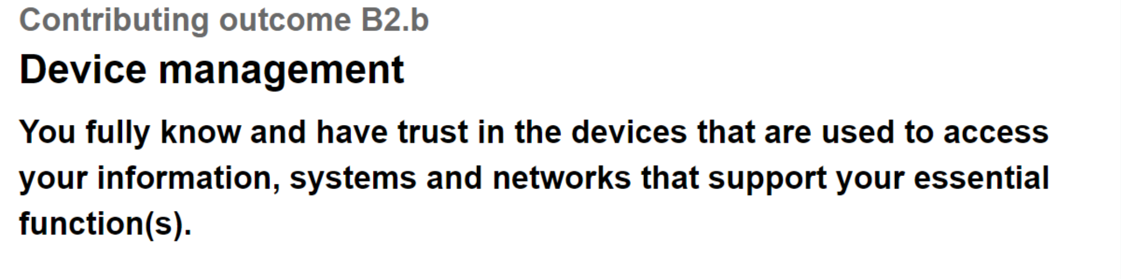
A#3 You perform certificate-based device identity management and only allow known devices to access systems necessary for the operation of your essential function(s).

A#4 You perform regular scans to detect unknown devices and investigate any findings.

Principle: B2 Identity and access control

Contributing outcome:
B2.b Device Management

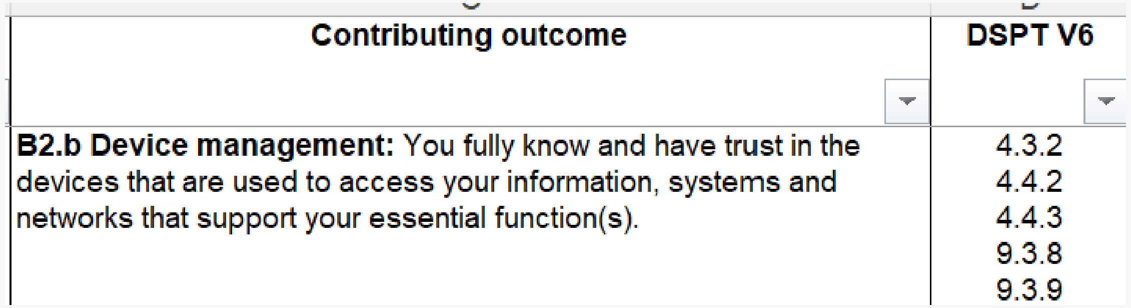
DSPT Mapping and Guidance



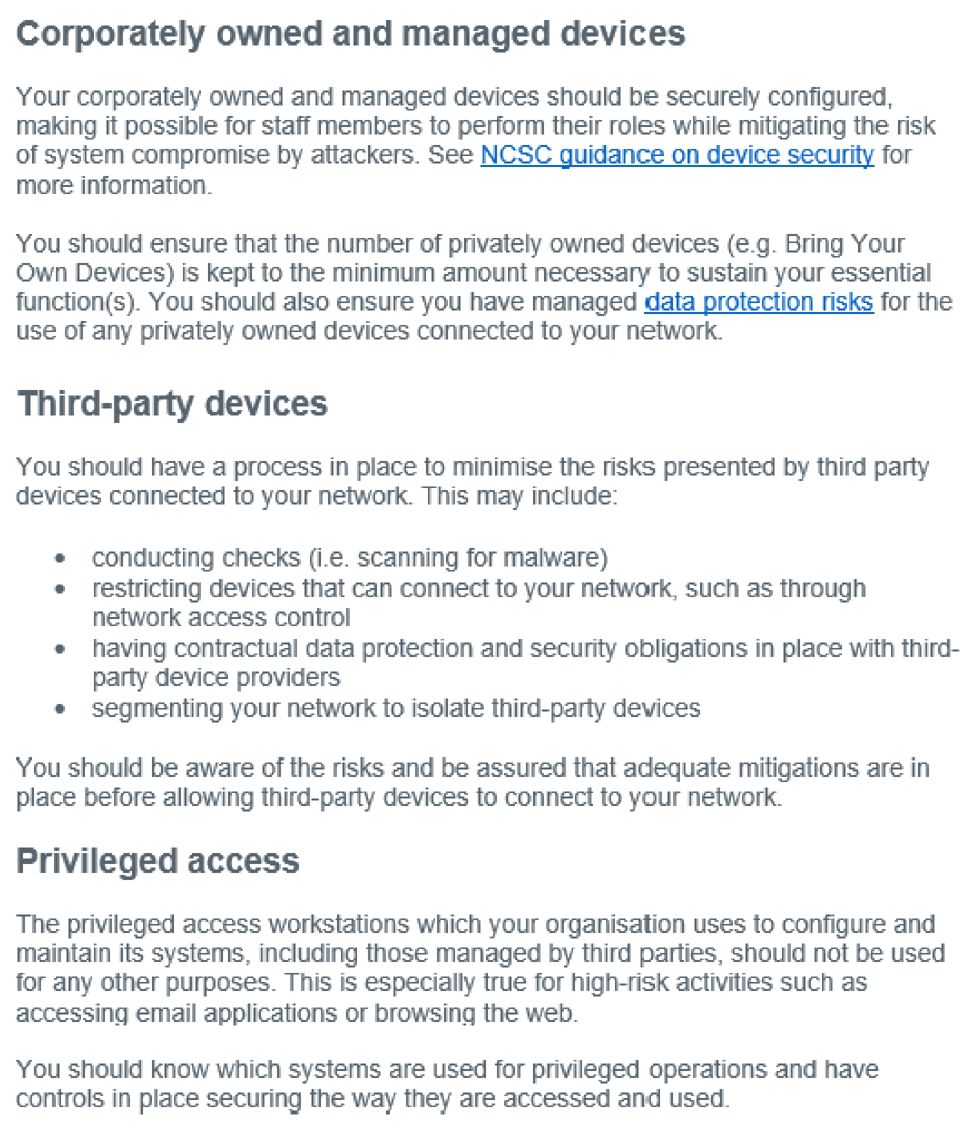
Contributing outcome B2.b

Device management

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



Contributing outcome	DSPT V6
B2.b Device management: You fully know and have trust in the devices that are used to access your information, systems and networks that support your essential function(s).	4.3.2 4.4.2 4.4.3 9.3.8 9.3.9



Corporately owned and managed devices

Your corporately owned and managed devices should be securely configured, making it possible for staff members to perform their roles while mitigating the risk of system compromise by attackers. See NCSC guidance on device security for more information.

You should ensure that the number of privately owned devices (e.g. Bring Your Own Devices) is kept to the minimum amount necessary to sustain your essential function(s). You should also ensure you have managed data protection risks for the use of any privately owned devices connected to your network.

Third-party devices

You should have a process in place to minimise the risks presented by third party devices connected to your network. This may include:

- conducting checks (i.e. scanning for malware)
- restricting devices that can connect to your network, such as through network access control
- having contractual data protection and security obligations in place with third-party device providers
- segmenting your network to isolate third-party devices

You should be aware of the risks and be assured that adequate mitigations are in place before allowing third-party devices to connect to your network.

Privileged access

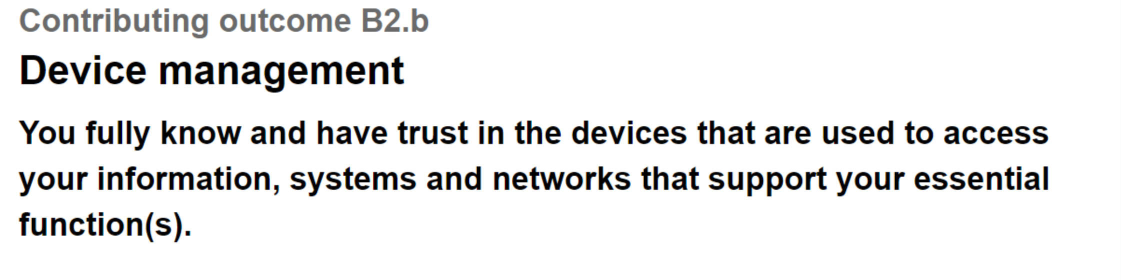
The privileged access workstations which your organisation uses to configure and maintain its systems, including those managed by third parties, should not be used for any other purposes. This is especially true for high-risk activities such as accessing email applications or browsing the web.

You should know which systems are used for privileged operations and have controls in place securing the way they are accessed and used.

Principle: B2 Identity and access control

Contributing outcome:
B2.b Device Management

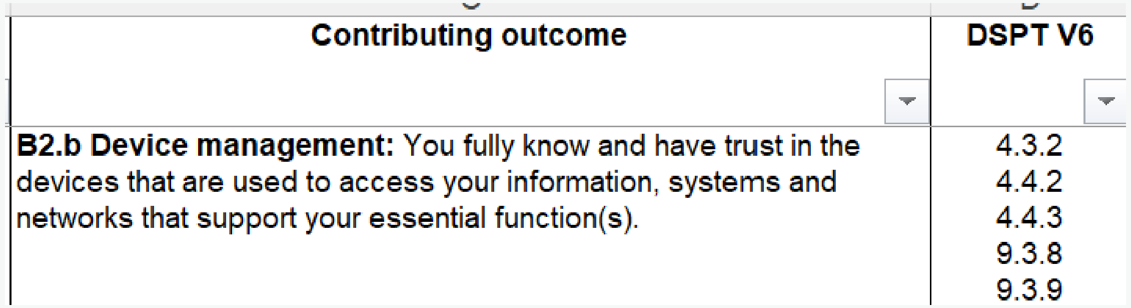
Supporting evidence



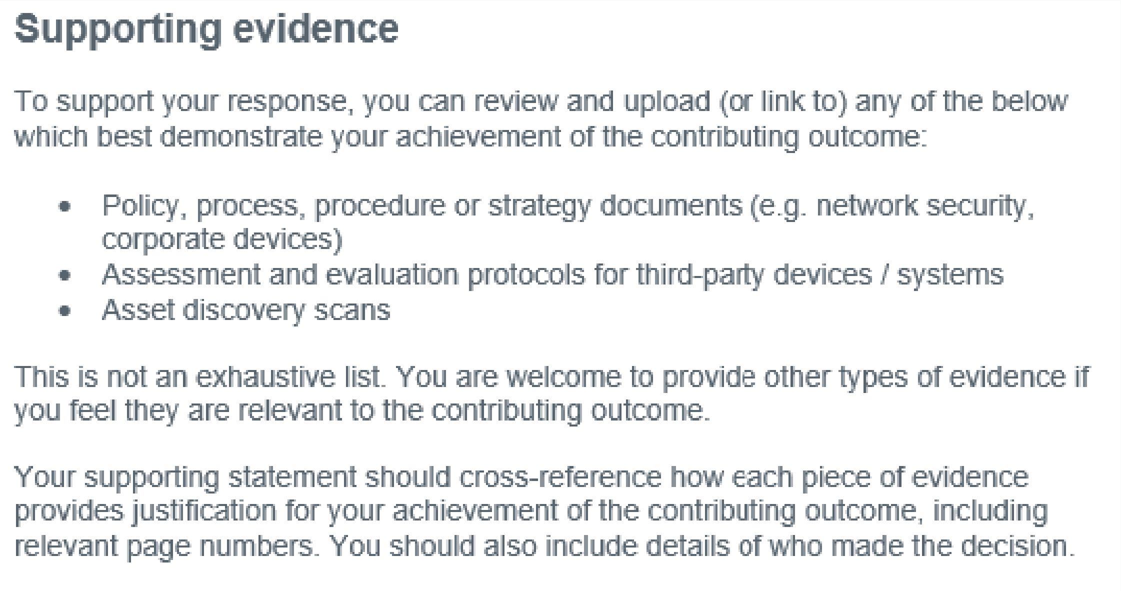
Contributing outcome B2.b

Device management

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



Contributing outcome	DSPT V6
B2.b Device management: You fully know and have trust in the devices that are used to access your information, systems and networks that support your essential function(s).	4.3.2 4.4.2 4.4.3 9.3.8 9.3.9



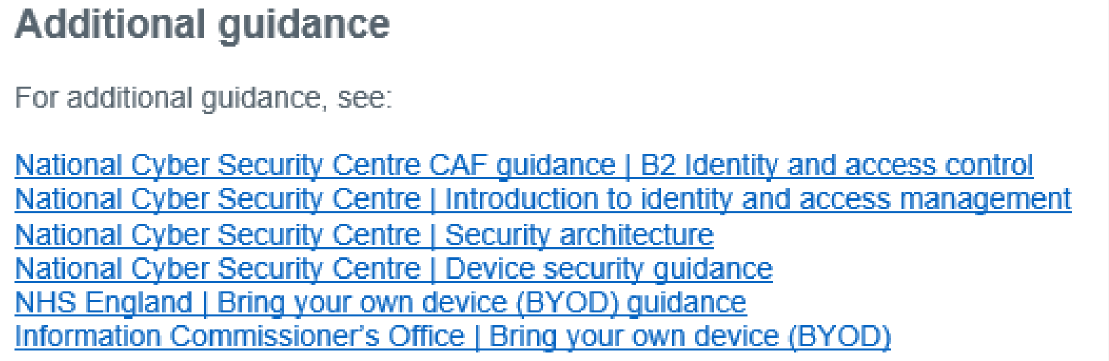
Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Policy, process, procedure or strategy documents (e.g. network security, corporate devices)
- Assessment and evaluation protocols for third-party devices / systems
- Asset discovery scans

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.



Additional guidance

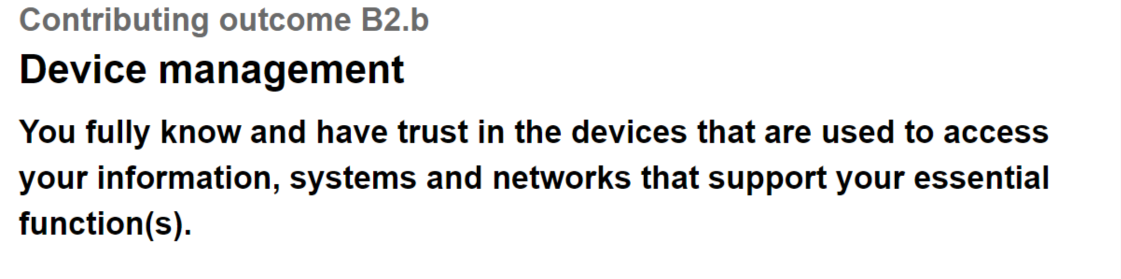
For additional guidance, see:

National Cyber Security Centre CAF guidance | B2 Identity and access control
National Cyber Security Centre | Introduction to identity and access management
National Cyber Security Centre | Security architecture
National Cyber Security Centre | Device security guidance
NHS England | Bring your own device (BYOD) guidance
Information Commissioner's Office | Bring your own device (BYOD)

Principle: B2 Identity and access control

Contributing outcome:
B2.b Device Management

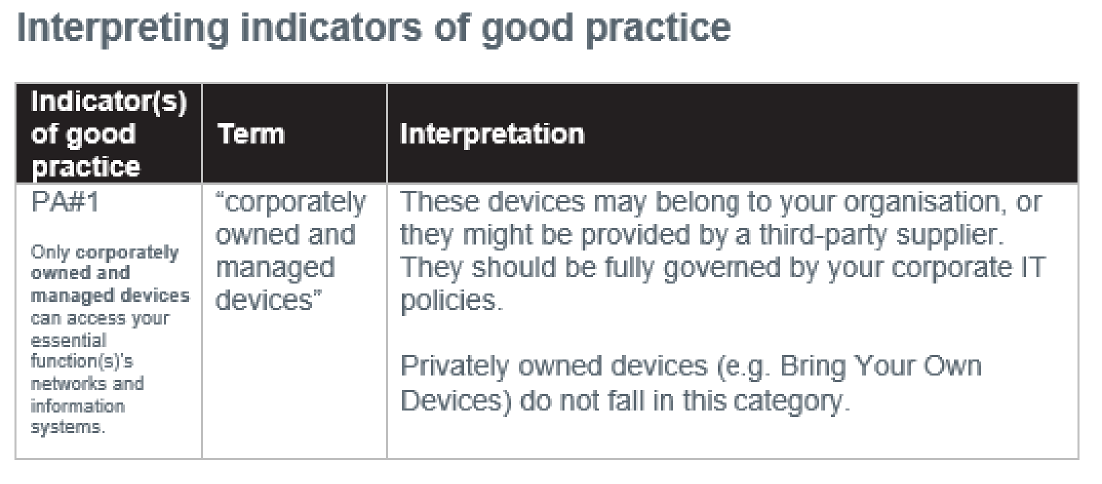
Interpretations



Contributing outcome B2.b

Device management

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

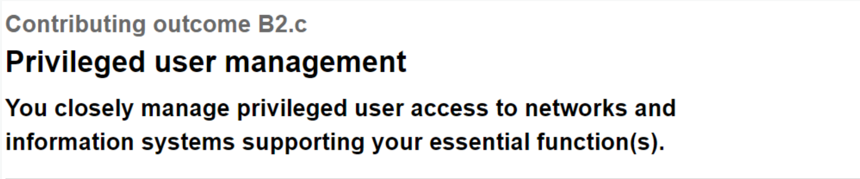


Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#1 **Only corporately owned and managed devices** can access your essential function(s)'s networks and information systems.	"corporately owned and managed devices"	These devices may belong to your organisation, or they might be provided by a third-party supplier. They should be fully governed by your corporate IT policies. Privately owned devices (e.g. Bring Your Own Devices) do not fall in this category.

Principle: B2 Identity and access control

Contributing outcome:
B2.c Privileged user management



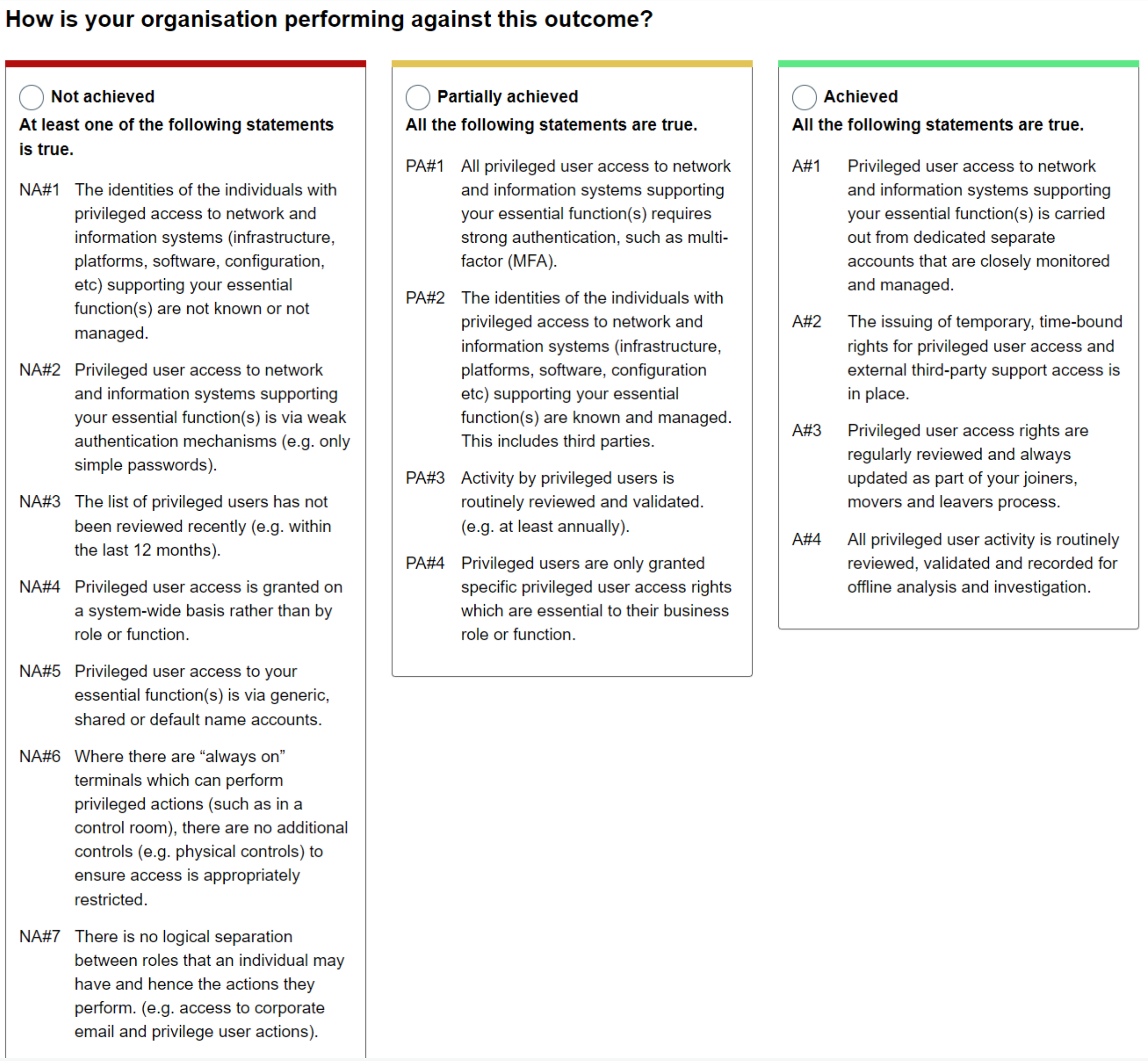
Contributing outcome B2.c

Privileged user management

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

Expectation

The baseline expectation for this contributing outcome is ***Not achieved***



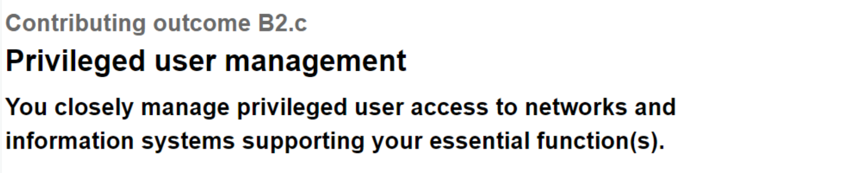
How is your organisation performing against this outcome?

○ **Not achieved**	○ **Partially achieved**	○ **Achieved**
At least one of the following statements is true.	**All the following statements are true.**	**All the following statements are true.**
NA#1 The identities of the individuals with privileged access to network and information systems (infrastructure, platforms, software, configuration, etc) supporting your essential function(s) are not known or not managed.	PA#1 All privileged user access to network and information systems supporting your essential function(s) requires strong authentication, such as multi-factor (MFA).	A#1 Privileged user access to network and information systems supporting your essential function(s) is carried out from dedicated separate accounts that are closely monitored and managed.
NA#2 Privileged user access to network and information systems supporting your essential function(s) is via weak authentication mechanisms (e.g. only simple passwords).	PA#2 The identities of the individuals with privileged access to network and information systems (infrastructure, platforms, software, configuration etc) supporting your essential function(s) are known and managed. This includes third parties.	A#2 The issuing of temporary, time-bound rights for privileged user access and external third-party support access is in place.
NA#3 The list of privileged users has not been reviewed recently (e.g. within the last 12 months).	PA#3 Activity by privileged users is routinely reviewed and validated. (e.g. at least annually).	A#3 Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process.
NA#4 Privileged user access is granted on a system-wide basis rather than by role or function.	PA#4 Privileged users are only granted specific privileged user access rights which are essential to their business role or function.	A#4 All privileged user activity is routinely reviewed, validated and recorded for offline analysis and investigation.
NA#5 Privileged user access to your essential function(s) is via generic, shared or default name accounts.		
NA#6 Where there are "always on" terminals which can perform privileged actions (such as in a control room), there are no additional controls (e.g. physical controls) to ensure access is appropriately restricted.		
NA#7 There is no logical separation between roles that an individual may have and hence the actions they perform. (e.g. access to corporate email and privilege user actions).		

Principle: B2 Identity and access control

Contributing outcome:
B2.c Privileged user management

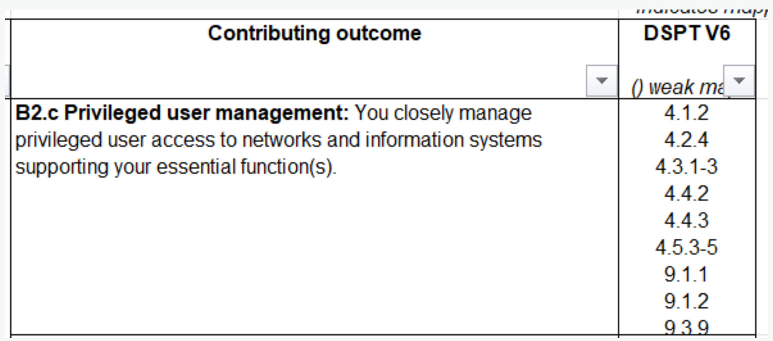
DSPT Mapping and Guidance



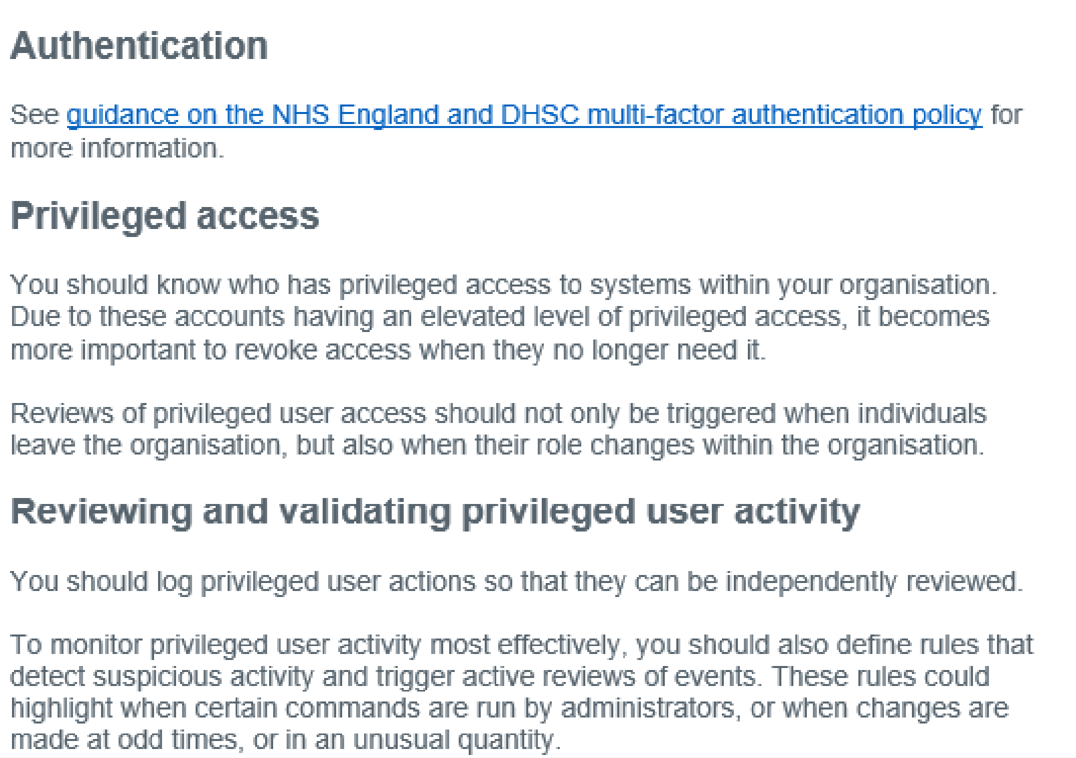
Contributing outcome B2.c

Privileged user management

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



Contributing outcome	DSPT V6 () weak ma
B2.c Privileged user management: You closely manage privileged user access to networks and information systems supporting your essential function(s).	4.1.2 4.2.4 4.3.1-3 4.4.2 4.4.3 4.5.3-5 9.1.1 9.1.2 9.3.9



Authentication

See guidance on the NHS England and DHSC multi-factor authentication policy for more information.

Privileged access

You should know who has privileged access to systems within your organisation. Due to these accounts having an elevated level of privileged access, it becomes more important to revoke access when they no longer need it.

Reviews of privileged user access should not only be triggered when individuals leave the organisation, but also when their role changes within the organisation.

Reviewing and validating privileged user activity

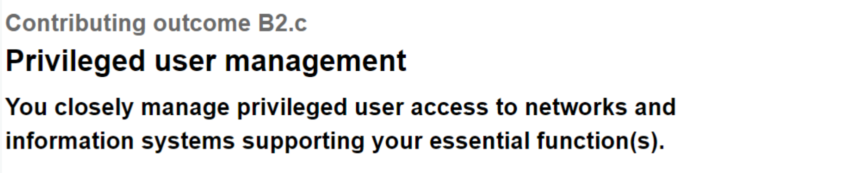
You should log privileged user actions so that they can be independently reviewed.

To monitor privileged user activity most effectively, you should also define rules that detect suspicious activity and trigger active reviews of events. These rules could highlight when certain commands are run by administrators, or when changes are made at odd times, or in an unusual quantity.

Principle: B2 Identity and access control

Contributing outcome:
B2.c Privileged user management

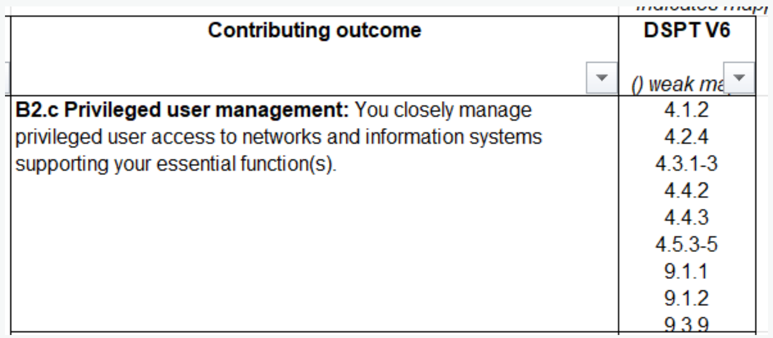
Supporting Evidence



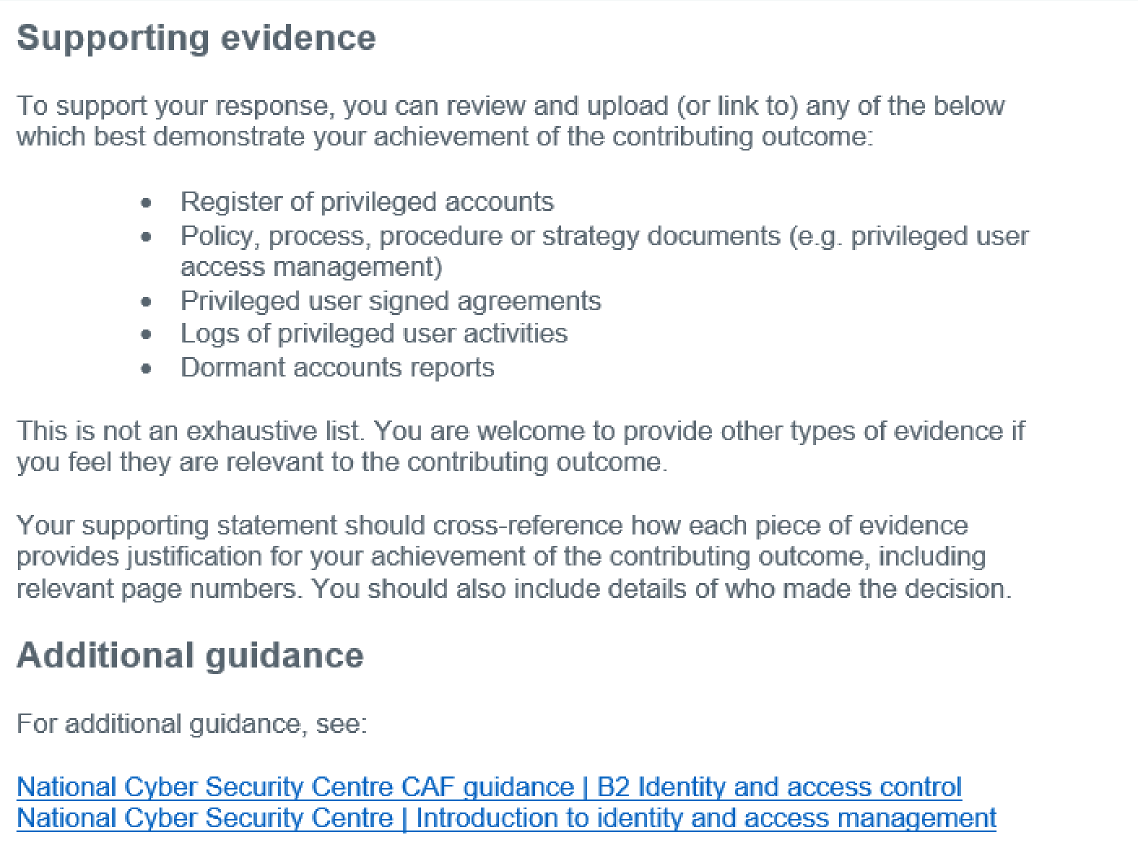
Contributing outcome B2.c

Privileged user management

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



Contributing outcome	DSPT V6 () weak ma
B2.c Privileged user management: You closely manage privileged user access to networks and information systems supporting your essential function(s).	4.1.2 4.2.4 4.3.1-3 4.4.2 4.4.3 4.5.3-5 9.1.1 9.1.2 9.3.9



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Register of privileged accounts
- Policy, process, procedure or strategy documents (e.g. privileged user access management)
- Privileged user signed agreements
- Logs of privileged user activities
- Dormant accounts reports

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

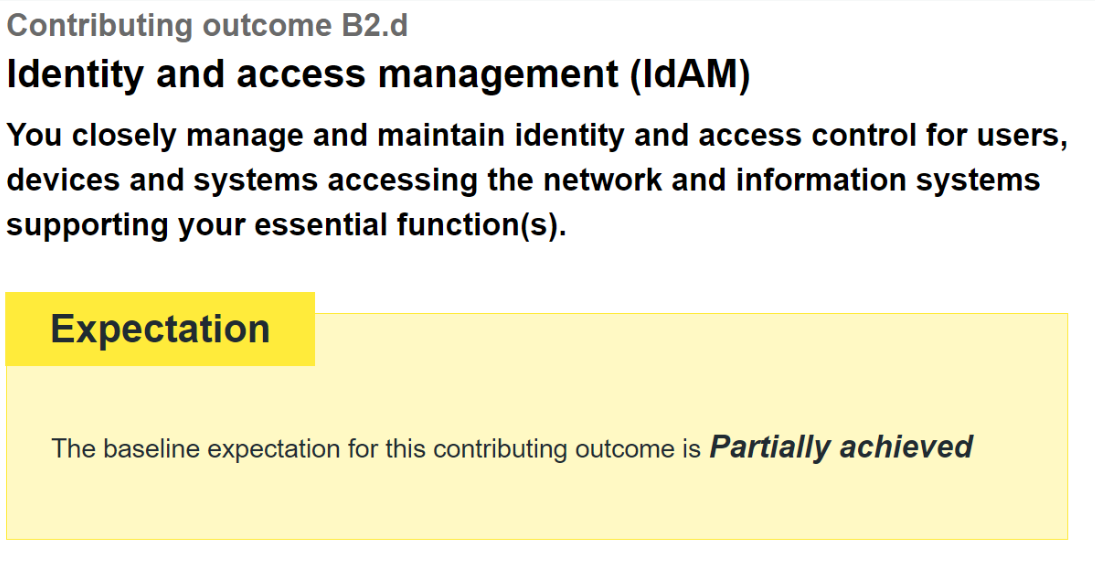
Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B2 Identity and access control
National Cyber Security Centre | Introduction to identity and access management

Principle: B2 Identity and access control

Contributing outcome:
B2.d Identity and access management (IdAM)



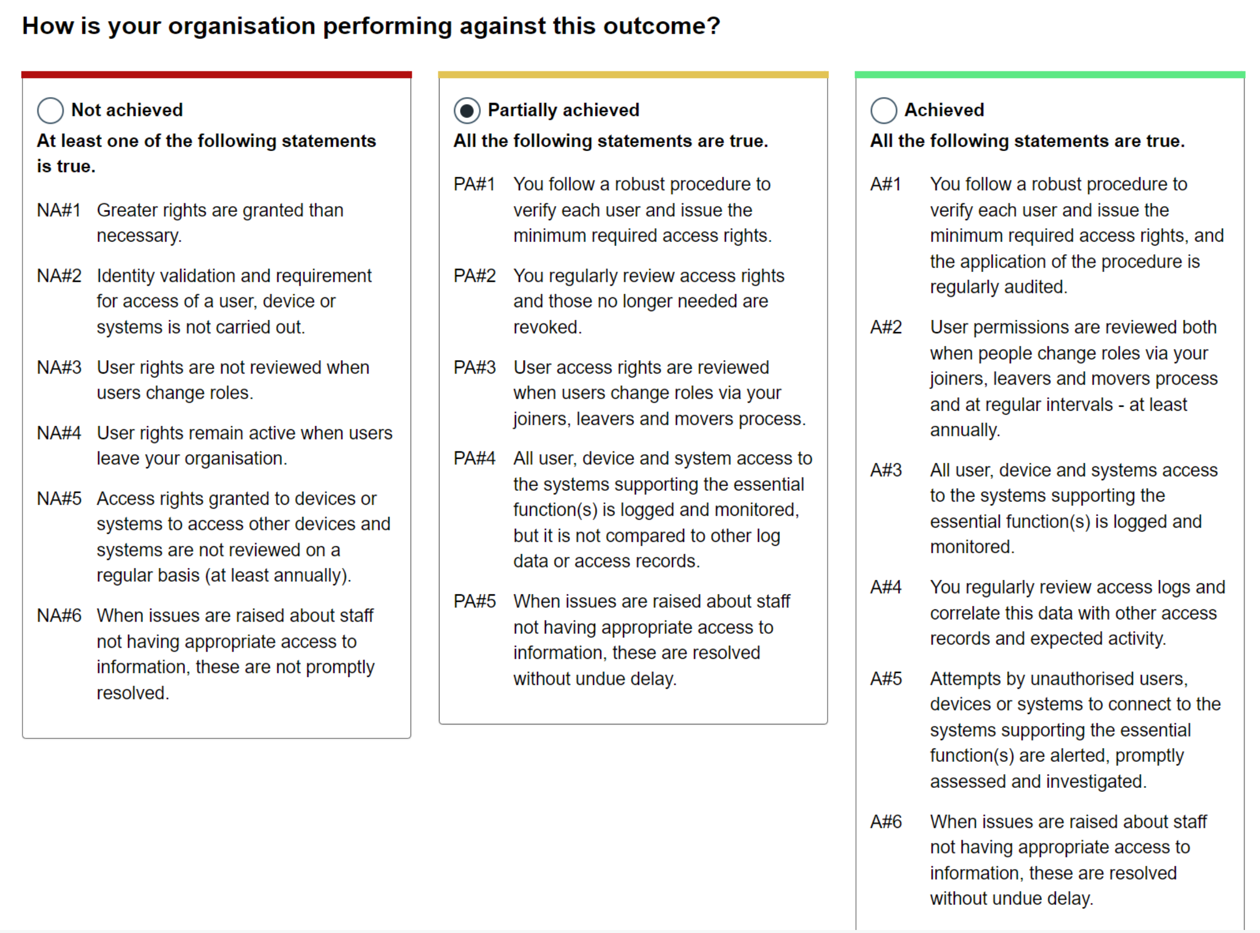
Contributing outcome B2.d

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).

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Greater rights are granted than necessary.

NA#2 Identity validation and requirement for access of a user, device or systems is not carried out.

NA#3 User rights are not reviewed when users change roles.

NA#4 User rights remain active when users leave your organisation.

NA#5 Access rights granted to devices or systems to access other devices and systems are not reviewed on a regular basis (at least annually).

NA#6 When issues are raised about staff not having appropriate access to information, these are not promptly resolved.

● **Partially achieved**

All the following statements are true.

PA#1 You follow a robust procedure to verify each user and issue the minimum required access rights.

PA#2 You regularly review access rights and those no longer needed are revoked.

PA#3 User access rights are reviewed when users change roles via your joiners, leavers and movers process.

PA#4 All user, device and system access to the systems supporting the essential function(s) is logged and monitored, but it is not compared to other log data or access records.

PA#5 When issues are raised about staff not having appropriate access to information, these are resolved without undue delay.

○ **Achieved**

All the following statements are true.

A#1 You follow a robust procedure to verify each user and issue the minimum required access rights, and the application of the procedure is regularly audited.

A#2 User permissions are reviewed both when people change roles via your joiners, leavers and movers process and at regular intervals - at least annually.

A#3 All user, device and systems access to the systems supporting the essential function(s) is logged and monitored.

A#4 You regularly review access logs and correlate this data with other access records and expected activity.

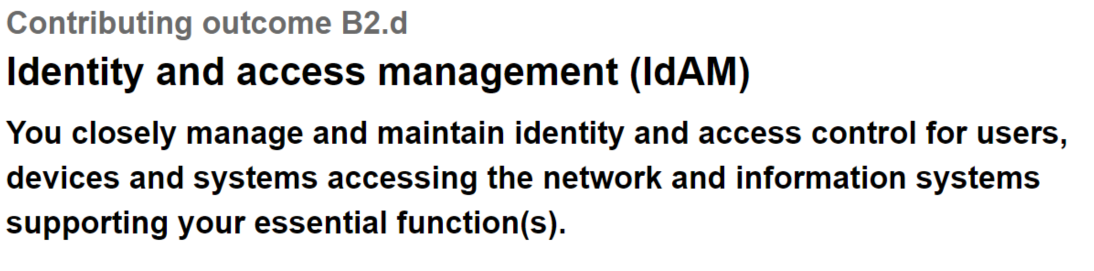
A#5 Attempts by unauthorised users, devices or systems to connect to the systems supporting the essential function(s) are alerted, promptly assessed and investigated.

A#6 When issues are raised about staff not having appropriate access to information, these are resolved without undue delay.

Principle: B2 Identity and access control

Contributing outcome:
B2.d Identity and access management (IdAM)

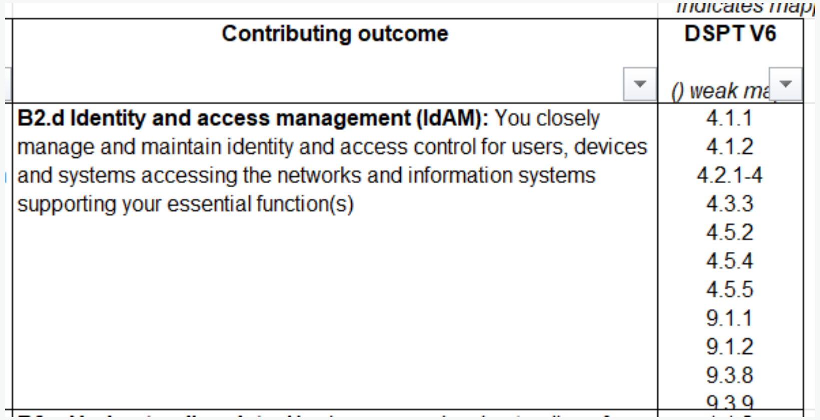
DSPT Mapping and Guidance



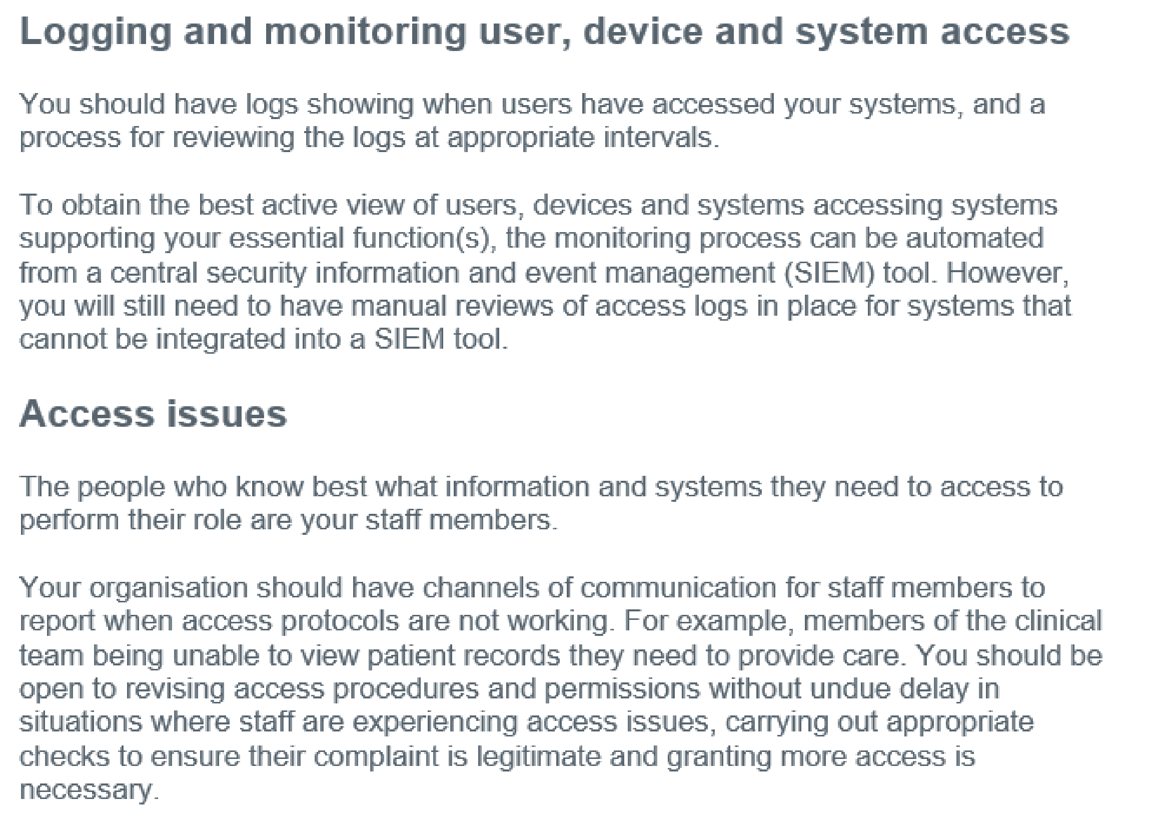
Contributing outcome B2.d

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).



Contributing outcome	indicates map DSPT V6 () weak ma
B2.d Identity and access management (IdAM): You closely manage and maintain identity and access control for users, devices and systems accessing the networks and information systems supporting your essential function(s)	4.1.1 4.1.2 4.2.1-4 4.3.3 4.5.2 4.5.4 4.5.5 9.1.1 9.1.2 9.3.8 9.3.9



Logging and monitoring user, device and system access

You should have logs showing when users have accessed your systems, and a process for reviewing the logs at appropriate intervals.

To obtain the best active view of users, devices and systems accessing systems supporting your essential function(s), the monitoring process can be automated from a central security information and event management (SIEM) tool. However, you will still need to have manual reviews of access logs in place for systems that cannot be integrated into a SIEM tool.

Access issues

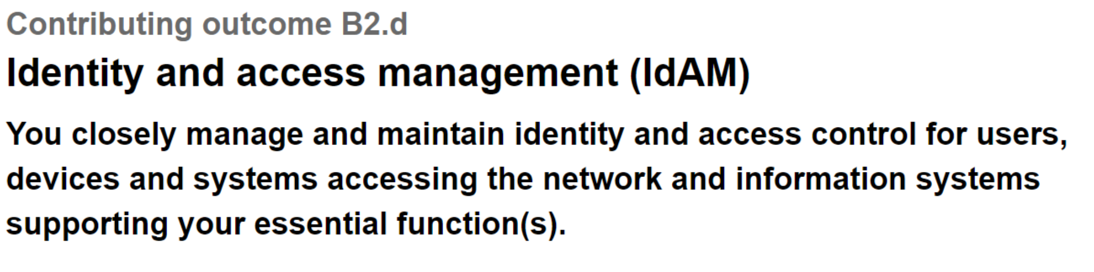
The people who know best what information and systems they need to access to perform their role are your staff members.

Your organisation should have channels of communication for staff members to report when access protocols are not working. For example, members of the clinical team being unable to view patient records they need to provide care. You should be open to revising access procedures and permissions without undue delay in situations where staff are experiencing access issues, carrying out appropriate checks to ensure their complaint is legitimate and granting more access is necessary.

Principle: B2 Identity and access control

Contributing outcome:
B2.d Identity and access management (IdAM)

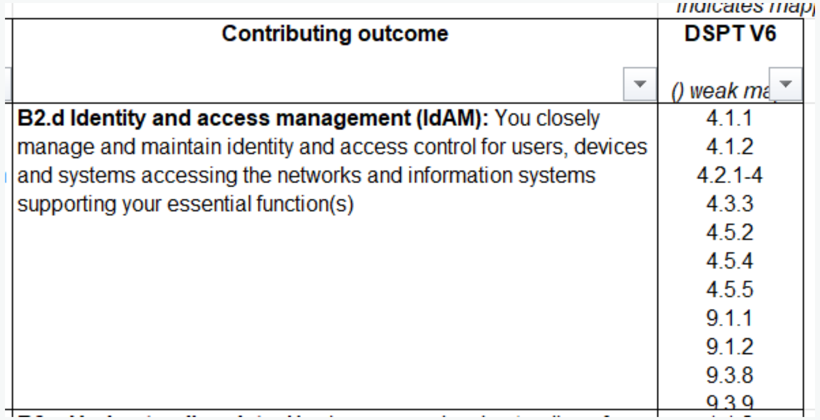
DSPT Mapping and Guidance



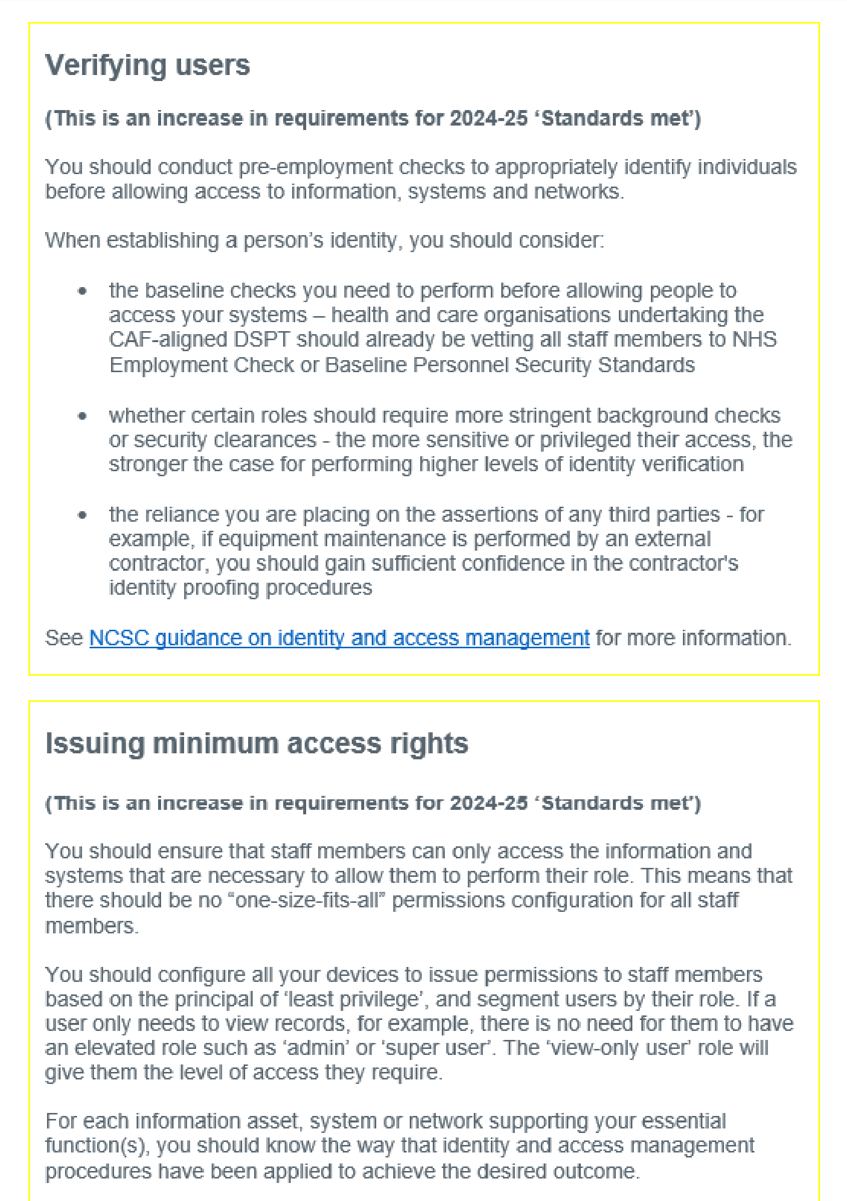
Contributing outcome B2.d

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).



Contributing outcome	indicates map DSPT V6 () weak ma
B2.d Identity and access management (IdAM): You closely manage and maintain identity and access control for users, devices and systems accessing the networks and information systems supporting your essential function(s)	4.1.1 4.1.2 4.2.1-4 4.3.3 4.5.2 4.5.4 4.5.5 9.1.1 9.1.2 9.3.8 9.3.9



Verifying users

(This is an increase in requirements for 2024-25 'Standards met')

You should conduct pre-employment checks to appropriately identify individuals before allowing access to information, systems and networks.

When establishing a person's identity, you should consider:

- the baseline checks you need to perform before allowing people to access your systems – health and care organisations undertaking the CAF-aligned DSPT should already be vetting all staff members to NHS Employment Check or Baseline Personnel Security Standards
- whether certain roles should require more stringent background checks or security clearances - the more sensitive or privileged their access, the stronger the case for performing higher levels of identity verification
- the reliance you are placing on the assertions of any third parties - for example, if equipment maintenance is performed by an external contractor, you should gain sufficient confidence in the contractor's identity proofing procedures

See NCSC guidance on identity and access management for more information.

Issuing minimum access rights

(This is an increase in requirements for 2024-25 'Standards met')

You should ensure that staff members can only access the information and systems that are necessary to allow them to perform their role. This means that there should be no "one-size-fits-all" permissions configuration for all staff members.

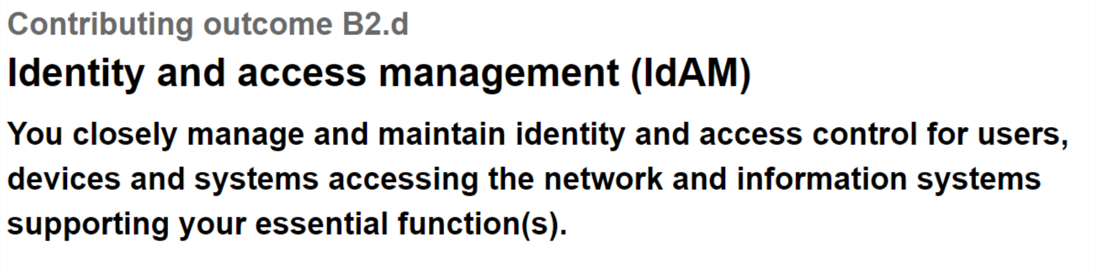
You should configure all your devices to issue permissions to staff members based on the principal of 'least privilege', and segment users by their role. If a user only needs to view records, for example, there is no need for them to have an elevated role such as 'admin' or 'super user'. The 'view-only user' role will give them the level of access they require.

For each information asset, system or network supporting your essential function(s), you should know the way that identity and access management procedures have been applied to achieve the desired outcome.

Principle: B2 Identity and access control

Contributing outcome:
B2.d Identity and access management (IdAM)

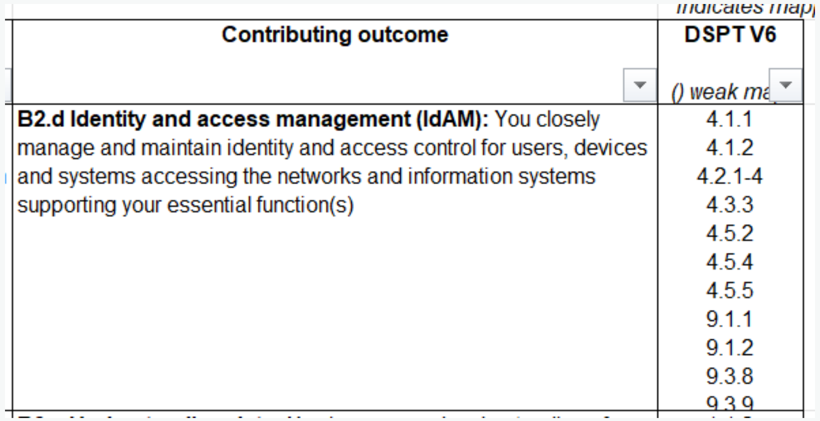
Supporting Evidence



Contributing outcome B2.d

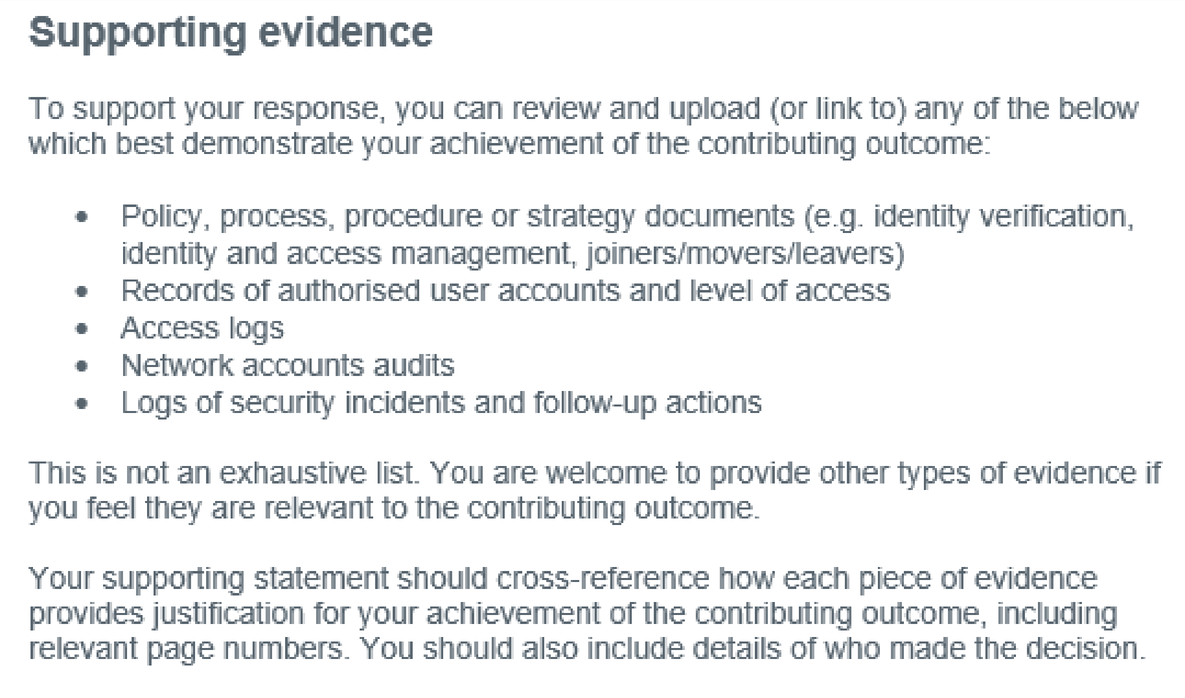
Identity and access management (IdAM)

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).



indicates map

Contributing outcome	DSPT V6 () weak ma
B2.d Identity and access management (IdAM): You closely manage and maintain identity and access control for users, devices and systems accessing the networks and information systems supporting your essential function(s)	4.1.1 4.1.2 4.2.1-4 4.3.3 4.5.2 4.5.4 4.5.5 9.1.1 9.1.2 9.3.8 9.3.9



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Policy, process, procedure or strategy documents (e.g. identity verification, identity and access management, joiners/movers/leavers)
- Records of authorised user accounts and level of access
- Access logs
- Network accounts audits
- Logs of security incidents and follow-up actions

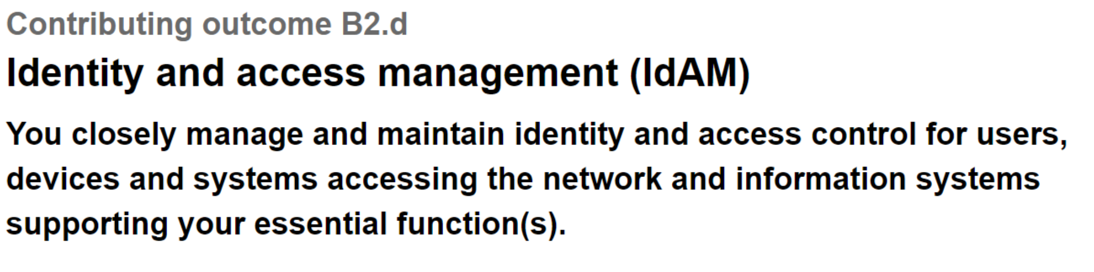
This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

Principle: B2 Identity and access control

Contributing outcome:
B2.d Identity and access management (IdAM)

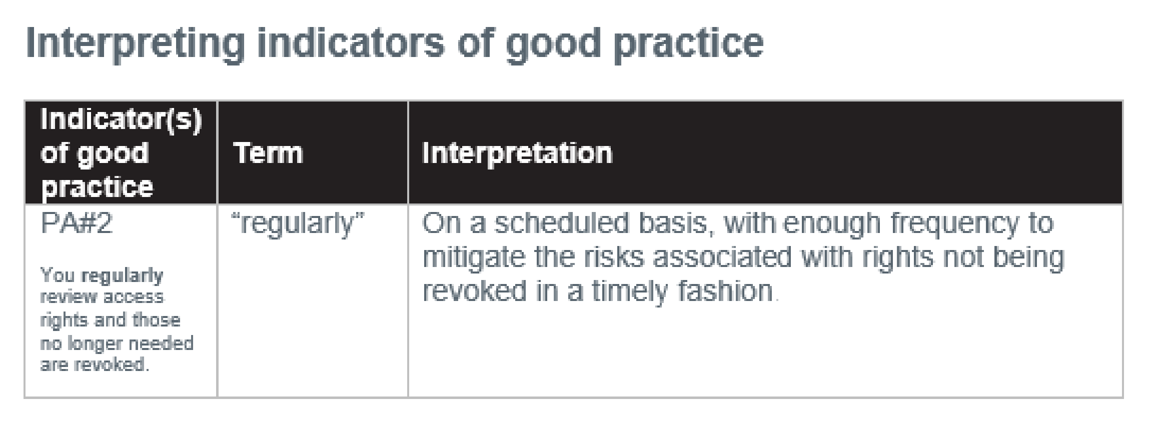
Interpretations



Contributing outcome 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).

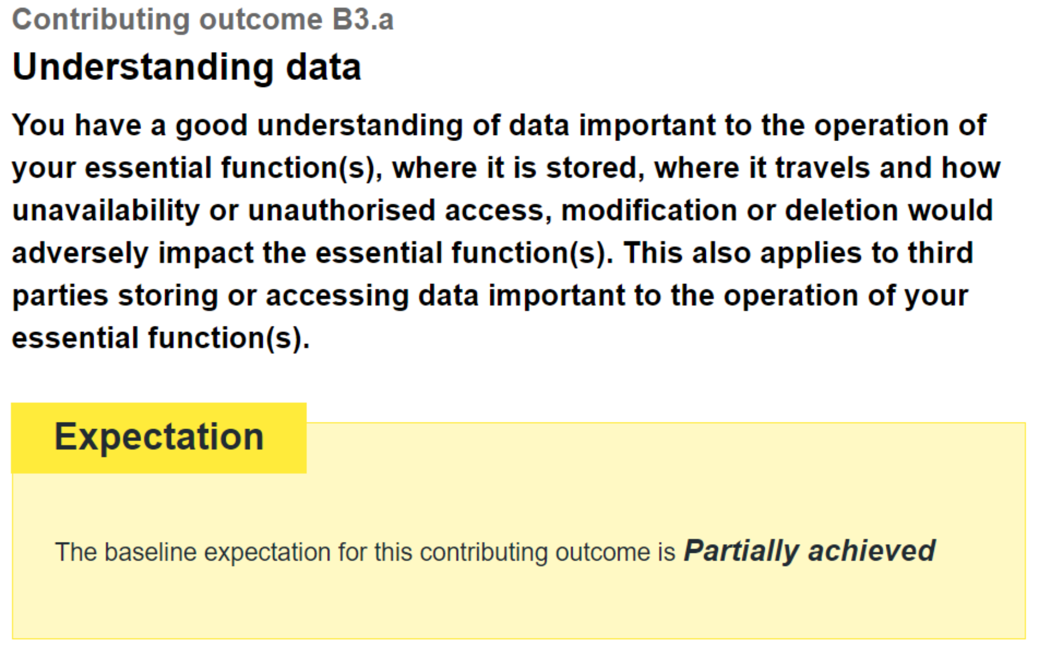


Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#2 You regularly review access rights and those no longer needed are revoked.	"regularly"	On a scheduled basis, with enough frequency to mitigate the risks associated with rights not being revoked in a timely fashion.

Principle: B3 Data Security

Contributing outcome:
B3.a Understanding data



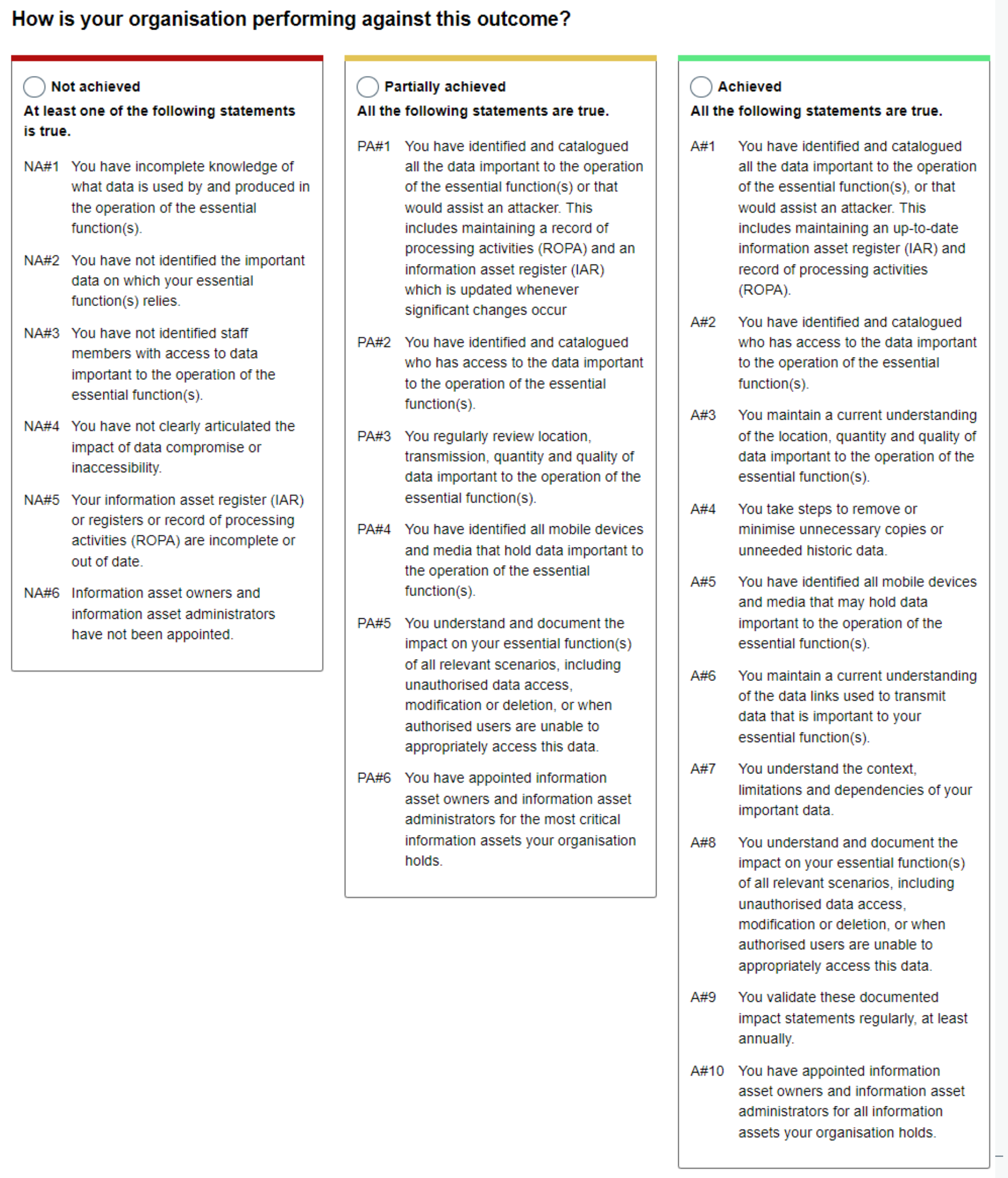
Contributing outcome B3.a

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).

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 You have incomplete knowledge of what data is used by and produced in the operation of the essential function(s).

NA#2 You have not identified the important data on which your essential function(s) relies.

NA#3 You have not identified staff members with access to data important to the operation of the essential function(s).

NA#4 You have not clearly articulated the impact of data compromise or inaccessibility.

NA#5 Your information asset register (IAR) or registers or record of processing activities (ROPA) are incomplete or out of date.

NA#6 Information asset owners and information asset administrators have not been appointed.

○ **Partially achieved**

All the following statements are true.

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. This includes maintaining a record of processing activities (ROPA) and an information asset register (IAR) which is updated whenever significant changes occur

PA#2 You have identified and catalogued who has access to the data important to the operation of the essential function(s).

PA#3 You regularly review location, transmission, quantity and quality of data important to the operation of the essential function(s).

PA#4 You have identified all mobile devices and media that hold data important to the operation of the essential function(s).

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.

PA#6 You have appointed information asset owners and information asset administrators for the most critical information assets your organisation holds.

○ **Achieved**

All the following statements are true.

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. This includes maintaining an up-to-date information asset register (IAR) and record of processing activities (ROPA).

A#2 You have identified and catalogued who has access to the data important to the operation of the essential function(s).

A#3 You maintain a current understanding of the location, quantity and quality of data important to the operation of the essential function(s).

A#4 You take steps to remove or minimise unnecessary copies or unneeded historic data.

A#5 You have identified all mobile devices and media that may hold data important to the operation of the essential function(s).

A#6 You maintain a current understanding of the data links used to transmit data that is important to your essential function(s).

A#7 You understand the context, limitations and dependencies of your important data.

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.

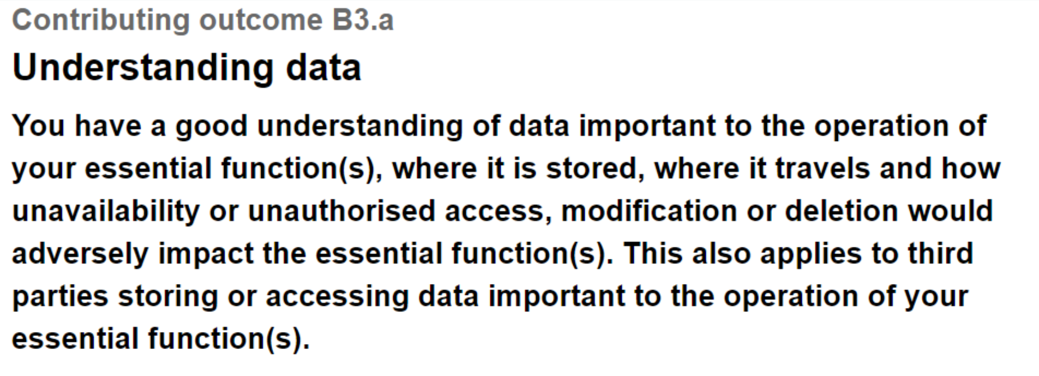
A#9 You validate these documented impact statements regularly, at least annually.

A#10 You have appointed information asset owners and information asset administrators for all information assets your organisation holds.

Principle: B3 Data Security

Contributing outcome:
B3.a Understanding data

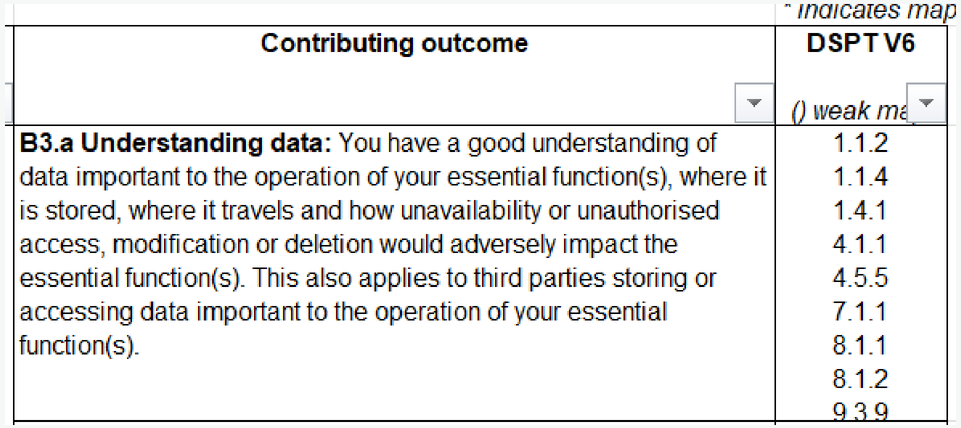
DSPT Mapping and Guidance



Contributing outcome B3.a

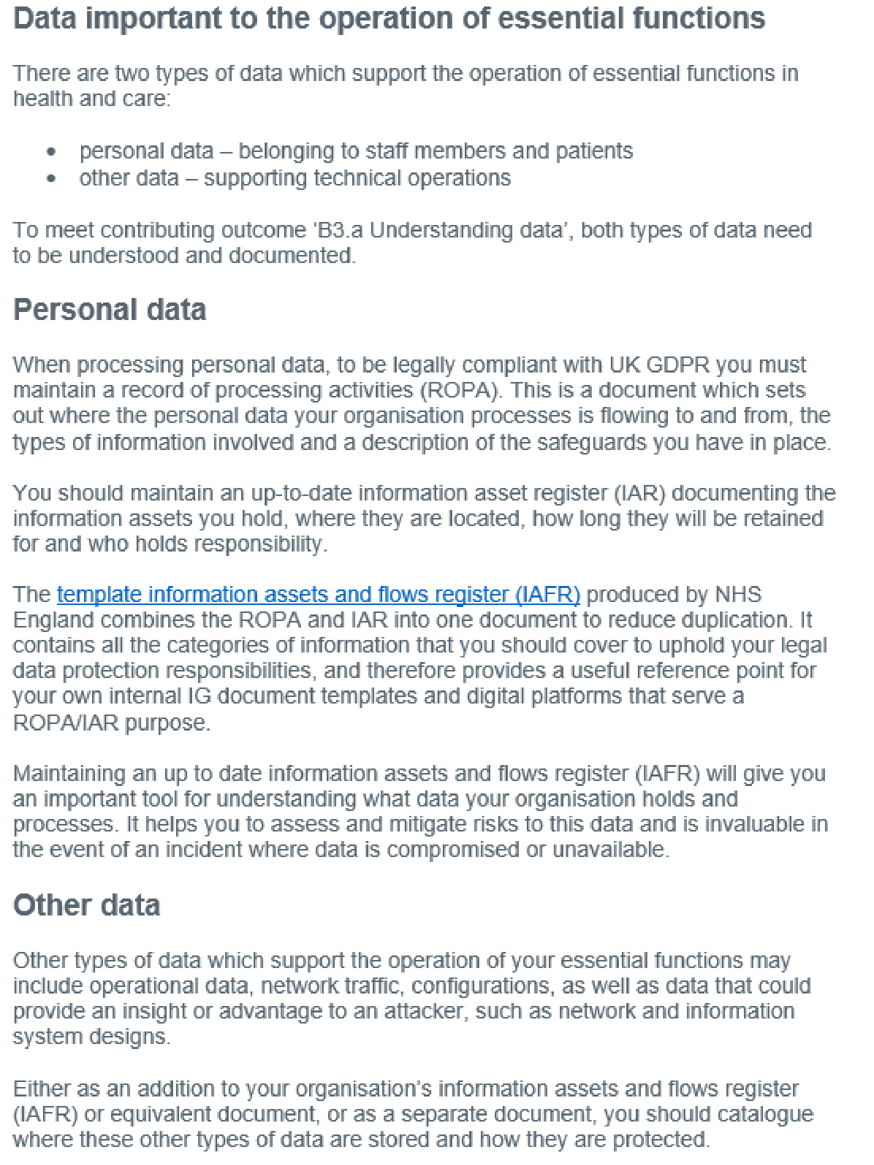
Understanding data

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).



* indicates map

Contributing outcome	DSPT V6 () weak ma
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).	1.1.2 1.1.4 1.4.1 4.1.1 4.5.5 7.1.1 8.1.1 8.1.2 9.3.9



Data important to the operation of essential functions

There are two types of data which support the operation of essential functions in health and care:

- personal data – belonging to staff members and patients
- other data – supporting technical operations

To meet contributing outcome 'B3.a Understanding data', both types of data need to be understood and documented.

Personal data

When processing personal data, to be legally compliant with UK GDPR you must maintain a record of processing activities (ROPA). This is a document which sets out where the personal data your organisation processes is flowing to and from, the types of information involved and a description of the safeguards you have in place.

You should maintain an up-to-date information asset register (IAR) documenting the information assets you hold, where they are located, how long they will be retained for and who holds responsibility.

The template information assets and flows register (IAFR) produced by NHS England combines the ROPA and IAR into one document to reduce duplication. It contains all the categories of information that you should cover to uphold your legal data protection responsibilities, and therefore provides a useful reference point for your own internal IG document templates and digital platforms that serve a ROPA/IAR purpose.

Maintaining an up to date information assets and flows register (IAFR) will give you an important tool for understanding what data your organisation holds and processes. It helps you to assess and mitigate risks to this data and is invaluable in the event of an incident where data is compromised or unavailable.

Other data

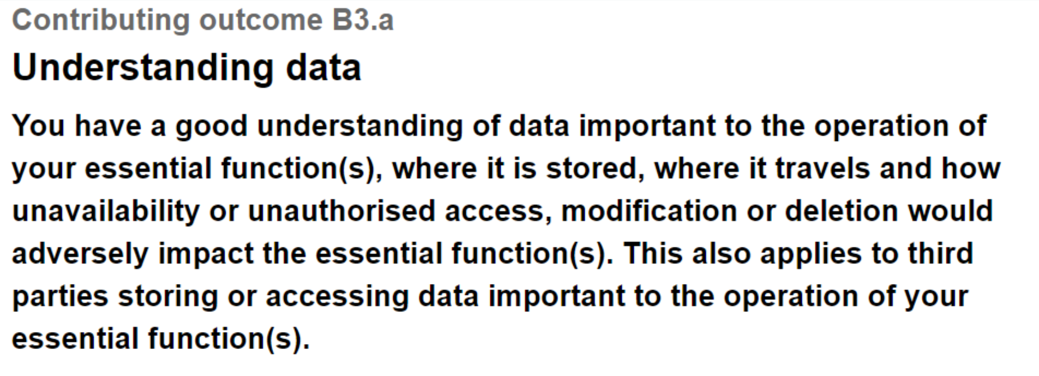
Other types of data which support the operation of your essential functions may include operational data, network traffic, configurations, as well as data that could provide an insight or advantage to an attacker, such as network and information system designs.

Either as an addition to your organisation's information assets and flows register (IAFR) or equivalent document, or as a separate document, you should catalogue where these other types of data are stored and how they are protected.

Principle: B3 Data Security

Contributing outcome:
B3.a Understanding data

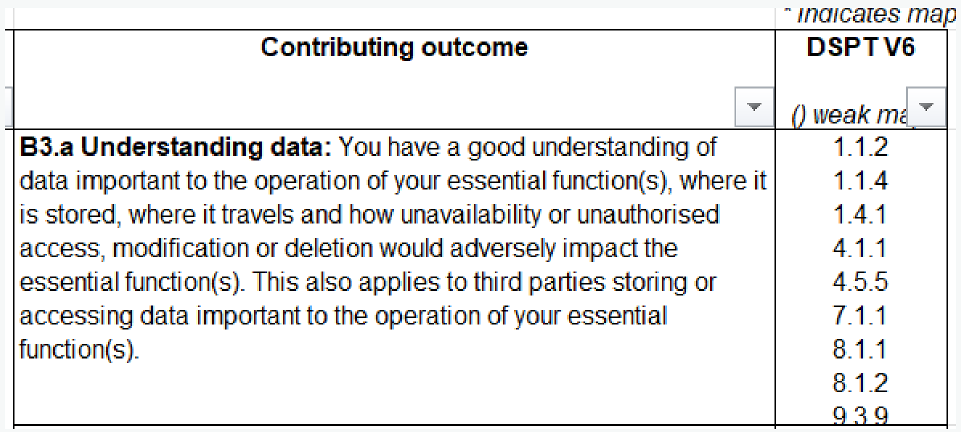
DSPT Mapping and Guidance



Contributing outcome B3.a

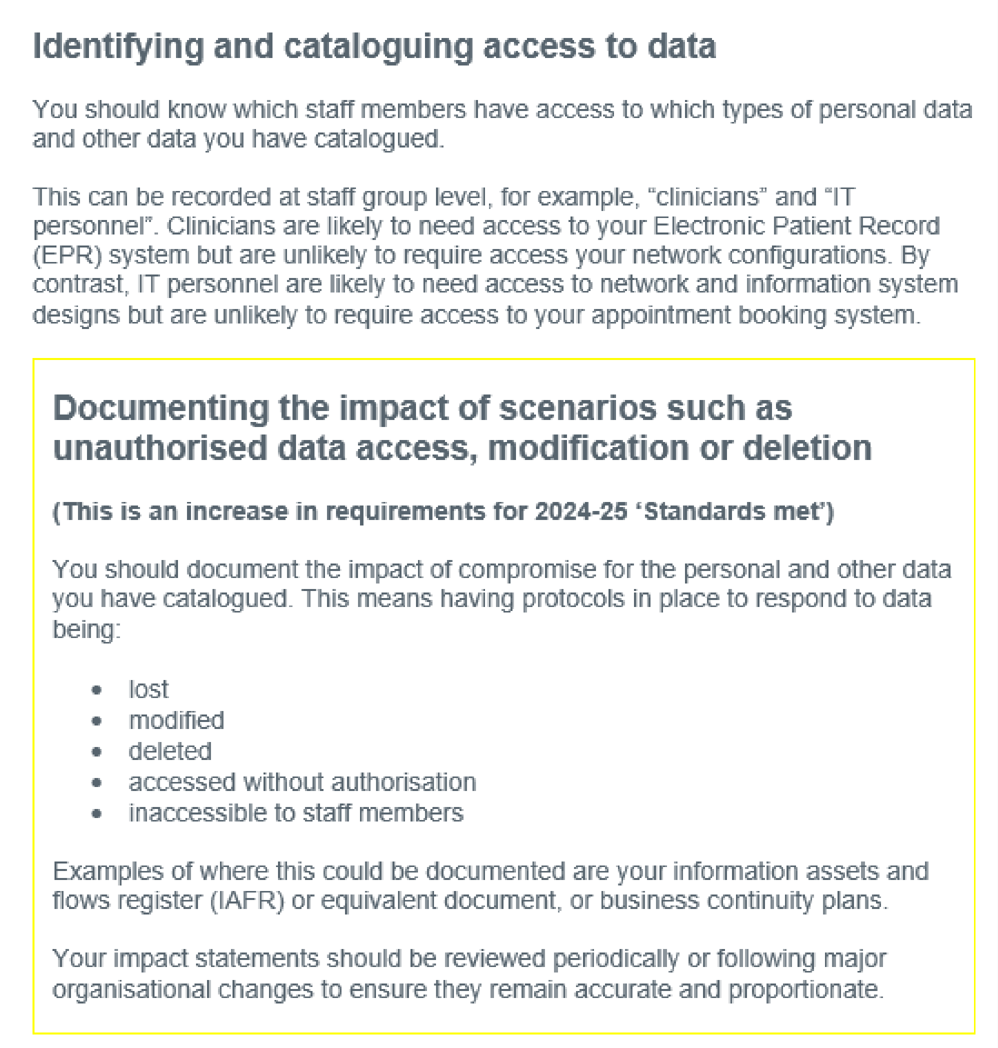
Understanding data

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).



** indicates map*

Contributing outcome	DSPT V6 *() weak ma*
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).	1.1.2 1.1.4 1.4.1 4.1.1 4.5.5 7.1.1 8.1.1 8.1.2 9.3.9



Identifying and cataloguing access to data

You should know which staff members have access to which types of personal data and other data you have catalogued.

This can be recorded at staff group level, for example, “clinicians” and “IT personnel”. Clinicians are likely to need access to your Electronic Patient Record (EPR) system but are unlikely to require access your network configurations. By contrast, IT personnel are likely to need access to network and information system designs but are unlikely to require access to your appointment booking system.

Documenting the impact of scenarios such as unauthorised data access, modification or deletion

(This is an increase in requirements for 2024-25 ‘Standards met’)

You should document the impact of compromise for the personal and other data you have catalogued. This means having protocols in place to respond to data being:

- lost
- modified
- deleted
- accessed without authorisation
- inaccessible to staff members

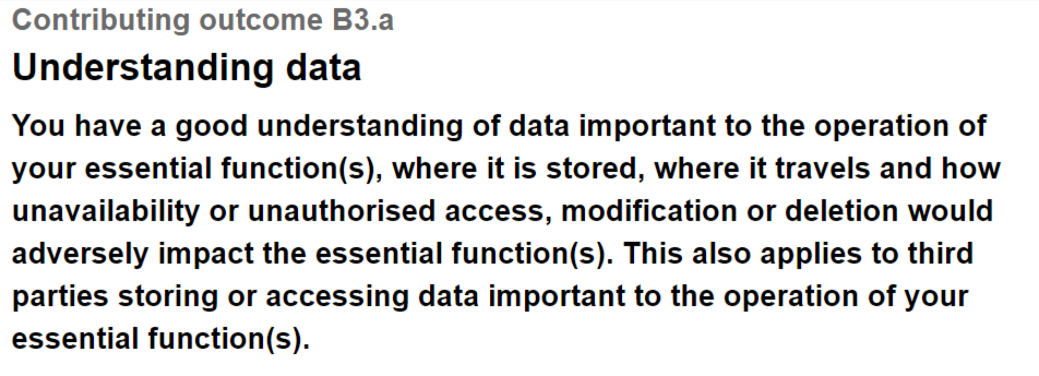
Examples of where this could be documented are your information assets and flows register (IAFR) or equivalent document, or business continuity plans.

Your impact statements should be reviewed periodically or following major organisational changes to ensure they remain accurate and proportionate.

Principle: B3 Data Security

Contributing outcome:
B3.a Understanding data

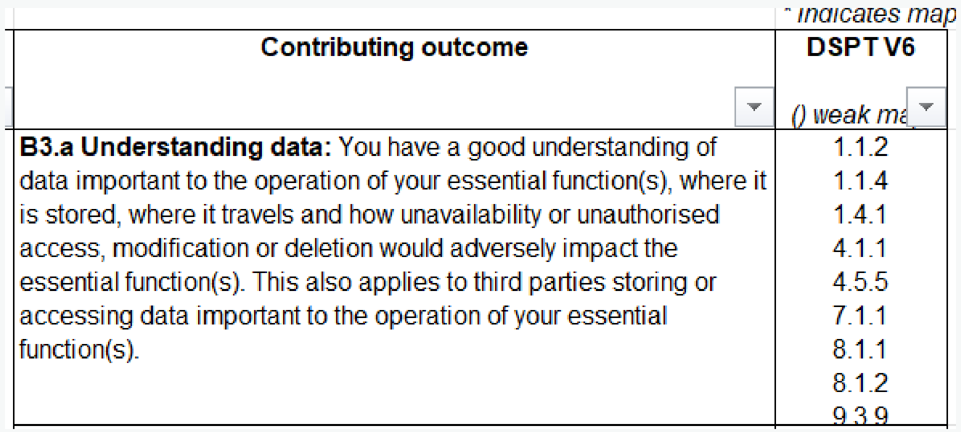
Supporting Evidence



Contributing outcome B3.a

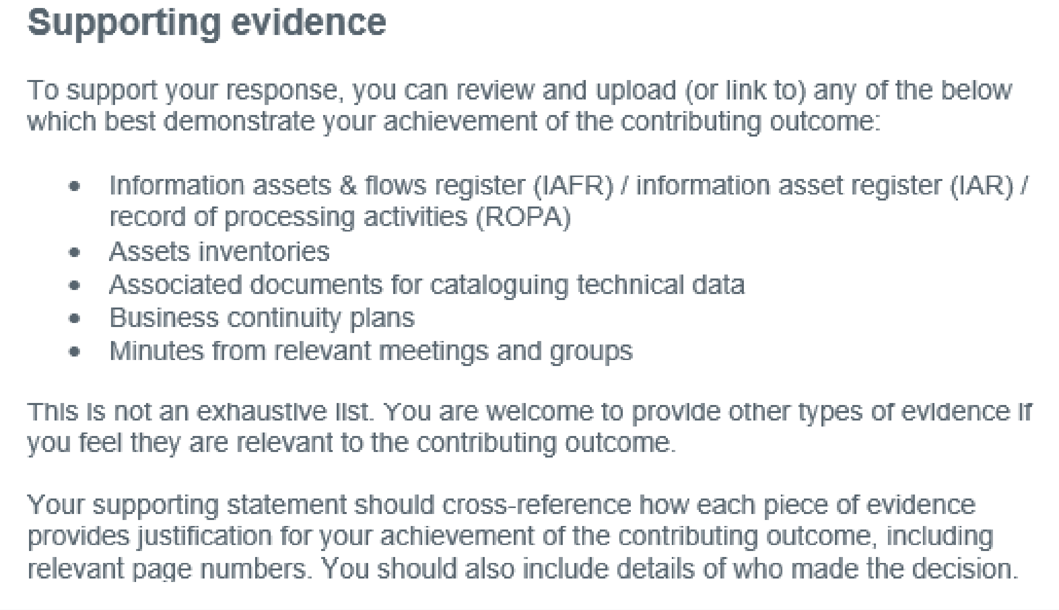
Understanding data

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).



* indicates map

Contributing outcome	DSPT V6 () weak ma
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).	1.1.2 1.1.4 1.4.1 4.1.1 4.5.5 7.1.1 8.1.1 8.1.2 9.3.9



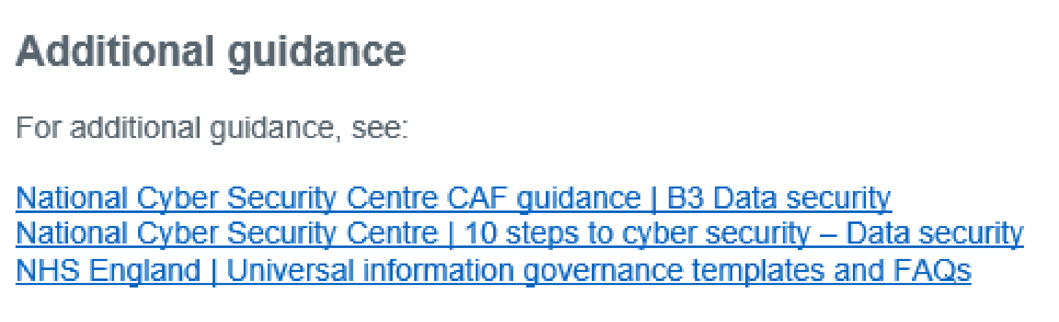
Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Information assets & flows register (IAFR) / information asset register (IAR) / record of processing activities (ROPA)
- Assets inventories
- Associated documents for cataloguing technical data
- Business continuity plans
- Minutes from relevant meetings and groups

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.



Additional guidance

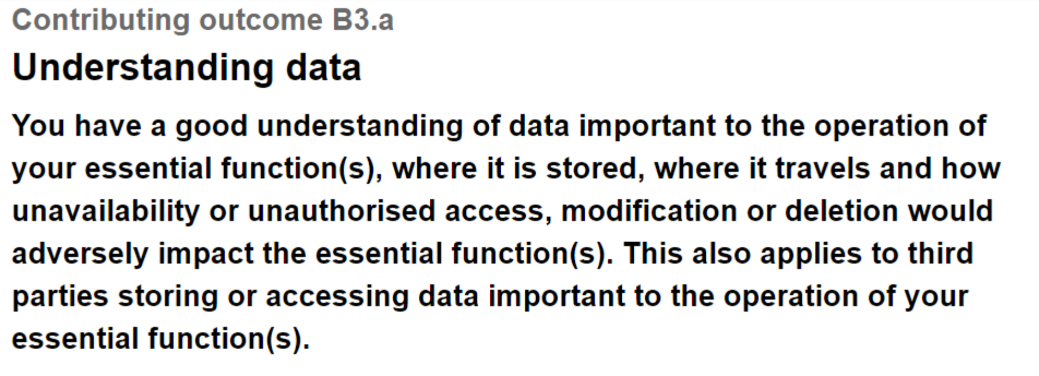
For additional guidance, see:

National Cyber Security Centre CAF guidance | B3 Data security
National Cyber Security Centre | 10 steps to cyber security – Data security
NHS England | Universal information governance templates and FAQs

Principle: B3 Data Security

Contributing outcome:
B3.a Understanding data

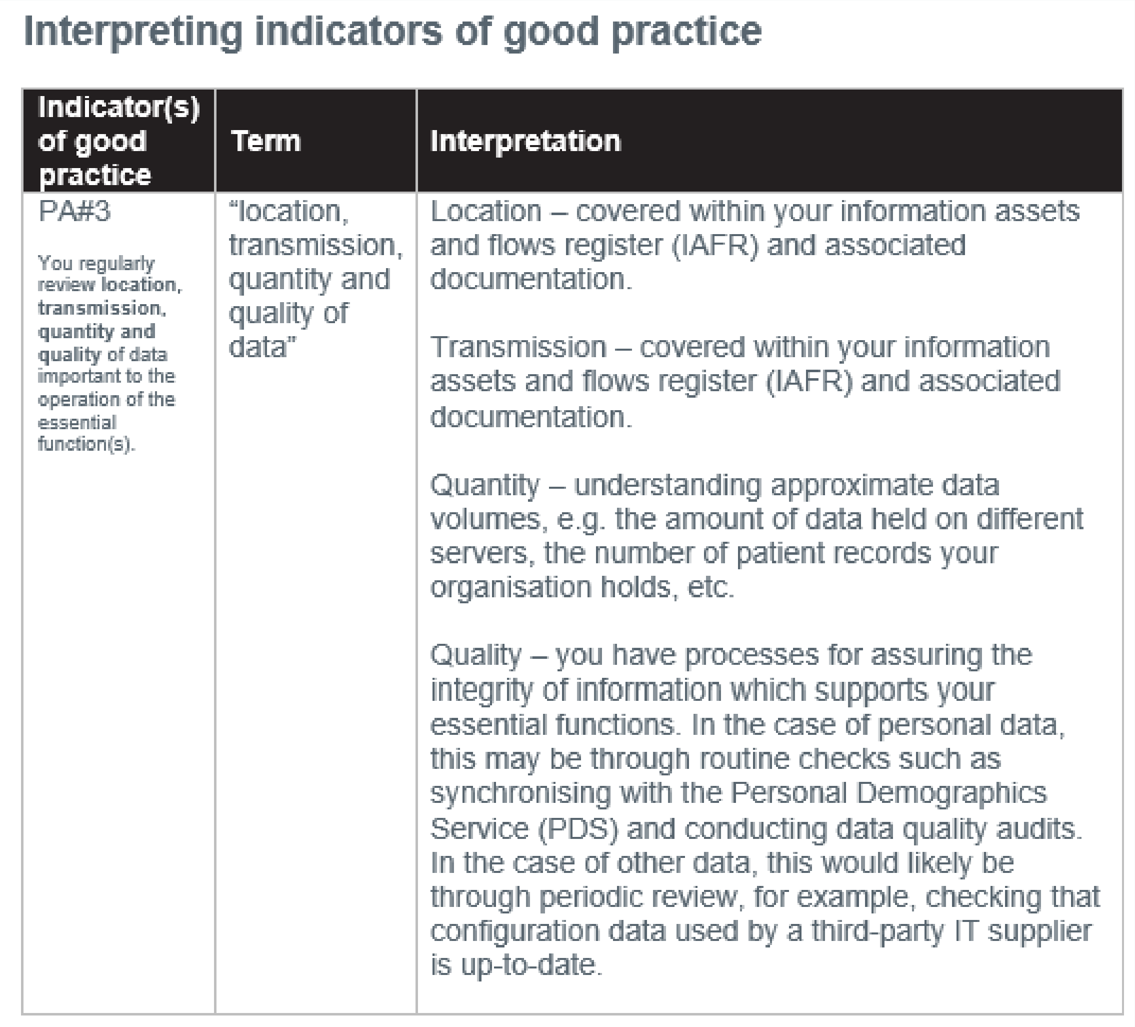
Interpretations



Contributing outcome 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).

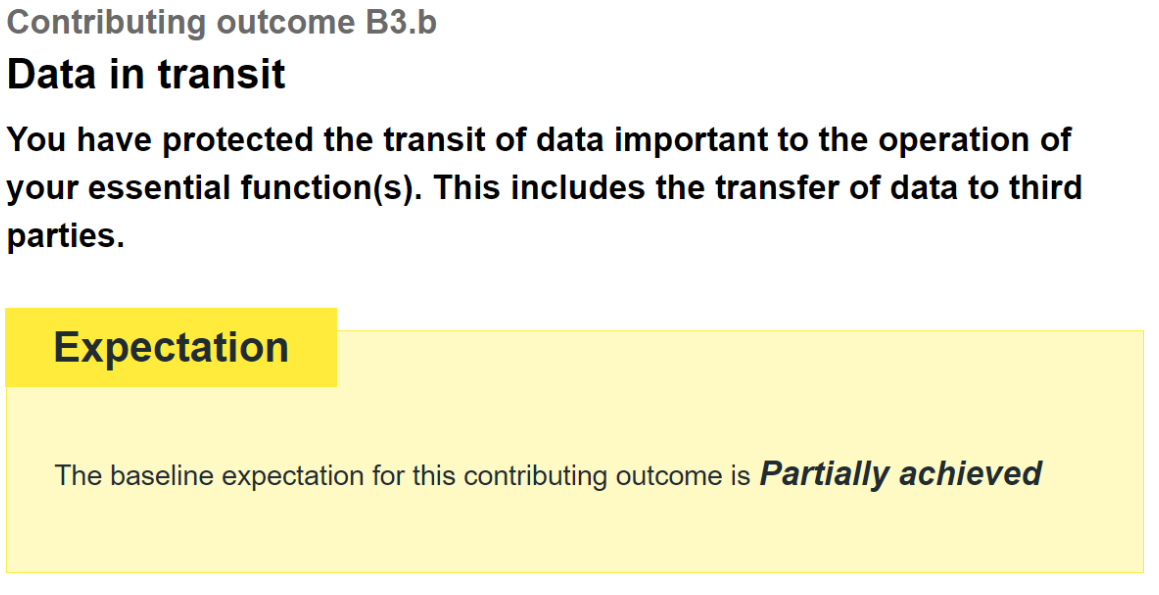


Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#3 You regularly review **location, transmission, quantity and quality** of data important to the operation of the essential function(s).	"location, transmission, quantity and quality of data"	Location – covered within your information assets and flows register (IAFR) and associated documentation. Transmission – covered within your information assets and flows register (IAFR) and associated documentation. Quantity – understanding approximate data volumes, e.g. the amount of data held on different servers, the number of patient records your organisation holds, etc. Quality – you have processes for assuring the integrity of information which supports your essential functions. In the case of personal data, this may be through routine checks such as synchronising with the Personal Demographics Service (PDS) and conducting data quality audits. In the case of other data, this would likely be through periodic review, for example, checking that configuration data used by a third-party IT supplier is up-to-date.

Principle: B3 Data Security

Contributing outcome:
B3.b Data in transit



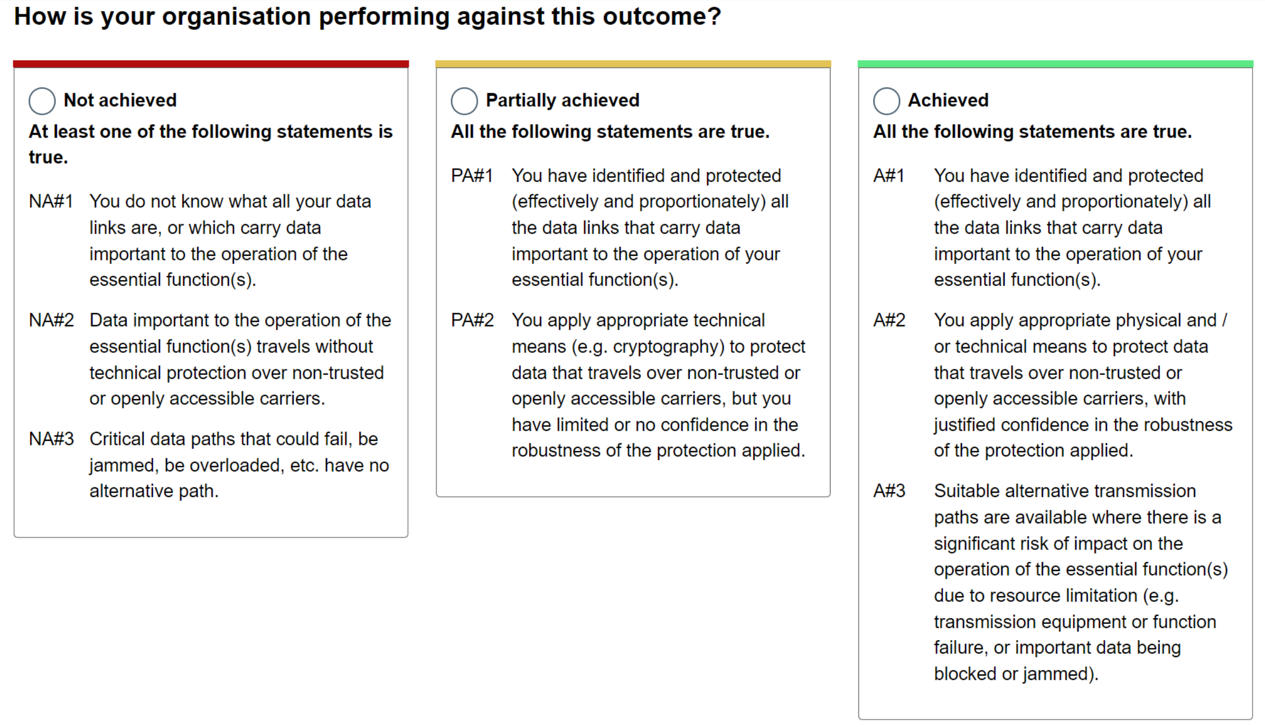
Contributing outcome B3.b

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.

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



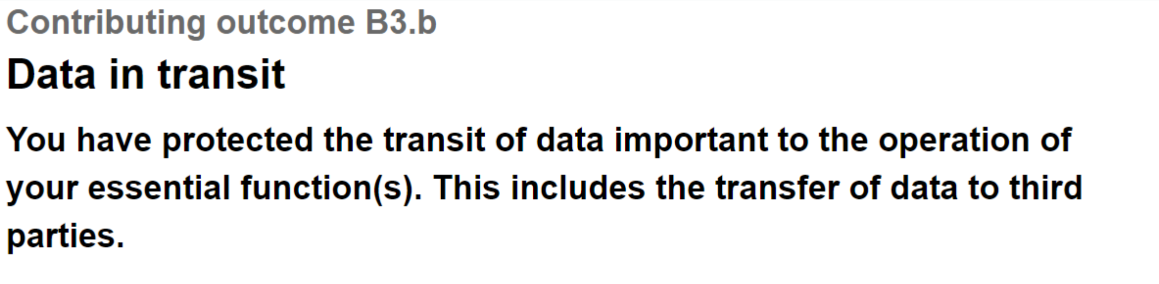
How is your organisation performing against this outcome?

○ **Not achieved**	○ **Partially achieved**	○ **Achieved**
At least one of the following statements is true.	**All the following statements are true.**	**All the following statements are true.**
NA#1 You do not know what all your data links are, or which carry data important to the operation of the essential function(s).	PA#1 You have identified and protected (effectively and proportionately) all the data links that carry data important to the operation of your essential function(s).	A#1 You have identified and protected (effectively and proportionately) all the data links that carry data important to the operation of your essential function(s).
NA#2 Data important to the operation of the essential function(s) travels without technical protection over non-trusted or openly accessible carriers.	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.	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.
NA#3 Critical data paths that could fail, be jammed, be overloaded, etc. have no alternative path.		A#3 Suitable alternative transmission paths are available where there is a significant risk of impact on the operation of the essential function(s) due to resource limitation (e.g. transmission equipment or function failure, or important data being blocked or jammed).

Principle: B3 Data Security

Contributing outcome:
B3.b Data in transit

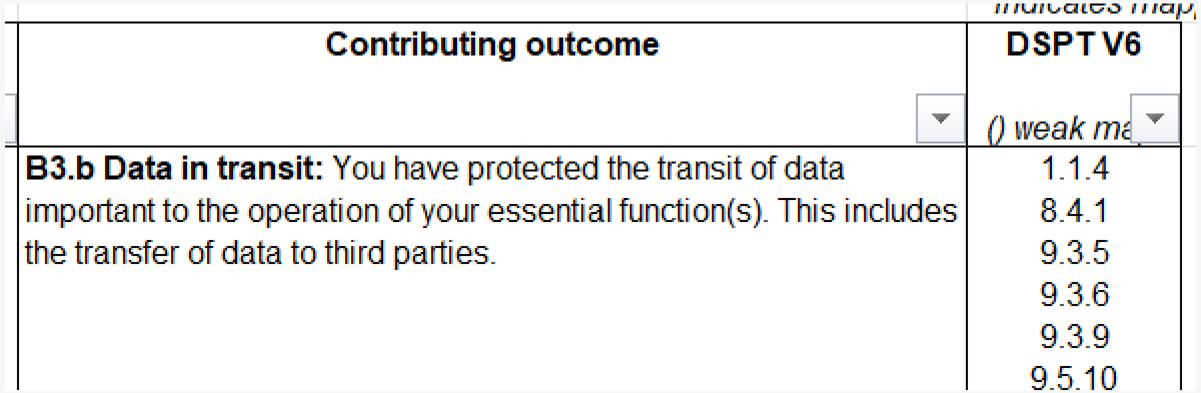
DSPT Mapping and Guidance



Contributing outcome B3.b

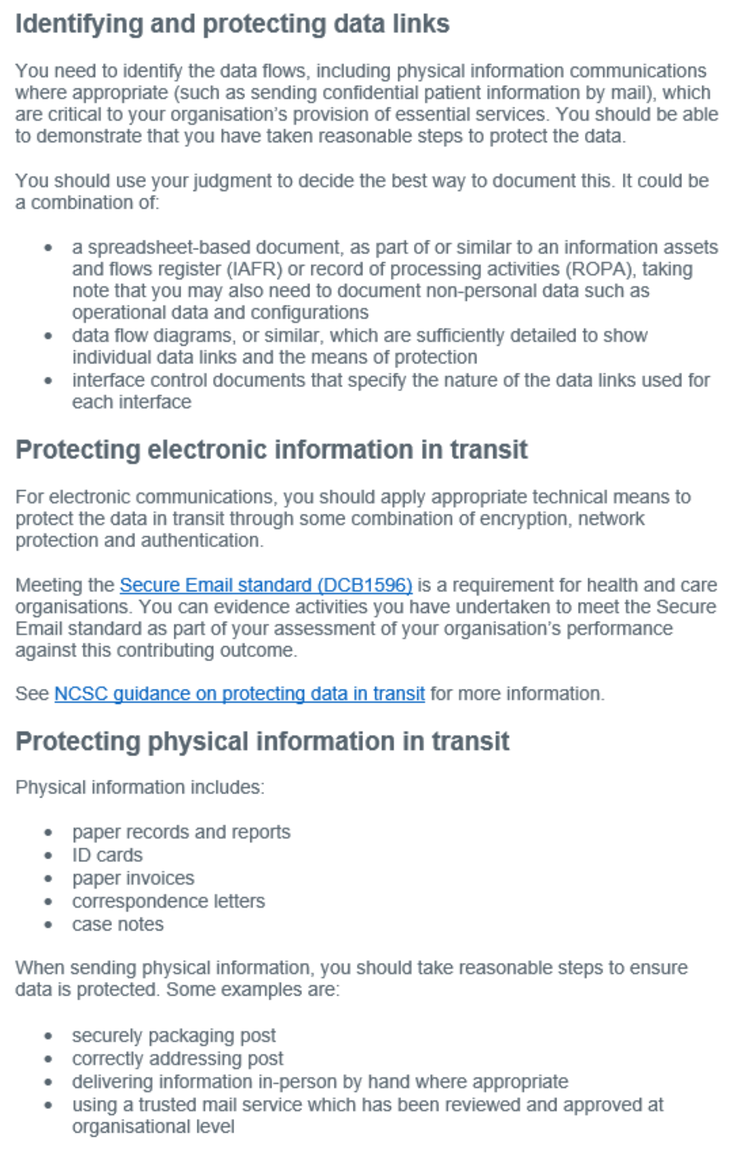
Data in transit

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.



indicates map

Contributing outcome	DSPT V6 () weak ma
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.	1.1.4 8.4.1 9.3.5 9.3.6 9.3.9 9.5.10



Identifying and protecting data links

You need to identify the data flows, including physical information communications where appropriate (such as sending confidential patient information by mail), which are critical to your organisation's provision of essential services. You should be able to demonstrate that you have taken reasonable steps to protect the data.

You should use your judgment to decide the best way to document this. It could be a combination of:

- a spreadsheet-based document, as part of or similar to an information assets and flows register (IAFR) or record of processing activities (ROPA), taking note that you may also need to document non-personal data such as operational data and configurations
- data flow diagrams, or similar, which are sufficiently detailed to show individual data links and the means of protection
- interface control documents that specify the nature of the data links used for each interface

Protecting electronic information in transit

For electronic communications, you should apply appropriate technical means to protect the data in transit through some combination of encryption, network protection and authentication.

Meeting the Secure Email standard (DCB1596) is a requirement for health and care organisations. You can evidence activities you have undertaken to meet the Secure Email standard as part of your assessment of your organisation's performance against this contributing outcome.

See NCSC guidance on protecting data in transit for more information.

Protecting physical information in transit

Physical information includes:

- paper records and reports
- ID cards
- paper invoices
- correspondence letters
- case notes

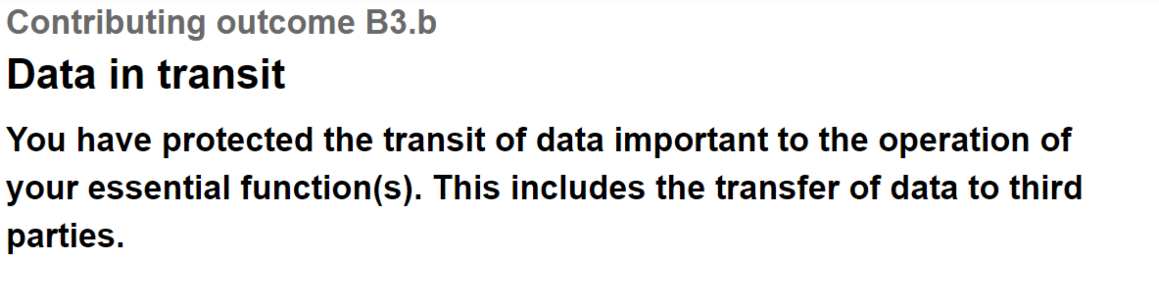
When sending physical information, you should take reasonable steps to ensure data is protected. Some examples are:

- securely packaging post
- correctly addressing post
- delivering information in-person by hand where appropriate
- using a trusted mail service which has been reviewed and approved at organisational level

Principle: B3 Data Security

Contributing outcome:
B3.b Data in transit

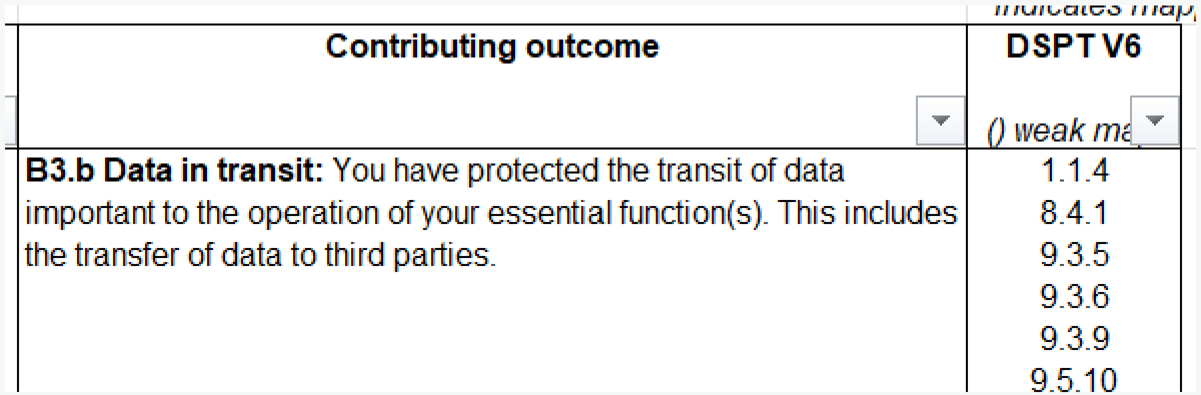
DSPT Mapping and Guidance



Contributing outcome B3.b

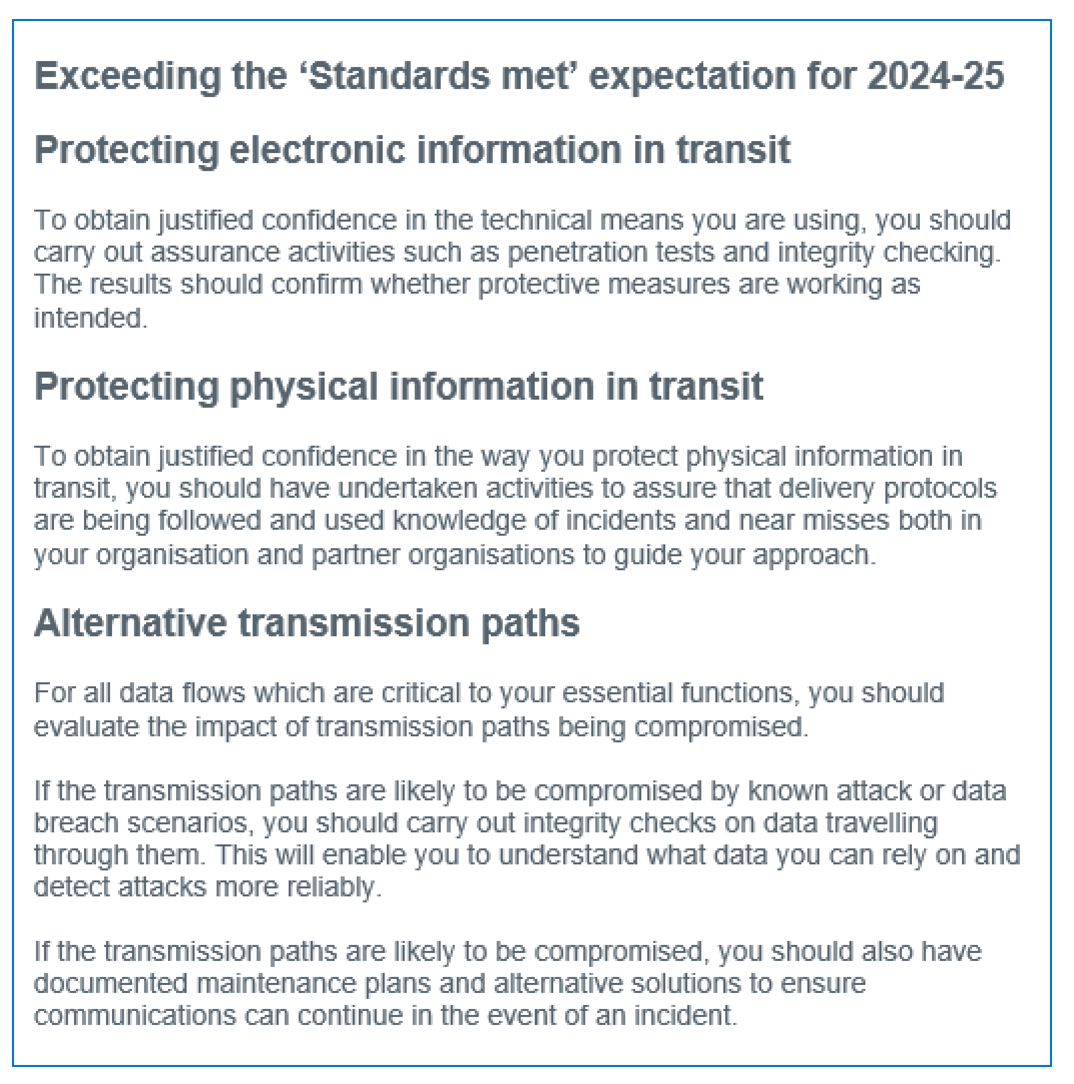
Data in transit

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.



indicates map

Contributing outcome	DSPT V6 () weak ma
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.	1.1.4 8.4.1 9.3.5 9.3.6 9.3.9 9.5.10



Exceeding the 'Standards met' expectation for 2024-25

Protecting electronic information in transit

To obtain justified confidence in the technical means you are using, you should carry out assurance activities such as penetration tests and integrity checking. The results should confirm whether protective measures are working as intended.

Protecting physical information in transit

To obtain justified confidence in the way you protect physical information in transit, you should have undertaken activities to assure that delivery protocols are being followed and used knowledge of incidents and near misses both in your organisation and partner organisations to guide your approach.

Alternative transmission paths

For all data flows which are critical to your essential functions, you should evaluate the impact of transmission paths being compromised.

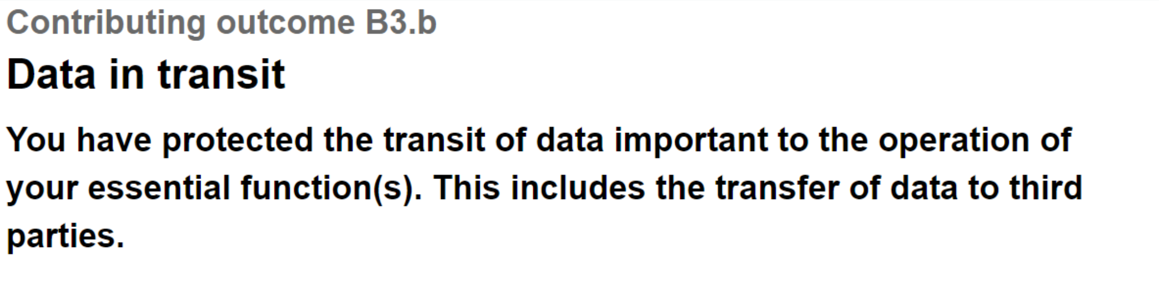
If the transmission paths are likely to be compromised by known attack or data breach scenarios, you should carry out integrity checks on data travelling through them. This will enable you to understand what data you can rely on and detect attacks more reliably.

If the transmission paths are likely to be compromised, you should also have documented maintenance plans and alternative solutions to ensure communications can continue in the event of an incident.

Principle: B3 Data Security

Contributing outcome:
B3.b Data in transit

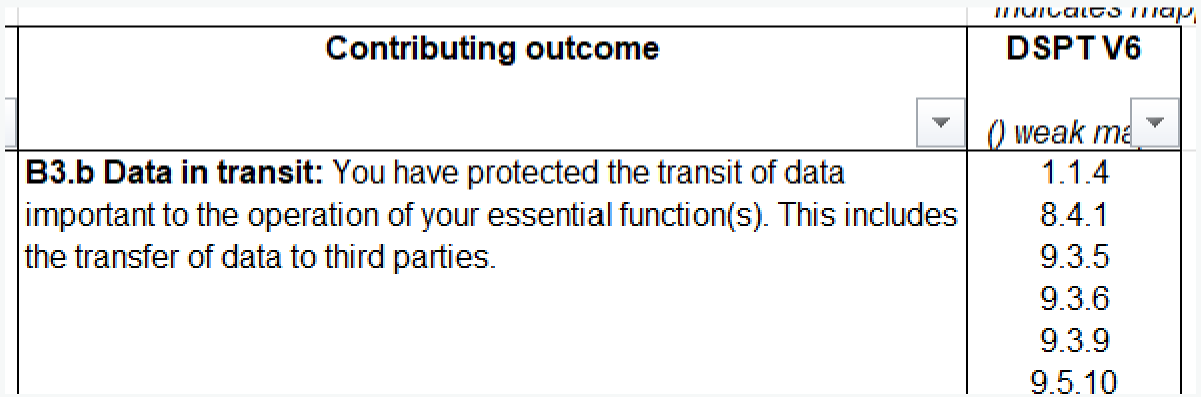
Supporting Evidence



Contributing outcome B3.b

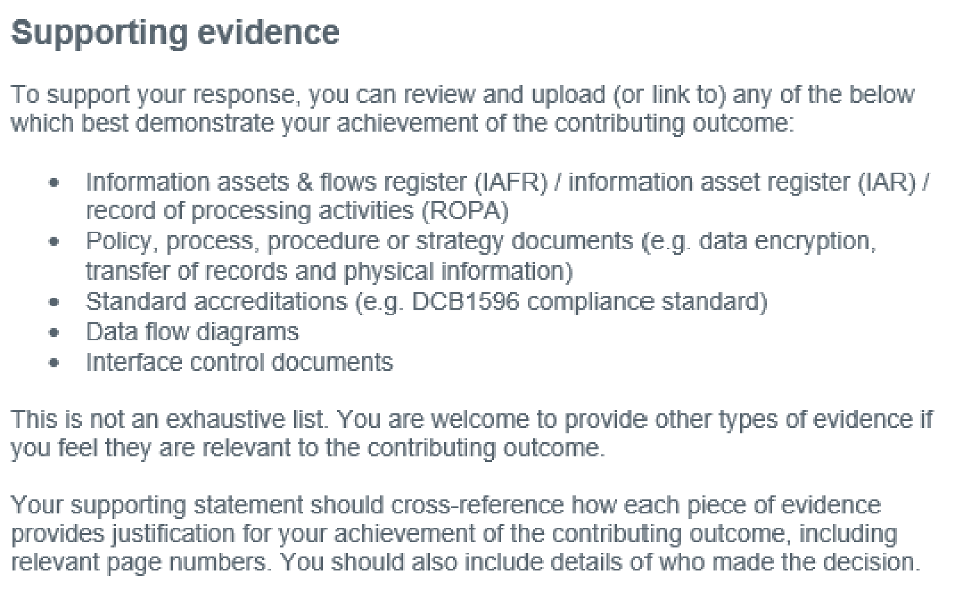
Data in transit

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.



indicates map

Contributing outcome	DSPT V6 () weak ma
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.	1.1.4 8.4.1 9.3.5 9.3.6 9.3.9 9.5.10



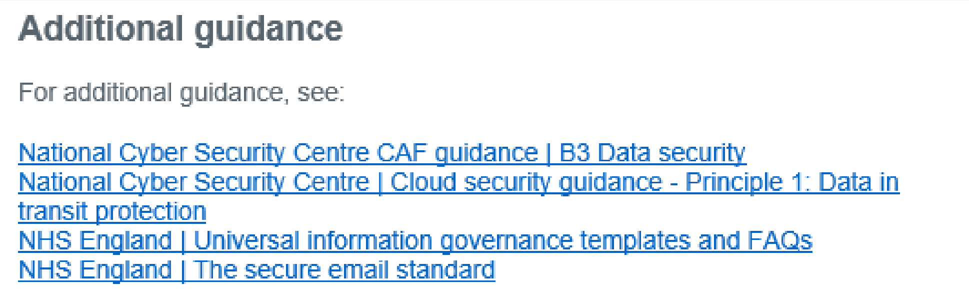
Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Information assets & flows register (IAFR) / information asset register (IAR) / record of processing activities (ROPA)
- Policy, process, procedure or strategy documents (e.g. data encryption, transfer of records and physical information)
- Standard accreditations (e.g. DCB1596 compliance standard)
- Data flow diagrams
- Interface control documents

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.



Additional guidance

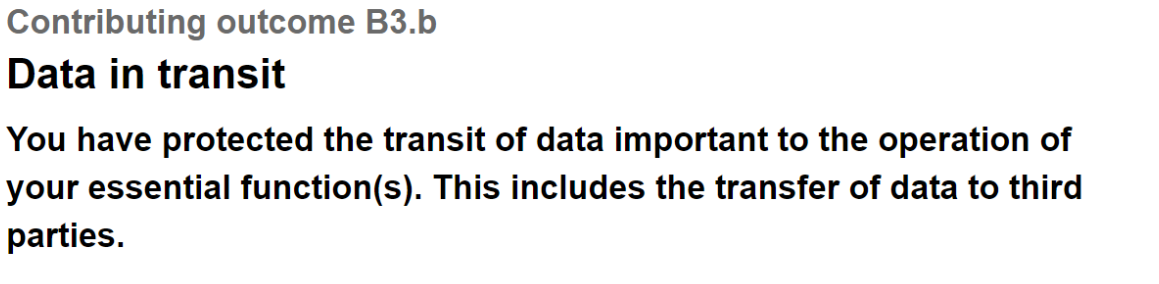
For additional guidance, see:

National Cyber Security Centre CAF guidance | B3 Data security
National Cyber Security Centre | Cloud security guidance - Principle 1: Data in transit protection
NHS England | Universal information governance templates and FAQs
NHS England | The secure email standard

Principle: B3 Data Security

Contributing outcome:
B3.b Data in transit

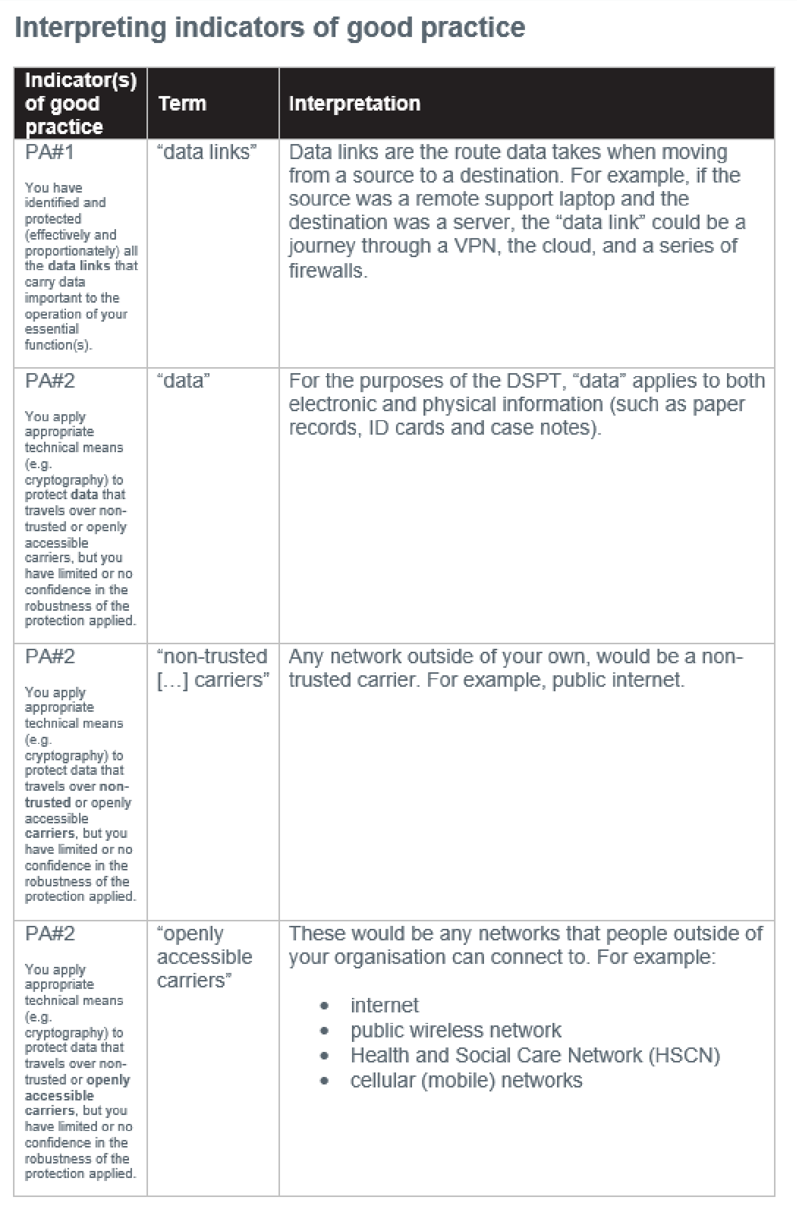
Supporting Evidence



Contributing outcome 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.

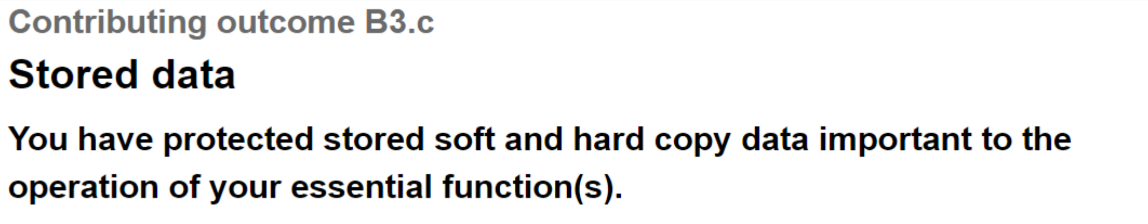


Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#1 You have identified and protected (effectively and proportionately) all the **data links** that carry data important to the operation of your essential function(s).	“data links”	Data links are the route data takes when moving from a source to a destination. For example, if the source was a remote support laptop and the destination was a server, the “data link” could be a journey through a VPN, the cloud, and a series of firewalls.
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.	“data”	For the purposes of the DSPT, “data” applies to both electronic and physical information (such as paper records, ID cards and case notes).
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.	“non-trusted […] carriers”	Any network outside of your own, would be a non-trusted carrier. For example, public internet.
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.	“openly accessible carriers”	These would be any networks that people outside of your organisation can connect to. For example: • internet • public wireless network • Health and Social Care Network (HSCN) • cellular (mobile) networks

Principle: B3 Data Security

Contributing outcome:
B3.c Stored data



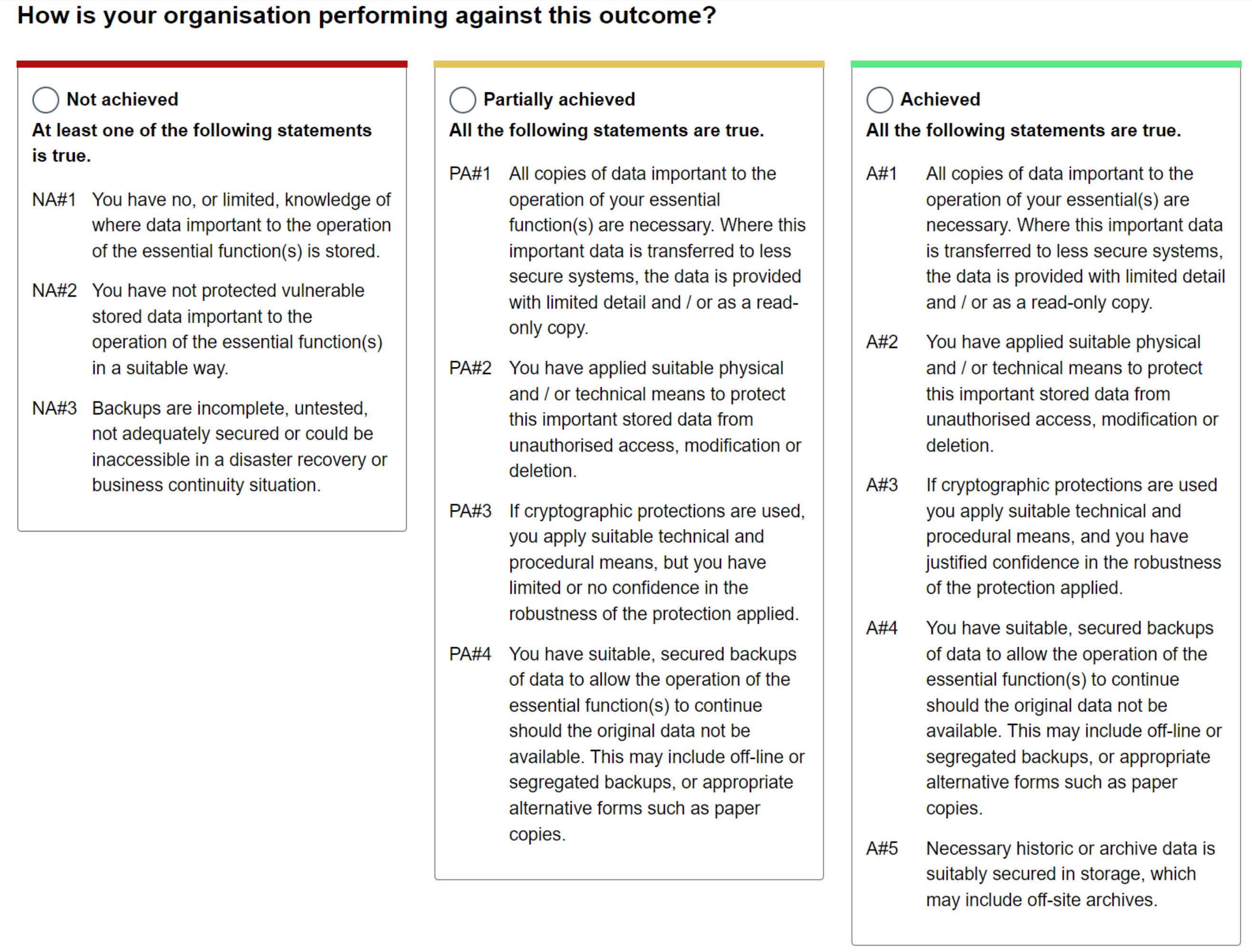
Contributing outcome B3.c

Stored data

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

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 You have no, or limited, knowledge of where data important to the operation of the essential function(s) is stored.

NA#2 You have not protected vulnerable stored data important to the operation of the essential function(s) in a suitable way.

NA#3 Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.

○ **Partially achieved**

All the following statements are true.

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.

PA#2 You have applied suitable physical and / or technical means to protect this important stored data from unauthorised access, modification or deletion.

PA#3 If cryptographic protections are used, you apply suitable technical and procedural means, but you have limited or no confidence in the robustness of the protection applied.

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 off-line or segregated backups, or appropriate alternative forms such as paper copies.

○ **Achieved**

All the following statements are true.

A#1 All copies of data important to the operation of your essential(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.

A#2 You have applied suitable physical and / or technical means to protect this important stored data from unauthorised access, modification or deletion.

A#3 If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied.

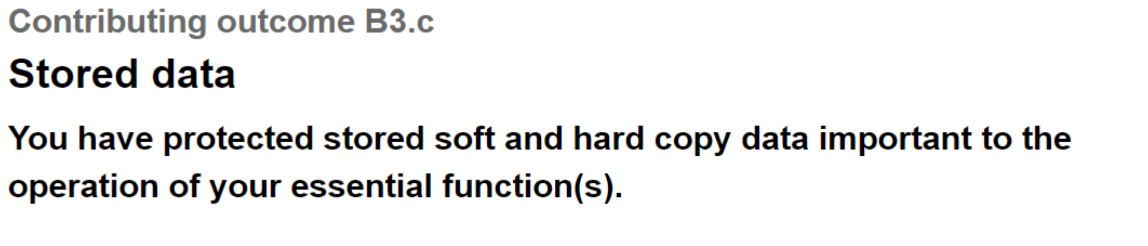
A#4 You have suitable, secured backups of data to allow the operation of the essential function(s) to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.

A#5 Necessary historic or archive data is suitably secured in storage, which may include off-site archives.

Principle: B3 Data Security

Contributing outcome:
B3.c Stored data

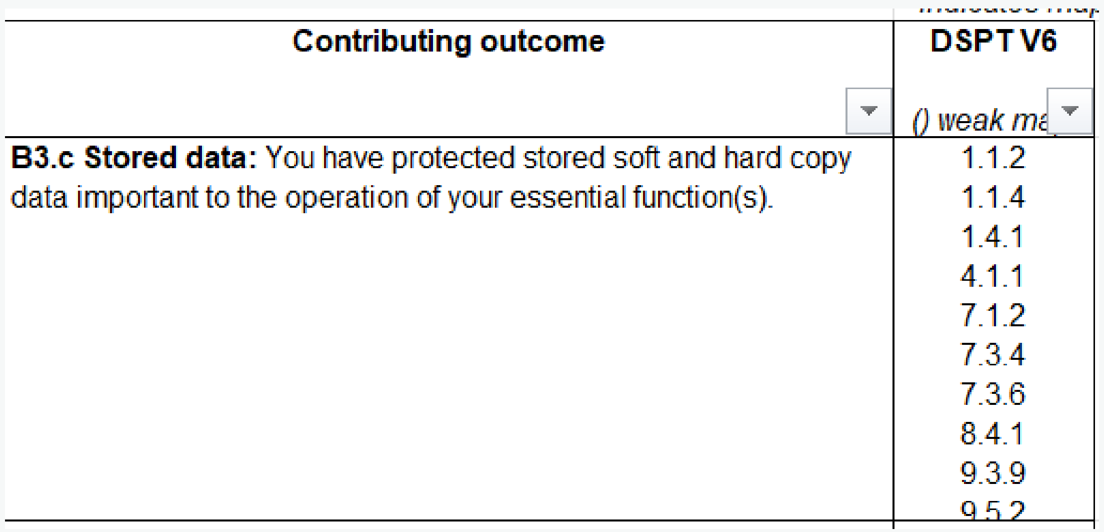
DSPT Mapping and Guidance



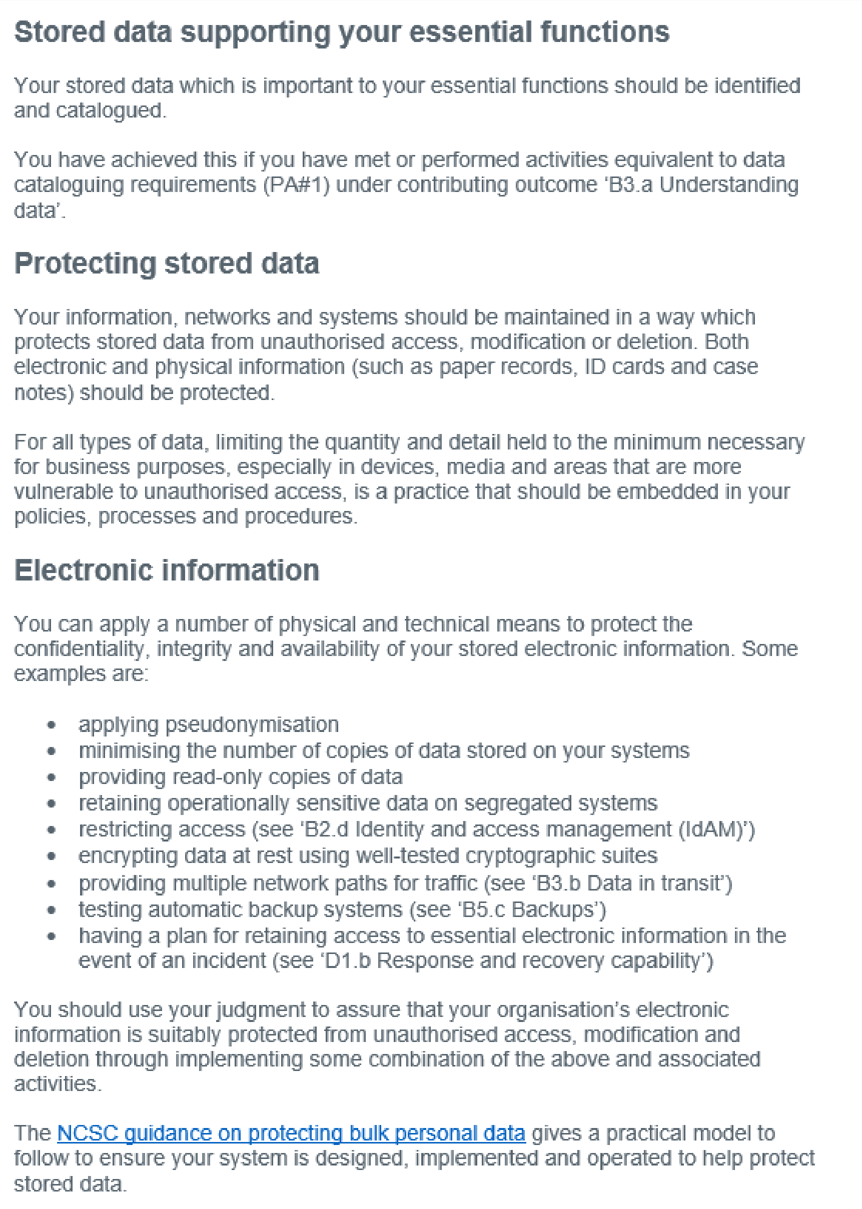
Contributing outcome B3.c

Stored data

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



Contributing outcome	DSPT V6 () weak ma
B3.c Stored data: You have protected stored soft and hard copy data important to the operation of your essential function(s).	1.1.2 1.1.4 1.4.1 4.1.1 7.1.2 7.3.4 7.3.6 8.4.1 9.3.9 9.5.2



Stored data supporting your essential functions

Your stored data which is important to your essential functions should be identified and catalogued.

You have achieved this if you have met or performed activities equivalent to data cataloguing requirements (PA#1) under contributing outcome 'B3.a Understanding data'.

Protecting stored data

Your information, networks and systems should be maintained in a way which protects stored data from unauthorised access, modification or deletion. Both electronic and physical information (such as paper records, ID cards and case notes) should be protected.

For all types of data, limiting the quantity and detail held to the minimum necessary for business purposes, especially in devices, media and areas that are more vulnerable to unauthorised access, is a practice that should be embedded in your policies, processes and procedures.

Electronic information

You can apply a number of physical and technical means to protect the confidentiality, integrity and availability of your stored electronic information. Some examples are:

- applying pseudonymisation
- minimising the number of copies of data stored on your systems
- providing read-only copies of data
- retaining operationally sensitive data on segregated systems
- restricting access (see 'B2.d Identity and access management (IdAM)')
- encrypting data at rest using well-tested cryptographic suites
- providing multiple network paths for traffic (see 'B3.b Data in transit')
- testing automatic backup systems (see 'B5.c Backups')
- having a plan for retaining access to essential electronic information in the event of an incident (see 'D1.b Response and recovery capability')

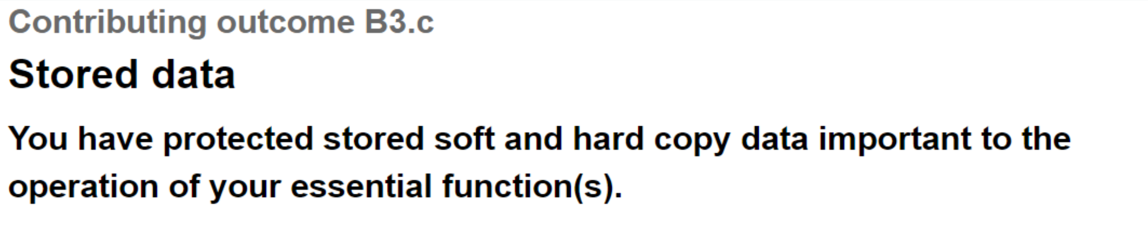
You should use your judgment to assure that your organisation's electronic information is suitably protected from unauthorised access, modification and deletion through implementing some combination of the above and associated activities.

The NCSC guidance on protecting bulk personal data gives a practical model to follow to ensure your system is designed, implemented and operated to help protect stored data.

Principle: B3 Data Security

Contributing outcome:
B3.c Stored data

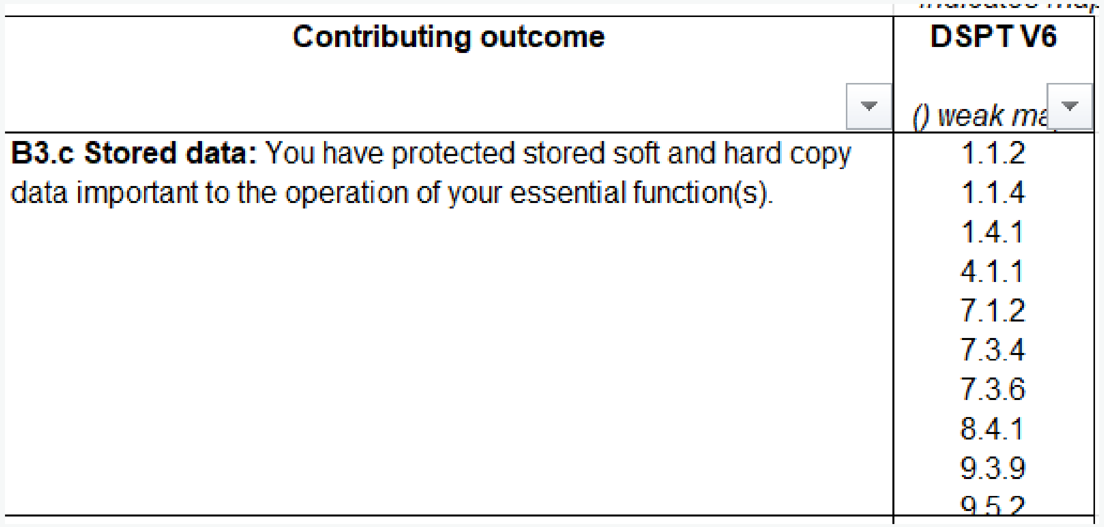
DSPT Mapping and Guidance



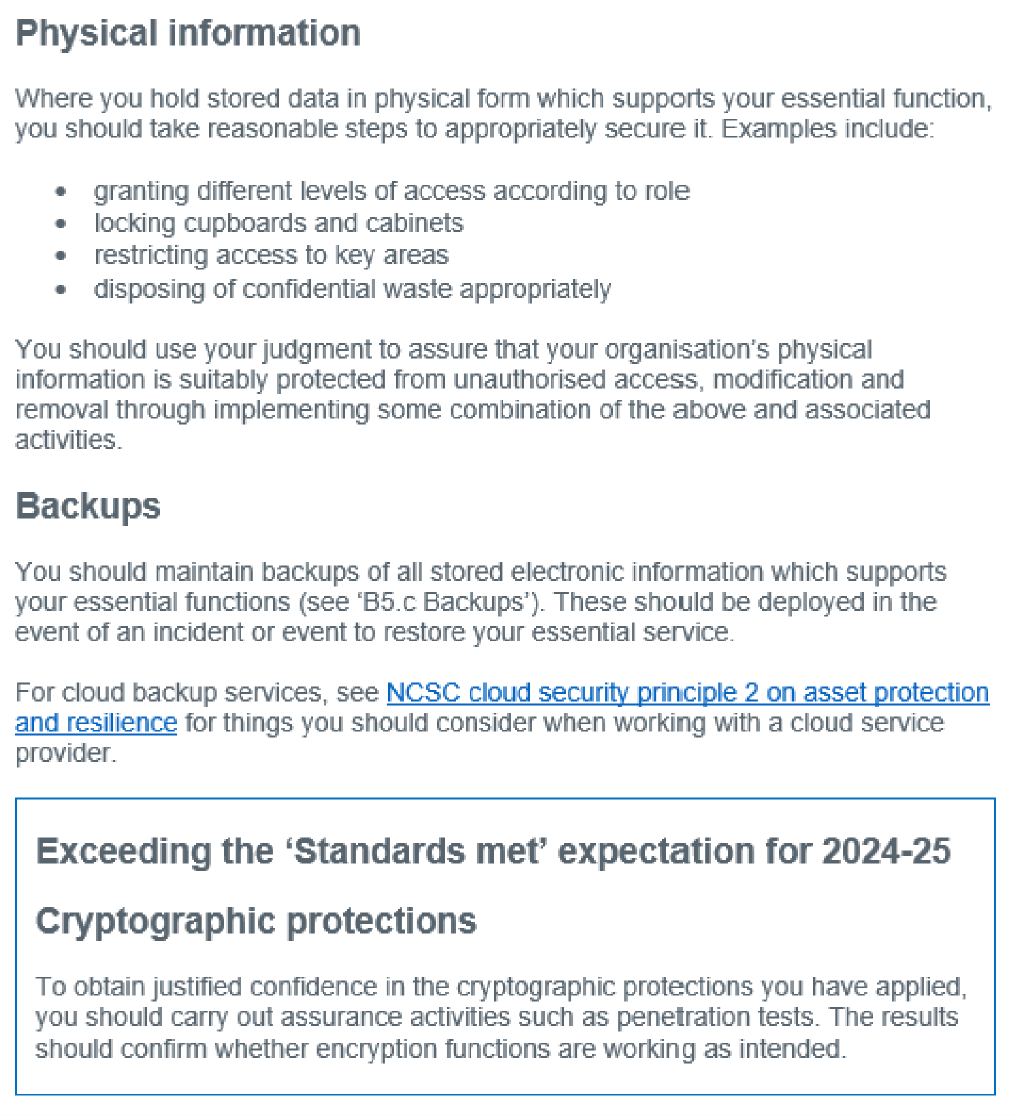
Contributing outcome B3.c

Stored data

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



Contributing outcome	DSPT V6 *() weak ma*
B3.c Stored data: You have protected stored soft and hard copy data important to the operation of your essential function(s).	1.1.2 1.1.4 1.4.1 4.1.1 7.1.2 7.3.4 7.3.6 8.4.1 9.3.9 9.5.2



Physical information

Where you hold stored data in physical form which supports your essential function, you should take reasonable steps to appropriately secure it. Examples include:

- granting different levels of access according to role
- locking cupboards and cabinets
- restricting access to key areas
- disposing of confidential waste appropriately

You should use your judgment to assure that your organisation's physical information is suitably protected from unauthorised access, modification and removal through implementing some combination of the above and associated activities.

Backups

You should maintain backups of all stored electronic information which supports your essential functions (see 'B5.c Backups'). These should be deployed in the event of an incident or event to restore your essential service.

For cloud backup services, see NCSC cloud security principle 2 on asset protection and resilience for things you should consider when working with a cloud service provider.

Exceeding the 'Standards met' expectation for 2024-25

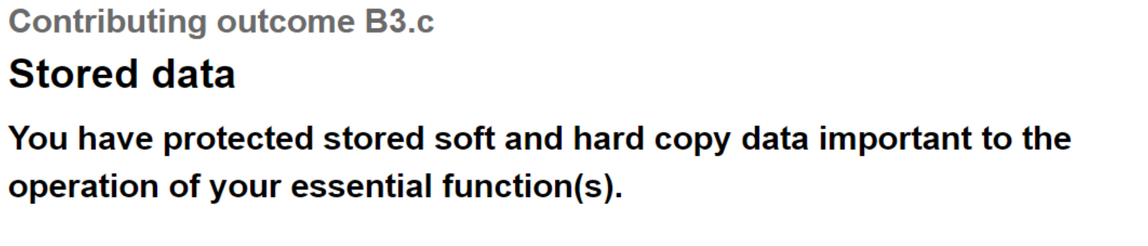
Cryptographic protections

To obtain justified confidence in the cryptographic protections you have applied, you should carry out assurance activities such as penetration tests. The results should confirm whether encryption functions are working as intended.

Principle: B3 Data Security

Contributing outcome:
B3.c Stored data

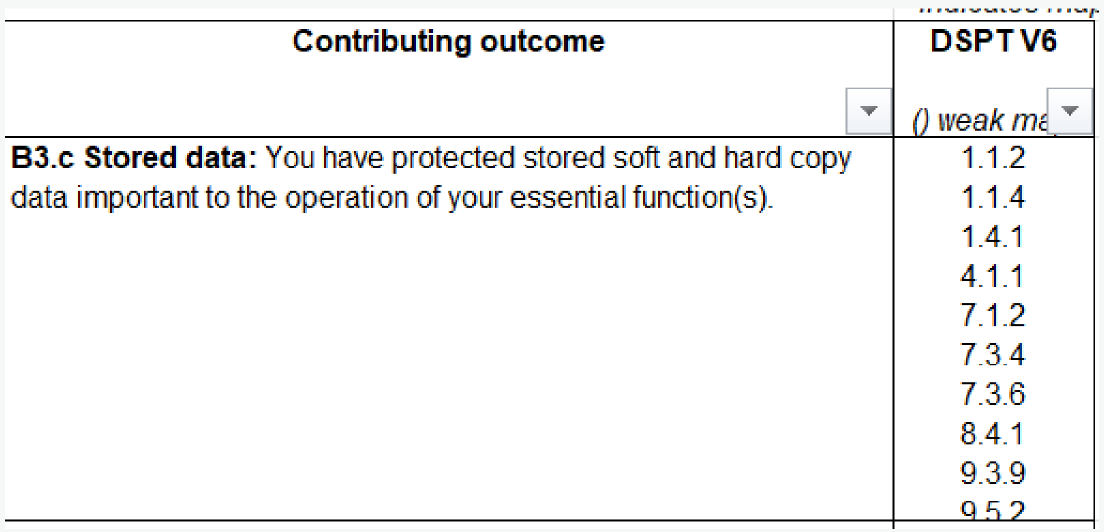
Supporting Evidence



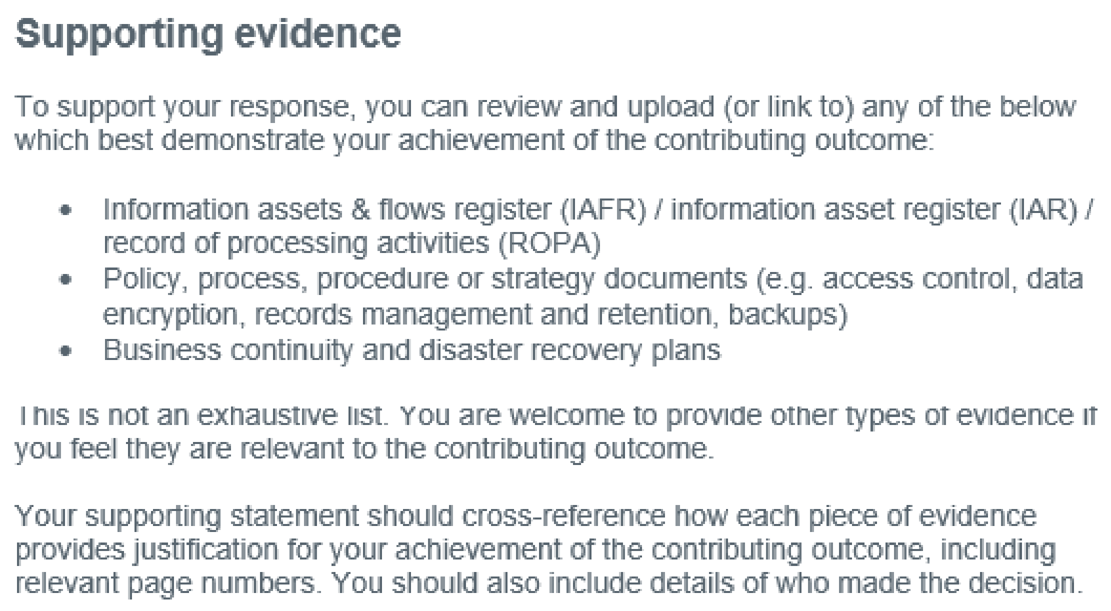
Contributing outcome B3.c

Stored data

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



Contributing outcome	DSPT V6 *() weak ma*
B3.c Stored data: You have protected stored soft and hard copy data important to the operation of your essential function(s).	1.1.2 1.1.4 1.4.1 4.1.1 7.1.2 7.3.4 7.3.6 8.4.1 9.3.9 9.5.2



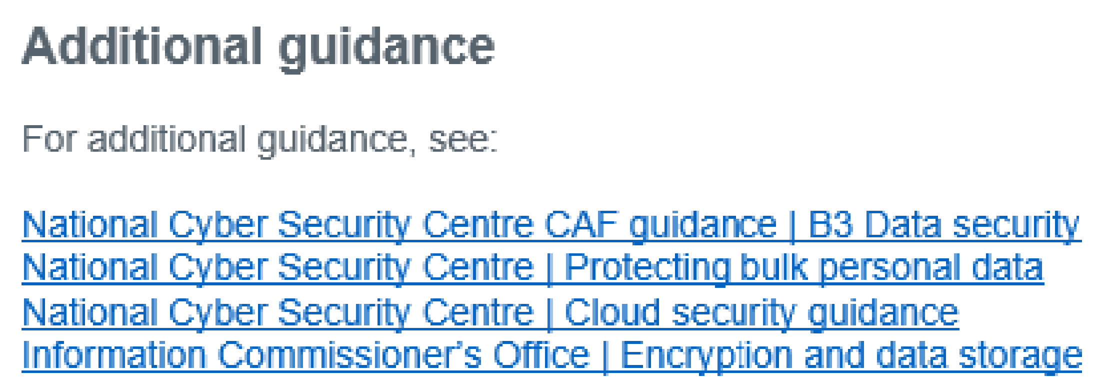
Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Information assets & flows register (IAFR) / information asset register (IAR) / record of processing activities (ROPA)
- Policy, process, procedure or strategy documents (e.g. access control, data encryption, records management and retention, backups)
- Business continuity and disaster recovery plans

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.



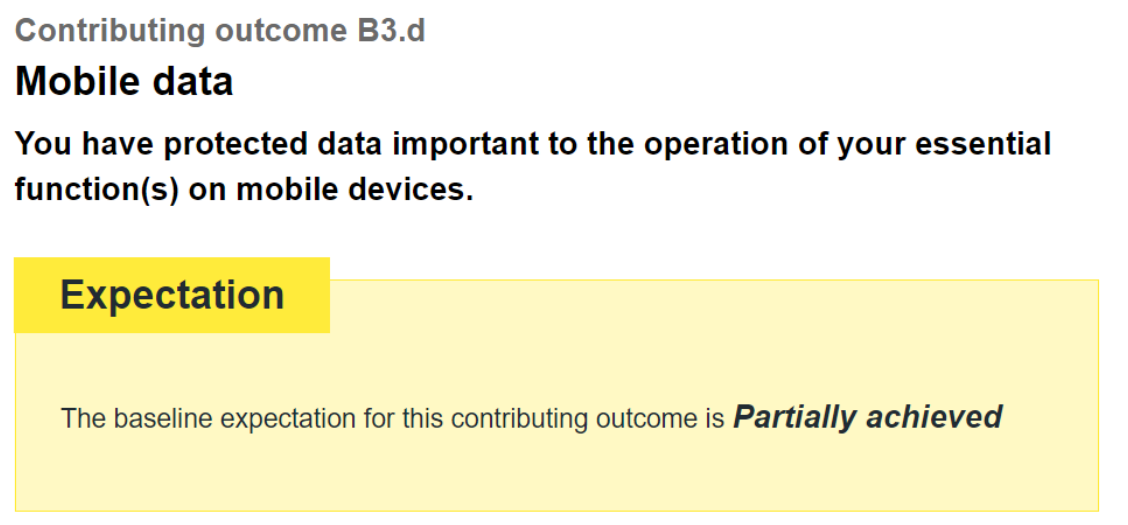
Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B3 Data security
National Cyber Security Centre | Protecting bulk personal data
National Cyber Security Centre | Cloud security guidance
Information Commissioner's Office | Encryption and data storage

Principle: B3 Data Security

Contributing outcome:
B3.d Mobile data



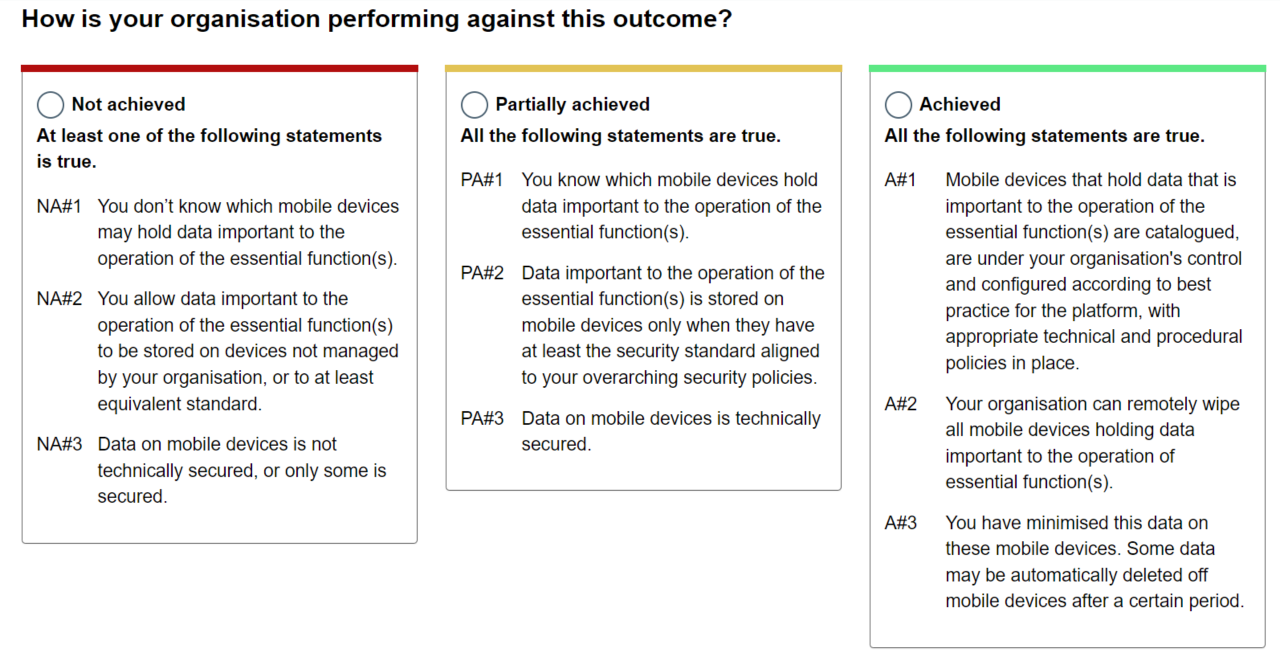
Contributing outcome B3.d

Mobile data

You have protected data important to the operation of your essential function(s) on mobile devices.

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 You don't know which mobile devices may hold data important to the operation of the essential function(s).

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.

NA#3 Data on mobile devices is not technically secured, or only some is secured.

○ **Partially achieved**

All the following statements are true.

PA#1 You know which mobile devices hold data important to the operation of the essential function(s).

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.

PA#3 Data on mobile devices is technically secured.

○ **Achieved**

All the following statements are true.

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.

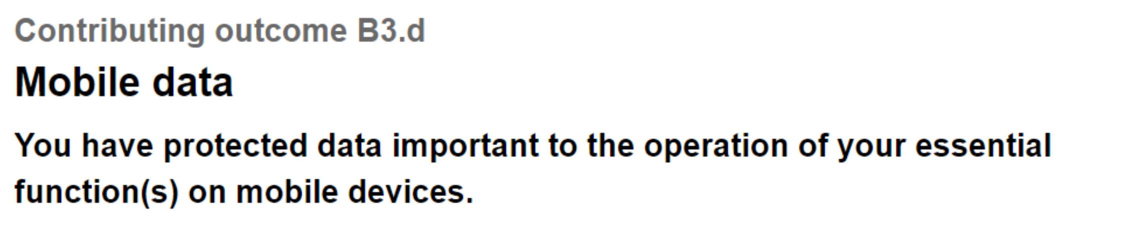
A#2 Your organisation can remotely wipe all mobile devices holding data important to the operation of essential function(s).

A#3 You have minimised this data on these mobile devices. Some data may be automatically deleted off mobile devices after a certain period.

Principle: B3 Data Security

Contributing outcome:
B3.d Mobile data

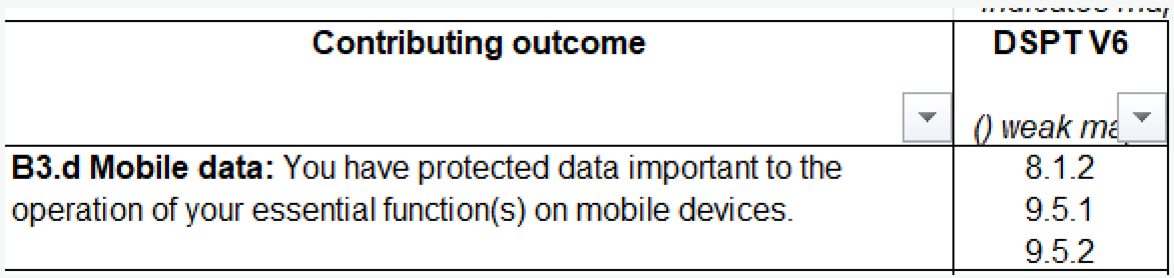
DSPT Mapping and Guidance



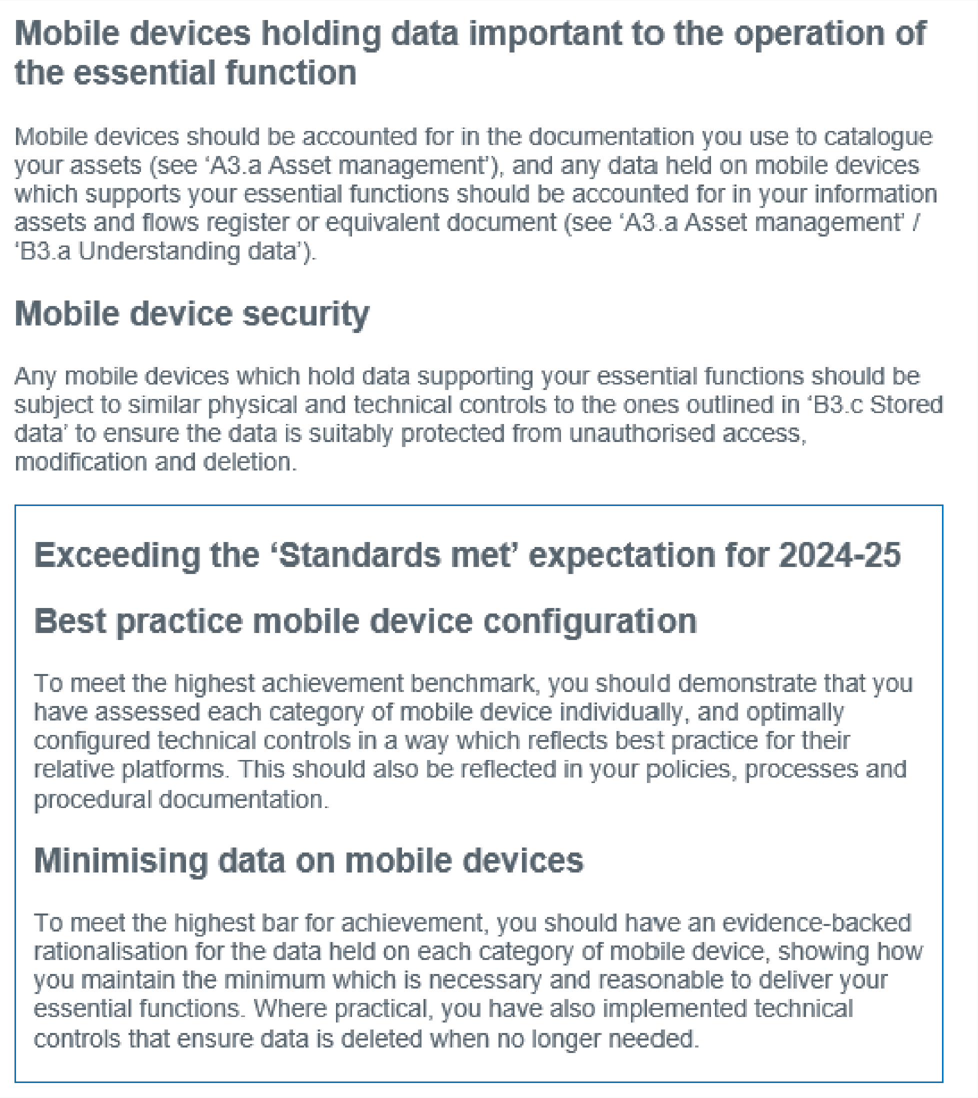
Contributing outcome B3.d

Mobile data

You have protected data important to the operation of your essential function(s) on mobile devices.



Contributing outcome	DSPT V6 () weak ma
B3.d Mobile data: You have protected data important to the operation of your essential function(s) on mobile devices.	8.1.2 9.5.1 9.5.2



Mobile devices holding data important to the operation of the essential function

Mobile devices should be accounted for in the documentation you use to catalogue your assets (see 'A3.a Asset management'), and any data held on mobile devices which supports your essential functions should be accounted for in your information assets and flows register or equivalent document (see 'A3.a Asset management' / 'B3.a Understanding data').

Mobile device security

Any mobile devices which hold data supporting your essential functions should be subject to similar physical and technical controls to the ones outlined in 'B3.c Stored data' to ensure the data is suitably protected from unauthorised access, modification and deletion.

Exceeding the 'Standards met' expectation for 2024-25

Best practice mobile device configuration

To meet the highest achievement benchmark, you should demonstrate that you have assessed each category of mobile device individually, and optimally configured technical controls in a way which reflects best practice for their relative platforms. This should also be reflected in your policies, processes and procedural documentation.

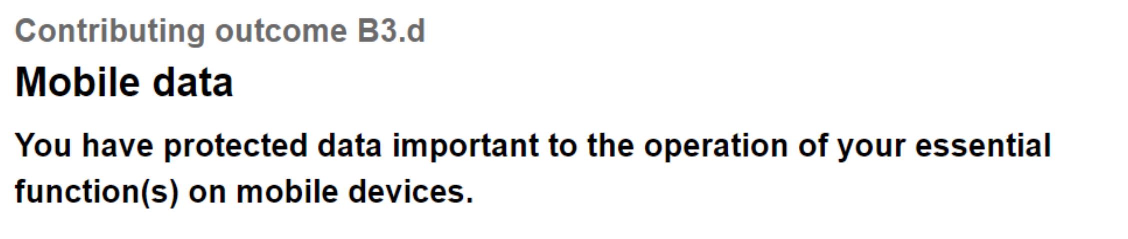
Minimising data on mobile devices

To meet the highest bar for achievement, you should have an evidence-backed rationalisation for the data held on each category of mobile device, showing how you maintain the minimum which is necessary and reasonable to deliver your essential functions. Where practical, you have also implemented technical controls that ensure data is deleted when no longer needed.

Principle: B3 Data Security

Contributing outcome: B3.d Mobile data

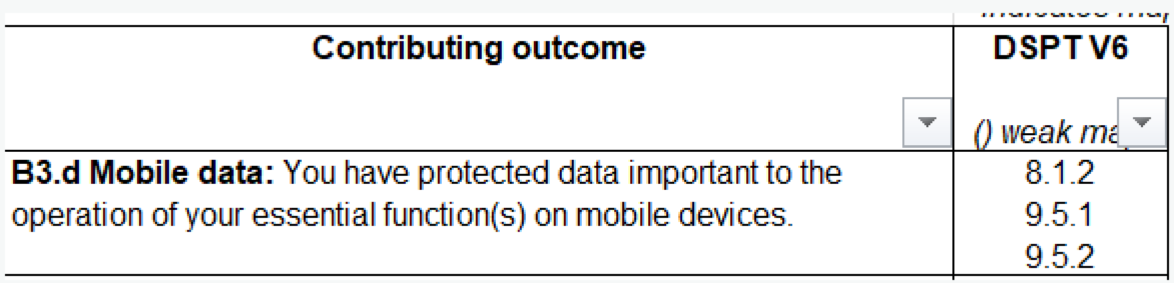
Supporting Evidence



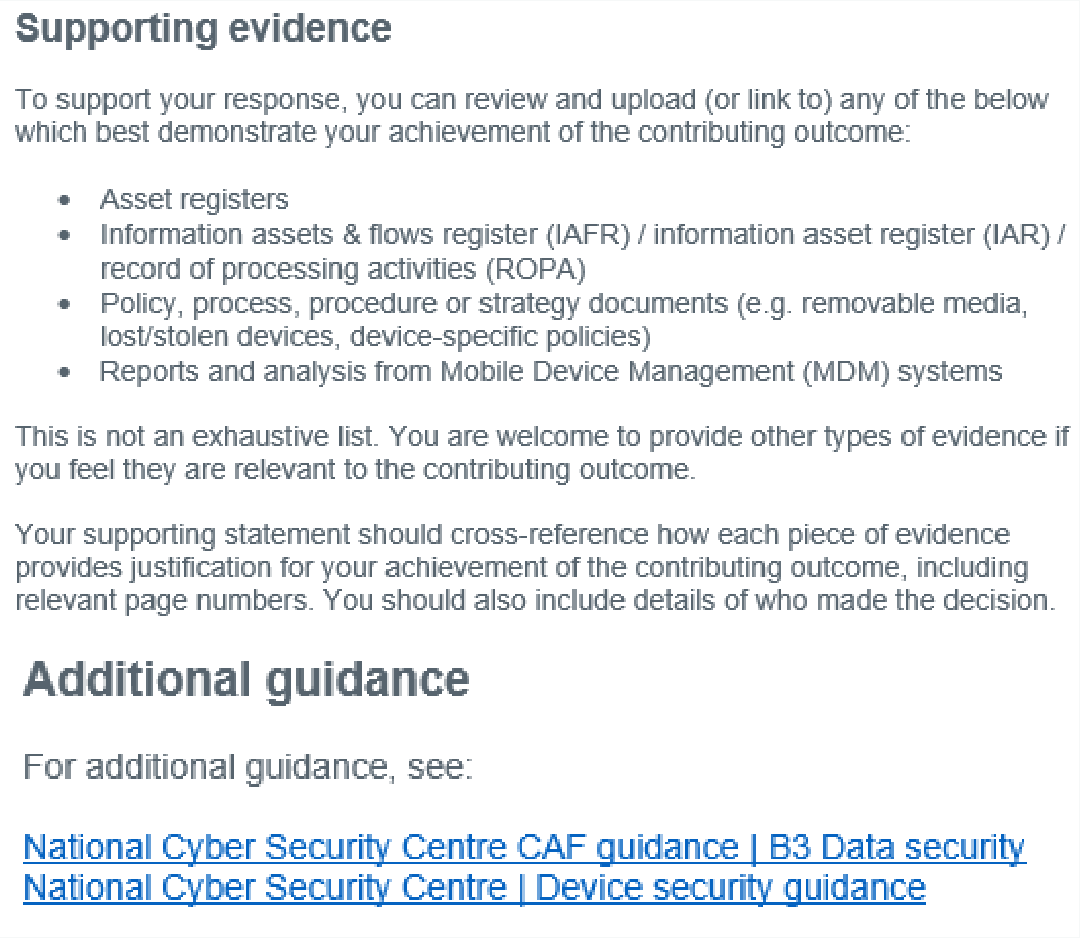
Contributing outcome B3.d

Mobile data

You have protected data important to the operation of your essential function(s) on mobile devices.



Contributing outcome	DSPT V6 () weak me
B3.d Mobile data: You have protected data important to the operation of your essential function(s) on mobile devices.	8.1.2 9.5.1 9.5.2



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Asset registers
- Information assets & flows register (IAFR) / information asset register (IAR) / record of processing activities (ROPA)
- Policy, process, procedure or strategy documents (e.g. removable media, lost/stolen devices, device-specific policies)
- Reports and analysis from Mobile Device Management (MDM) systems

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

Additional guidance

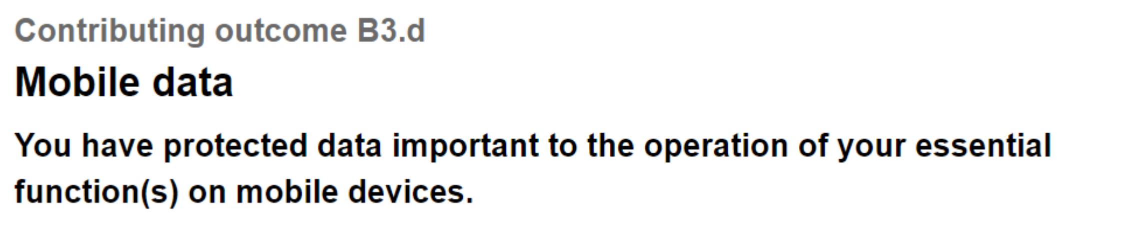
For additional guidance, see:

National Cyber Security Centre CAF guidance | B3 Data security
National Cyber Security Centre | Device security guidance

Principle: B3 Data Security

Contributing outcome:
B3.d Mobile data

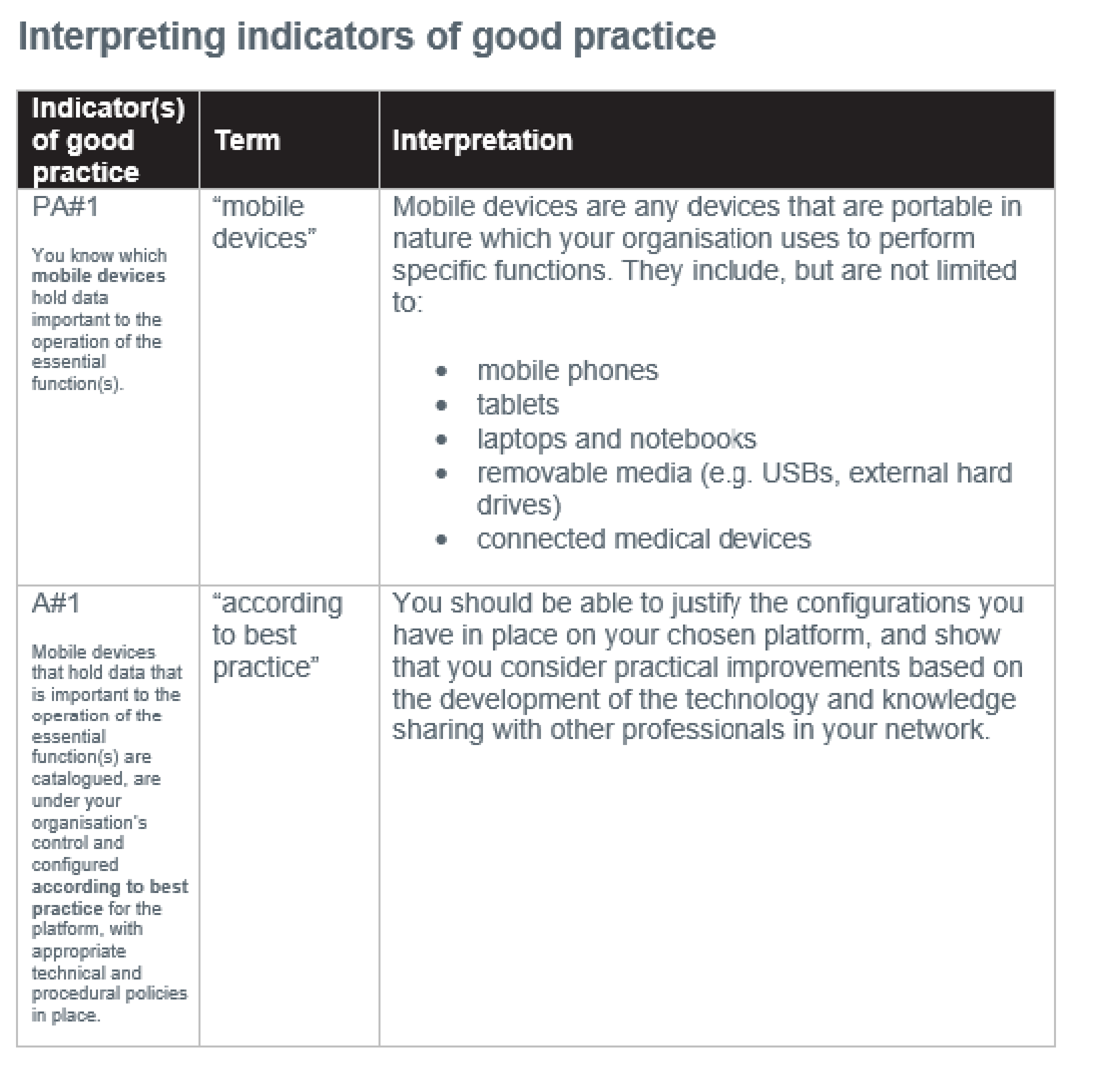
Interpretations



Contributing outcome B3.d

Mobile data

You have protected data important to the operation of your essential function(s) on mobile devices.



Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#1 You know which **mobile devices** hold data important to the operation of the essential function(s).	"mobile devices"	Mobile devices are any devices that are portable in nature which your organisation uses to perform specific functions. They include, but are not limited to: • mobile phones • tablets • laptops and notebooks • removable media (e.g. USBs, external hard drives) • connected medical devices
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.	"according to best practice"	You should be able to justify the configurations you have in place on your chosen platform, and show that you consider practical improvements based on the development of the technology and knowledge sharing with other professionals in your network.

Half time Quiz

A quick one

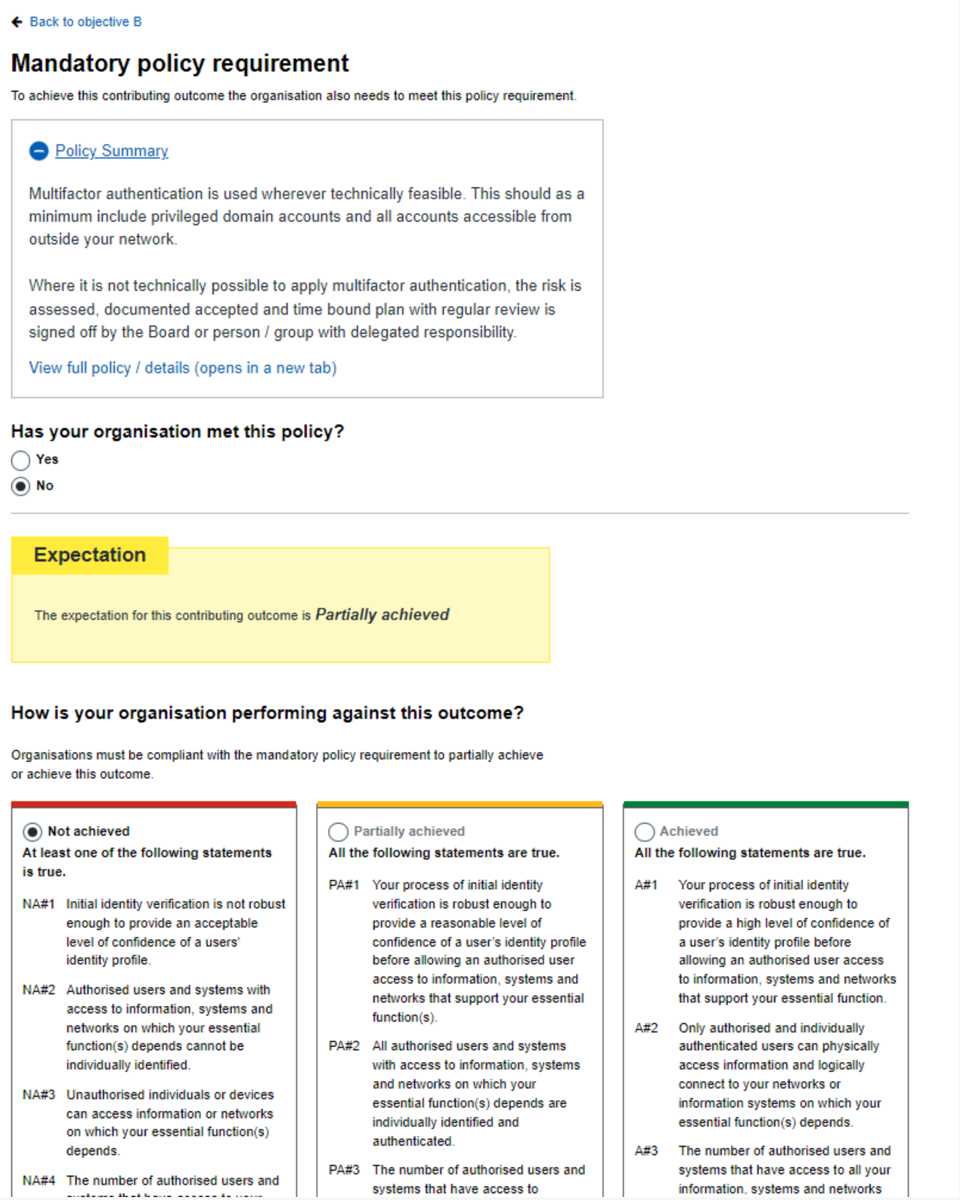
Why are Partially achieved and achieved not available to select?

Like the option you think is correct

a) Disagreement in the team

b) Organisation has not met the MFA policy

c) Not enough resources



Mandatory policy requirement

To achieve this contributing outcome the organisation also needs to meet this policy requirement.

Policy Summary

Multifactor authentication is used wherever technically feasible. This should as a minimum include privileged domain accounts and all accounts accessible from outside your network.

Where it is not technically possible to apply multifactor authentication, the risk is assessed, documented accepted and time bound plan with regular review is signed off by the Board or person / group with delegated responsibility.

View full policy / details (opens in a new tab)

Has your organisation met this policy?

○ Yes

● No

Expectation

The expectation for this contributing outcome is ***Partially achieved***

How is your organisation performing against this outcome?

Organisations must be compliant with the mandatory policy requirement to partially achieve or achieve this outcome.

● **Not achieved**

At least one of the following statements is true.

NA#1 Initial identity verification is not robust enough to provide an acceptable level of confidence of a users' identity profile.

NA#2 Authorised users and systems with access to information, systems and networks on which your essential function(s) depends cannot be individually identified.

NA#3 Unauthorised individuals or devices can access information or networks on which your essential function(s) depends.

NA#4 The number of authorised users and

○ Partially achieved

All the following statements are true.

PA#1 Your process of initial identity verification is robust enough to provide a reasonable level of confidence of a user's identity profile before allowing an authorised user access to information, systems and networks that support your essential function(s).

PA#2 All authorised users and systems with access to information, systems and networks on which your essential function(s) depends are individually identified and authenticated.

PA#3 The number of authorised users and systems that have access to

○ Achieved

All the following statements are true.

A#1 Your process of initial identity verification is robust enough to provide a high level of confidence of a user's identity profile before allowing an authorised user access to information, systems and networks that support your essential function.

A#2 Only authorised and individually authenticated users can physically access information and logically connect to your networks or information systems on which your essential function(s) depends.

A#3 The number of authorised users and systems that have access to all your information, systems and networks

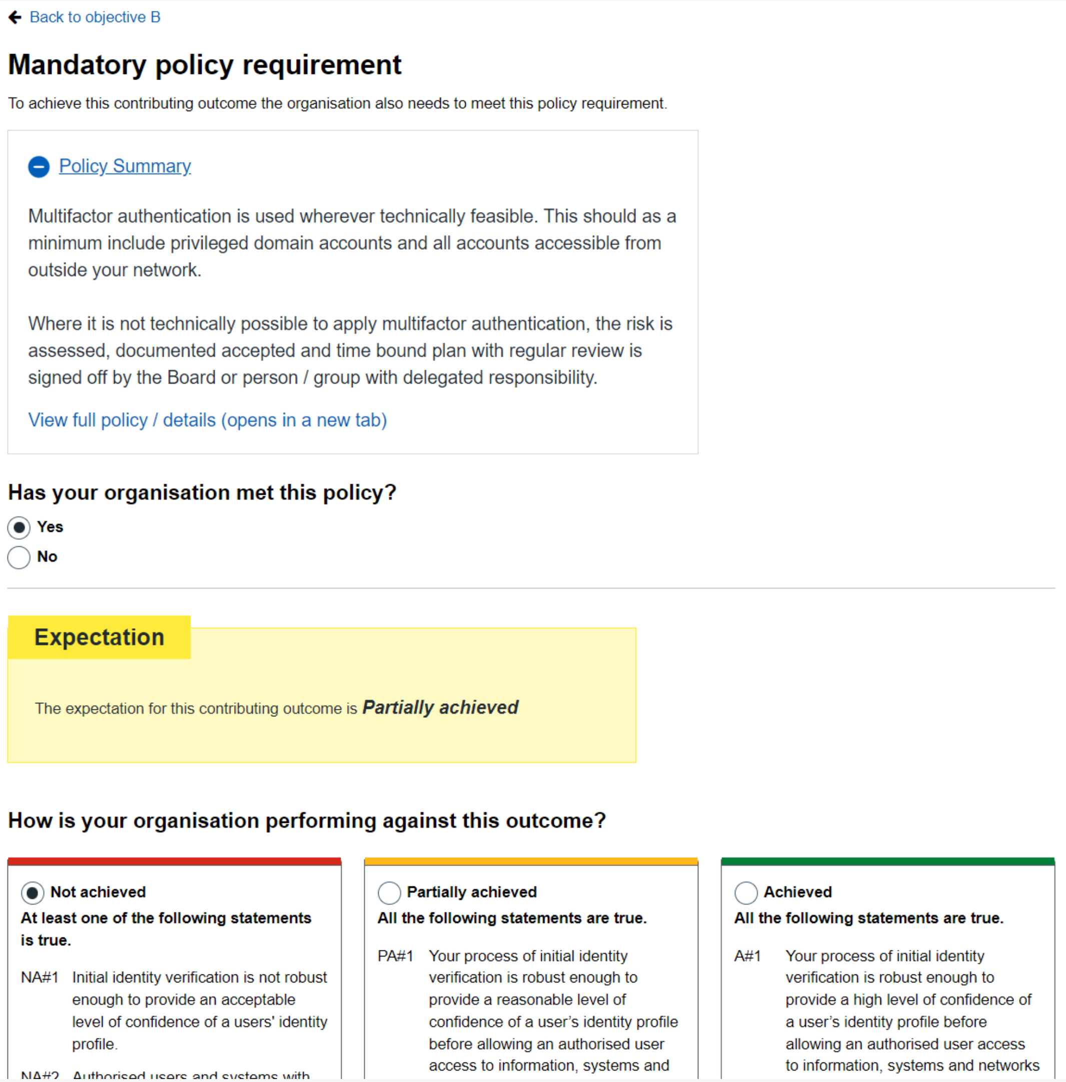
Why are Partially achieved and achieved not available to select?

Like the option you think is correct

a) Disagreement in the team

b) Organisation has not met the MFA policy

c) Not enough resources



Mandatory policy requirement

To achieve this contributing outcome the organisation also needs to meet this policy requirement.

Multifactor authentication is used wherever technically feasible. This should as a minimum include privileged domain accounts and all accounts accessible from outside your network.

Where it is not technically possible to apply multifactor authentication, the risk is assessed, documented accepted and time bound plan with regular review is signed off by the Board or person / group with delegated responsibility.

Has your organisation met this policy?

● Yes

○ No

Expectation

The expectation for this contributing outcome is ***Partially achieved***

How is your organisation performing against this outcome?

● **Not achieved**

At least one of the following statements is true.

NA#1 Initial identity verification is not robust enough to provide an acceptable level of confidence of a users' identity profile.

NA#2 Authorised users and systems with

○ **Partially achieved**

All the following statements are true.

PA#1 Your process of initial identity verification is robust enough to provide a reasonable level of confidence of a user's identity profile before allowing an authorised user access to information, systems and

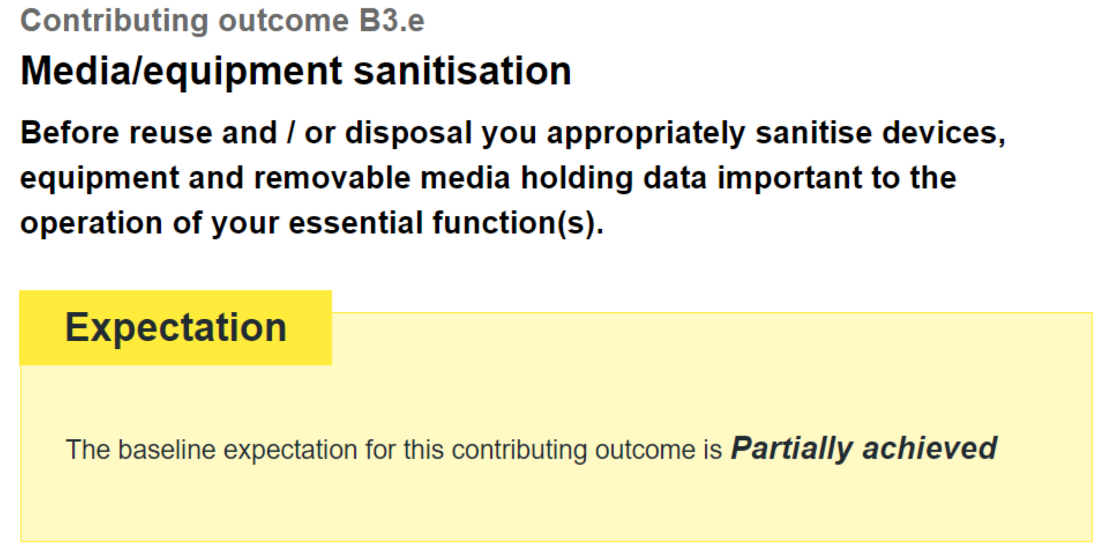
○ **Achieved**

All the following statements are true.

A#1 Your process of initial identity verification is robust enough to provide a high level of confidence of a user's identity profile before allowing an authorised user access to information, systems and networks

Principle: B3 Data Security

Contributing outcome:
B3.e Media/equipment sanitisation



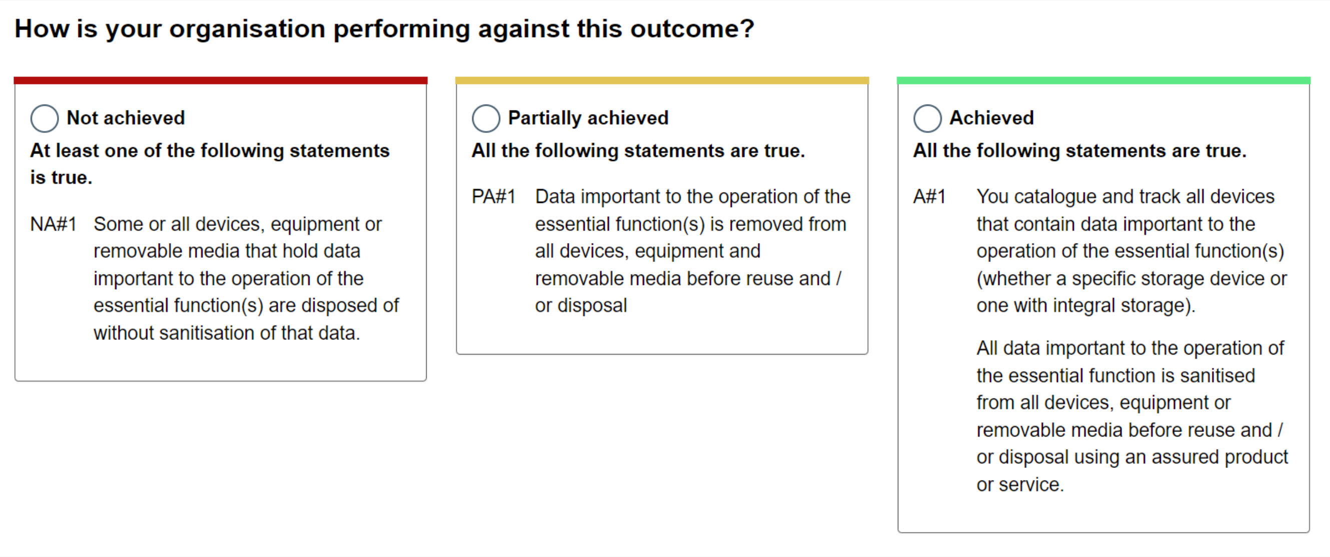
Contributing outcome B3.e

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).

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Some or all devices, equipment or removable media that hold data important to the operation of the essential function(s) are disposed of without sanitisation of that data.

○ **Partially achieved**

All the following statements are true.

PA#1 Data important to the operation of the essential function(s) is removed from all devices, equipment and removable media before reuse and / or disposal

○ **Achieved**

All the following statements are true.

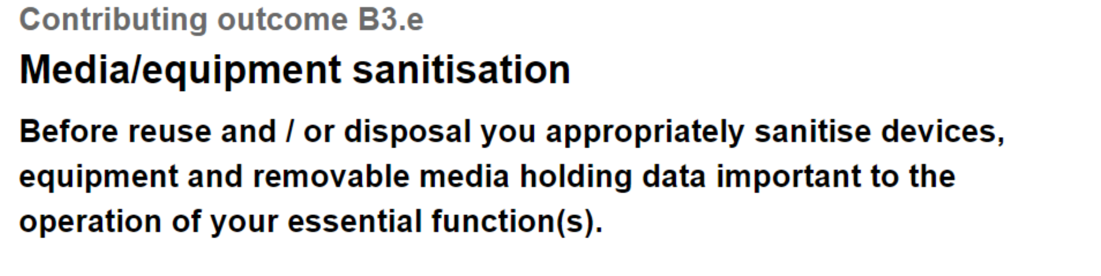
A#1 You catalogue and track all devices that contain data important to the operation of the essential function(s) (whether a specific storage device or one with integral storage).

All data important to the operation of the essential function is sanitised from all devices, equipment or removable media before reuse and / or disposal using an assured product or service.

Principle: B3 Data Security

Contributing outcome:
B3.e Media/equipment sanitisation

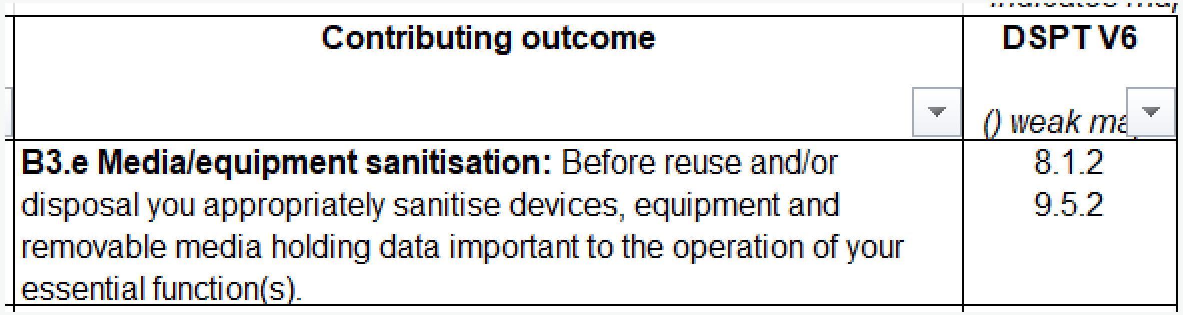
DSPT Mapping and Guidance



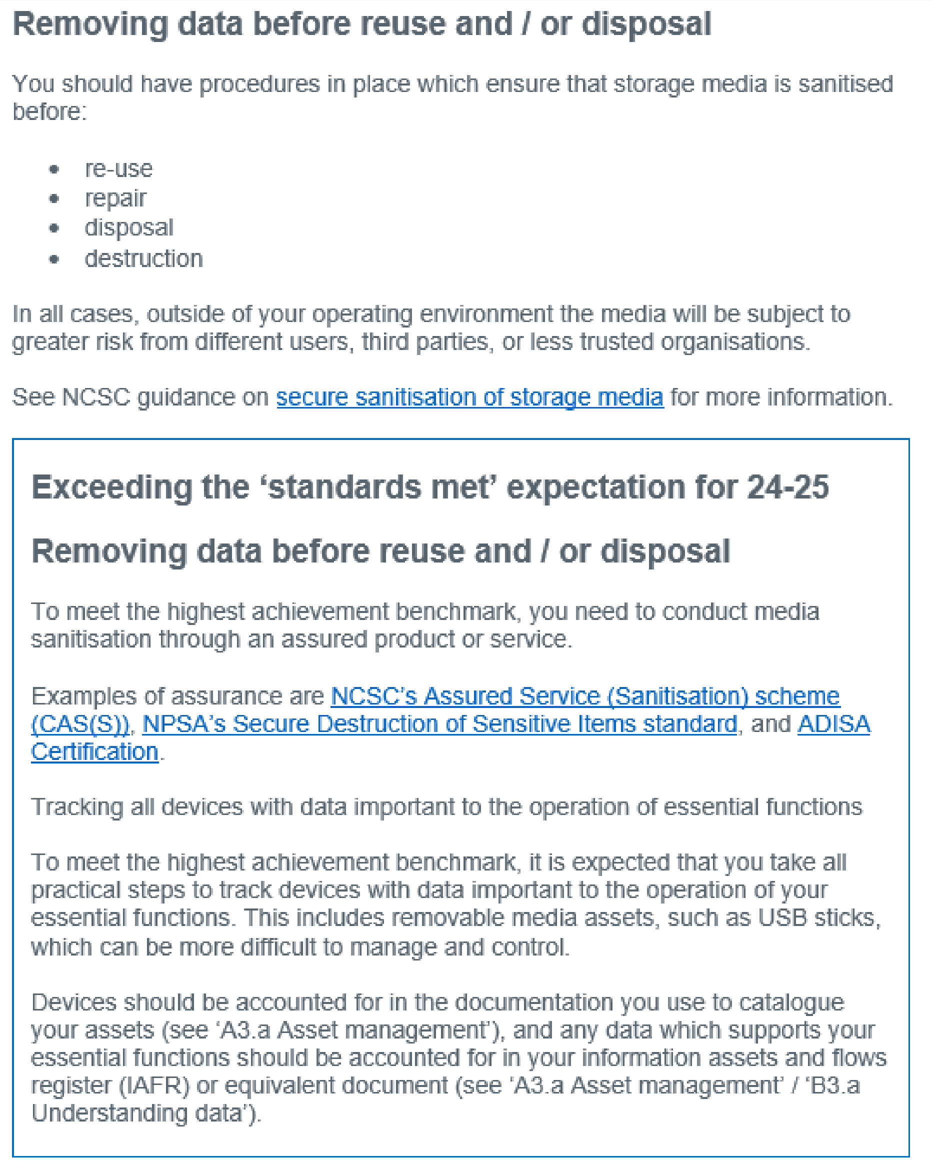
Contributing outcome B3.e

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).



Contributing outcome	DSPT V6 () weak ma
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).	8.1.2 9.5.2



Removing data before reuse and / or disposal

You should have procedures in place which ensure that storage media is sanitised before:

- re-use
- repair
- disposal
- destruction

In all cases, outside of your operating environment the media will be subject to greater risk from different users, third parties, or less trusted organisations.

See NCSC guidance on secure sanitisation of storage media for more information.

Exceeding the 'standards met' expectation for 24-25

Removing data before reuse and / or disposal

To meet the highest achievement benchmark, you need to conduct media sanitisation through an assured product or service.

Examples of assurance are NCSC's Assured Service (Sanitisation) scheme (CAS(S)), NPSA's Secure Destruction of Sensitive Items standard, and ADISA Certification.

Tracking all devices with data important to the operation of essential functions

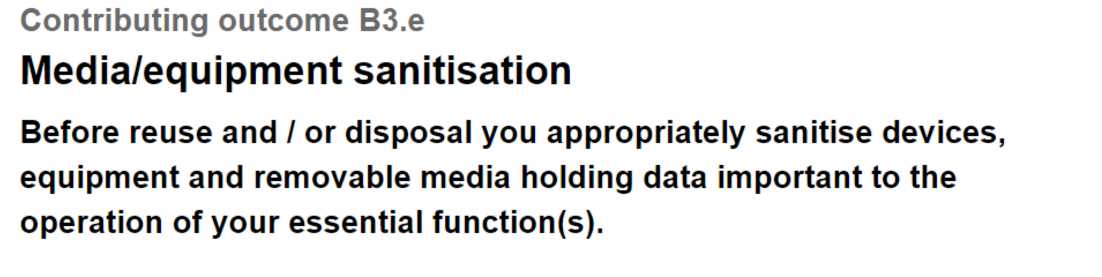
To meet the highest achievement benchmark, it is expected that you take all practical steps to track devices with data important to the operation of your essential functions. This includes removable media assets, such as USB sticks, which can be more difficult to manage and control.

Devices should be accounted for in the documentation you use to catalogue your assets (see 'A3.a Asset management'), and any data which supports your essential functions should be accounted for in your information assets and flows register (IAFR) or equivalent document (see 'A3.a Asset management' / 'B3.a Understanding data').

Principle: B3 Data Security

Contributing outcome:
B3.e Media/equipment sanitisation

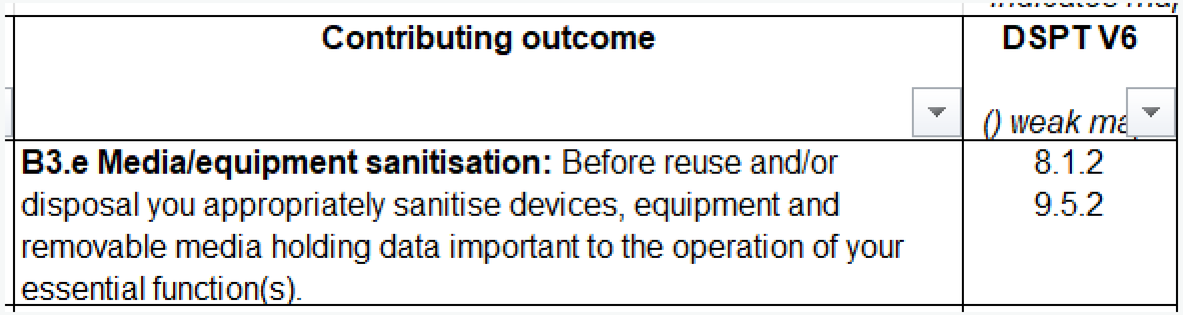
Supporting Evidence



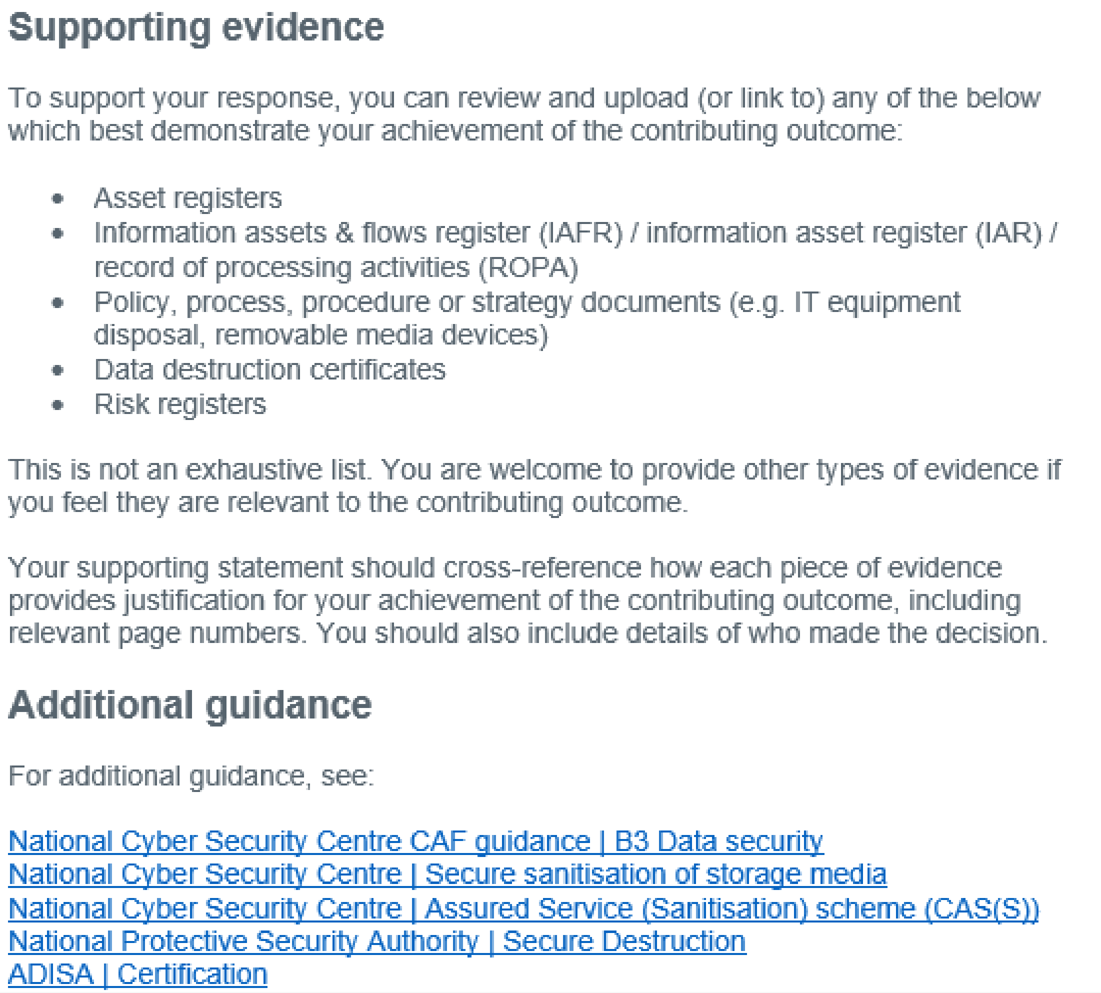
Contributing outcome B3.e

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).



Contributing outcome	DSPT V6 *() weak ma*
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).	8.1.2 9.5.2



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Asset registers
- Information assets & flows register (IAFR) / information asset register (IAR) / record of processing activities (ROPA)
- Policy, process, procedure or strategy documents (e.g. IT equipment disposal, removable media devices)
- Data destruction certificates
- Risk registers

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

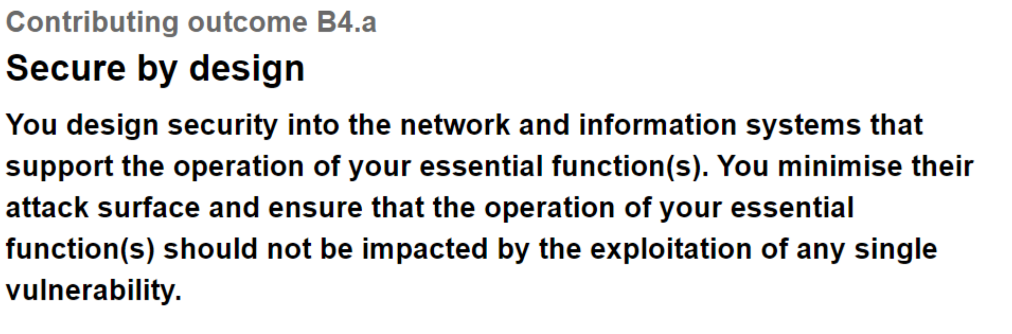
Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B3 Data security
National Cyber Security Centre | Secure sanitisation of storage media
National Cyber Security Centre | Assured Service (Sanitisation) scheme (CAS(S))
National Protective Security Authority | Secure Destruction
ADISA | Certification

Principle: B4 System Security

Contributing outcome:
B4.a Secure by design



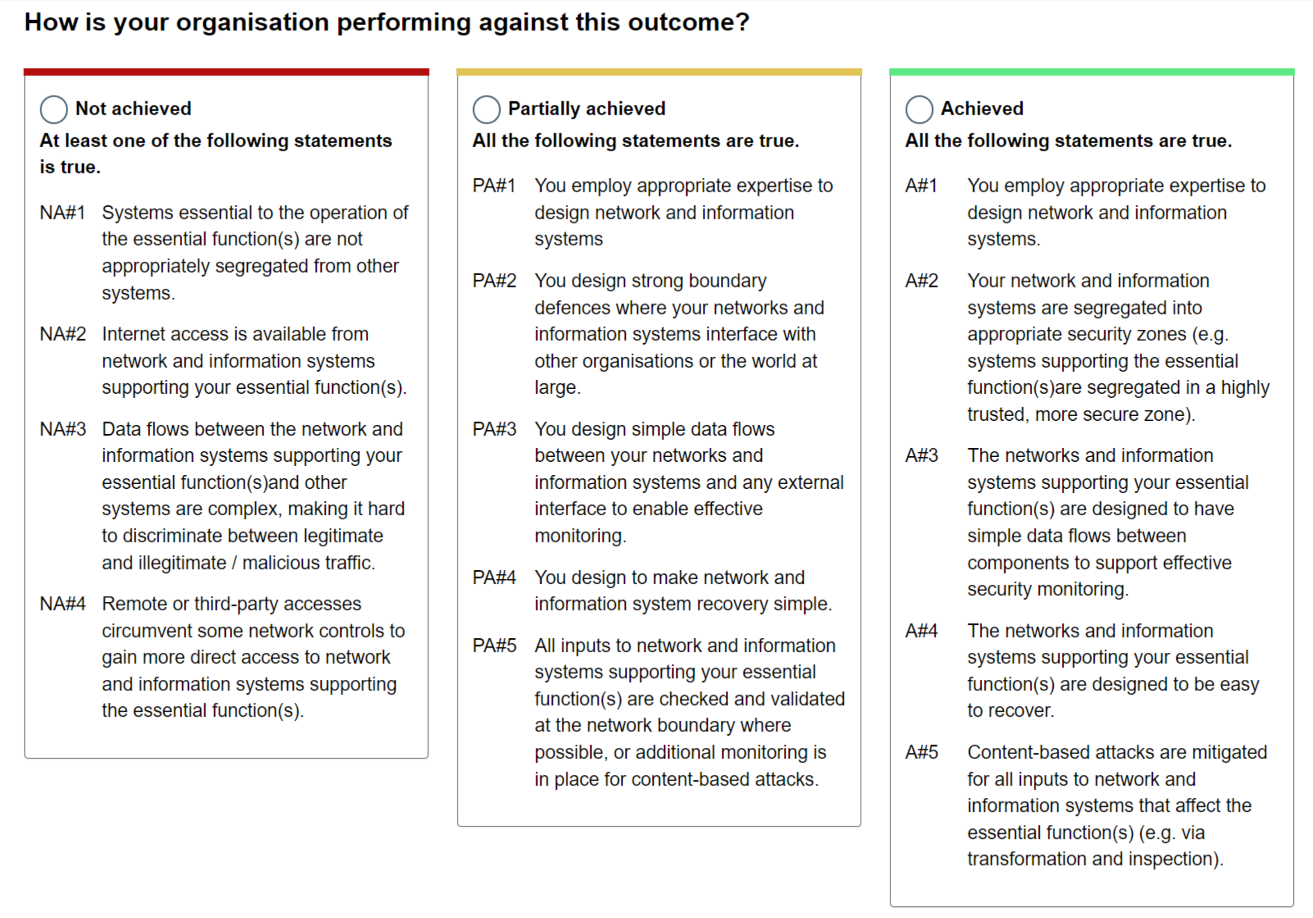
Contributing outcome B4.a

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.

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Systems essential to the operation of the essential function(s) are not appropriately segregated from other systems.

NA#2 Internet access is available from network and information systems supporting your essential function(s).

NA#3 Data flows between the network and information systems supporting your essential function(s)and other systems are complex, making it hard to discriminate between legitimate and illegitimate / malicious traffic.

NA#4 Remote or third-party accesses circumvent some network controls to gain more direct access to network and information systems supporting the essential function(s).

○ **Partially achieved**

All the following statements are true.

PA#1 You employ appropriate expertise to design network and information systems

PA#2 You design strong boundary defences where your networks and information systems interface with other organisations or the world at large.

PA#3 You design simple data flows between your networks and information systems and any external interface to enable effective monitoring.

PA#4 You design to make network and information system recovery simple.

PA#5 All inputs to network and information systems supporting your essential function(s) are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.

○ **Achieved**

All the following statements are true.

A#1 You employ appropriate expertise to design network and information systems.

A#2 Your network and information systems are segregated into appropriate security zones (e.g. systems supporting the essential function(s)are segregated in a highly trusted, more secure zone).

A#3 The networks and information systems supporting your essential function(s) are designed to have simple data flows between components to support effective security monitoring.

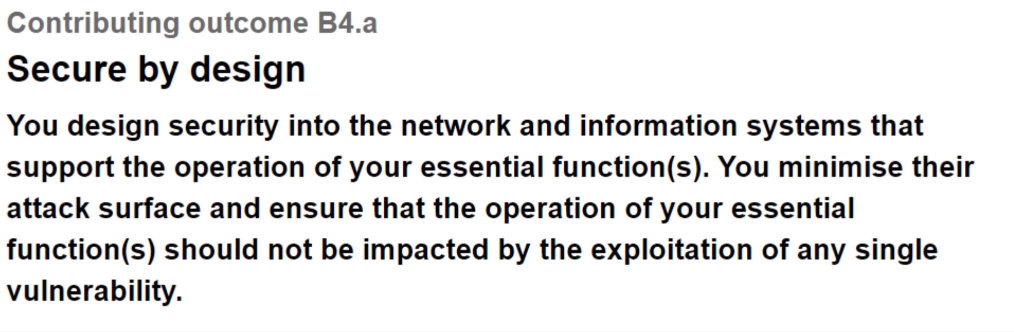
A#4 The networks and information systems supporting your essential function(s) are designed to be easy to recover.

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).

Principle: B4 System Security

Contributing outcome:
B4.a Secure by design

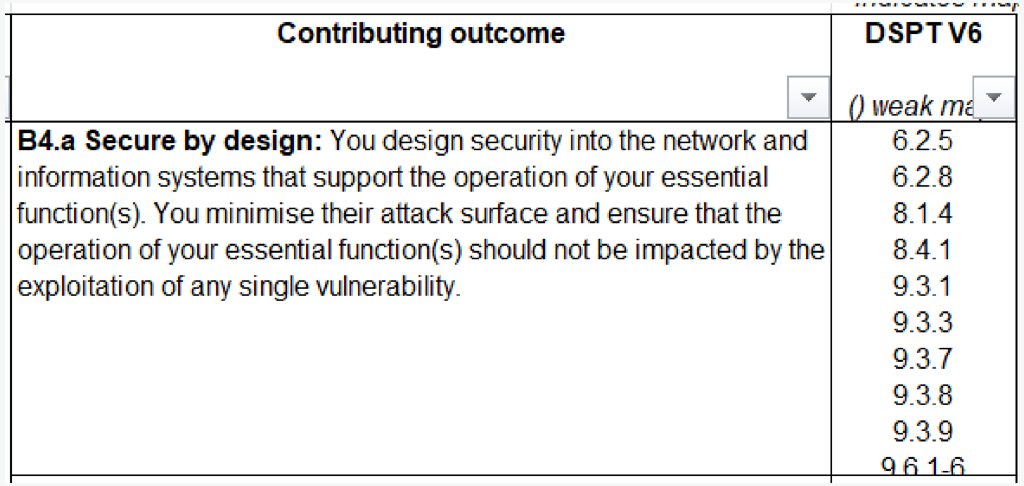
DSPT Mapping and Guidance



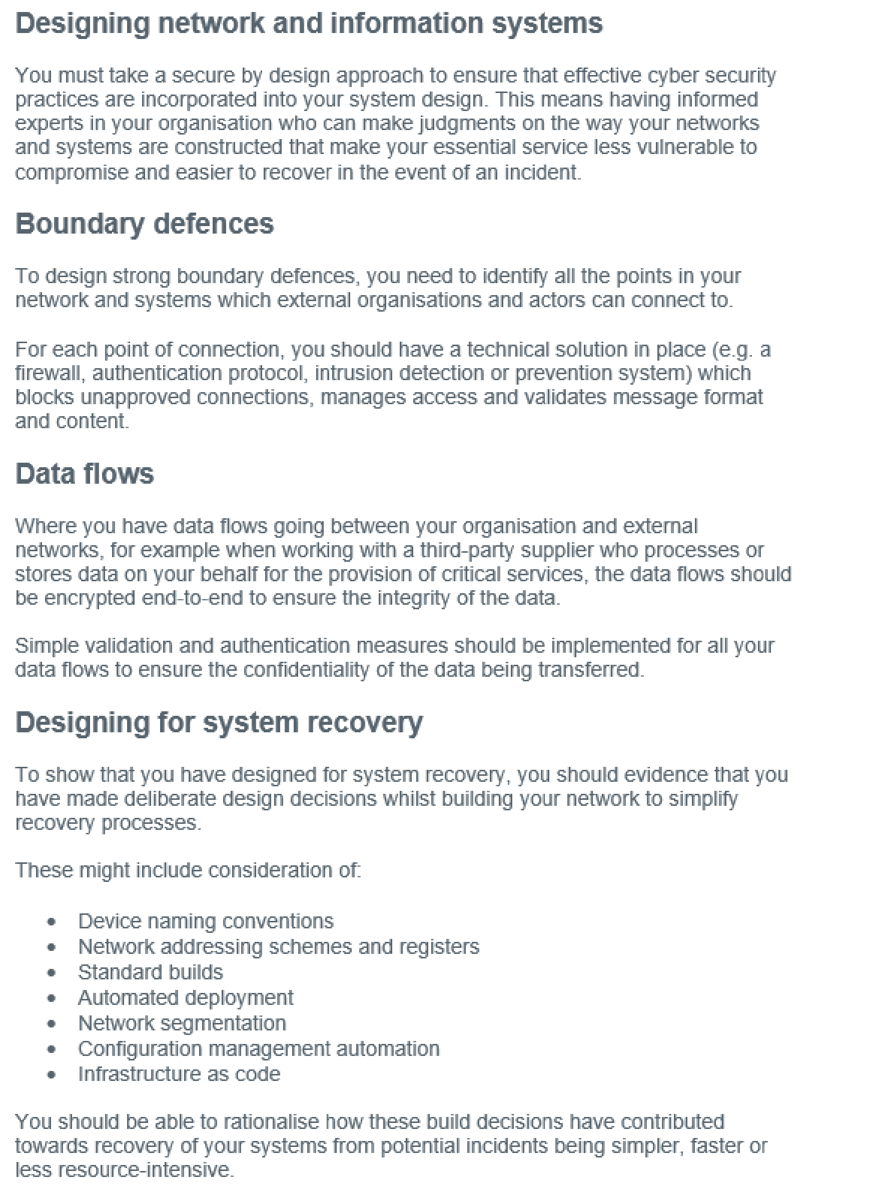
Contributing outcome B4.a

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.



Contributing outcome	DSPT V6 *() weak ma*
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.	6.2.5 6.2.8 8.1.4 8.4.1 9.3.1 9.3.3 9.3.7 9.3.8 9.3.9 9.6.1-6



Designing network and information systems

You must take a secure by design approach to ensure that effective cyber security practices are incorporated into your system design. This means having informed experts in your organisation who can make judgments on the way your networks and systems are constructed that make your essential service less vulnerable to compromise and easier to recover in the event of an incident.

Boundary defences

To design strong boundary defences, you need to identify all the points in your network and systems which external organisations and actors can connect to.

For each point of connection, you should have a technical solution in place (e.g. a firewall, authentication protocol, intrusion detection or prevention system) which blocks unapproved connections, manages access and validates message format and content.

Data flows

Where you have data flows going between your organisation and external networks, for example when working with a third-party supplier who processes or stores data on your behalf for the provision of critical services, the data flows should be encrypted end-to-end to ensure the integrity of the data.

Simple validation and authentication measures should be implemented for all your data flows to ensure the confidentiality of the data being transferred.

Designing for system recovery

To show that you have designed for system recovery, you should evidence that you have made deliberate design decisions whilst building your network to simplify recovery processes.

These might include consideration of:

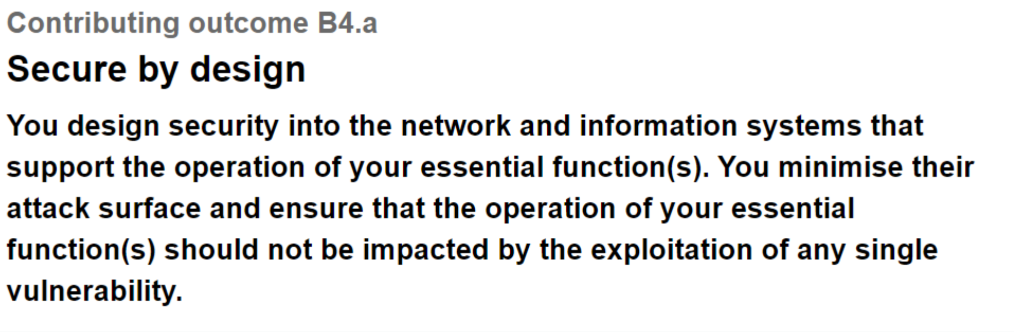
- Device naming conventions
- Network addressing schemes and registers
- Standard builds
- Automated deployment
- Network segmentation
- Configuration management automation
- Infrastructure as code

You should be able to rationalise how these build decisions have contributed towards recovery of your systems from potential incidents being simpler, faster or less resource-intensive.

Principle: B4 System Security

Contributing outcome:
B4.a Secure by design

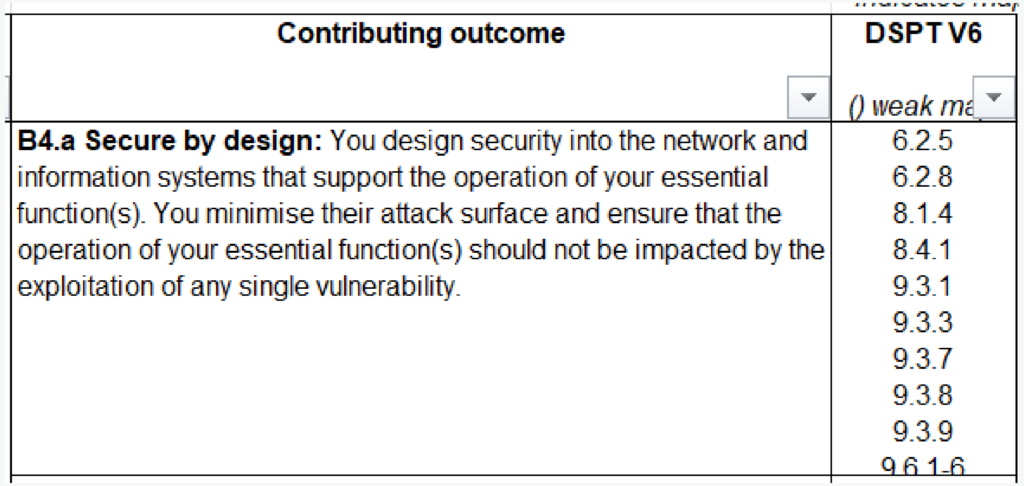
DSPT Mapping and Guidance



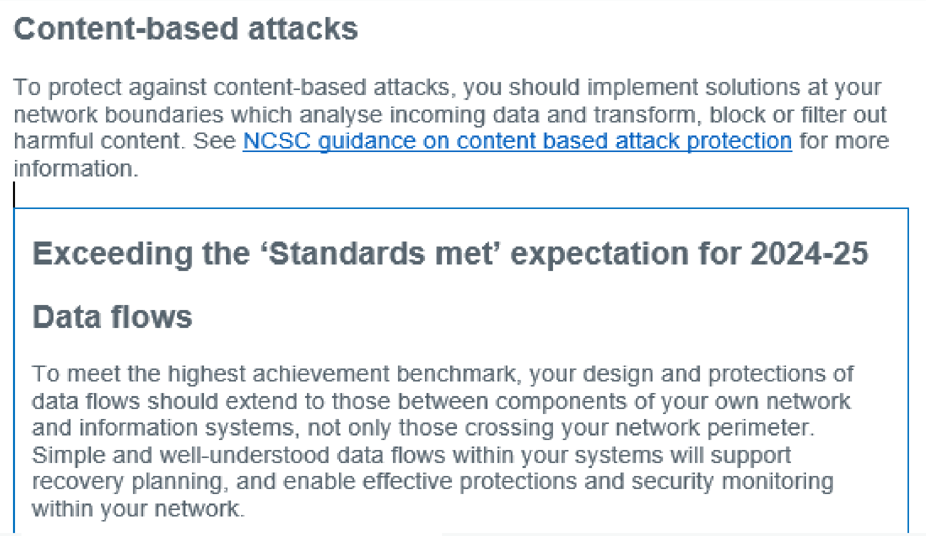
Contributing outcome B4.a

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.



Contributing outcome	DSPT V6 () weak ma
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.	6.2.5 6.2.8 8.1.4 8.4.1 9.3.1 9.3.3 9.3.7 9.3.8 9.3.9 9.6.1-6



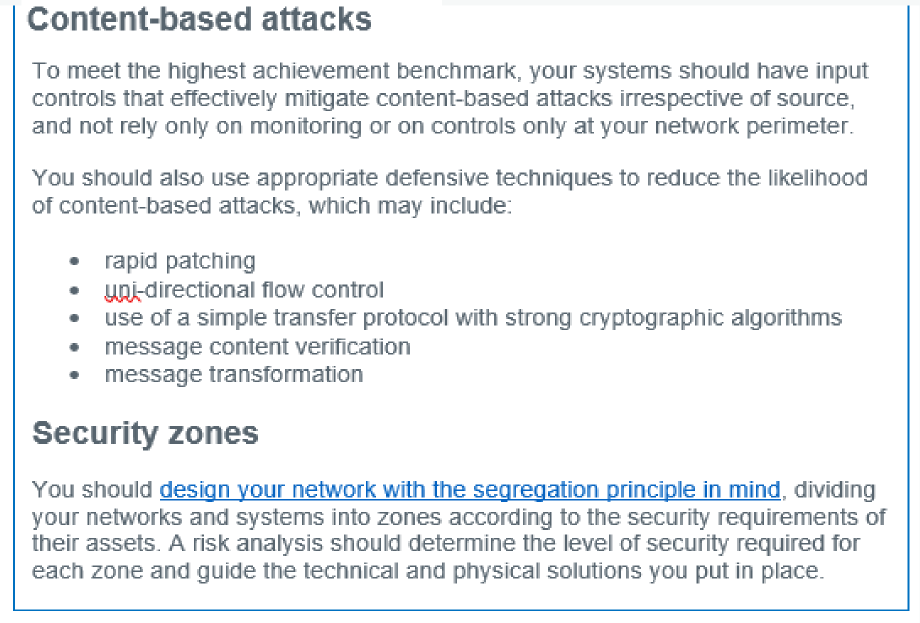
Content-based attacks

To protect against content-based attacks, you should implement solutions at your network boundaries which analyse incoming data and transform, block or filter out harmful content. See NCSC guidance on content based attack protection for more information.

Exceeding the 'Standards met' expectation for 2024-25

Data flows

To meet the highest achievement benchmark, your design and protections of data flows should extend to those between components of your own network and information systems, not only those crossing your network perimeter. Simple and well-understood data flows within your systems will support recovery planning, and enable effective protections and security monitoring within your network.



Content-based attacks

To meet the highest achievement benchmark, your systems should have input controls that effectively mitigate content-based attacks irrespective of source, and not rely only on monitoring or on controls only at your network perimeter.

You should also use appropriate defensive techniques to reduce the likelihood of content-based attacks, which may include:

- rapid patching
- uni-directional flow control
- use of a simple transfer protocol with strong cryptographic algorithms
- message content verification
- message transformation

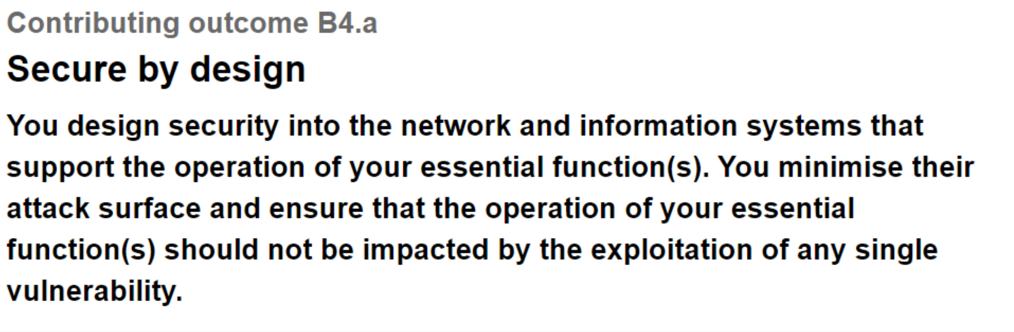
Security zones

You should design your network with the segregation principle in mind, dividing your networks and systems into zones according to the security requirements of their assets. A risk analysis should determine the level of security required for each zone and guide the technical and physical solutions you put in place.

Principle: B4 System Security

Contributing outcome:
B4.a Secure by design

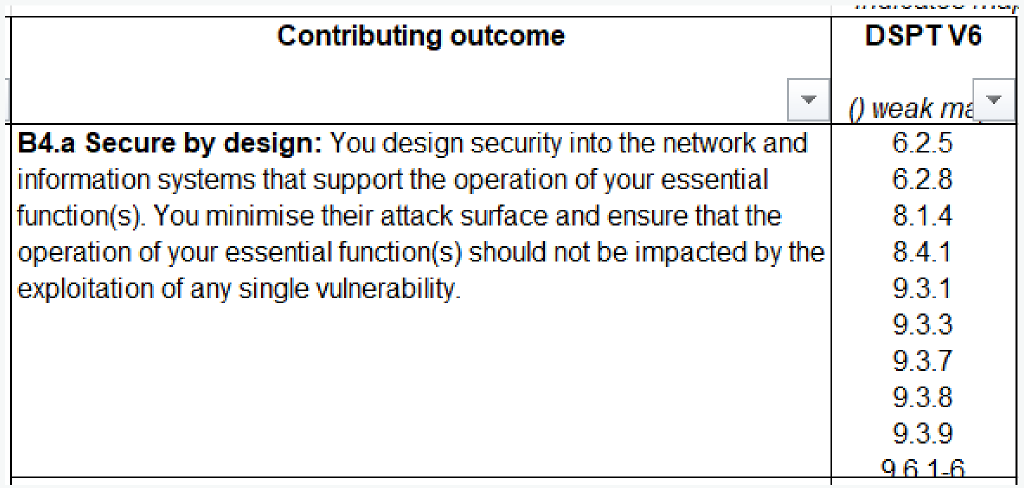
Supporting Evidence



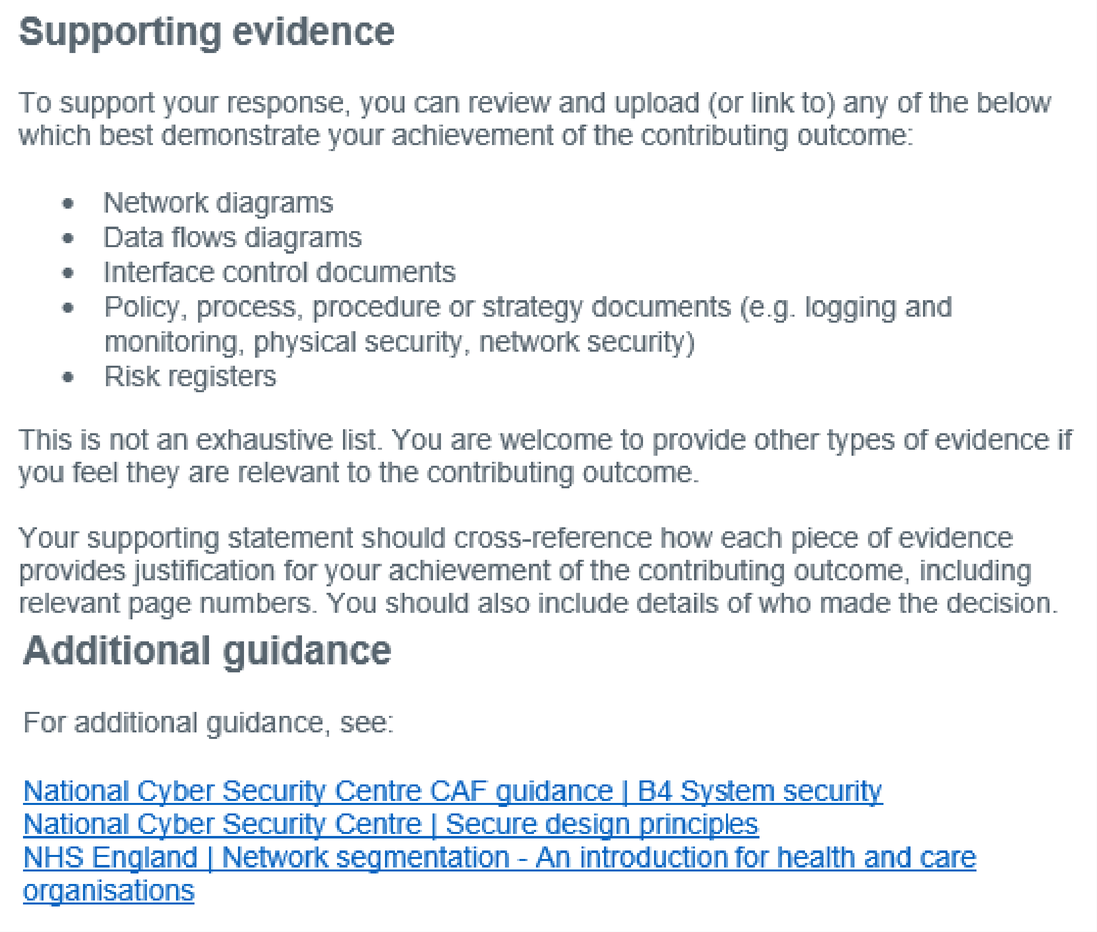
Contributing outcome B4.a

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.



Contributing outcome	DSPT V6 *() weak ma*
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.	6.2.5 6.2.8 8.1.4 8.4.1 9.3.1 9.3.3 9.3.7 9.3.8 9.3.9 9.6.1-6



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Network diagrams
- Data flows diagrams
- Interface control documents
- Policy, process, procedure or strategy documents (e.g. logging and monitoring, physical security, network security)
- Risk registers

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

Additional guidance

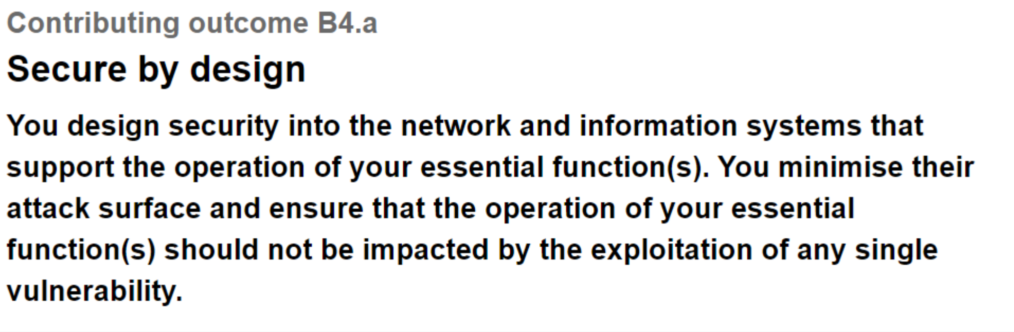
For additional guidance, see:

National Cyber Security Centre CAF guidance | B4 System security
National Cyber Security Centre | Secure design principles
NHS England | Network segmentation - An introduction for health and care organisations

Principle: B4 System Security

Contributing outcome:
B4.a Secure by design

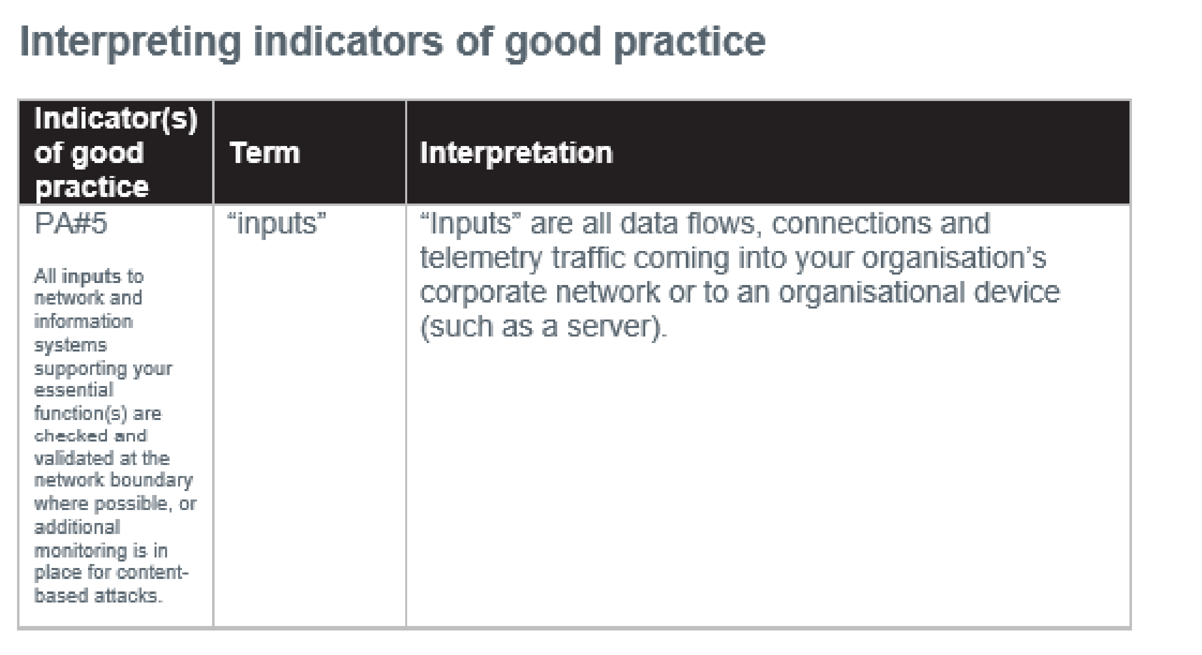
Interpretation



Contributing outcome 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.

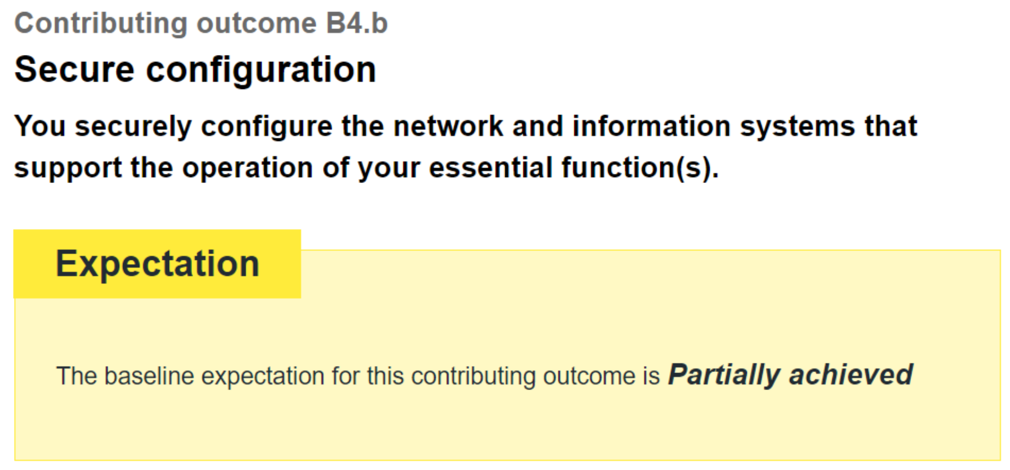


Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#5 All **inputs** to network and information systems supporting your essential function(s) are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.	“inputs”	“Inputs” are all data flows, connections and telemetry traffic coming into your organisation’s corporate network or to an organisational device (such as a server).

Principle: B4 System Security

Contributing outcome:
B4.b Secure configuration



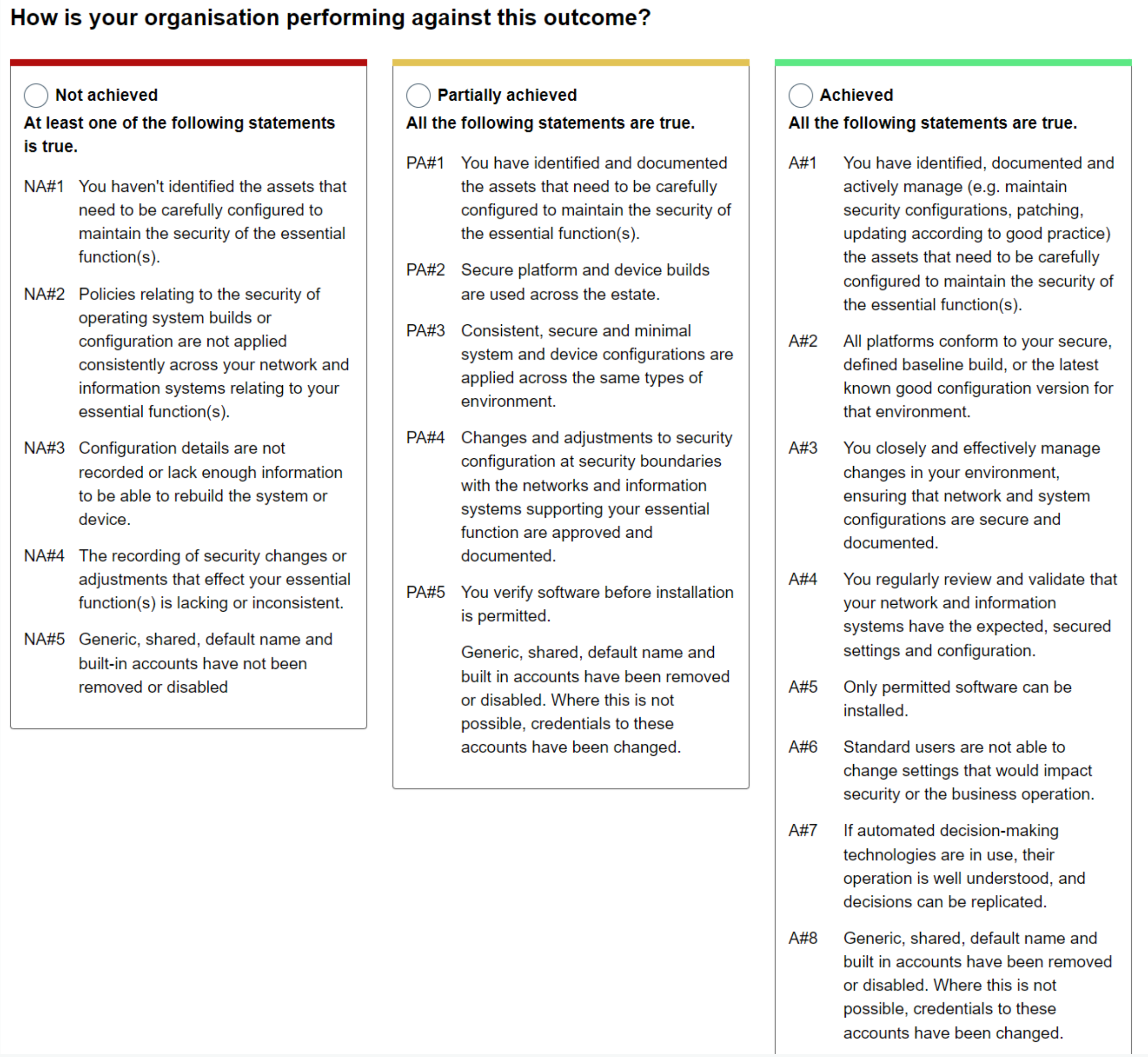
Contributing outcome B4.b

Secure configuration

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

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 You haven't identified the assets that need to be carefully configured to maintain the security of the essential function(s).

NA#2 Policies relating to the security of operating system builds or configuration are not applied consistently across your network and information systems relating to your essential function(s).

NA#3 Configuration details are not recorded or lack enough information to be able to rebuild the system or device.

NA#4 The recording of security changes or adjustments that effect your essential function(s) is lacking or inconsistent.

NA#5 Generic, shared, default name and built-in accounts have not been removed or disabled

○ **Partially achieved**

All the following statements are true.

PA#1 You have identified and documented the assets that need to be carefully configured to maintain the security of the essential function(s).

PA#2 Secure platform and device builds are used across the estate.

PA#3 Consistent, secure and minimal system and device configurations are applied across the same types of environment.

PA#4 Changes and adjustments to security configuration at security boundaries with the networks and information systems supporting your essential function are approved and documented.

PA#5 You verify software before installation is permitted.

Generic, shared, default name and built in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed.

○ **Achieved**

All the following statements are true.

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).

A#2 All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment.

A#3 You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.

A#4 You regularly review and validate that your network and information systems have the expected, secured settings and configuration.

A#5 Only permitted software can be installed.

A#6 Standard users are not able to change settings that would impact security or the business operation.

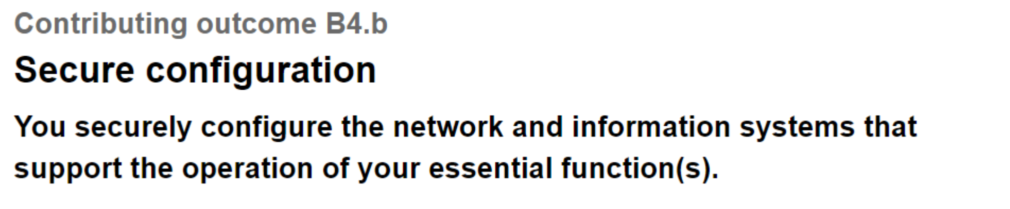
A#7 If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated.

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.

Principle: B4 System Security

Contributing outcome:
B4.b Secure configuration

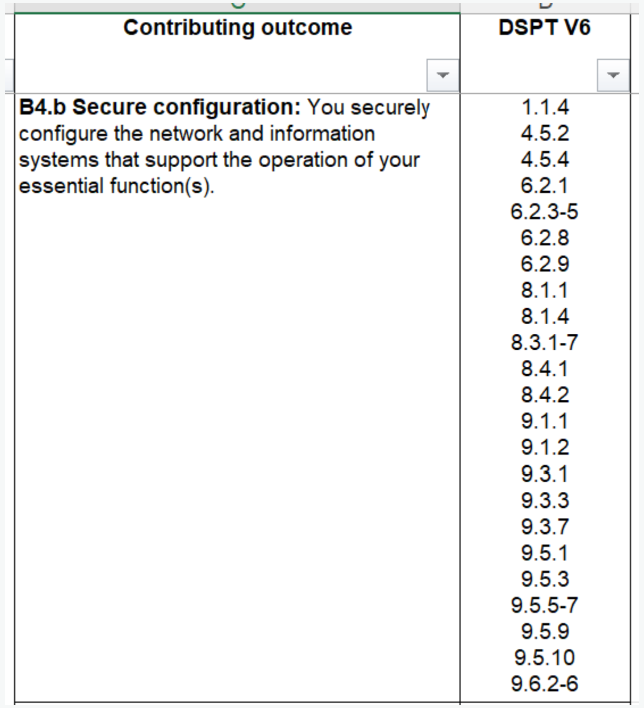
DSPT Mapping and Guidance



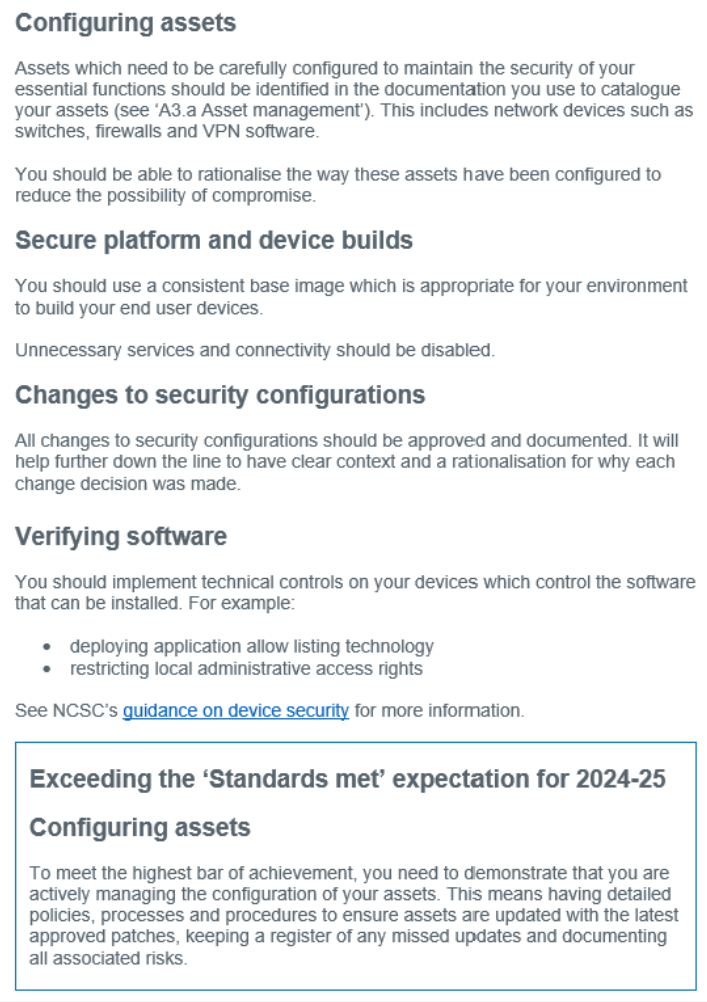
Contributing outcome B4.b

Secure configuration

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



Contributing outcome	DSPT V6
B4.b Secure configuration: You securely configure the network and information systems that support the operation of your essential function(s).	1.1.4 4.5.2 4.5.4 6.2.1 6.2.3-5 6.2.8 6.2.9 8.1.1 8.1.4 8.3.1-7 8.4.1 8.4.2 9.1.1 9.1.2 9.3.1 9.3.3 9.3.7 9.5.1 9.5.3 9.5.5-7 9.5.9 9.5.10 9.6.2-6



Configuring assets

Assets which need to be carefully configured to maintain the security of your essential functions should be identified in the documentation you use to catalogue your assets (see ‘A3.a Asset management’). This includes network devices such as switches, firewalls and VPN software.

You should be able to rationalise the way these assets have been configured to reduce the possibility of compromise.

Secure platform and device builds

You should use a consistent base image which is appropriate for your environment to build your end user devices.

Unnecessary services and connectivity should be disabled.

Changes to security configurations

All changes to security configurations should be approved and documented. It will help further down the line to have clear context and a rationalisation for why each change decision was made.

Verifying software

You should implement technical controls on your devices which control the software that can be installed. For example:

- deploying application allow listing technology
- restricting local administrative access rights

See NCSC’s guidance on device security for more information.

Exceeding the ‘Standards met’ expectation for 2024-25

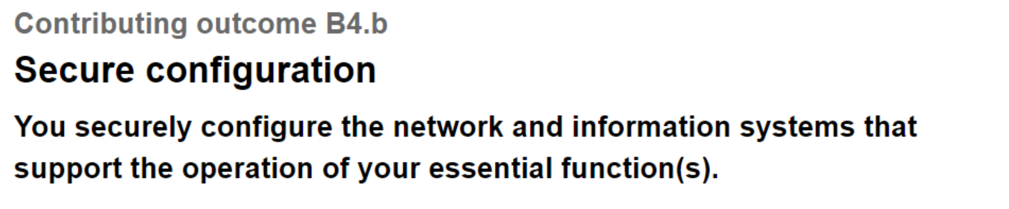
Configuring assets

To meet the highest bar of achievement, you need to demonstrate that you are actively managing the configuration of your assets. This means having detailed policies, processes and procedures to ensure assets are updated with the latest approved patches, keeping a register of any missed updates and documenting all associated risks.

Principle: B4 System Security

Contributing outcome:
B4.b Secure configuration

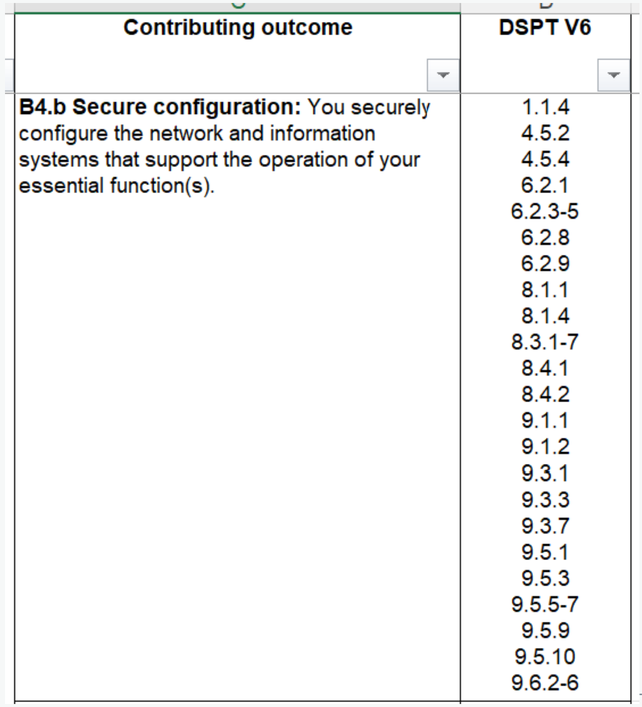
Supporting Evidence



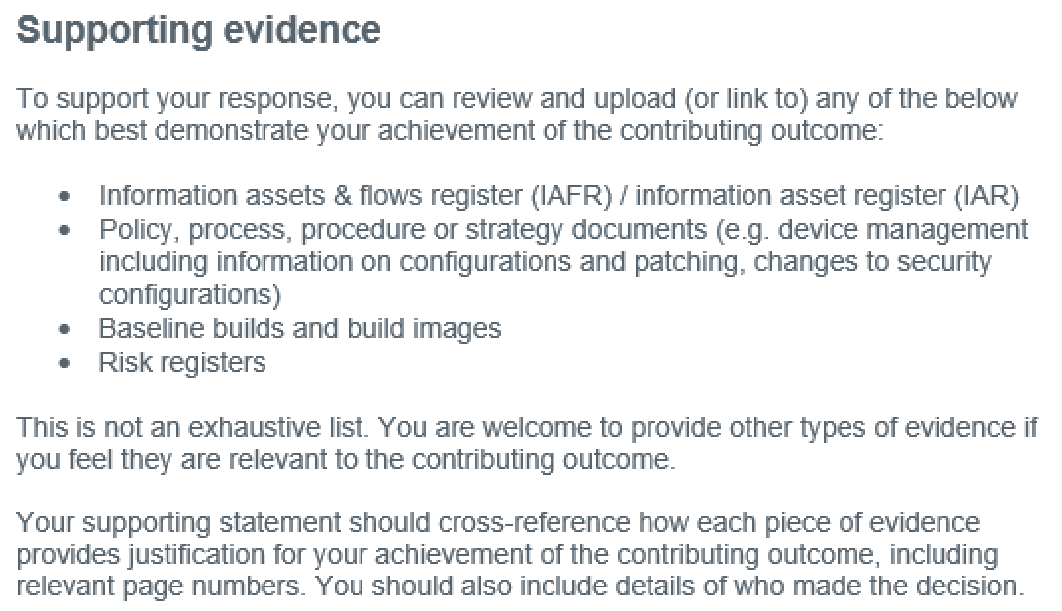
Contributing outcome B4.b

Secure configuration

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



Contributing outcome	DSPT V6
B4.b Secure configuration: You securely configure the network and information systems that support the operation of your essential function(s).	1.1.4 4.5.2 4.5.4 6.2.1 6.2.3-5 6.2.8 6.2.9 8.1.1 8.1.4 8.3.1-7 8.4.1 8.4.2 9.1.1 9.1.2 9.3.1 9.3.3 9.3.7 9.5.1 9.5.3 9.5.5-7 9.5.9 9.5.10 9.6.2-6



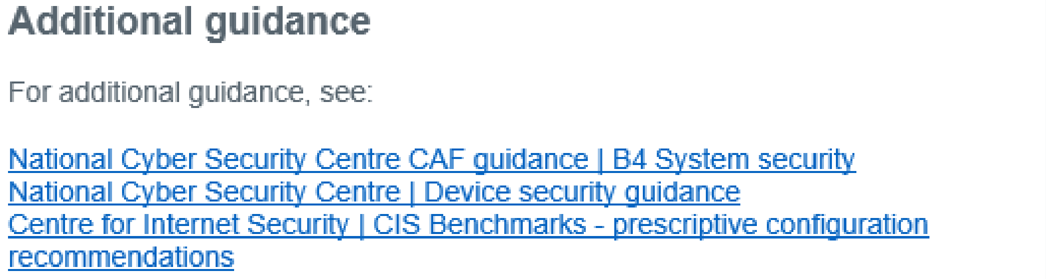
Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Information assets & flows register (IAFR) / information asset register (IAR)
- Policy, process, procedure or strategy documents (e.g. device management including information on configurations and patching, changes to security configurations)
- Baseline builds and build images
- Risk registers

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.



Additional guidance

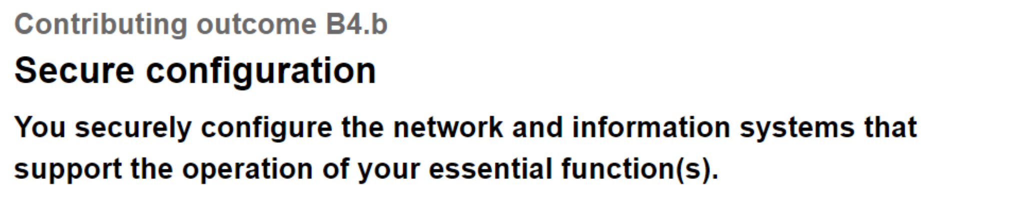
For additional guidance, see:

National Cyber Security Centre CAF guidance | B4 System security
National Cyber Security Centre | Device security guidance
Centre for Internet Security | CIS Benchmarks - prescriptive configuration recommendations

Principle: B4 System Security

Contributing outcome:
B4.b Secure configuration

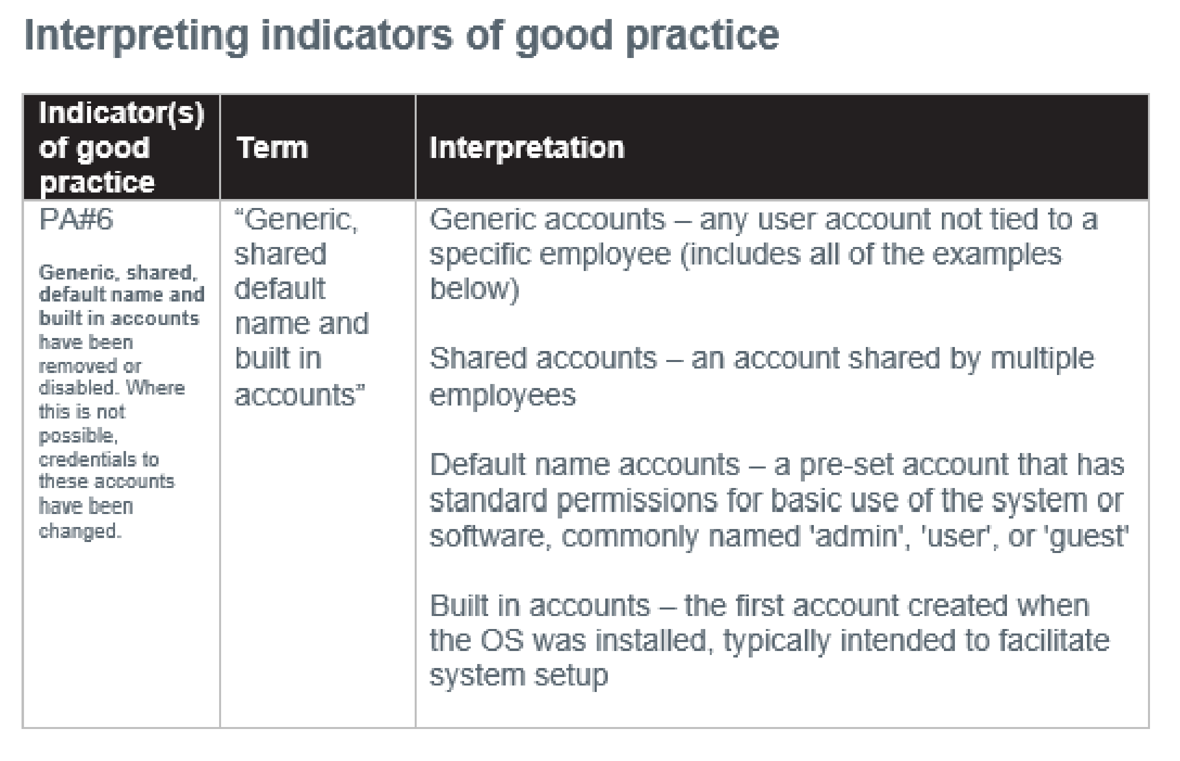
Interpretation



Contributing outcome B4.b

Secure configuration

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

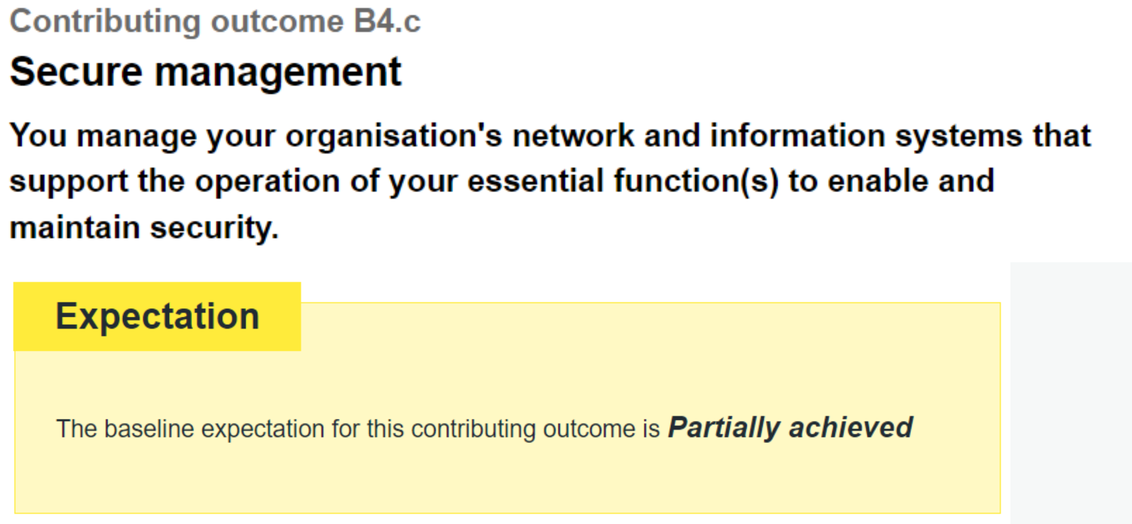


Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
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.	“Generic, shared default name and built in accounts”	Generic accounts – any user account not tied to a specific employee (includes all of the examples below) Shared accounts – an account shared by multiple employees Default name accounts – a pre-set account that has standard permissions for basic use of the system or software, commonly named 'admin', 'user', or 'guest' Built in accounts – the first account created when the OS was installed, typically intended to facilitate system setup

Principle: B4 System Security

Contributing outcome:
B4.c Secure management



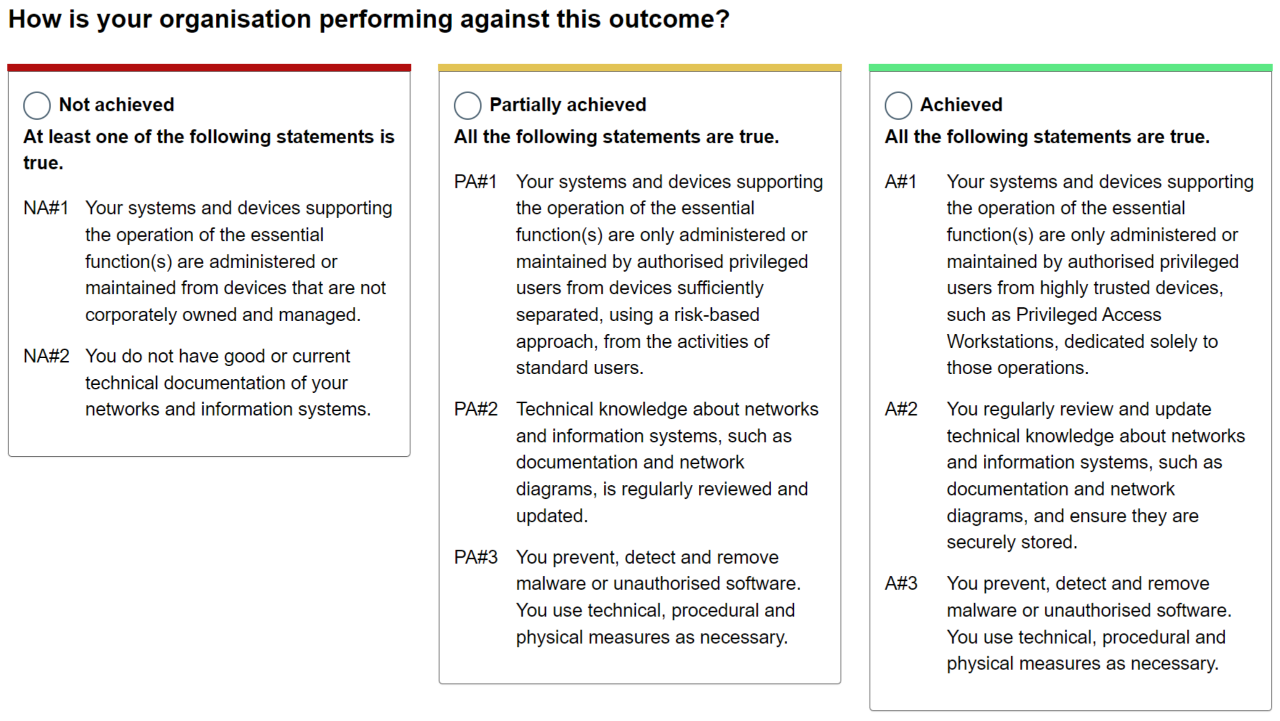
Contributing outcome B4.c

Secure management

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

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Your systems and devices supporting the operation of the essential function(s) are administered or maintained from devices that are not corporately owned and managed.

NA#2 You do not have good or current technical documentation of your networks and information systems.

○ **Partially achieved**

All the following statements are true.

PA#1 Your systems and devices supporting the operation of the essential function(s) are only administered or maintained by authorised privileged users from devices sufficiently separated, using a risk-based approach, from the activities of standard users.

PA#2 Technical knowledge about networks and information systems, such as documentation and network diagrams, is regularly reviewed and updated.

PA#3 You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.

○ **Achieved**

All the following statements are true.

A#1 Your systems and devices supporting the operation of the essential function(s) are only administered or maintained by authorised privileged users from highly trusted devices, such as Privileged Access Workstations, dedicated solely to those operations.

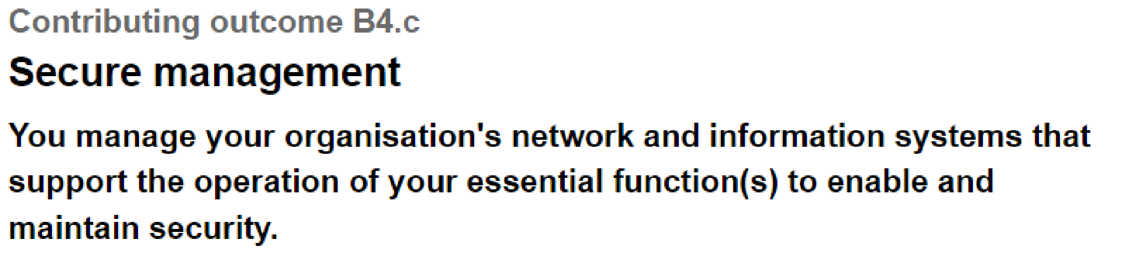
A#2 You regularly review and update technical knowledge about networks and information systems, such as documentation and network diagrams, and ensure they are securely stored.

A#3 You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.

Principle: B4 System Security

Contributing outcome:
B4.c Secure management

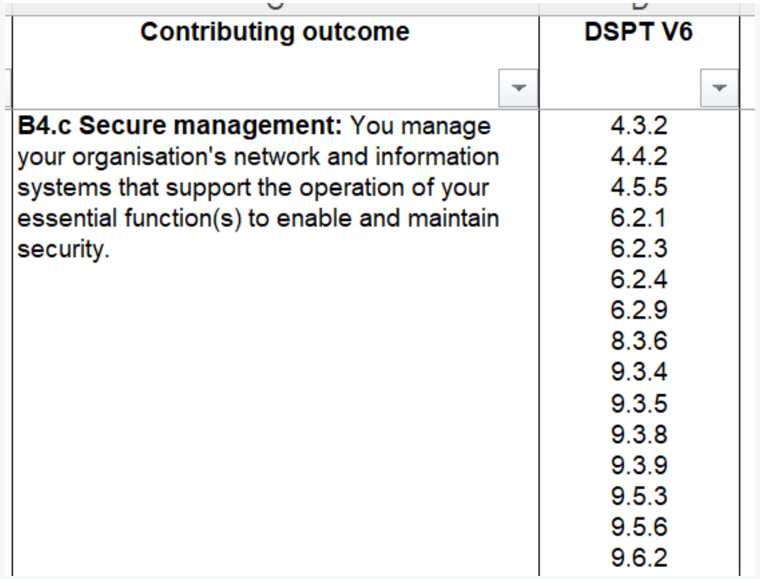
DSPT Mapping and Guidance



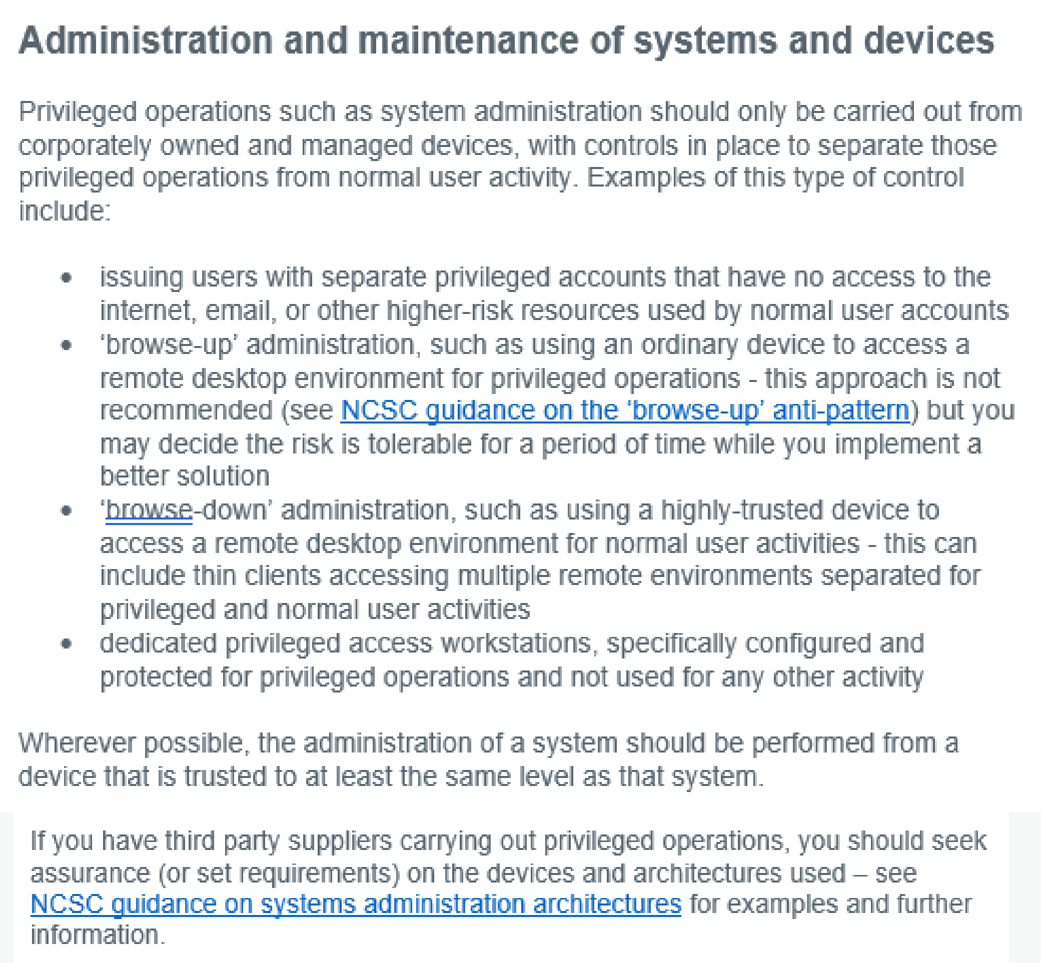
Contributing outcome B4.c

Secure management

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



Contributing outcome	DSPT V6
B4.c Secure management: You manage your organisation's network and information systems that support the operation of your essential function(s) to enable and maintain security.	4.3.2 4.4.2 4.5.5 6.2.1 6.2.3 6.2.4 6.2.9 8.3.6 9.3.4 9.3.5 9.3.8 9.3.9 9.5.3 9.5.6 9.6.2



Administration and maintenance of systems and devices

Privileged operations such as system administration should only be carried out from corporately owned and managed devices, with controls in place to separate those privileged operations from normal user activity. Examples of this type of control include:

- issuing users with separate privileged accounts that have no access to the internet, email, or other higher-risk resources used by normal user accounts
- 'browse-up' administration, such as using an ordinary device to access a remote desktop environment for privileged operations - this approach is not recommended (see NCSC guidance on the 'browse-up' anti-pattern) but you may decide the risk is tolerable for a period of time while you implement a better solution
- 'browse-down' administration, such as using a highly-trusted device to access a remote desktop environment for normal user activities - this can include thin clients accessing multiple remote environments separated for privileged and normal user activities
- dedicated privileged access workstations, specifically configured and protected for privileged operations and not used for any other activity

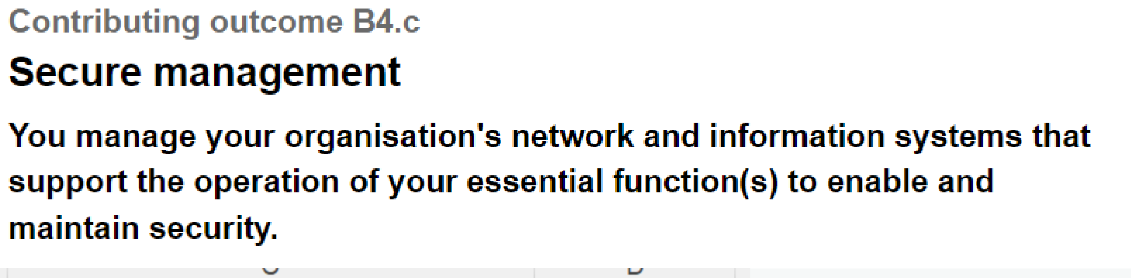
Wherever possible, the administration of a system should be performed from a device that is trusted to at least the same level as that system.

If you have third party suppliers carrying out privileged operations, you should seek assurance (or set requirements) on the devices and architectures used – see NCSC guidance on systems administration architectures for examples and further information.

Principle: B4 System Security

Contributing outcome:
B4.c Secure management

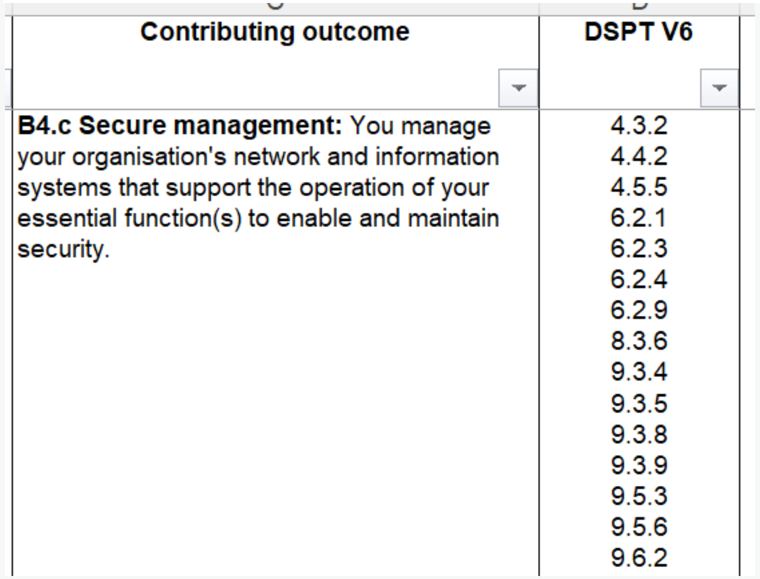
DSPT Mapping and Guidance



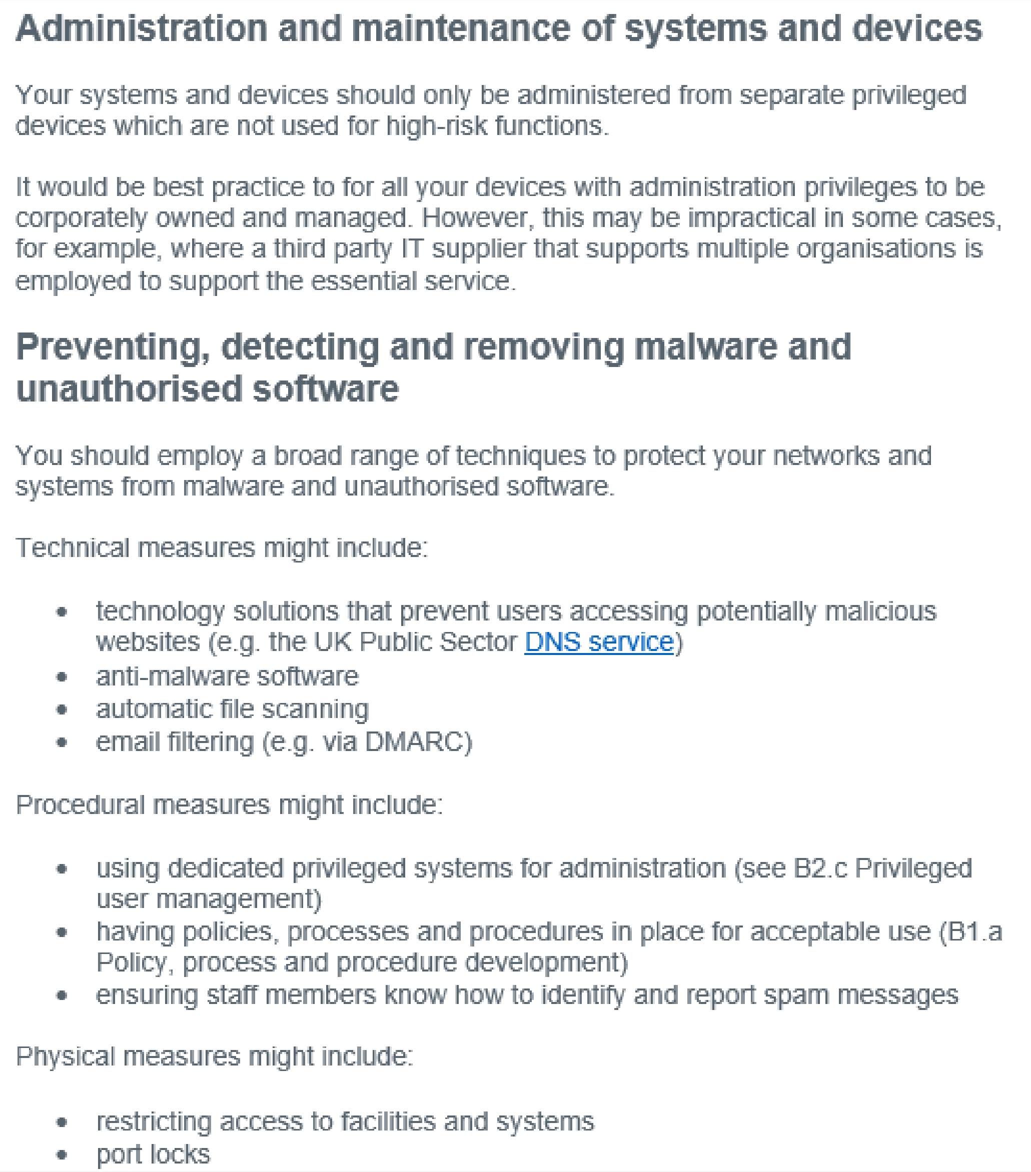
Contributing outcome B4.c

Secure management

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



Contributing outcome	DSPT V6
B4.c Secure management: You manage your organisation's network and information systems that support the operation of your essential function(s) to enable and maintain security.	4.3.2 4.4.2 4.5.5 6.2.1 6.2.3 6.2.4 6.2.9 8.3.6 9.3.4 9.3.5 9.3.8 9.3.9 9.5.3 9.5.6 9.6.2



Administration and maintenance of systems and devices

Your systems and devices should only be administered from separate privileged devices which are not used for high-risk functions.

It would be best practice to for all your devices with administration privileges to be corporately owned and managed. However, this may be impractical in some cases, for example, where a third party IT supplier that supports multiple organisations is employed to support the essential service.

Preventing, detecting and removing malware and unauthorised software

You should employ a broad range of techniques to protect your networks and systems from malware and unauthorised software.

Technical measures might include:

- technology solutions that prevent users accessing potentially malicious websites (e.g. the UK Public Sector DNS service)
- anti-malware software
- automatic file scanning
- email filtering (e.g. via DMARC)

Procedural measures might include:

- using dedicated privileged systems for administration (see B2.c Privileged user management)
- having policies, processes and procedures in place for acceptable use (B1.a Policy, process and procedure development)
- ensuring staff members know how to identify and report spam messages

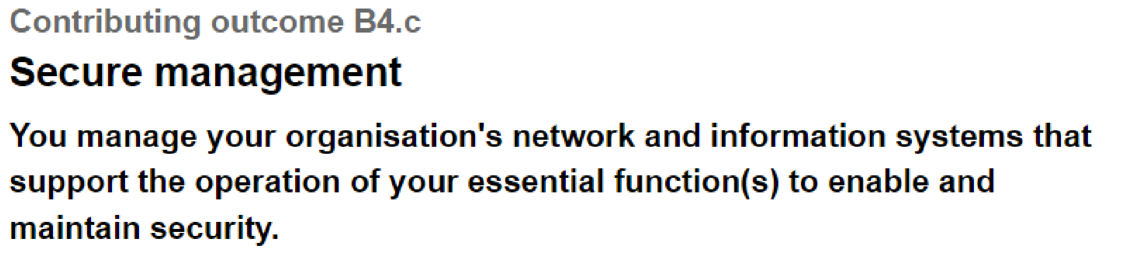
Physical measures might include:

- restricting access to facilities and systems
- port locks

Principle: B4 System Security

Contributing outcome:
B4.c Secure management

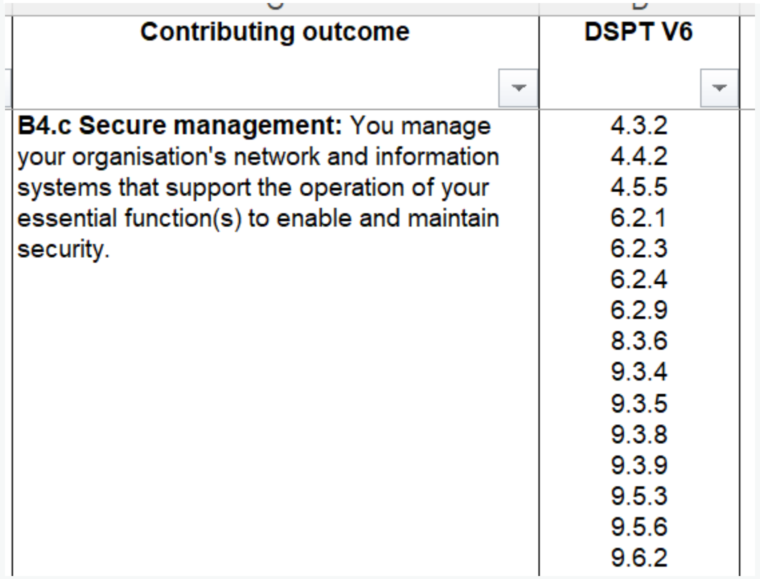
Supporting Evidence



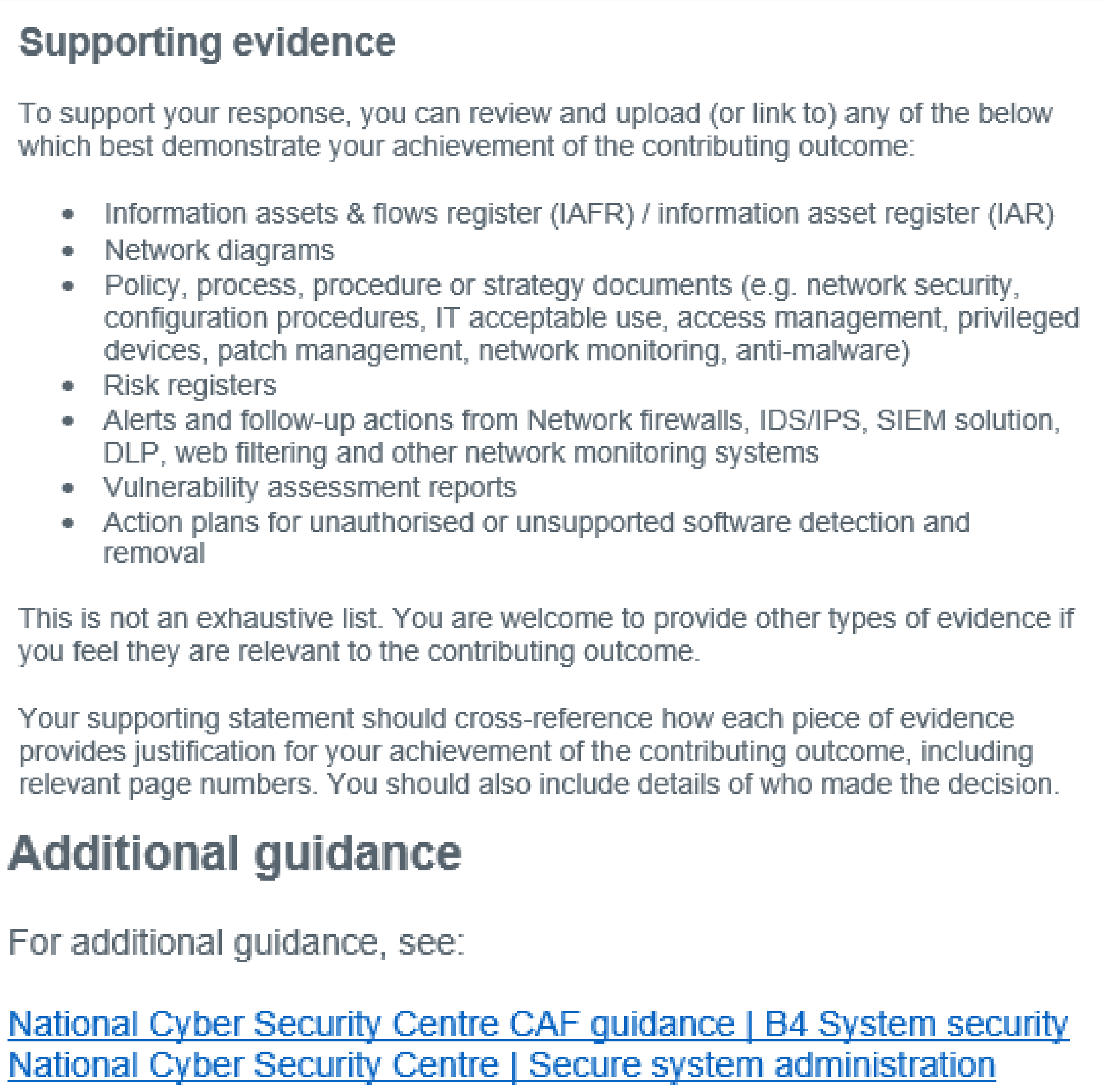
Contributing outcome B4.c

Secure management

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



Contributing outcome	DSPT V6
B4.c Secure management: You manage your organisation's network and information systems that support the operation of your essential function(s) to enable and maintain security.	4.3.2 4.4.2 4.5.5 6.2.1 6.2.3 6.2.4 6.2.9 8.3.6 9.3.4 9.3.5 9.3.8 9.3.9 9.5.3 9.5.6 9.6.2



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Information assets & flows register (IAFR) / information asset register (IAR)
- Network diagrams
- Policy, process, procedure or strategy documents (e.g. network security, configuration procedures, IT acceptable use, access management, privileged devices, patch management, network monitoring, anti-malware)
- Risk registers
- Alerts and follow-up actions from Network firewalls, IDS/IPS, SIEM solution, DLP, web filtering and other network monitoring systems
- Vulnerability assessment reports
- Action plans for unauthorised or unsupported software detection and removal

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

Additional guidance

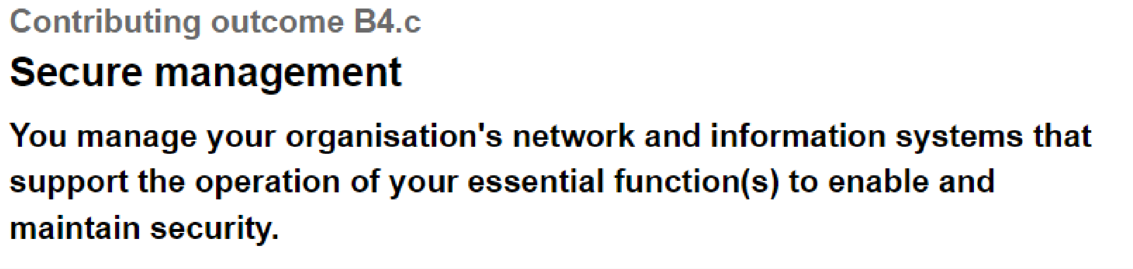
For additional guidance, see:

National Cyber Security Centre CAF guidance | B4 System security
National Cyber Security Centre | Secure system administration

Principle: B4 System Security

Contributing outcome:
B4.c Secure management

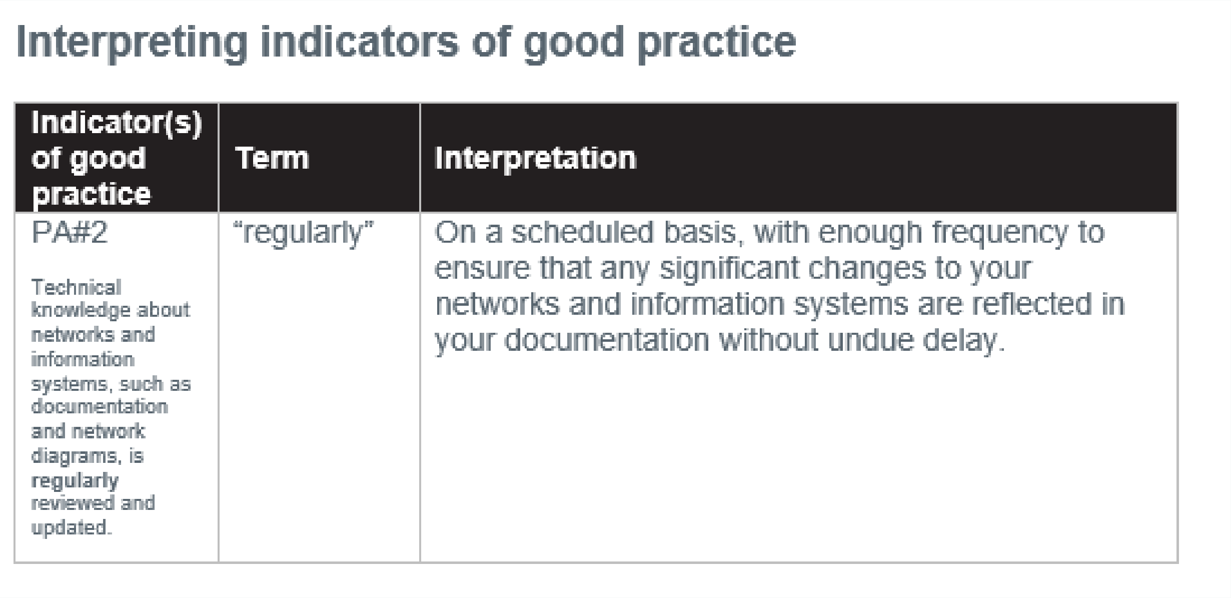
Interpretations



Contributing outcome B4.c

Secure management

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

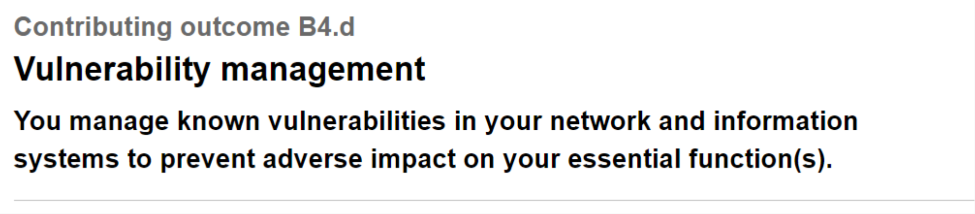


Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#2 Technical knowledge about networks and information systems, such as documentation and network diagrams, is **regularly** reviewed and updated.	"regularly"	On a scheduled basis, with enough frequency to ensure that any significant changes to your networks and information systems are reflected in your documentation without undue delay.

Principle: B4 System Security

Contributing outcome:
B4.d Vulnerability management



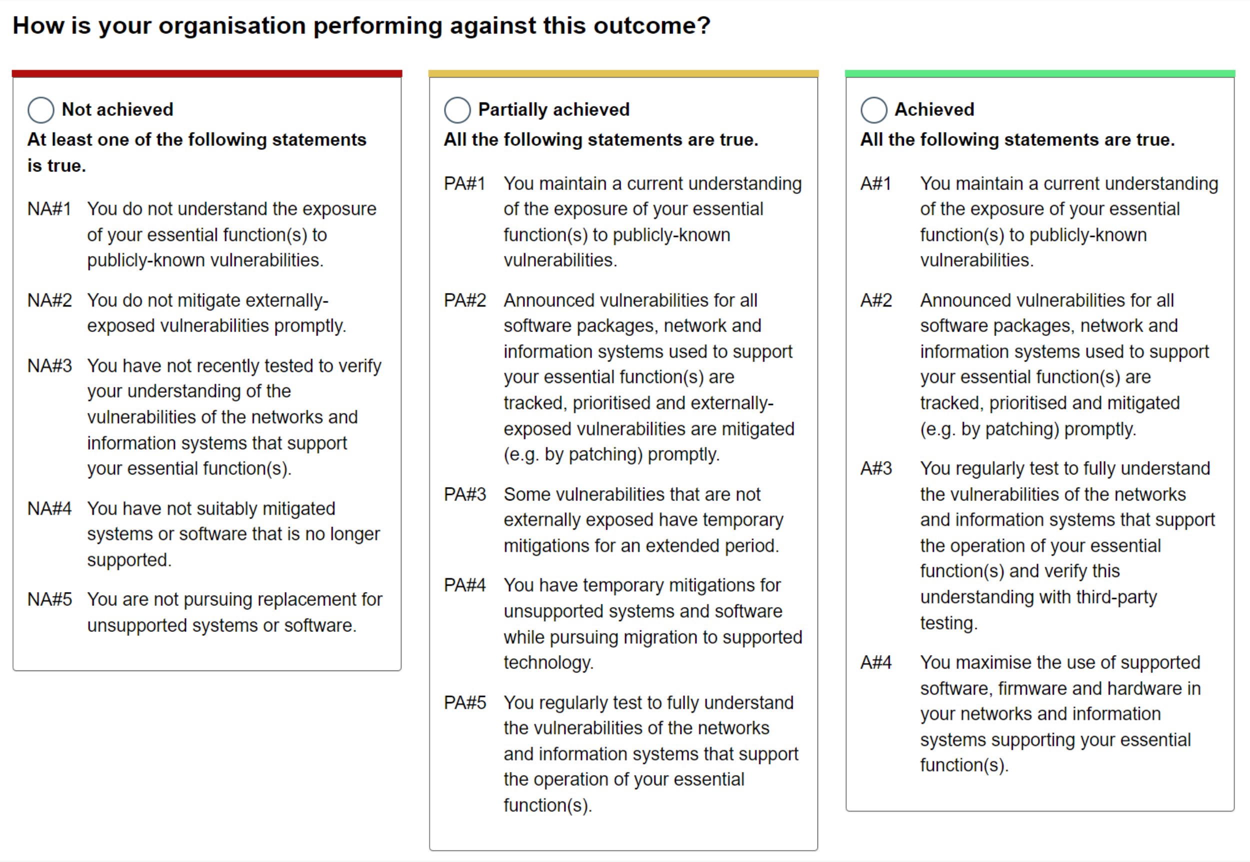
Contributing outcome B4.d

Vulnerability management

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

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 You do not understand the exposure of your essential function(s) to publicly-known vulnerabilities.

NA#2 You do not mitigate externally-exposed vulnerabilities promptly.

NA#3 You have not recently tested to verify your understanding of the vulnerabilities of the networks and information systems that support your essential function(s).

NA#4 You have not suitably mitigated systems or software that is no longer supported.

NA#5 You are not pursuing replacement for unsupported systems or software.

○ **Partially achieved**

All the following statements are true.

PA#1 You maintain a current understanding of the exposure of your essential function(s) to publicly-known vulnerabilities.

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.

PA#3 Some vulnerabilities that are not externally exposed have temporary mitigations for an extended period.

PA#4 You have temporary mitigations for unsupported systems and software while pursuing migration to supported technology.

PA#5 You regularly test to fully understand the vulnerabilities of the networks and information systems that support the operation of your essential function(s).

○ **Achieved**

All the following statements are true.

A#1 You maintain a current understanding of the exposure of your essential function(s) to publicly-known vulnerabilities.

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.

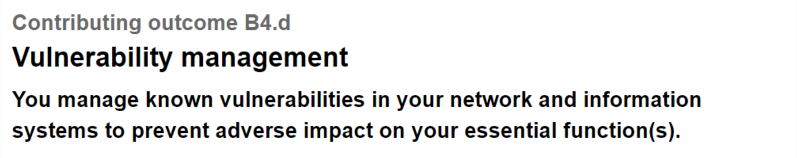
A#3 You regularly test to fully understand the vulnerabilities of the networks and information systems that support the operation of your essential function(s) and verify this understanding with third-party testing.

A#4 You maximise the use of supported software, firmware and hardware in your networks and information systems supporting your essential function(s).

Principle: B4 System Security

Contributing outcome:
B4.d Vulnerability management

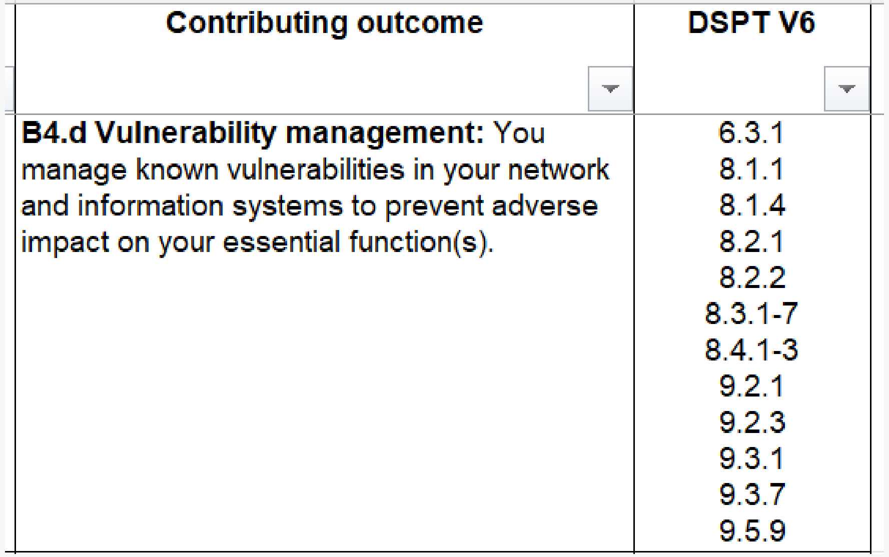
DSPT Mapping and Guidance



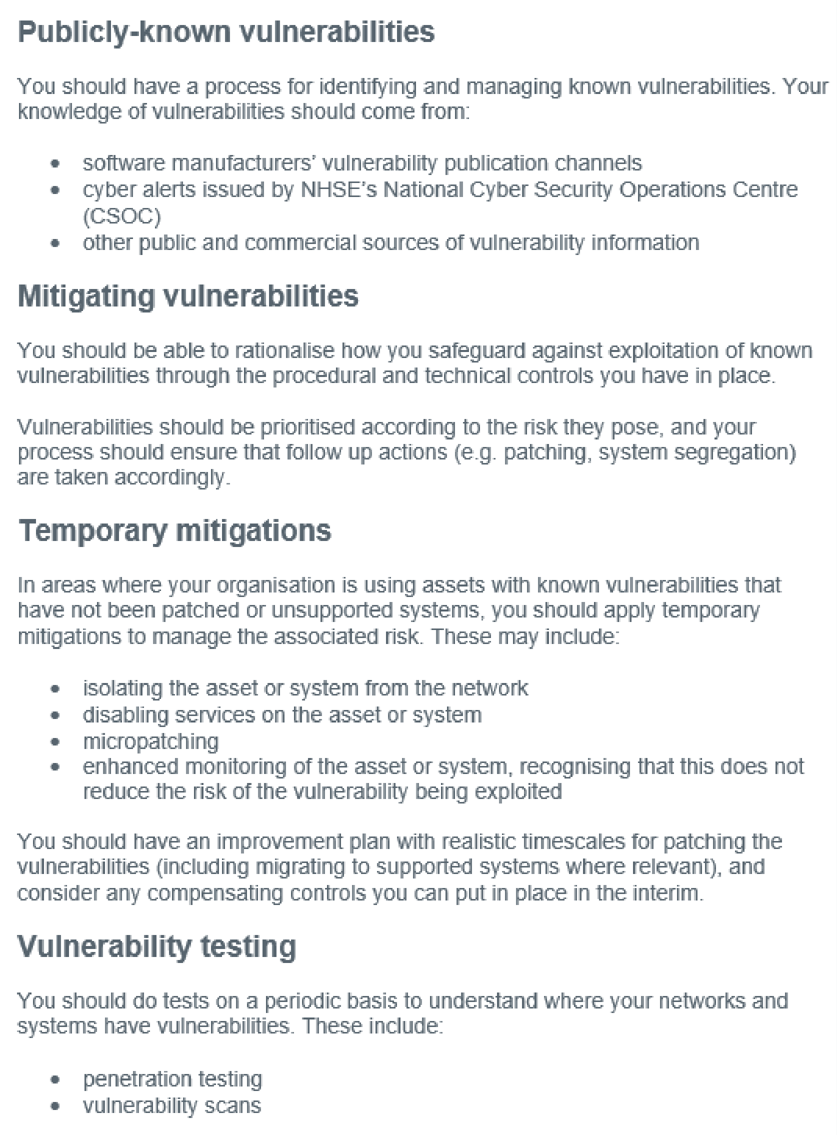
Contributing outcome B4.d

Vulnerability management

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



Contributing outcome	DSPT V6
B4.d Vulnerability management: You manage known vulnerabilities in your network and information systems to prevent adverse impact on your essential function(s).	6.3.1 8.1.1 8.1.4 8.2.1 8.2.2 8.3.1-7 8.4.1-3 9.2.1 9.2.3 9.3.1 9.3.7 9.5.9



Publicly-known vulnerabilities

You should have a process for identifying and managing known vulnerabilities. Your knowledge of vulnerabilities should come from:

- software manufacturers' vulnerability publication channels
- cyber alerts issued by NHSE's National Cyber Security Operations Centre (CSOC)
- other public and commercial sources of vulnerability information

Mitigating vulnerabilities

You should be able to rationalise how you safeguard against exploitation of known vulnerabilities through the procedural and technical controls you have in place.

Vulnerabilities should be prioritised according to the risk they pose, and your process should ensure that follow up actions (e.g. patching, system segregation) are taken accordingly.

Temporary mitigations

In areas where your organisation is using assets with known vulnerabilities that have not been patched or unsupported systems, you should apply temporary mitigations to manage the associated risk. These may include:

- isolating the asset or system from the network
- disabling services on the asset or system
- micropatching
- enhanced monitoring of the asset or system, recognising that this does not reduce the risk of the vulnerability being exploited

You should have an improvement plan with realistic timescales for patching the vulnerabilities (including migrating to supported systems where relevant), and consider any compensating controls you can put in place in the interim.

Vulnerability testing

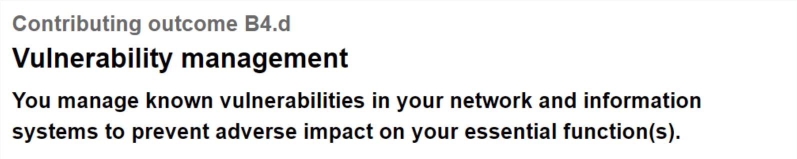
You should do tests on a periodic basis to understand where your networks and systems have vulnerabilities. These include:

- penetration testing
- vulnerability scans

Principle: B4 System Security

Contributing outcome:
B4.d Vulnerability management

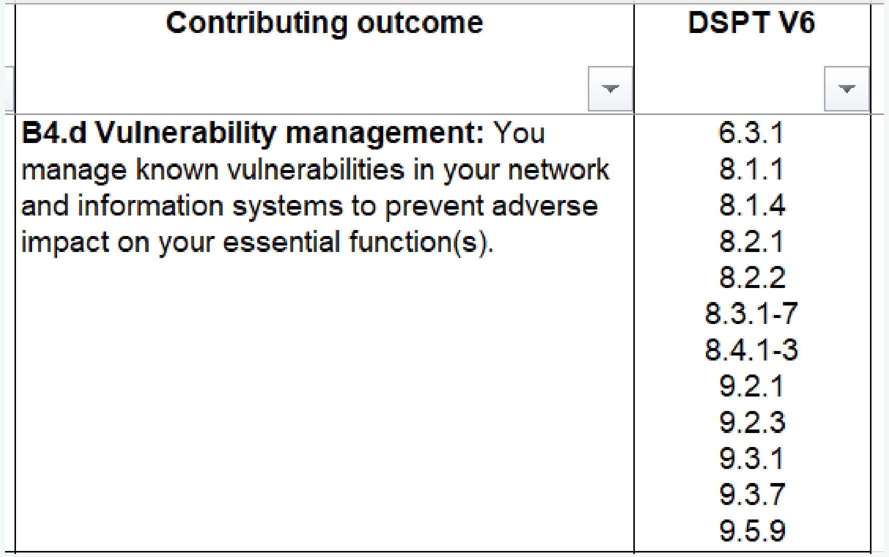
DSPT Mapping and Guidance



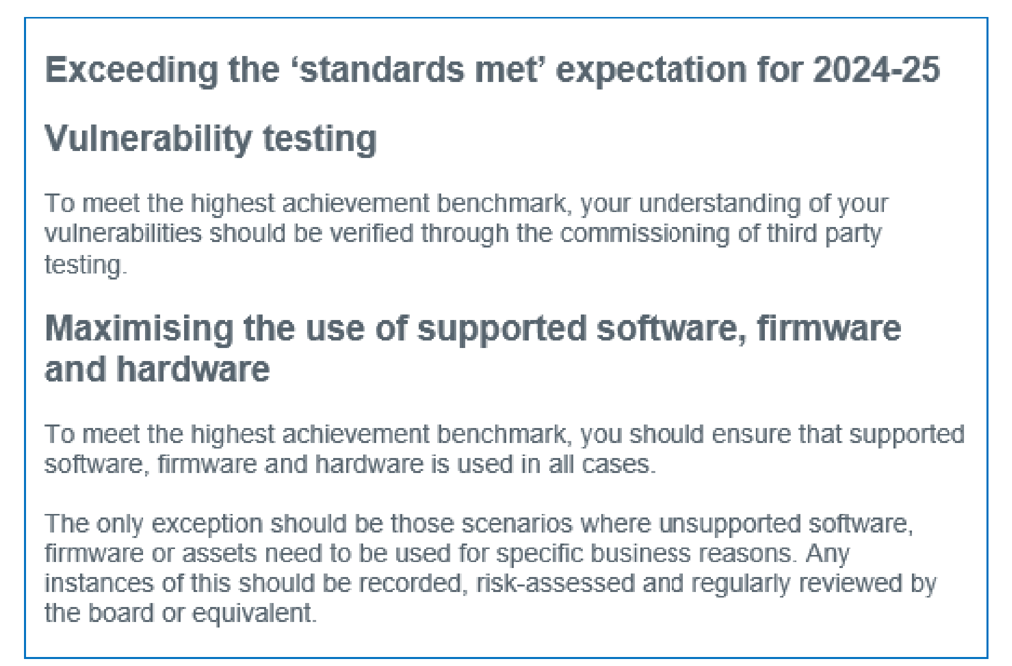
Contributing outcome B4.d

Vulnerability management

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



Contributing outcome	DSPT V6
B4.d Vulnerability management: You manage known vulnerabilities in your network and information systems to prevent adverse impact on your essential function(s).	6.3.1 8.1.1 8.1.4 8.2.1 8.2.2 8.3.1-7 8.4.1-3 9.2.1 9.2.3 9.3.1 9.3.7 9.5.9



Exceeding the ‘standards met’ expectation for 2024-25

Vulnerability testing

To meet the highest achievement benchmark, your understanding of your vulnerabilities should be verified through the commissioning of third party testing.

Maximising the use of supported software, firmware and hardware

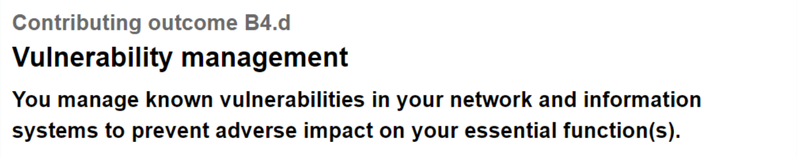
To meet the highest achievement benchmark, you should ensure that supported software, firmware and hardware is used in all cases.

The only exception should be those scenarios where unsupported software, firmware or assets need to be used for specific business reasons. Any instances of this should be recorded, risk-assessed and regularly reviewed by the board or equivalent.

Principle: B4 System Security

Contributing outcome:
B4.d Vulnerability management

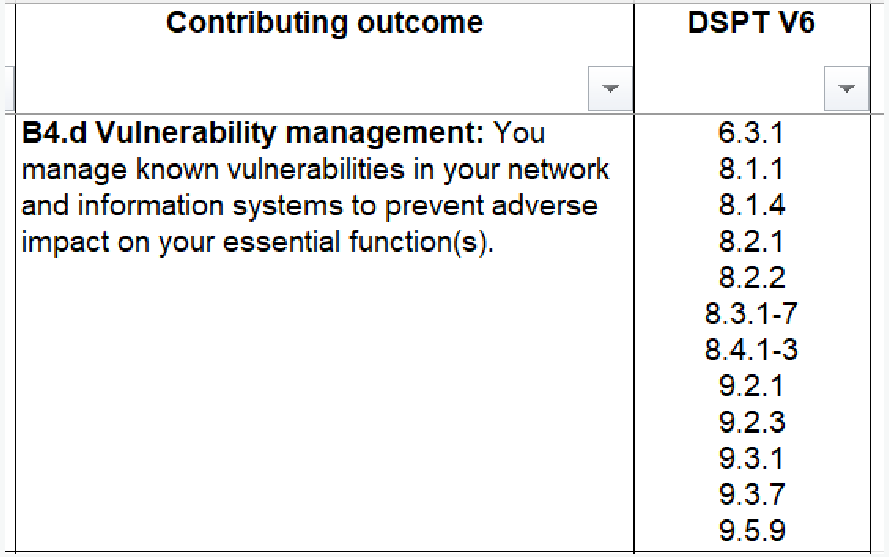
Supporting Evidence



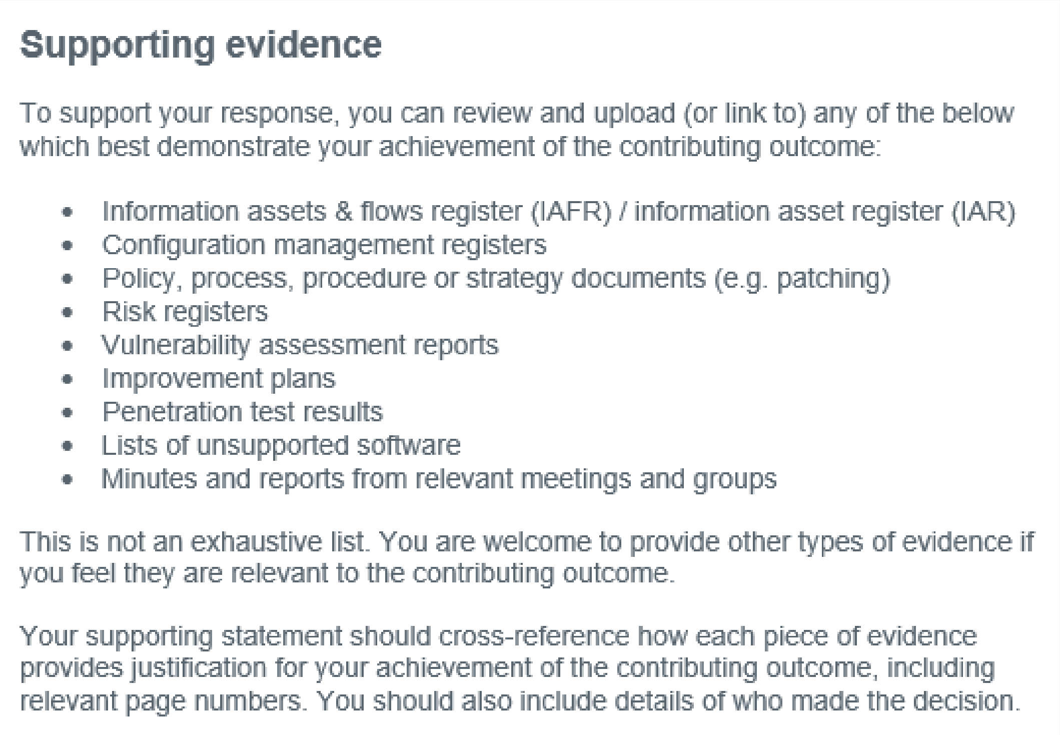
Contributing outcome B4.d

Vulnerability management

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



Contributing outcome	DSPT V6
B4.d Vulnerability management: You manage known vulnerabilities in your network and information systems to prevent adverse impact on your essential function(s).	6.3.1 8.1.1 8.1.4 8.2.1 8.2.2 8.3.1-7 8.4.1-3 9.2.1 9.2.3 9.3.1 9.3.7 9.5.9



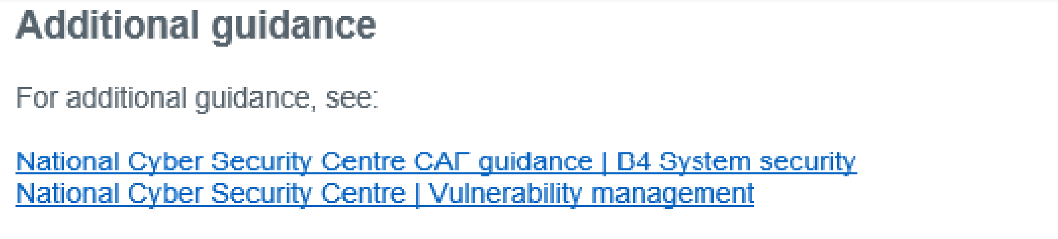
Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Information assets & flows register (IAFR) / information asset register (IAR)
- Configuration management registers
- Policy, process, procedure or strategy documents (e.g. patching)
- Risk registers
- Vulnerability assessment reports
- Improvement plans
- Penetration test results
- Lists of unsupported software
- Minutes and reports from relevant meetings and groups

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.



Additional guidance

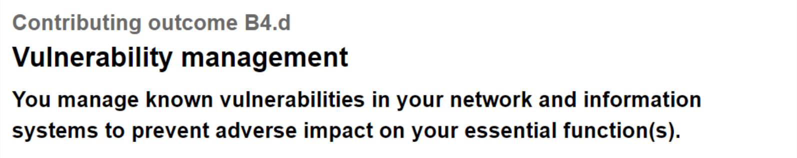
For additional guidance, see:

National Cyber Security Centre CAF guidance | B4 System security
National Cyber Security Centre | Vulnerability management

Principle: B4 System Security

Contributing outcome:
B4.d Vulnerability management

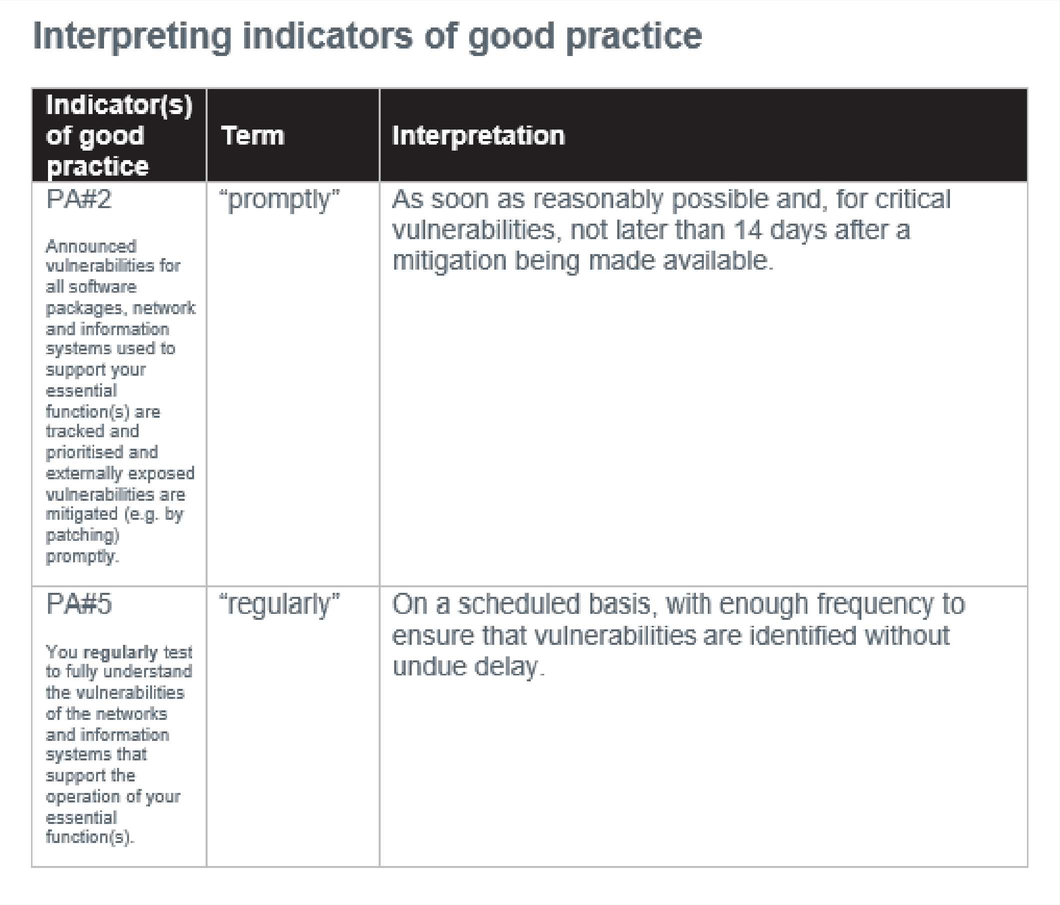
Interpretations



Contributing outcome B4.d

Vulnerability management

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



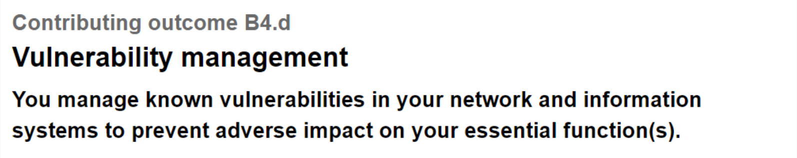
Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#2 Announced vulnerabilities for all software packages, network and information systems used to support your essential function(s) are tracked and prioritised and externally exposed vulnerabilities are mitigated (e.g. by patching) promptly.	"promptly"	As soon as reasonably possible and, for critical vulnerabilities, not later than 14 days after a mitigation being made available.
PA#5 You **regularly** test to fully understand the vulnerabilities of the networks and information systems that support the operation of your essential function(s).	"regularly"	On a scheduled basis, with enough frequency to ensure that vulnerabilities are identified without undue delay.

Principle: B4 System Security

Contributing outcome:
B4.d Vulnerability management

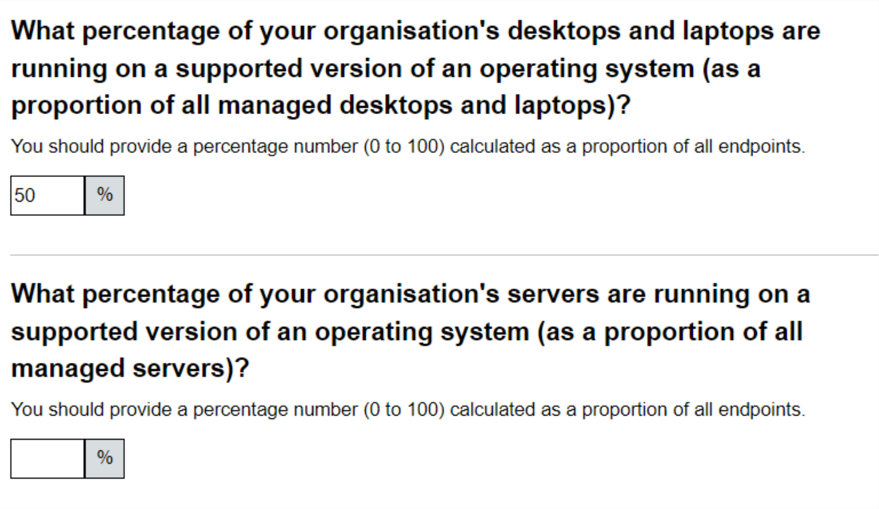
Specific Data Collections



Contributing outcome B4.d

Vulnerability management

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



What percentage of your organisation's desktops and laptops are running on a supported version of an operating system (as a proportion of all managed desktops and laptops)?

You should provide a percentage number (0 to 100) calculated as a proportion of all endpoints.

50 %

What percentage of your organisation's servers are running on a supported version of an operating system (as a proportion of all managed servers)?

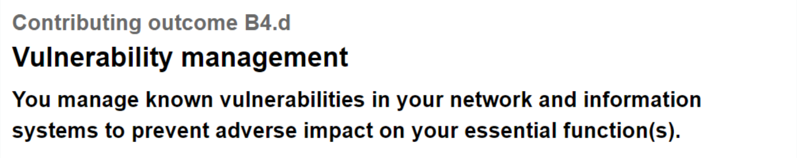
You should provide a percentage number (0 to 100) calculated as a proportion of all endpoints.

%

Principle: B4 System Security

Contributing outcome:
B4.d Vulnerability management

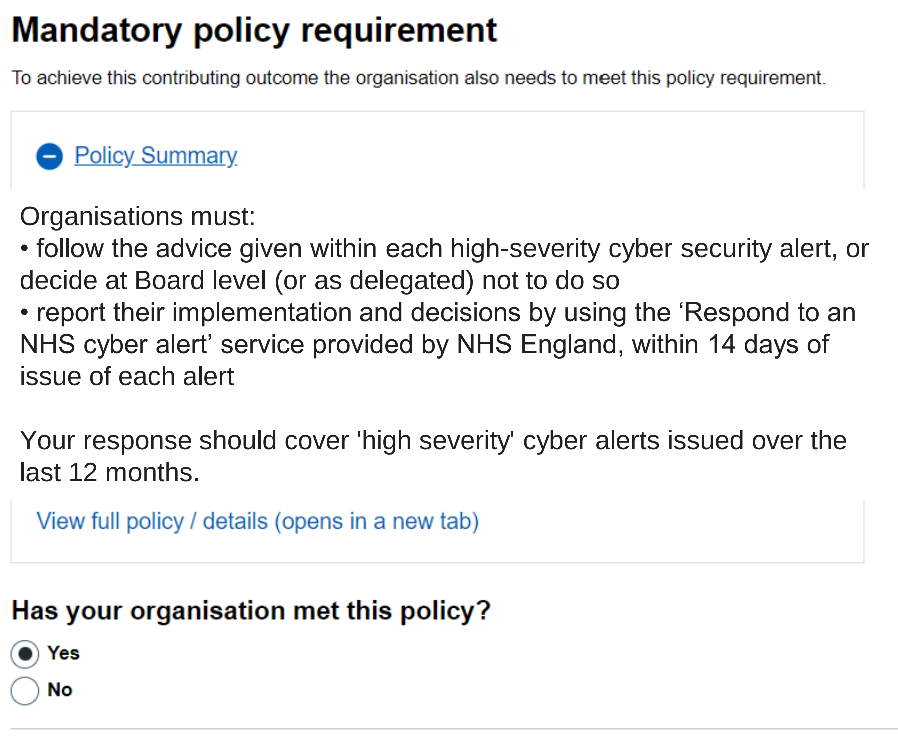
Specific Data Collections



Contributing outcome B4.d

Vulnerability management

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



Mandatory policy requirement

To achieve this contributing outcome the organisation also needs to meet this policy requirement.

Organisations must:
• follow the advice given within each high-severity cyber security alert, or decide at Board level (or as delegated) not to do so
• report their implementation and decisions by using the ‘Respond to an NHS cyber alert’ service provided by NHS England, within 14 days of issue of each alert

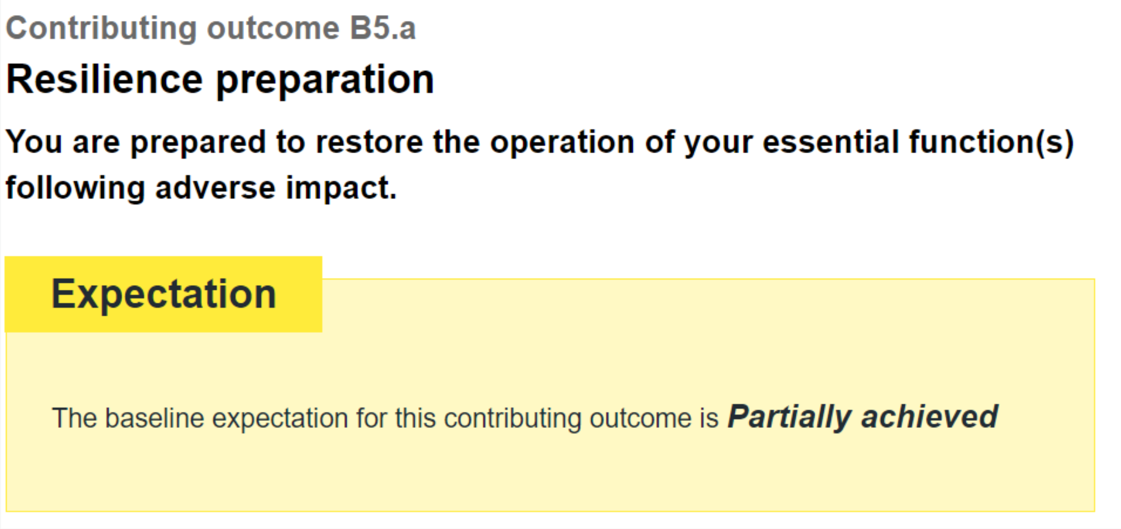
Your response should cover 'high severity' cyber alerts issued over the last 12 months.

Has your organisation met this policy?

● Yes
○ No

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.a Resilience preparation



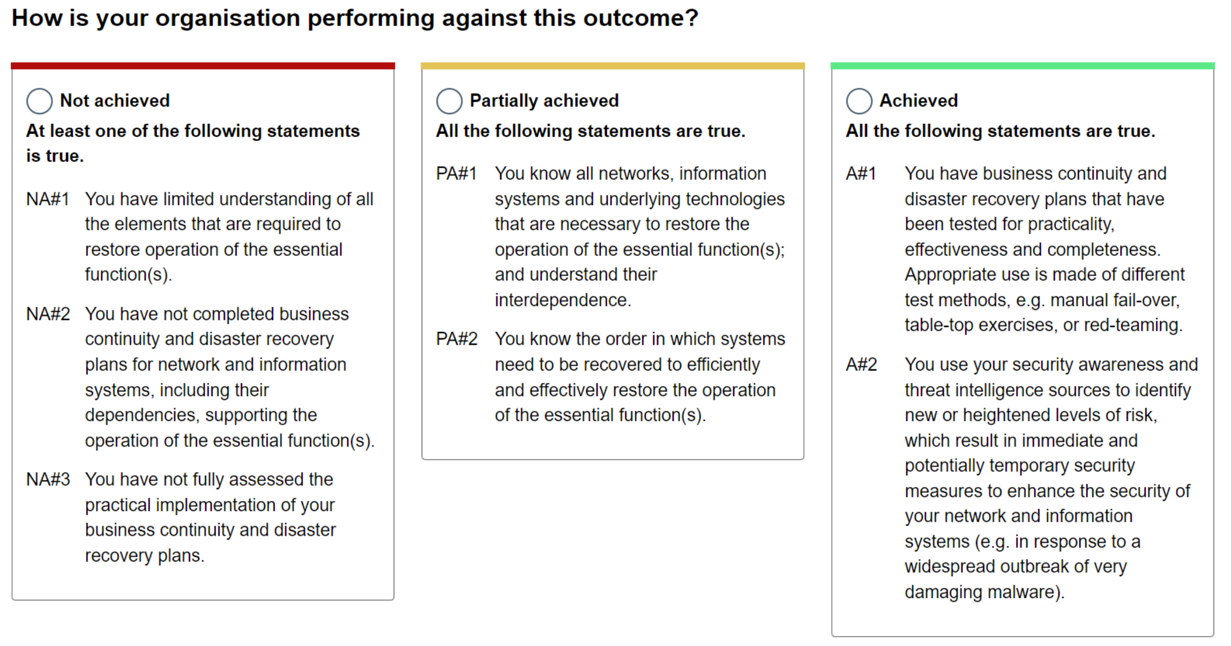
Contributing outcome B5.a

Resilience preparation

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

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



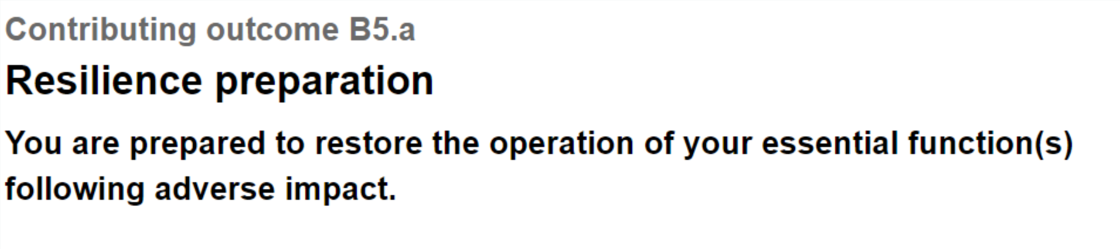
How is your organisation performing against this outcome?

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

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.a Resilience preparation

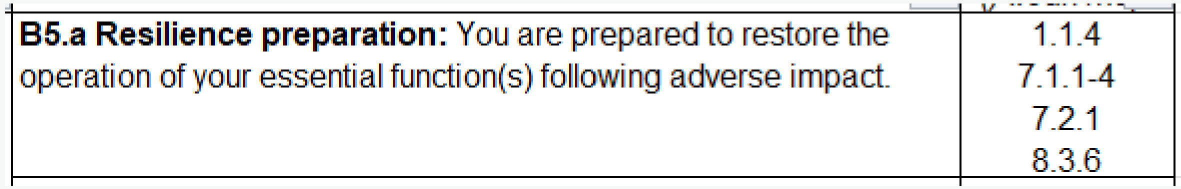
DSPT Mapping and Guidance



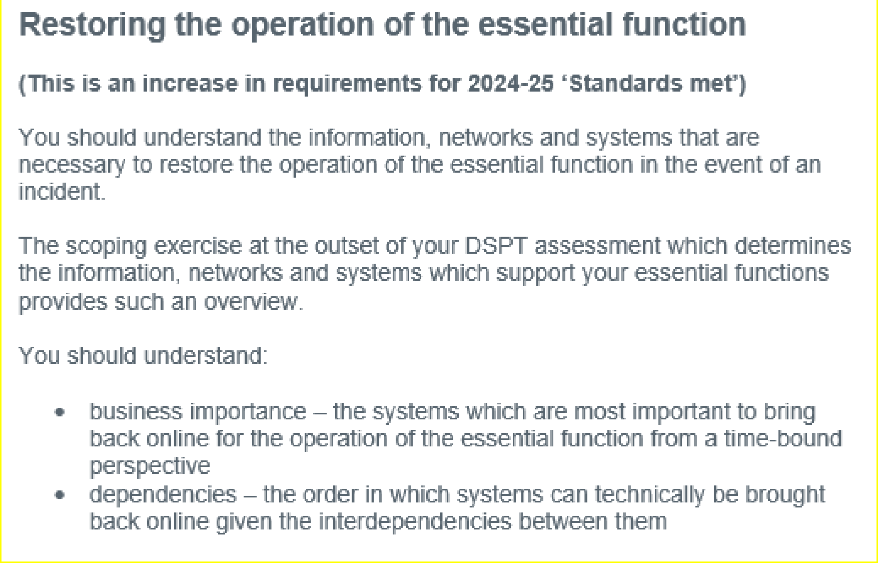
Contributing outcome B5.a

Resilience preparation

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



B5.a Resilience preparation: You are prepared to restore the operation of your essential function(s) following adverse impact.	1.1.4 7.1.1-4 7.2.1 8.3.6



Restoring the operation of the essential function

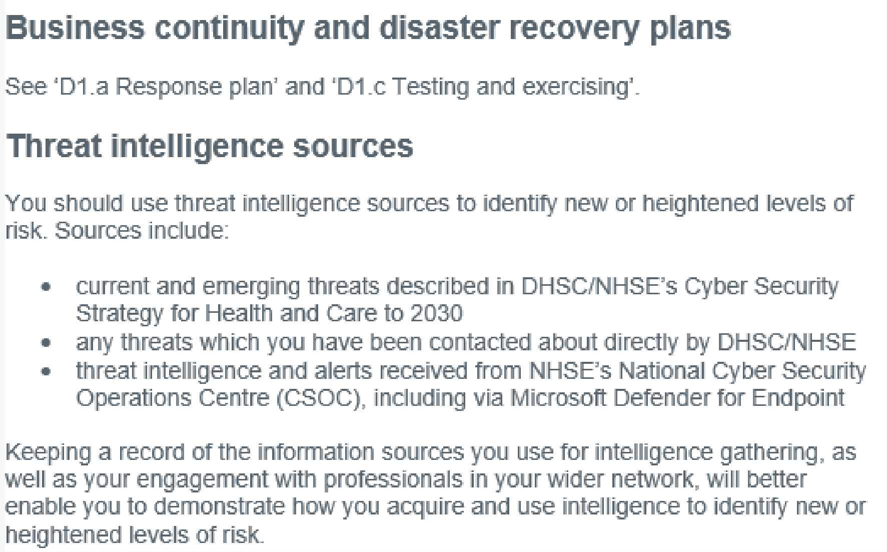
(This is an increase in requirements for 2024-25 'Standards met')

You should understand the information, networks and systems that are necessary to restore the operation of the essential function in the event of an incident.

The scoping exercise at the outset of your DSPT assessment which determines the information, networks and systems which support your essential functions provides such an overview.

You should understand:

- business importance – the systems which are most important to bring back online for the operation of the essential function from a time-bound perspective
- dependencies – the order in which systems can technically be brought back online given the interdependencies between them



Business continuity and disaster recovery plans

See 'D1.a Response plan' and 'D1.c Testing and exercising'.

Threat intelligence sources

You should use threat intelligence sources to identify new or heightened levels of risk. Sources include:

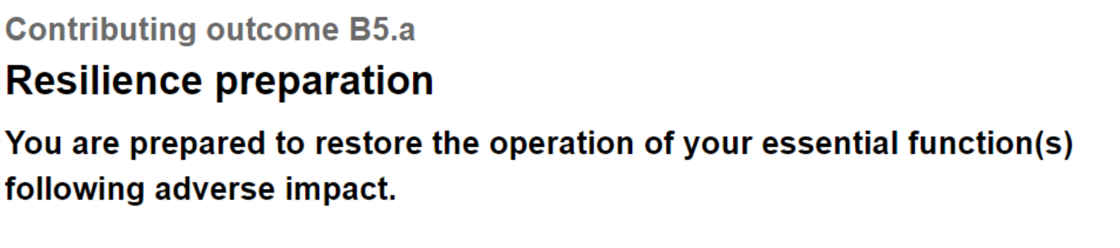
- current and emerging threats described in DHSC/NHSE's Cyber Security Strategy for Health and Care to 2030
- any threats which you have been contacted about directly by DHSC/NHSE
- threat intelligence and alerts received from NHSE's National Cyber Security Operations Centre (CSOC), including via Microsoft Defender for Endpoint

Keeping a record of the information sources you use for intelligence gathering, as well as your engagement with professionals in your wider network, will better enable you to demonstrate how you acquire and use intelligence to identify new or heightened levels of risk.

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.a Resilience preparation

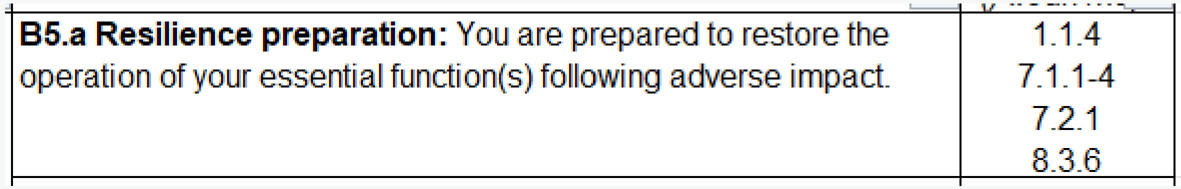
Supporting Evidence



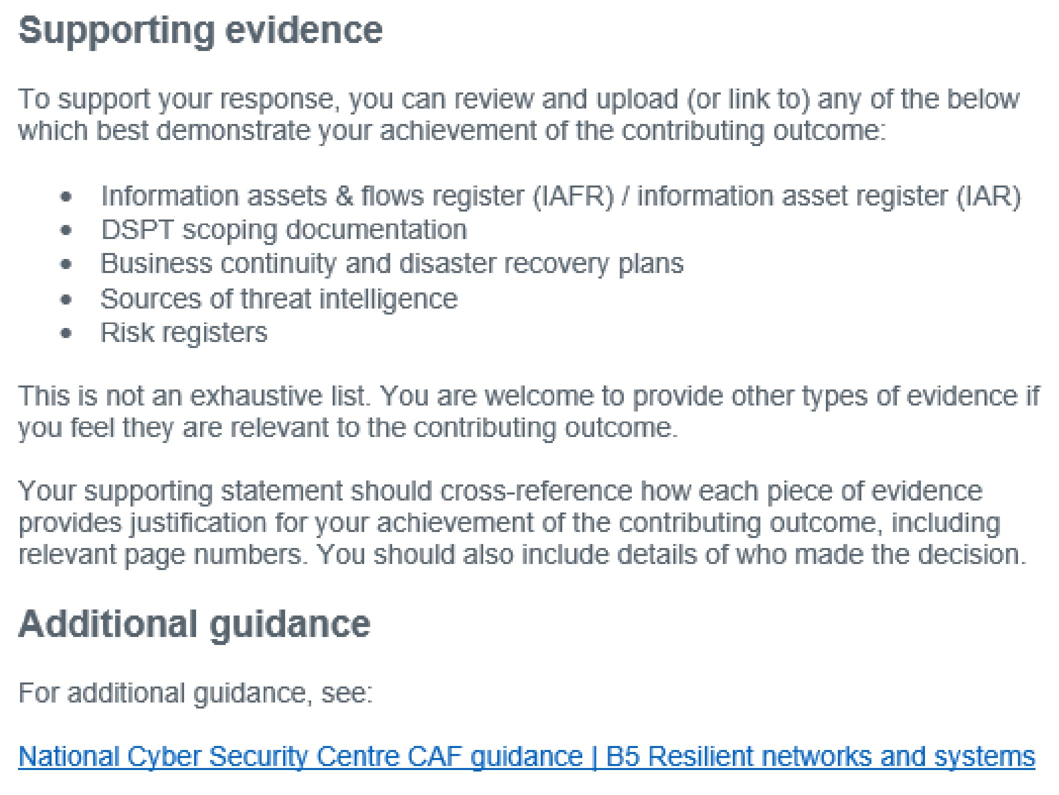
Contributing outcome B5.a

Resilience preparation

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



B5.a Resilience preparation: You are prepared to restore the operation of your essential function(s) following adverse impact.	1.1.4 7.1.1-4 7.2.1 8.3.6



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Information assets & flows register (IAFR) / information asset register (IAR)
- DSPT scoping documentation
- Business continuity and disaster recovery plans
- Sources of threat intelligence
- Risk registers

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

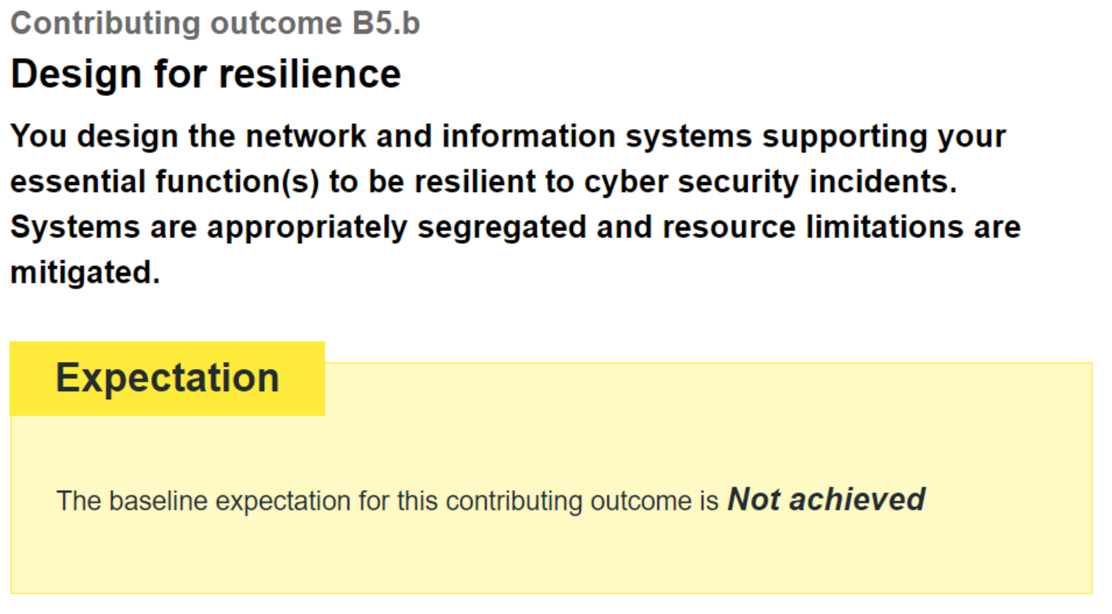
Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B5 Resilient networks and systems

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.b Design for resilience



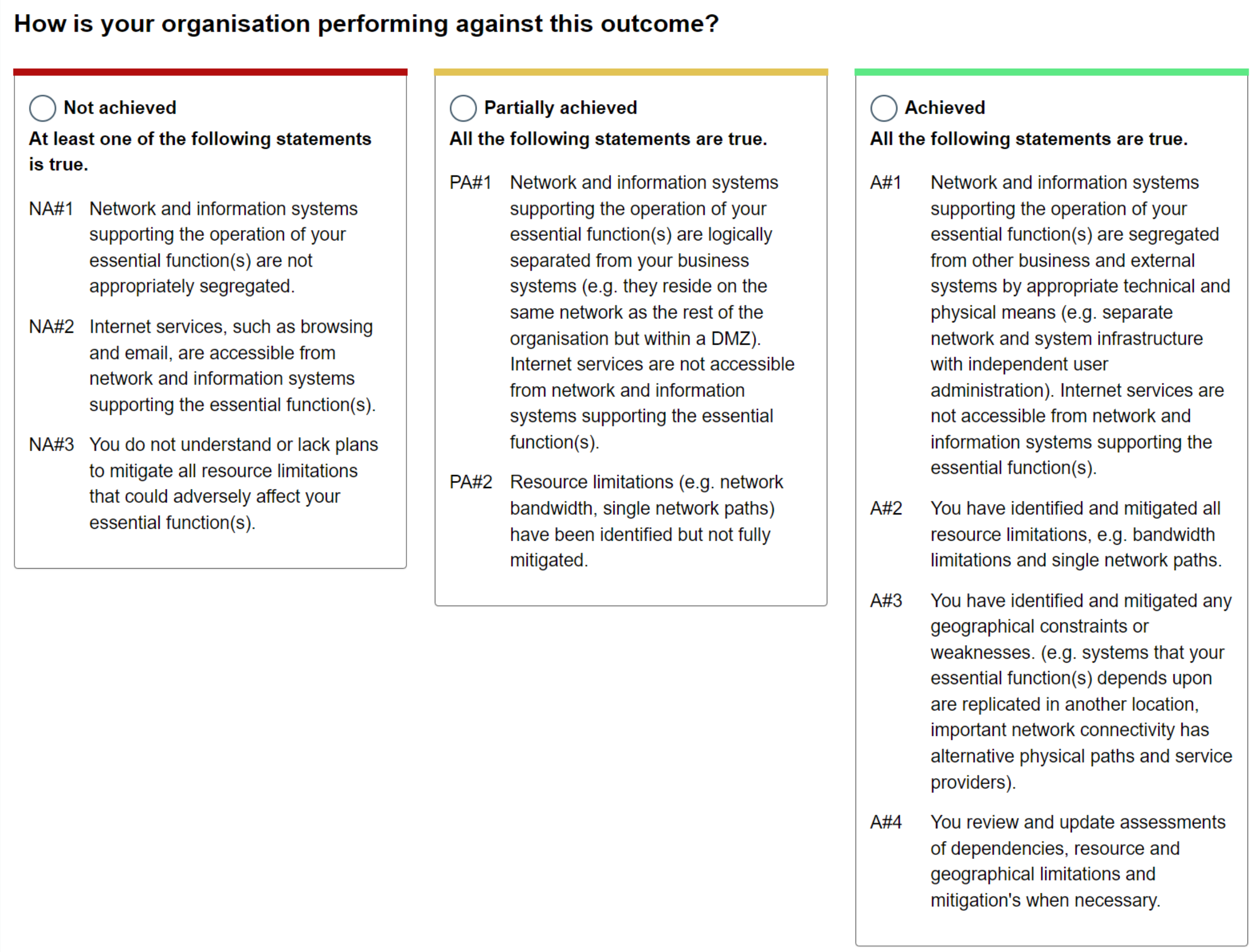
Contributing outcome B5.b

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.

Expectation

The baseline expectation for this contributing outcome is ***Not achieved***



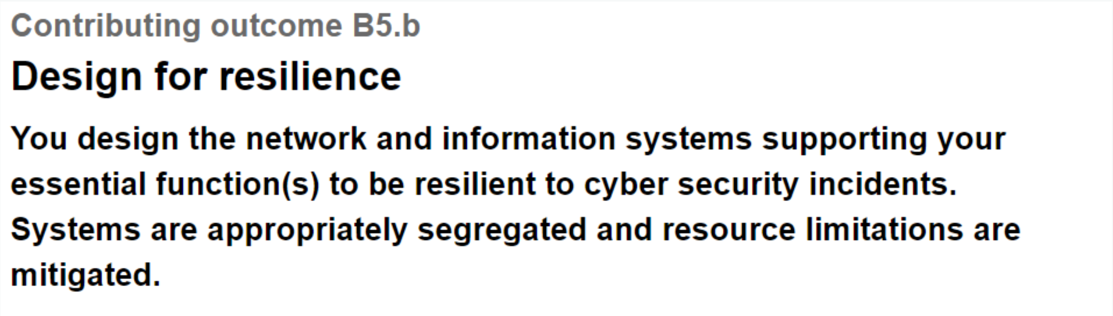
How is your organisation performing against this outcome?

○ Not achieved		○ Partially achieved		○ Achieved	
At least one of the following statements is true.		**All the following statements are true.**		**All the following statements are true.**	
NA#1	Network and information systems supporting the operation of your essential function(s) are not appropriately segregated.	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).	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).
NA#2	Internet services, such as browsing and email, are accessible from network and information systems supporting the essential function(s).	PA#2	Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.	A#2	You have identified and mitigated all resource limitations, e.g. bandwidth limitations and single network paths.
NA#3	You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential function(s).			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).
				A#4	You review and update assessments of dependencies, resource and geographical limitations and mitigation's when necessary.

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.b Design for resilience

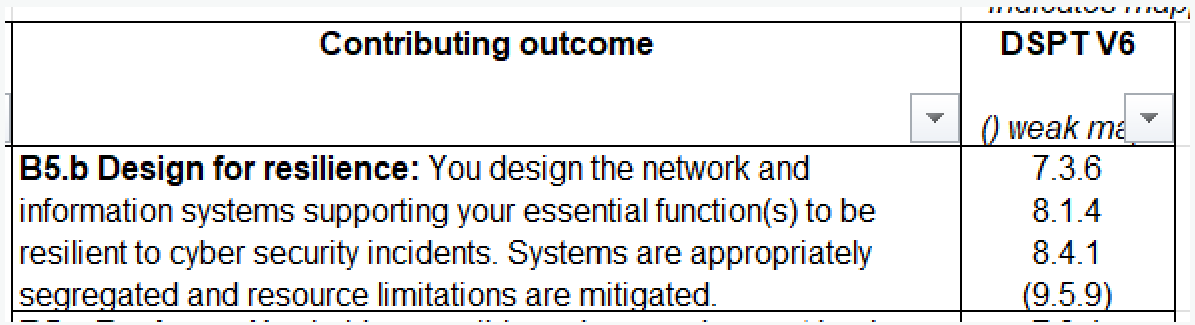
DSPT Mapping and Guidance



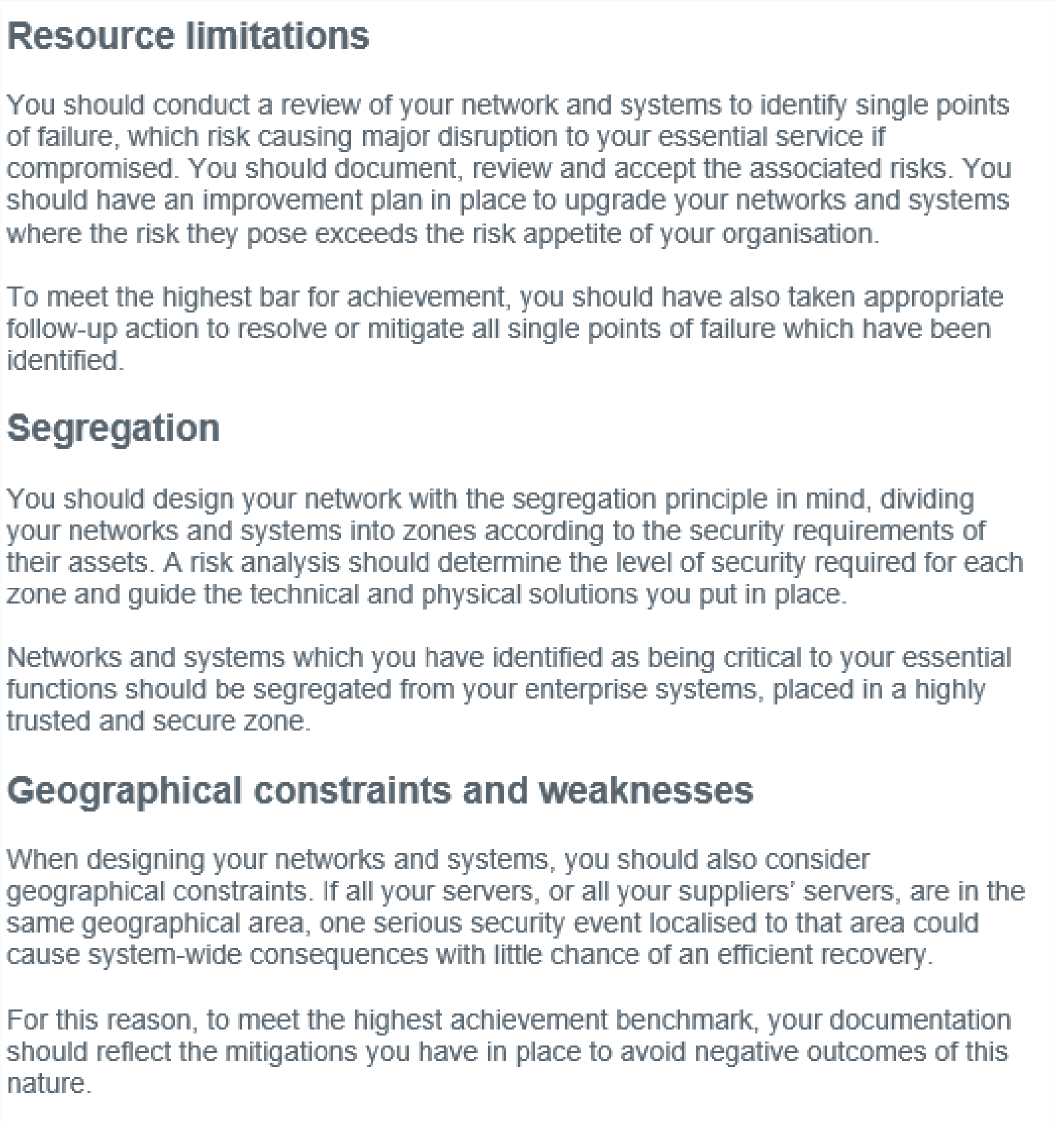
Contributing outcome B5.b

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.



Contributing outcome	DSPT V6 *() weak ma*
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.	7.3.6 8.1.4 8.4.1 (9.5.9)



Resource limitations

You should conduct a review of your network and systems to identify single points of failure, which risk causing major disruption to your essential service if compromised. You should document, review and accept the associated risks. You should have an improvement plan in place to upgrade your networks and systems where the risk they pose exceeds the risk appetite of your organisation.

To meet the highest bar for achievement, you should have also taken appropriate follow-up action to resolve or mitigate all single points of failure which have been identified.

Segregation

You should design your network with the segregation principle in mind, dividing your networks and systems into zones according to the security requirements of their assets. A risk analysis should determine the level of security required for each zone and guide the technical and physical solutions you put in place.

Networks and systems which you have identified as being critical to your essential functions should be segregated from your enterprise systems, placed in a highly trusted and secure zone.

Geographical constraints and weaknesses

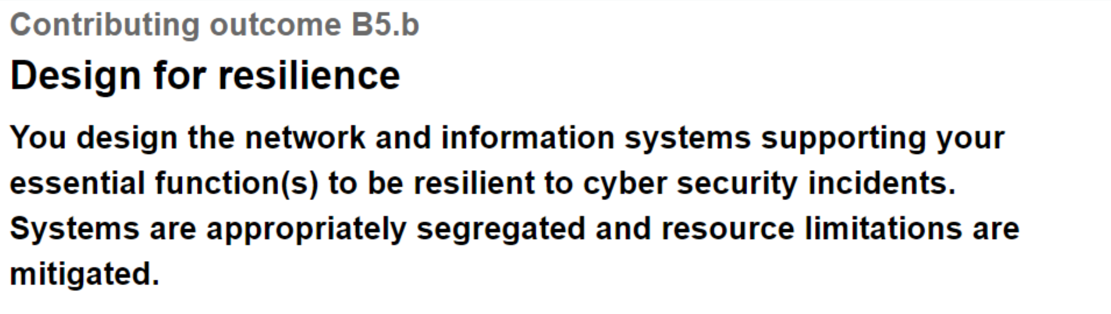
When designing your networks and systems, you should also consider geographical constraints. If all your servers, or all your suppliers' servers, are in the same geographical area, one serious security event localised to that area could cause system-wide consequences with little chance of an efficient recovery.

For this reason, to meet the highest achievement benchmark, your documentation should reflect the mitigations you have in place to avoid negative outcomes of this nature.

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.b Design for resilience

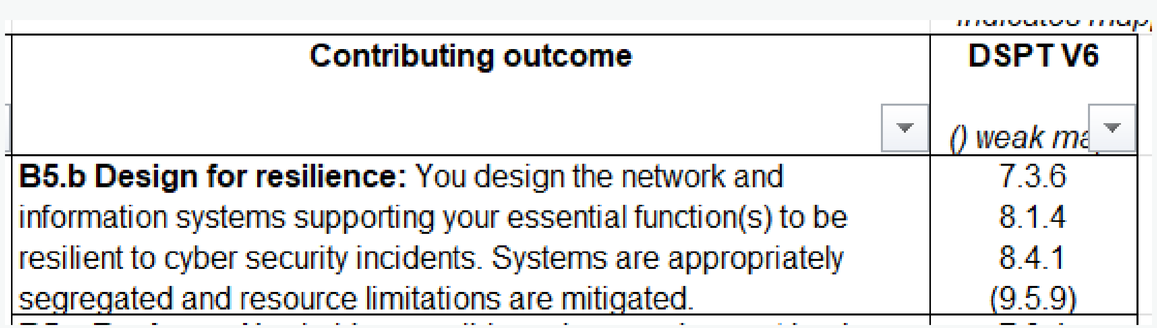
Supporting Evidence



Contributing outcome B5.b

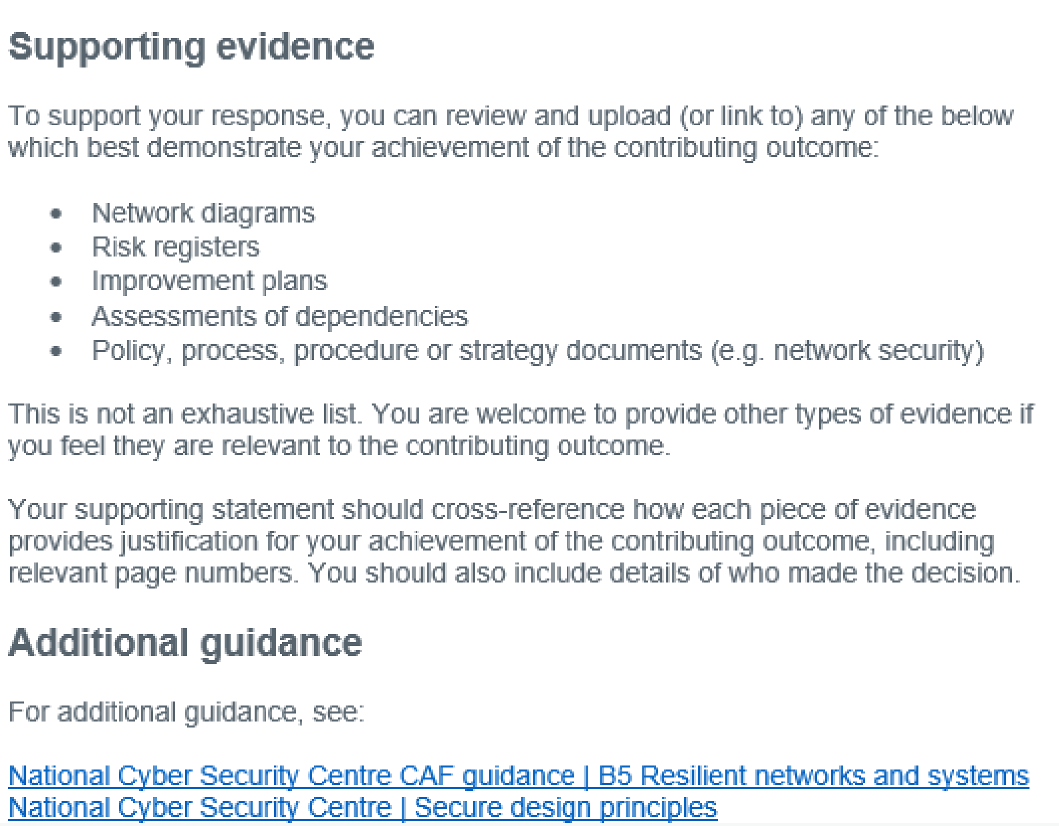
Design for resilience

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.



indicates map

Contributing outcome	DSPT V6 () weak ma
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.	7.3.6 8.1.4 8.4.1 (9.5.9)



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Network diagrams
- Risk registers
- Improvement plans
- Assessments of dependencies
- Policy, process, procedure or strategy documents (e.g. network security)

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

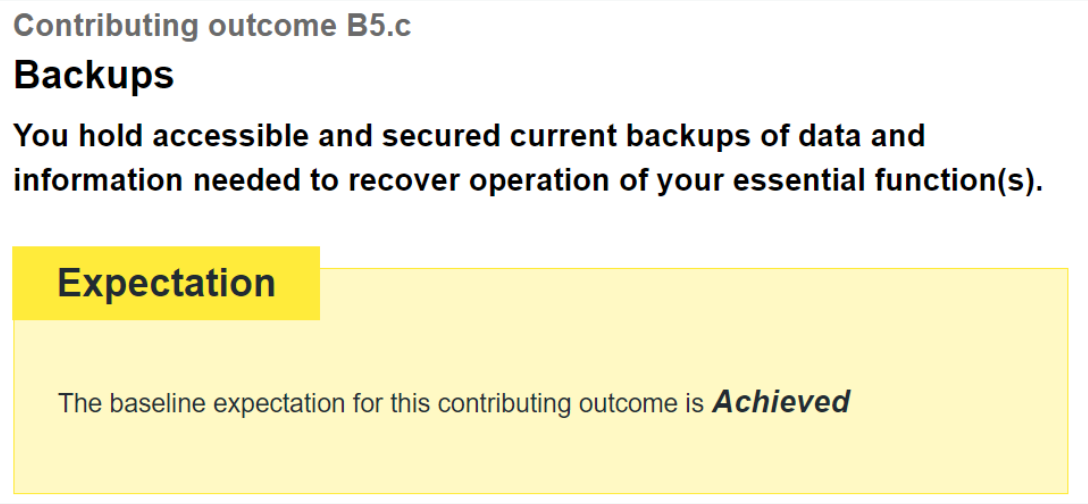
Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B5 Resilient networks and systems
National Cyber Security Centre | Secure design principles

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.c Backups



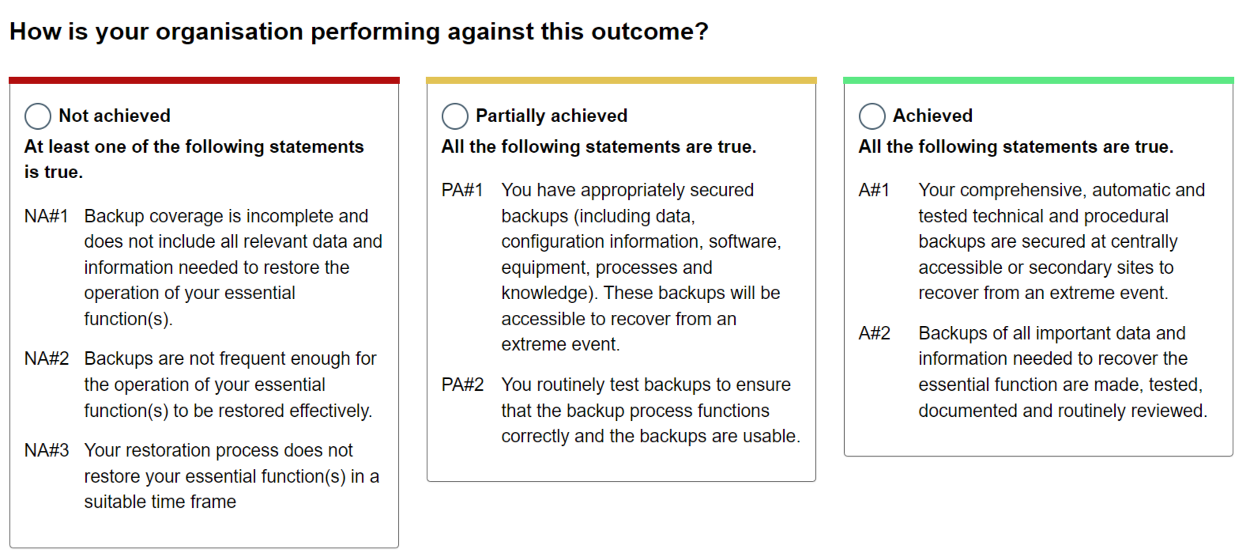
Contributing outcome B5.c

Backups

You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).

Expectation

The baseline expectation for this contributing outcome is ***Achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 Backup coverage is incomplete and does not include all relevant data and information needed to restore the operation of your essential function(s).

NA#2 Backups are not frequent enough for the operation of your essential function(s) to be restored effectively.

NA#3 Your restoration process does not restore your essential function(s) in a suitable time frame

○ **Partially achieved**

All the following statements are true.

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.

PA#2 You routinely test backups to ensure that the backup process functions correctly and the backups are usable.

○ **Achieved**

All the following statements are true.

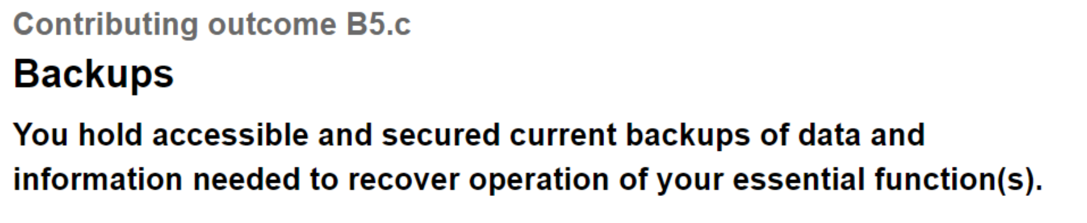
A#1 Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event.

A#2 Backups of all important data and information needed to recover the essential function are made, tested, documented and routinely reviewed.

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.c Backups

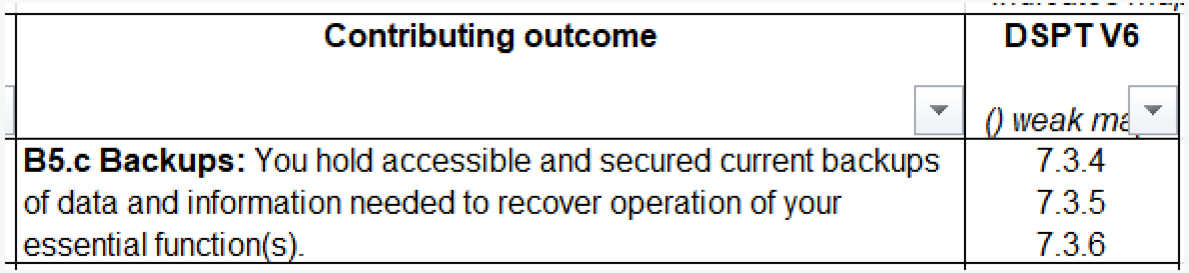
DSPT Mapping and Guidance



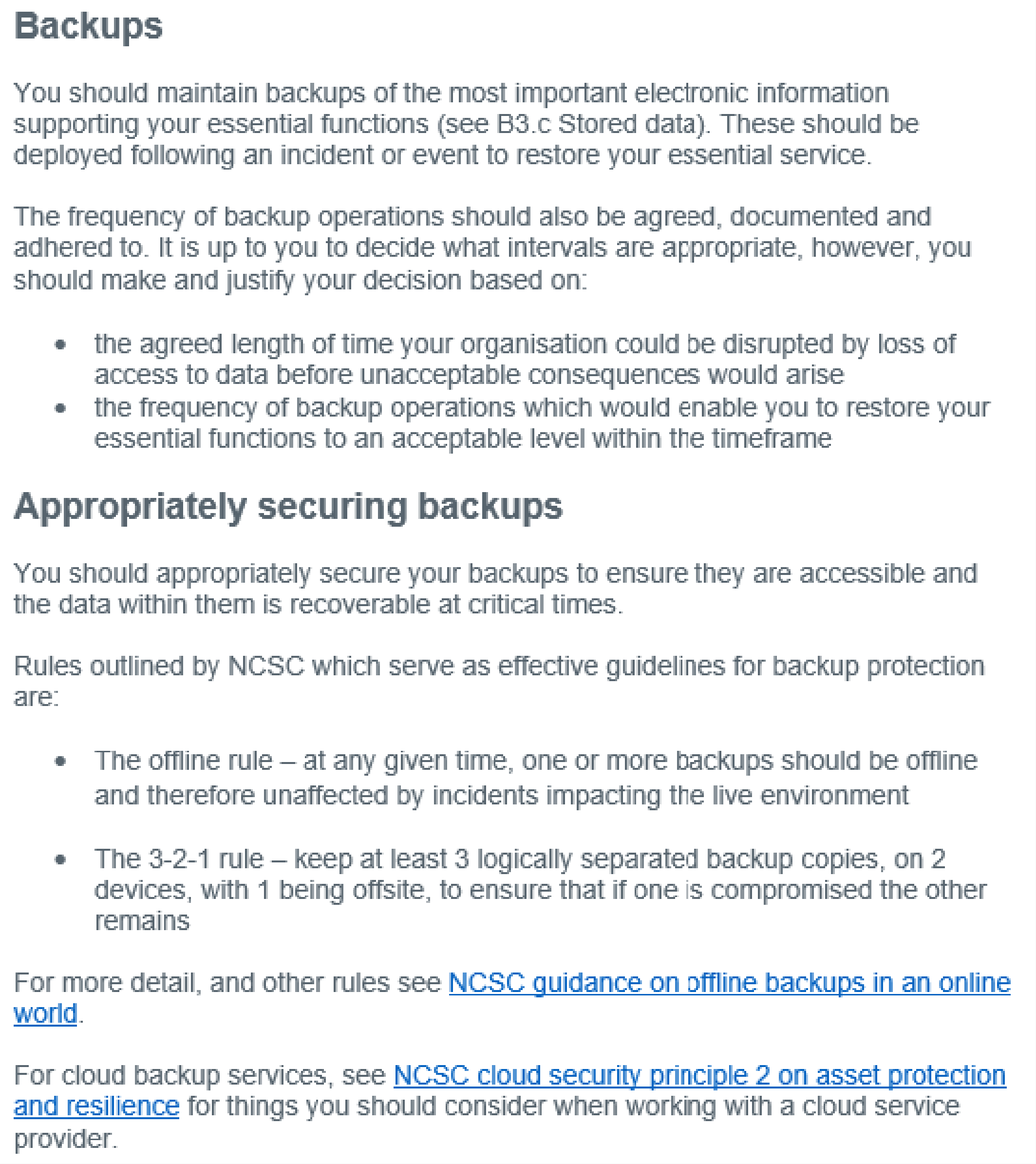
Contributing outcome B5.c

Backups

You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).



Contributing outcome	DSPT V6 *() weak ma*
B5.c Backups: You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).	7.3.4 7.3.5 7.3.6



Backups

You should maintain backups of the most important electronic information supporting your essential functions (see B3.c Stored data). These should be deployed following an incident or event to restore your essential service.

The frequency of backup operations should also be agreed, documented and adhered to. It is up to you to decide what intervals are appropriate, however, you should make and justify your decision based on:

- the agreed length of time your organisation could be disrupted by loss of access to data before unacceptable consequences would arise
- the frequency of backup operations which would enable you to restore your essential functions to an acceptable level within the timeframe

Appropriately securing backups

You should appropriately secure your backups to ensure they are accessible and the data within them is recoverable at critical times.

Rules outlined by NCSC which serve as effective guidelines for backup protection are:

- The offline rule – at any given time, one or more backups should be offline and therefore unaffected by incidents impacting the live environment

- The 3-2-1 rule – keep at least 3 logically separated backup copies, on 2 devices, with 1 being offsite, to ensure that if one is compromised the other remains

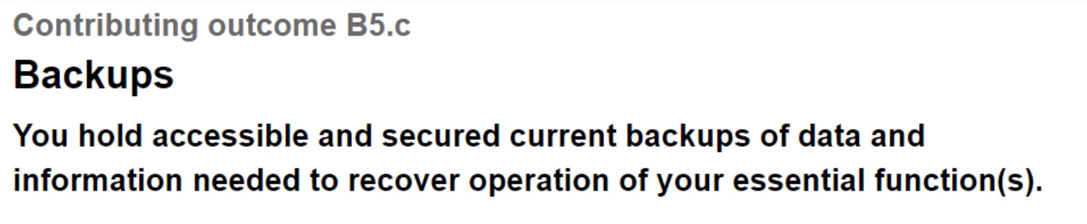
For more detail, and other rules see NCSC guidance on offline backups in an online world.

For cloud backup services, see NCSC cloud security principle 2 on asset protection and resilience for things you should consider when working with a cloud service provider.

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.c Backups

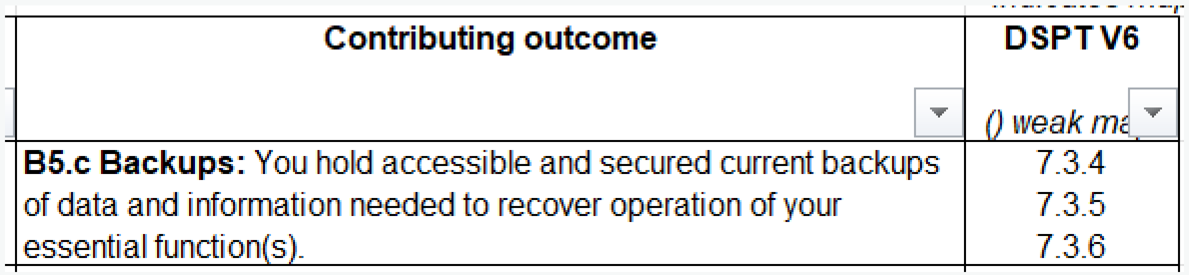
DSPT Mapping and Guidance



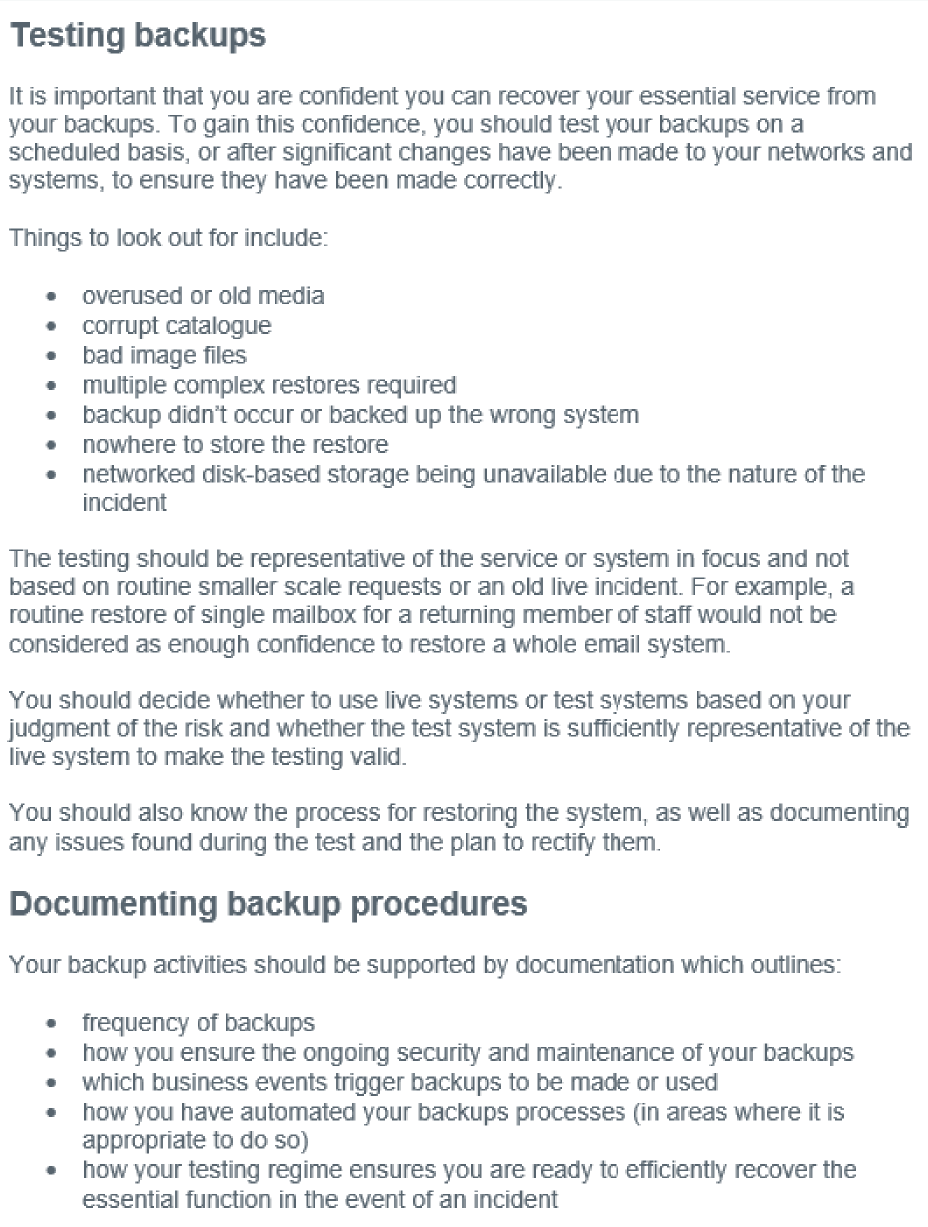
Contributing outcome B5.c

Backups

You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).



Contributing outcome	DSPT V6 *() weak ma*
B5.c Backups: You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).	7.3.4 7.3.5 7.3.6



Testing backups

It is important that you are confident you can recover your essential service from your backups. To gain this confidence, you should test your backups on a scheduled basis, or after significant changes have been made to your networks and systems, to ensure they have been made correctly.

Things to look out for include:

- overused or old media
- corrupt catalogue
- bad image files
- multiple complex restores required
- backup didn't occur or backed up the wrong system
- nowhere to store the restore
- networked disk-based storage being unavailable due to the nature of the incident

The testing should be representative of the service or system in focus and not based on routine smaller scale requests or an old live incident. For example, a routine restore of single mailbox for a returning member of staff would not be considered as enough confidence to restore a whole email system.

You should decide whether to use live systems or test systems based on your judgment of the risk and whether the test system is sufficiently representative of the live system to make the testing valid.

You should also know the process for restoring the system, as well as documenting any issues found during the test and the plan to rectify them.

Documenting backup procedures

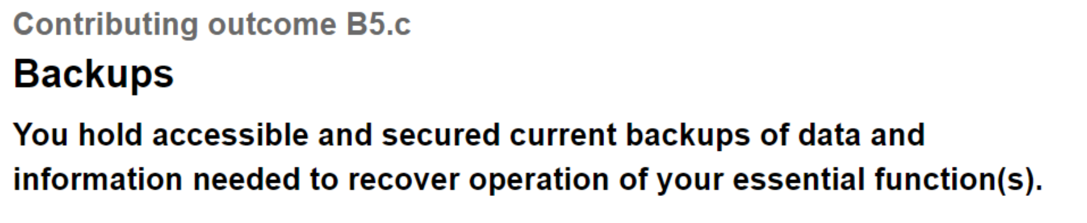
Your backup activities should be supported by documentation which outlines:

- frequency of backups
- how you ensure the ongoing security and maintenance of your backups
- which business events trigger backups to be made or used
- how you have automated your backups processes (in areas where it is appropriate to do so)
- how your testing regime ensures you are ready to efficiently recover the essential function in the event of an incident

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.c Backups

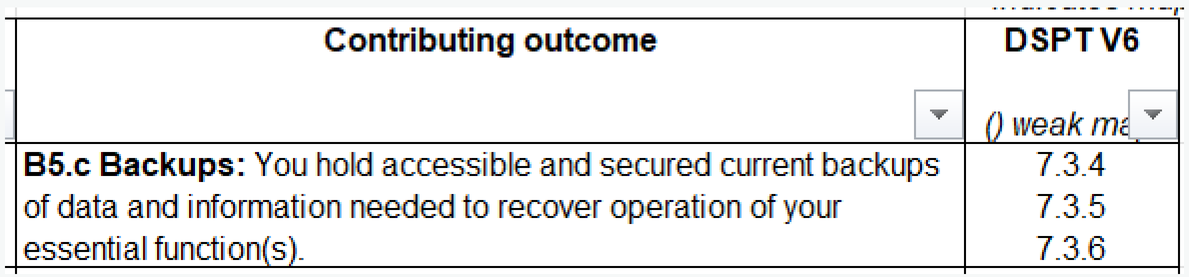
Supporting Evidence



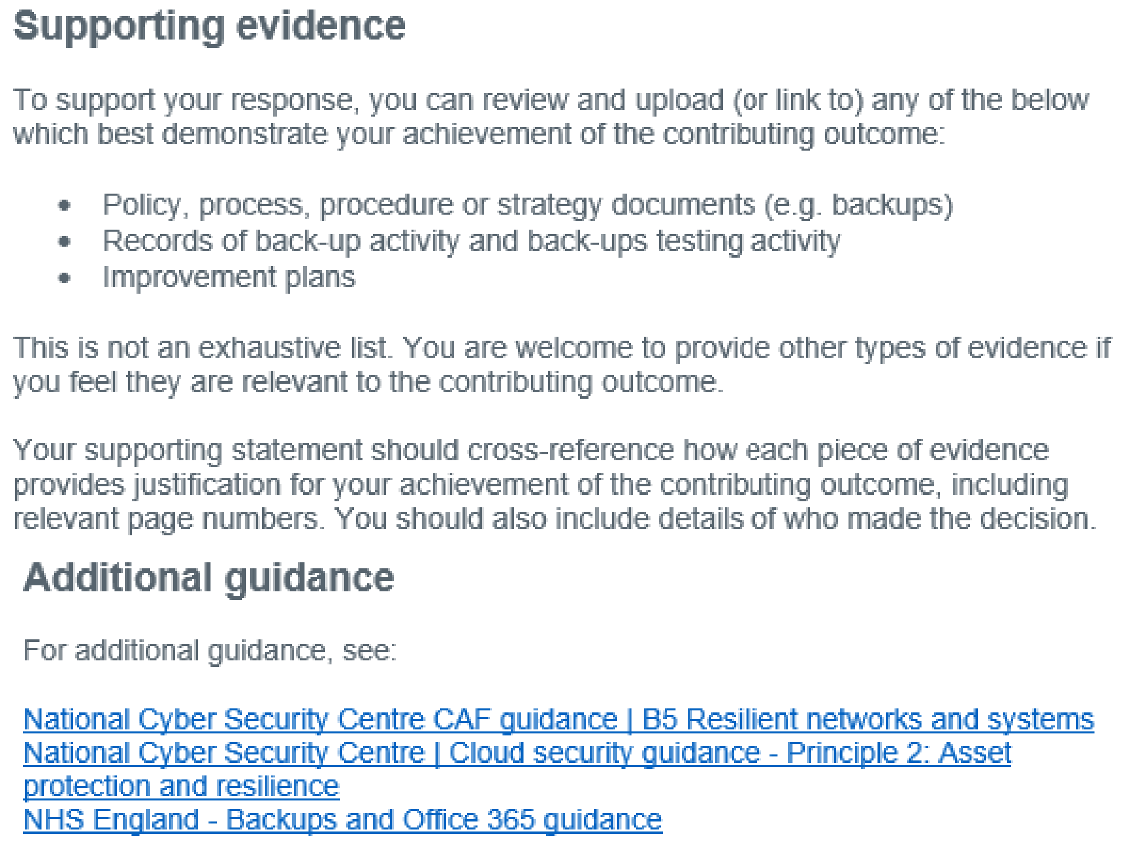
Contributing outcome B5.c

Backups

You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).



Contributing outcome	DSPT V6 *() weak ma*
B5.c Backups: You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).	7.3.4 7.3.5 7.3.6



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Policy, process, procedure or strategy documents (e.g. backups)
- Records of back-up activity and back-ups testing activity
- Improvement plans

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

Additional guidance

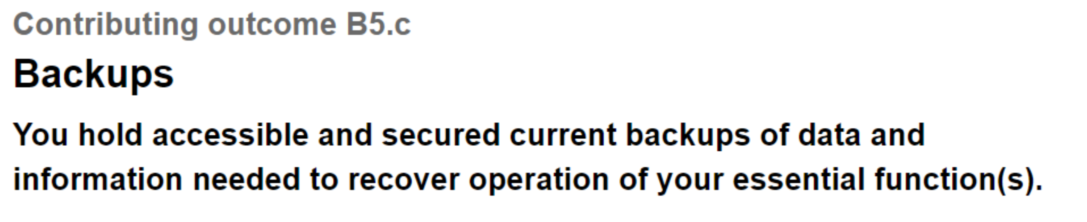
For additional guidance, see:

National Cyber Security Centre CAF guidance | B5 Resilient networks and systems
National Cyber Security Centre | Cloud security guidance - Principle 2: Asset protection and resilience
NHS England - Backups and Office 365 guidance

Principle: B5 Resilient networks and systems

Contributing outcome:
B5.c Backups

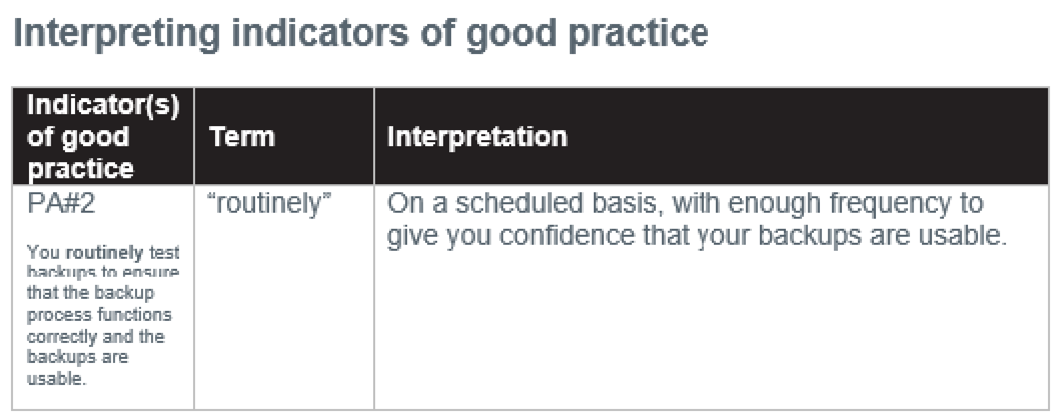
Interpretations



Contributing outcome B5.c

Backups

You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s).

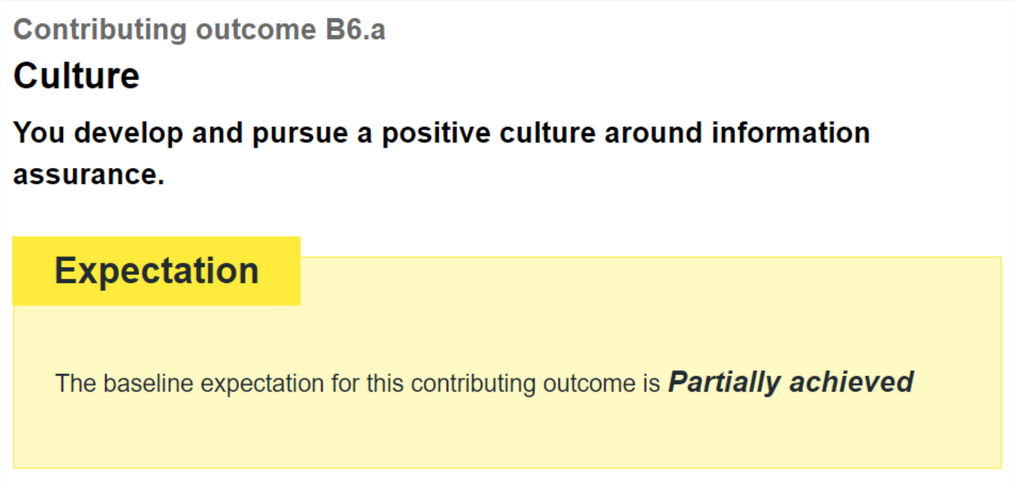


Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#2 You **routinely** test backups to ensure that the backup process functions correctly and the backups are usable.	"routinely"	On a scheduled basis, with enough frequency to give you confidence that your backups are usable.

Principle: B6 Staff awareness and training

Contributing outcome:
B6.a Culture



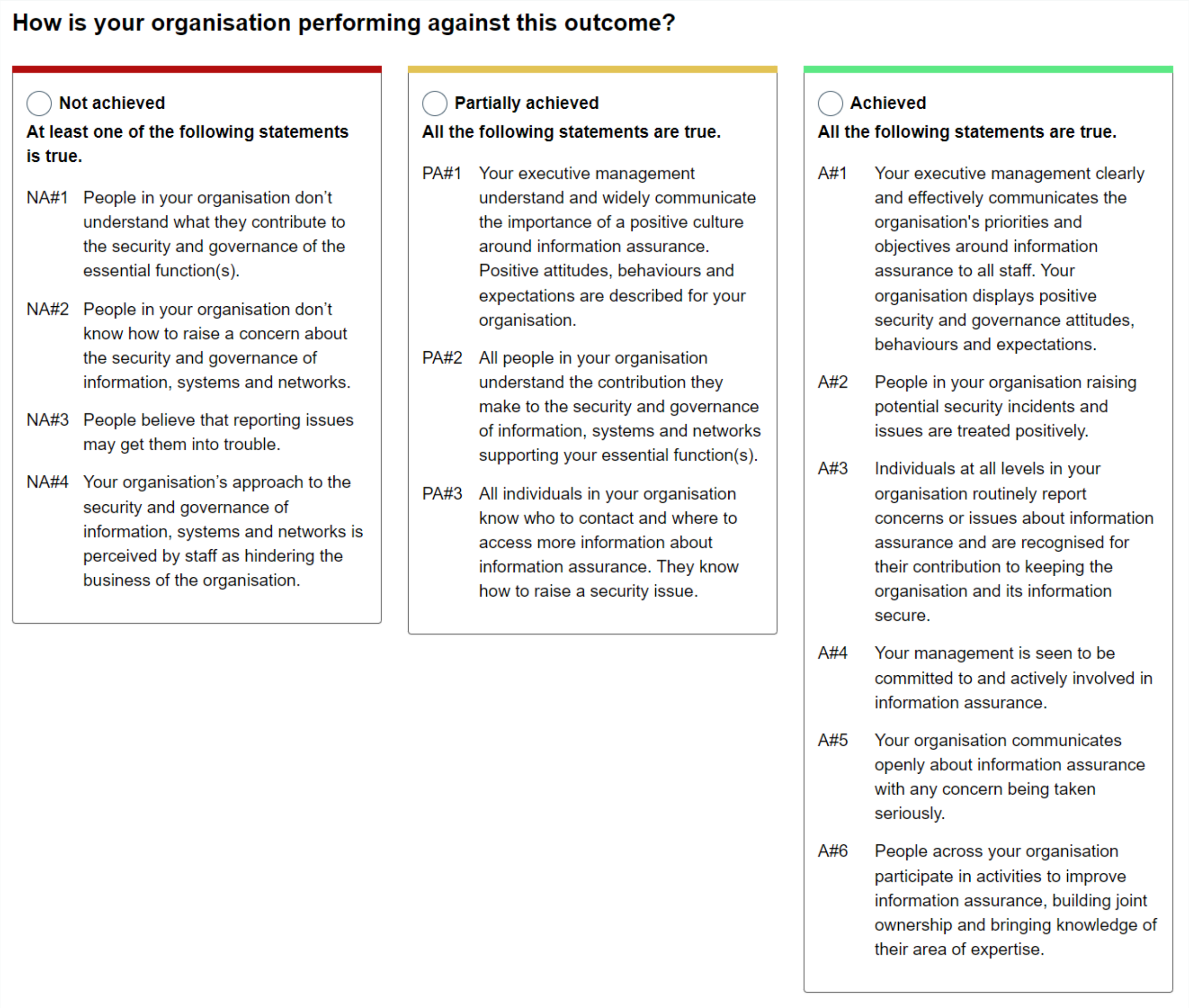
Contributing outcome B6.a

Culture

You develop and pursue a positive culture around information assurance.

Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 People in your organisation don’t understand what they contribute to the security and governance of the essential function(s).

NA#2 People in your organisation don’t know how to raise a concern about the security and governance of information, systems and networks.

NA#3 People believe that reporting issues may get them into trouble.

NA#4 Your organisation’s approach to the security and governance of information, systems and networks is perceived by staff as hindering the business of the organisation.

○ **Partially achieved**

All the following statements are true.

PA#1 Your executive management understand and widely communicate the importance of a positive culture around information assurance. Positive attitudes, behaviours and expectations are described for your organisation.

PA#2 All people in your organisation understand the contribution they make to the security and governance of information, systems and networks supporting your essential function(s).

PA#3 All individuals in your organisation know who to contact and where to access more information about information assurance. They know how to raise a security issue.

○ **Achieved**

All the following statements are true.

A#1 Your executive management clearly and effectively communicates the organisation's priorities and objectives around information assurance to all staff. Your organisation displays positive security and governance attitudes, behaviours and expectations.

A#2 People in your organisation raising potential security incidents and issues are treated positively.

A#3 Individuals at all levels in your organisation routinely report concerns or issues about information assurance and are recognised for their contribution to keeping the organisation and its information secure.

A#4 Your management is seen to be committed to and actively involved in information assurance.

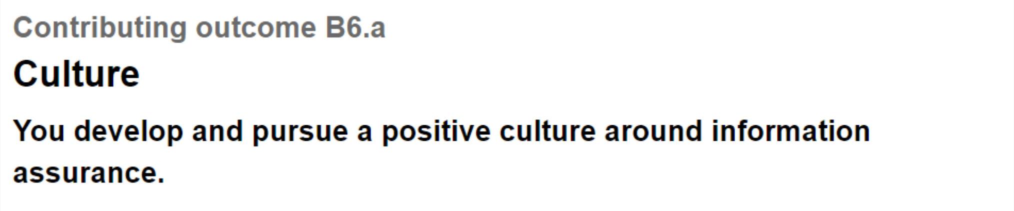
A#5 Your organisation communicates openly about information assurance with any concern being taken seriously.

A#6 People across your organisation participate in activities to improve information assurance, building joint ownership and bringing knowledge of their area of expertise.

Principle: B6 Staff awareness and training

Contributing outcome:
B6.a Culture

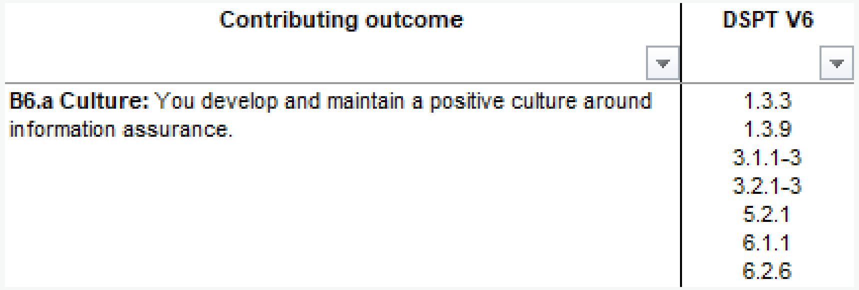
DSPT Mapping and Guidance



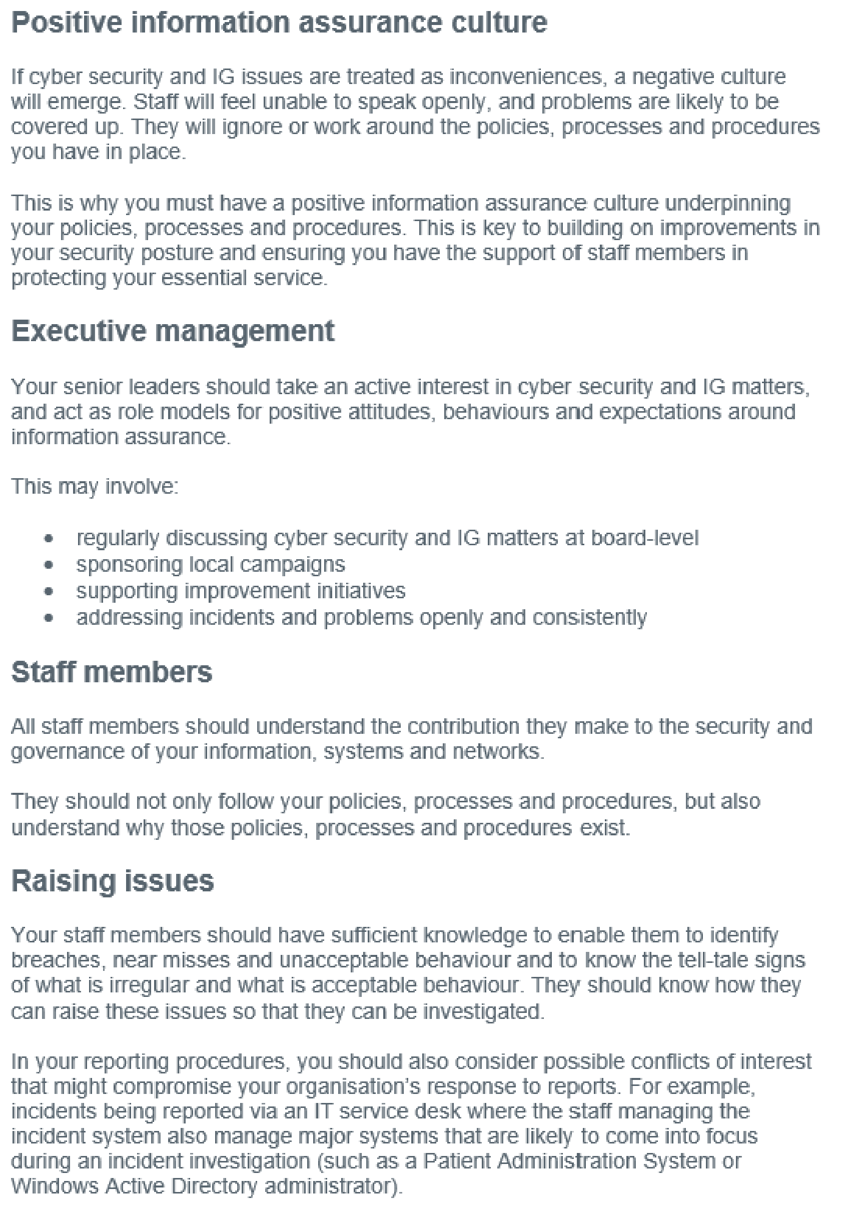
Contributing outcome B6.a

Culture

You develop and pursue a positive culture around information assurance.



Contributing outcome	DSPT V6
B6.a Culture: You develop and maintain a positive culture around information assurance.	1.3.3 1.3.9 3.1.1-3 3.2.1-3 5.2.1 6.1.1 6.2.6



Positive information assurance culture

If cyber security and IG issues are treated as inconveniences, a negative culture will emerge. Staff will feel unable to speak openly, and problems are likely to be covered up. They will ignore or work around the policies, processes and procedures you have in place.

This is why you must have a positive information assurance culture underpinning your policies, processes and procedures. This is key to building on improvements in your security posture and ensuring you have the support of staff members in protecting your essential service.

Executive management

Your senior leaders should take an active interest in cyber security and IG matters, and act as role models for positive attitudes, behaviours and expectations around information assurance.

This may involve:

- regularly discussing cyber security and IG matters at board-level
- sponsoring local campaigns
- supporting improvement initiatives
- addressing incidents and problems openly and consistently

Staff members

All staff members should understand the contribution they make to the security and governance of your information, systems and networks.

They should not only follow your policies, processes and procedures, but also understand why those policies, processes and procedures exist.

Raising issues

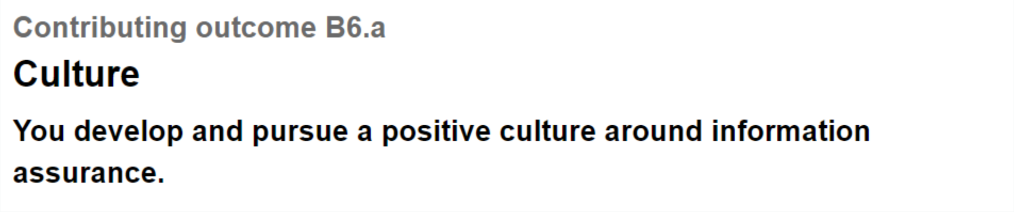
Your staff members should have sufficient knowledge to enable them to identify breaches, near misses and unacceptable behaviour and to know the tell-tale signs of what is irregular and what is acceptable behaviour. They should know how they can raise these issues so that they can be investigated.

In your reporting procedures, you should also consider possible conflicts of interest that might compromise your organisation's response to reports. For example, incidents being reported via an IT service desk where the staff managing the incident system also manage major systems that are likely to come into focus during an incident investigation (such as a Patient Administration System or Windows Active Directory administrator).

Principle: B6 Staff awareness and training

Contributing outcome:
B6.a Culture

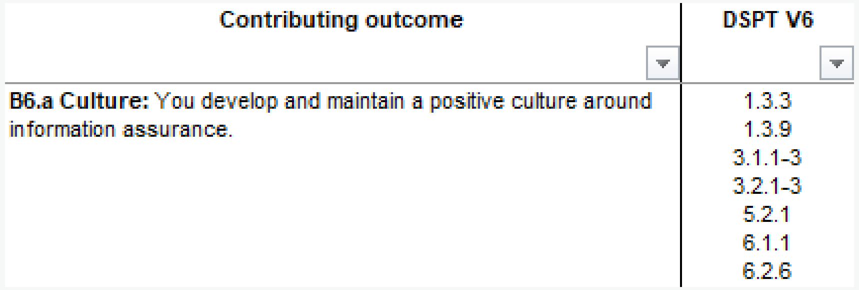
DSPT Mapping and Guidance



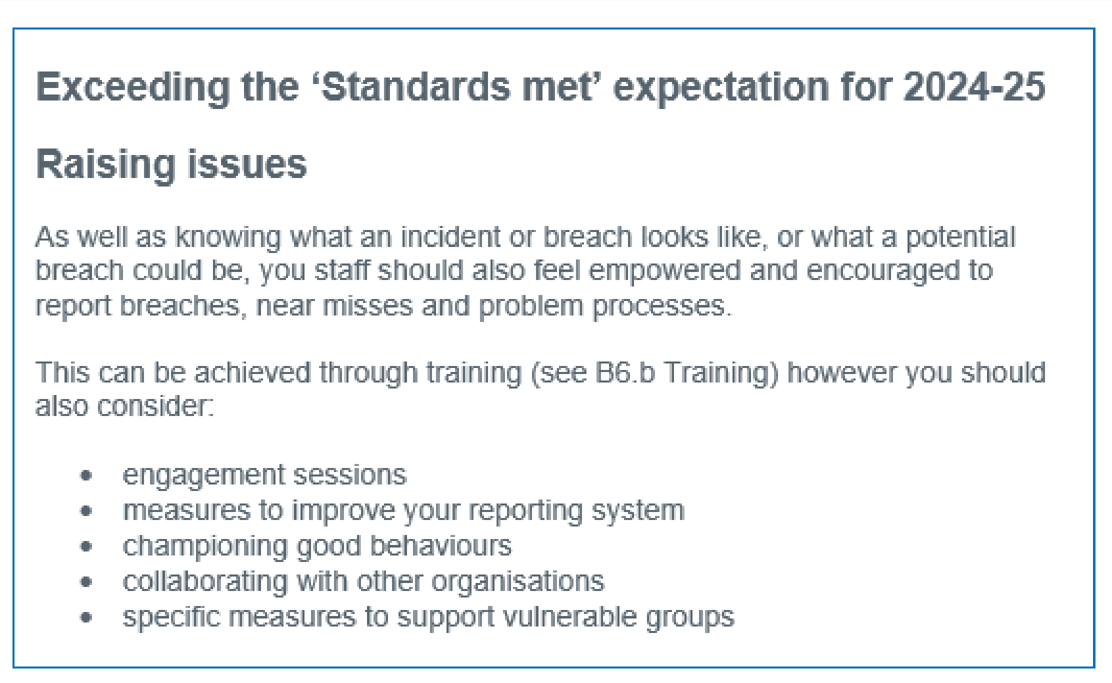
Contributing outcome B6.a

Culture

You develop and pursue a positive culture around information assurance.



Contributing outcome	DSPT V6
B6.a Culture: You develop and maintain a positive culture around information assurance.	1.3.3 1.3.9 3.1.1-3 3.2.1-3 5.2.1 6.1.1 6.2.6



Exceeding the 'Standards met' expectation for 2024-25

Raising issues

As well as knowing what an incident or breach looks like, or what a potential breach could be, you staff should also feel empowered and encouraged to report breaches, near misses and problem processes.

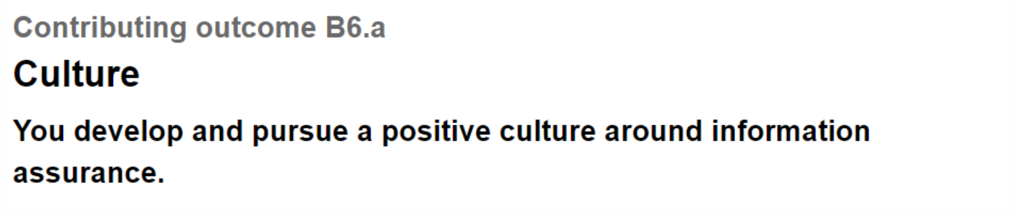
This can be achieved through training (see B6.b Training) however you should also consider:

- engagement sessions
- measures to improve your reporting system
- championing good behaviours
- collaborating with other organisations
- specific measures to support vulnerable groups

Principle: B6 Staff awareness and training

Contributing outcome:
B6.a Culture

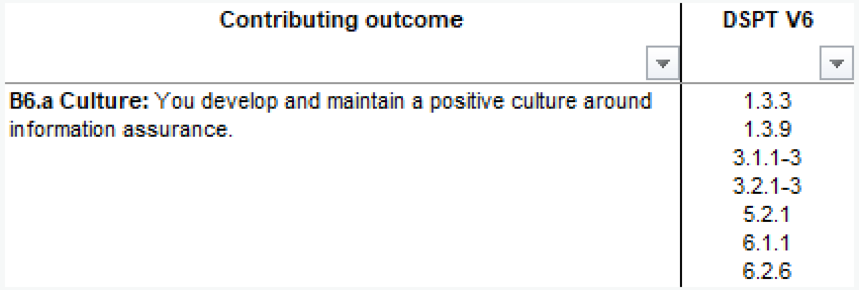
Supporting Evidence



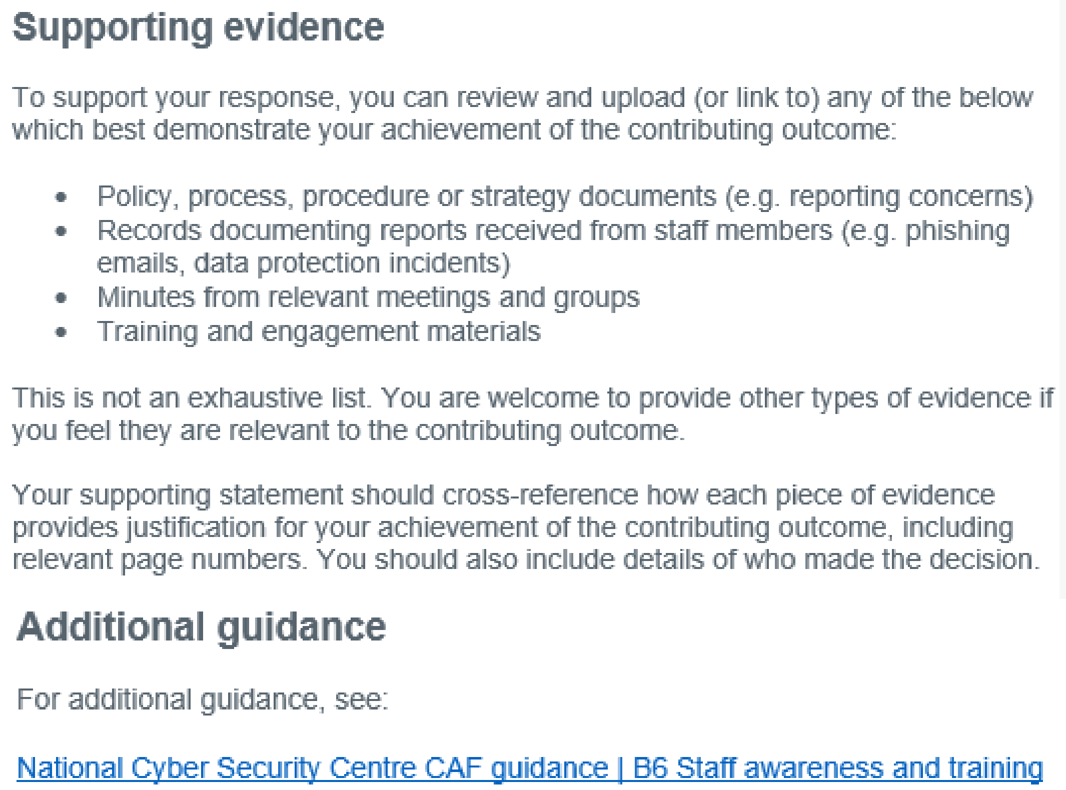
Contributing outcome B6.a

Culture

You develop and pursue a positive culture around information assurance.



Contributing outcome	DSPT V6
B6.a Culture: You develop and maintain a positive culture around information assurance.	1.3.3 1.3.9 3.1.1-3 3.2.1-3 5.2.1 6.1.1 6.2.6



Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Policy, process, procedure or strategy documents (e.g. reporting concerns)
- Records documenting reports received from staff members (e.g. phishing emails, data protection incidents)
- Minutes from relevant meetings and groups
- Training and engagement materials

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.

Additional guidance

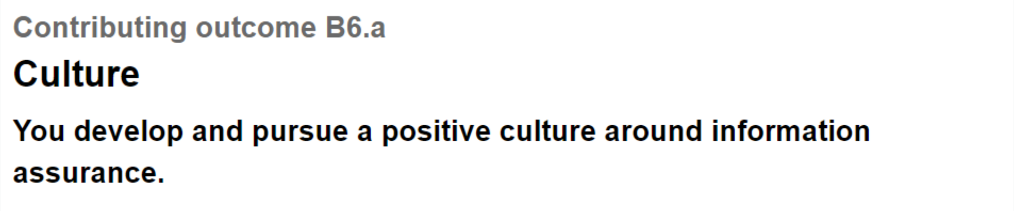
For additional guidance, see:

National Cyber Security Centre CAF guidance | B6 Staff awareness and training

Principle: B6 Staff awareness and training

Contributing outcome:
B6.a Culture

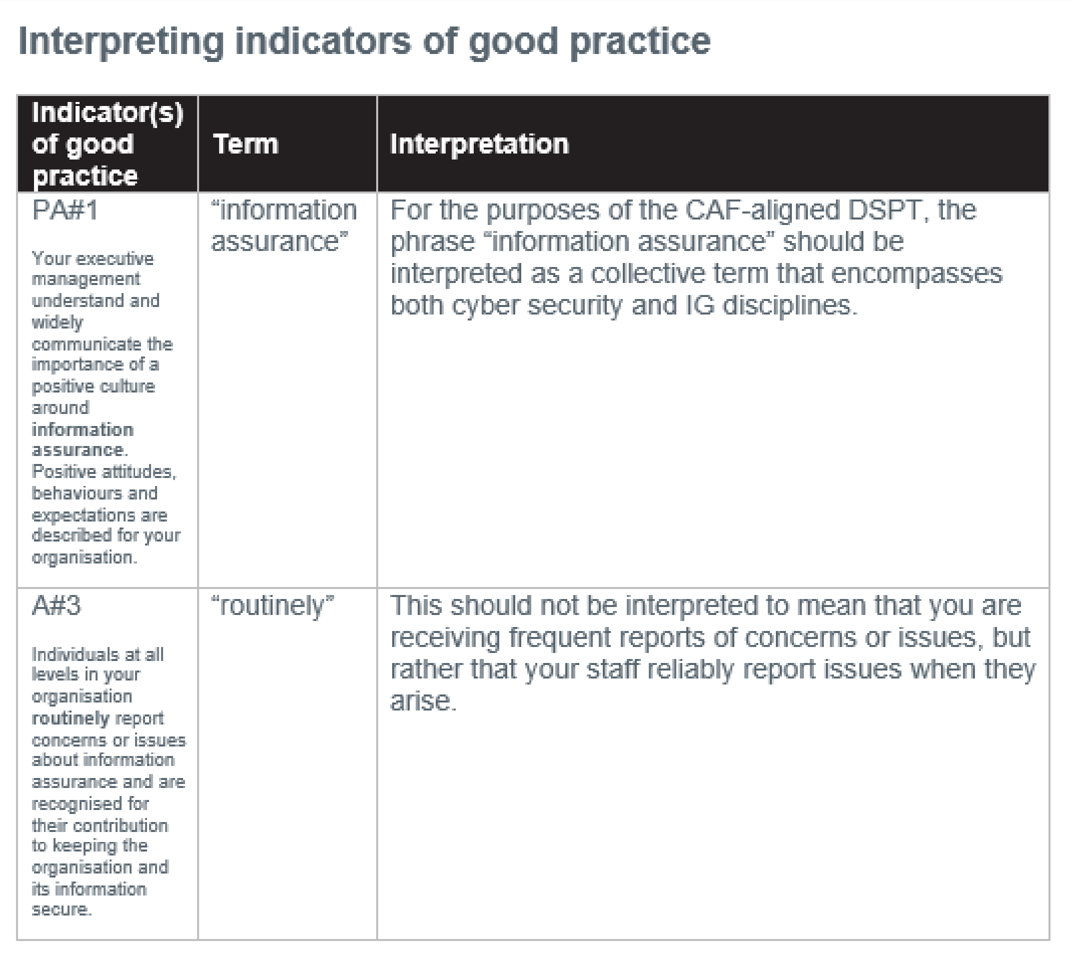
Interpretations



Contributing outcome B6.a

Culture

You develop and pursue a positive culture around information assurance.

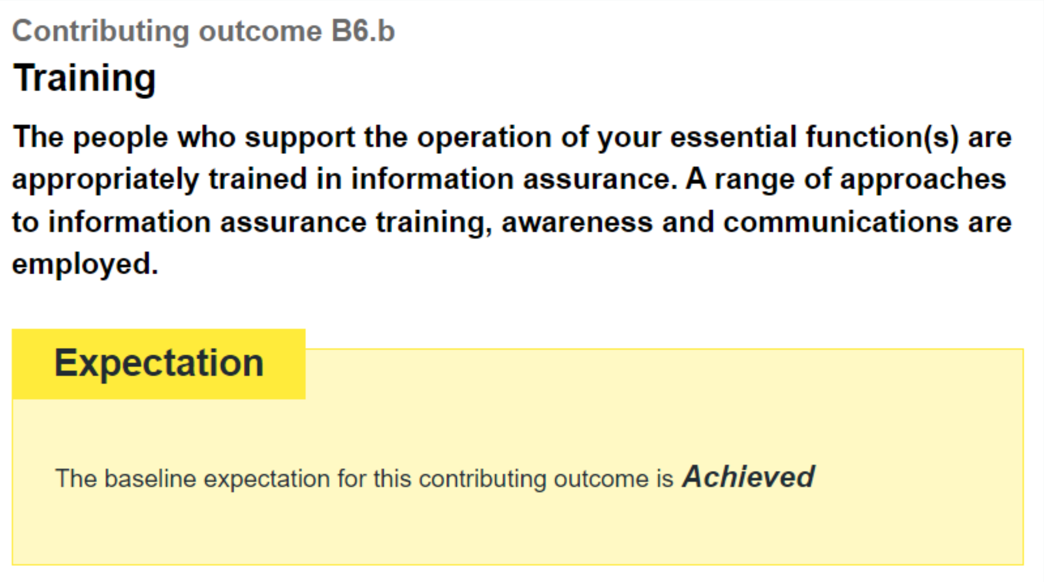


Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#1 Your executive management understand and widely communicate the importance of a positive culture around **information assurance**. Positive attitudes, behaviours and expectations are described for your organisation.	“information assurance”	For the purposes of the CAF-aligned DSPT, the phrase “information assurance” should be interpreted as a collective term that encompasses both cyber security and IG disciplines.
A#3 Individuals at all levels in your organisation **routinely** report concerns or issues about information assurance and are recognised for their contribution to keeping the organisation and its information secure.	“routinely”	This should not be interpreted to mean that you are receiving frequent reports of concerns or issues, but rather that your staff reliably report issues when they arise.

Principle: B6 Staff awareness and training

Contributing outcome:
B6.b Training



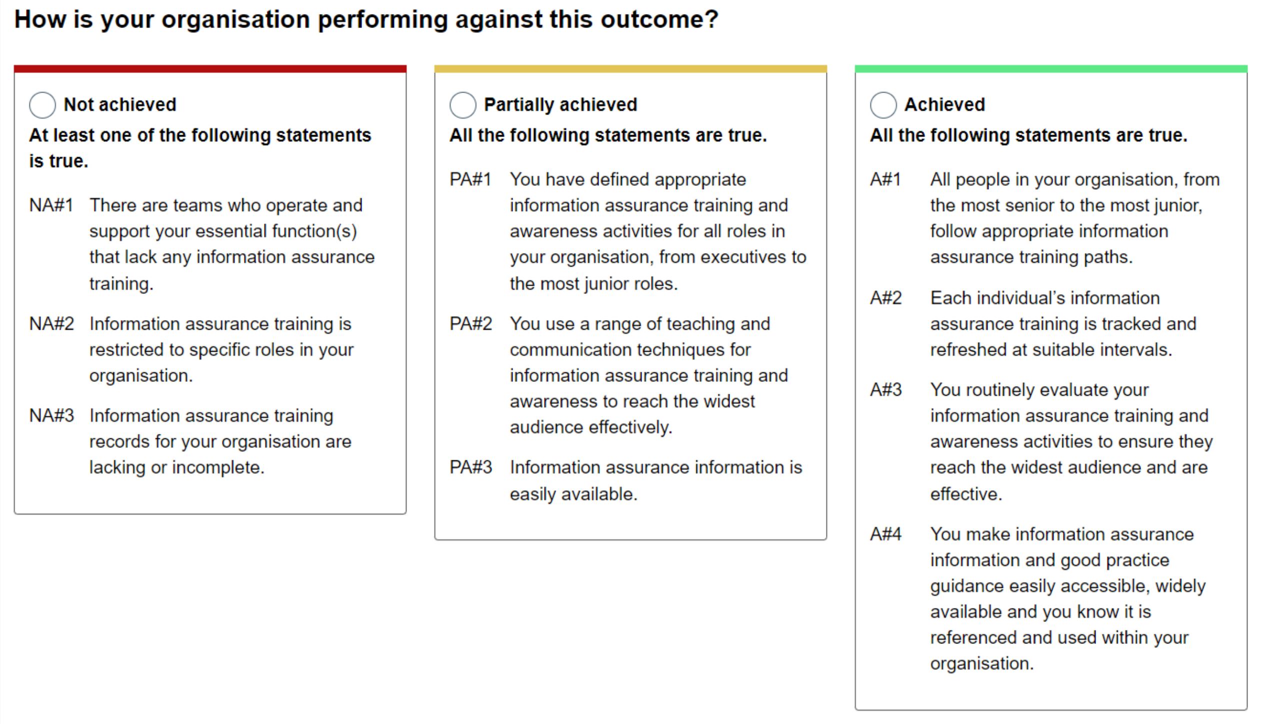
Contributing outcome B6.b

Training

The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.

Expectation

The baseline expectation for this contributing outcome is ***Achieved***



How is your organisation performing against this outcome?

○ **Not achieved**

At least one of the following statements is true.

NA#1 There are teams who operate and support your essential function(s) that lack any information assurance training.

NA#2 Information assurance training is restricted to specific roles in your organisation.

NA#3 Information assurance training records for your organisation are lacking or incomplete.

○ **Partially achieved**

All the following statements are true.

PA#1 You have defined appropriate information assurance training and awareness activities for all roles in your organisation, from executives to the most junior roles.

PA#2 You use a range of teaching and communication techniques for information assurance training and awareness to reach the widest audience effectively.

PA#3 Information assurance information is easily available.

○ **Achieved**

All the following statements are true.

A#1 All people in your organisation, from the most senior to the most junior, follow appropriate information assurance training paths.

A#2 Each individual's information assurance training is tracked and refreshed at suitable intervals.

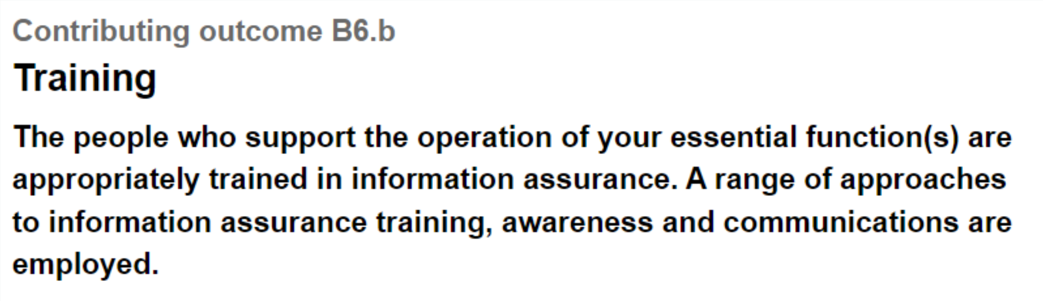
A#3 You routinely evaluate your information assurance training and awareness activities to ensure they reach the widest audience and are effective.

A#4 You make information assurance information and good practice guidance easily accessible, widely available and you know it is referenced and used within your organisation.

Principle: B6 Staff awareness and training

Contributing outcome:
B6.b Training

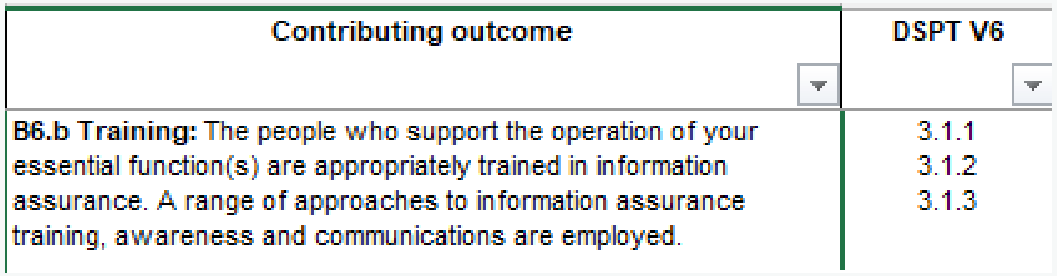
DSPT Mapping and Guidance



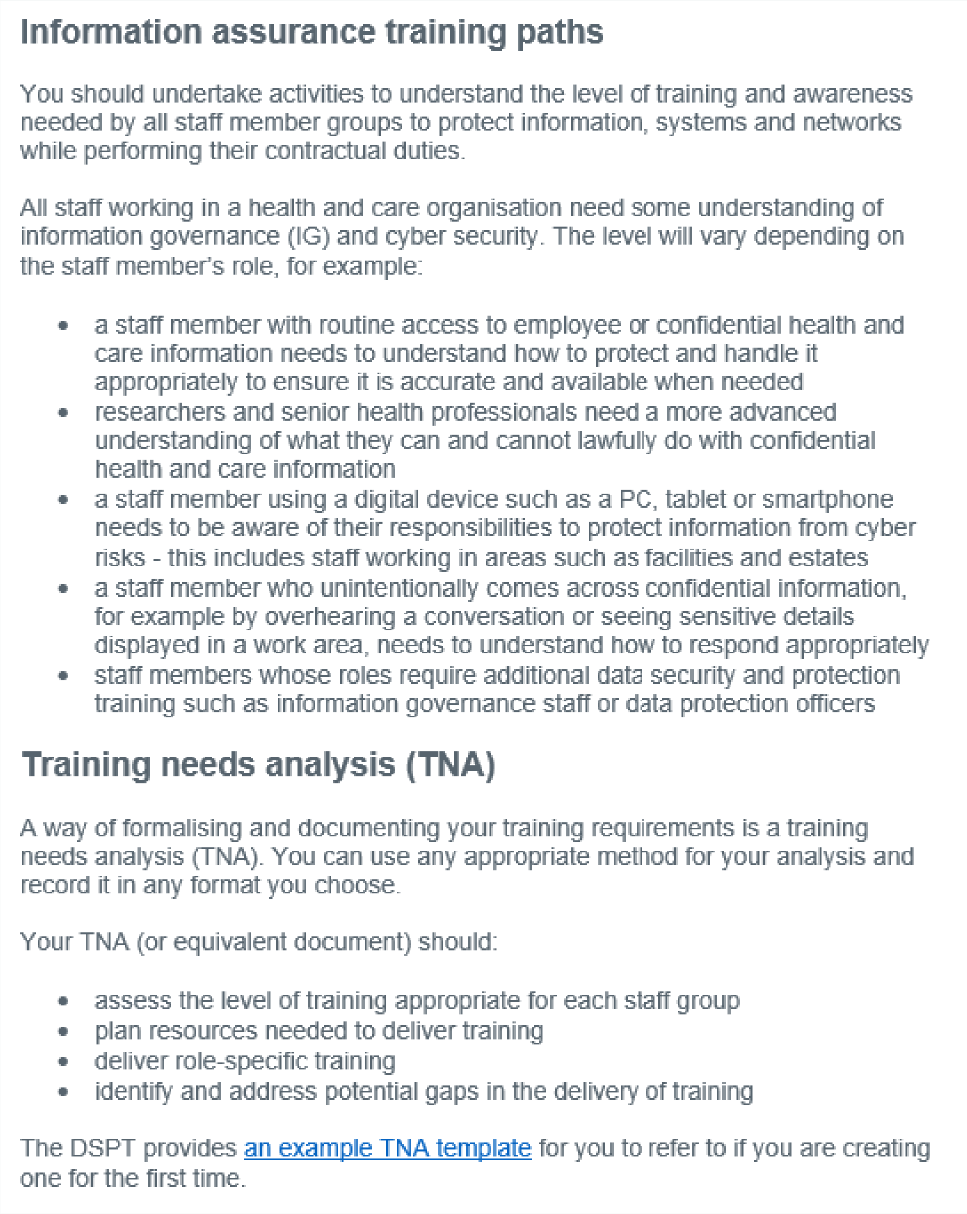
Contributing outcome B6.b

Training

The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.



Contributing outcome	DSPT V6
B6.b Training: The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.	3.1.1 3.1.2 3.1.3



Information assurance training paths

You should undertake activities to understand the level of training and awareness needed by all staff member groups to protect information, systems and networks while performing their contractual duties.

All staff working in a health and care organisation need some understanding of information governance (IG) and cyber security. The level will vary depending on the staff member's role, for example:

- a staff member with routine access to employee or confidential health and care information needs to understand how to protect and handle it appropriately to ensure it is accurate and available when needed
- researchers and senior health professionals need a more advanced understanding of what they can and cannot lawfully do with confidential health and care information
- a staff member using a digital device such as a PC, tablet or smartphone needs to be aware of their responsibilities to protect information from cyber risks - this includes staff working in areas such as facilities and estates
- a staff member who unintentionally comes across confidential information, for example by overhearing a conversation or seeing sensitive details displayed in a work area, needs to understand how to respond appropriately
- staff members whose roles require additional data security and protection training such as information governance staff or data protection officers

Training needs analysis (TNA)

A way of formalising and documenting your training requirements is a training needs analysis (TNA). You can use any appropriate method for your analysis and record it in any format you choose.

Your TNA (or equivalent document) should:

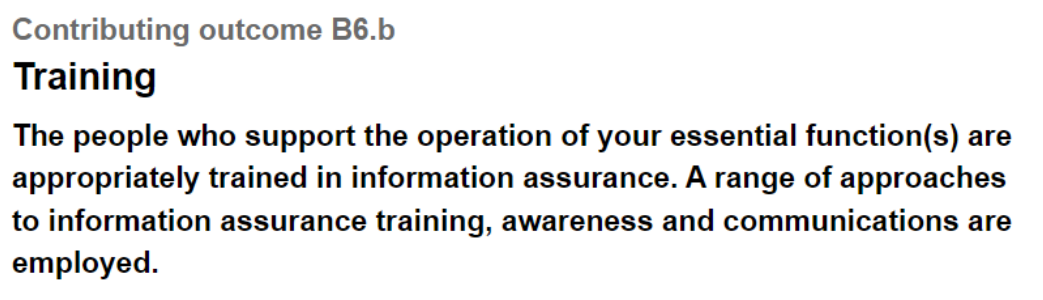
- assess the level of training appropriate for each staff group
- plan resources needed to deliver training
- deliver role-specific training
- identify and address potential gaps in the delivery of training

The DSPT provides an example TNA template for you to refer to if you are creating one for the first time.

Principle: B6 Staff awareness and training

Contributing outcome:
B6.b Training

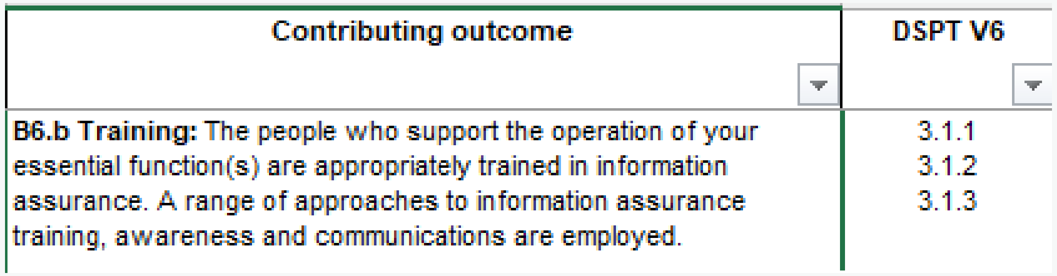
DSPT Mapping and Guidance



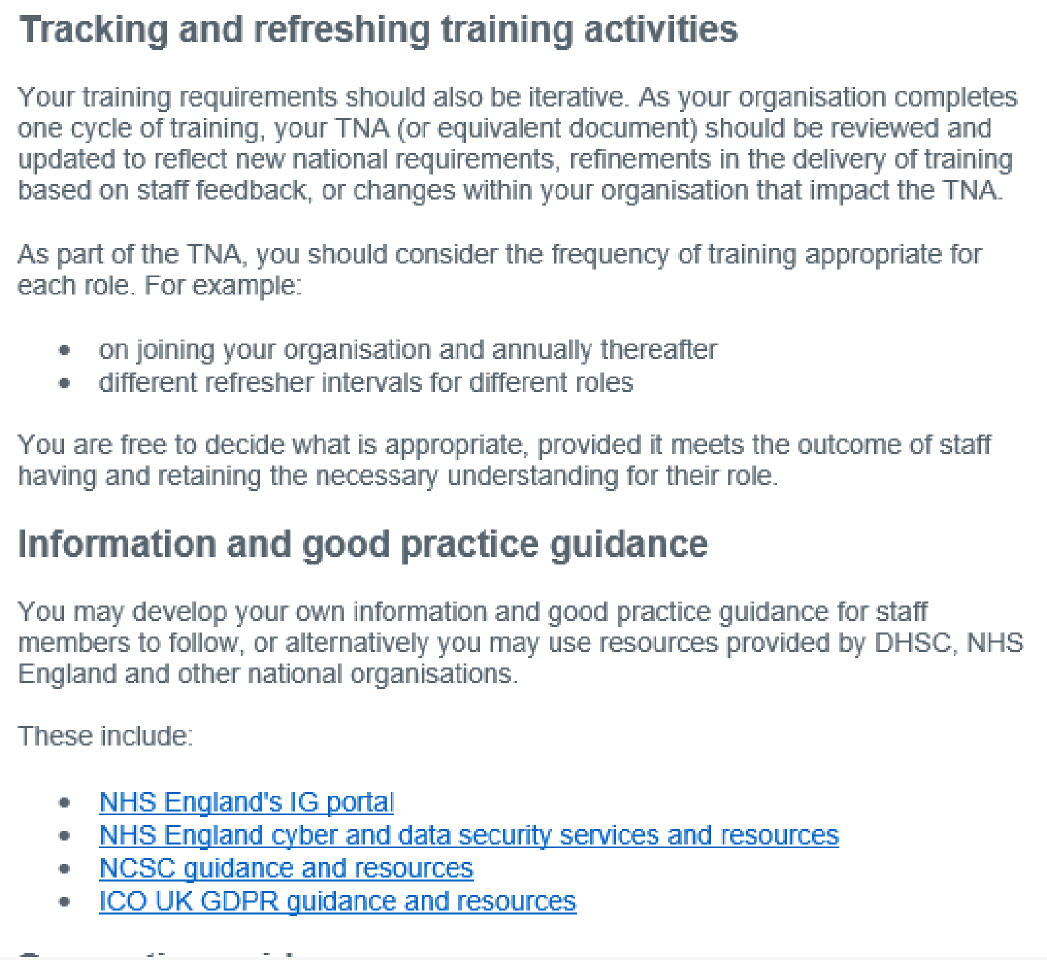
Contributing outcome B6.b

Training

The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.



Contributing outcome	DSPT V6
B6.b Training: The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.	3.1.1 3.1.2 3.1.3



Tracking and refreshing training activities

Your training requirements should also be iterative. As your organisation completes one cycle of training, your TNA (or equivalent document) should be reviewed and updated to reflect new national requirements, refinements in the delivery of training based on staff feedback, or changes within your organisation that impact the TNA.

As part of the TNA, you should consider the frequency of training appropriate for each role. For example:

- on joining your organisation and annually thereafter
- different refresher intervals for different roles

You are free to decide what is appropriate, provided it meets the outcome of staff having and retaining the necessary understanding for their role.

Information and good practice guidance

You may develop your own information and good practice guidance for staff members to follow, or alternatively you may use resources provided by DHSC, NHS England and other national organisations.

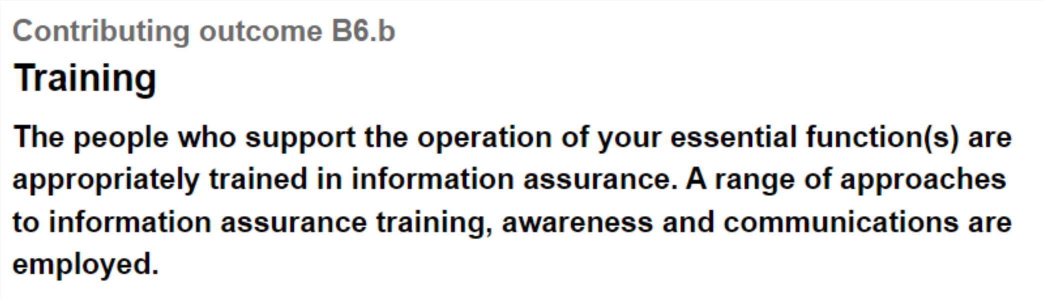
These include:

- NHS England's IG portal
- NHS England cyber and data security services and resources
- NCSC guidance and resources
- ICO UK GDPR guidance and resources

Principle: B6 Staff awareness and training

Contributing outcome: B6.b Training

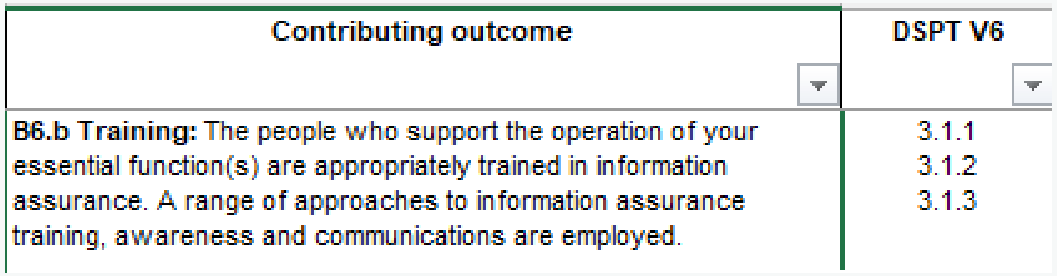
Supporting Evidence



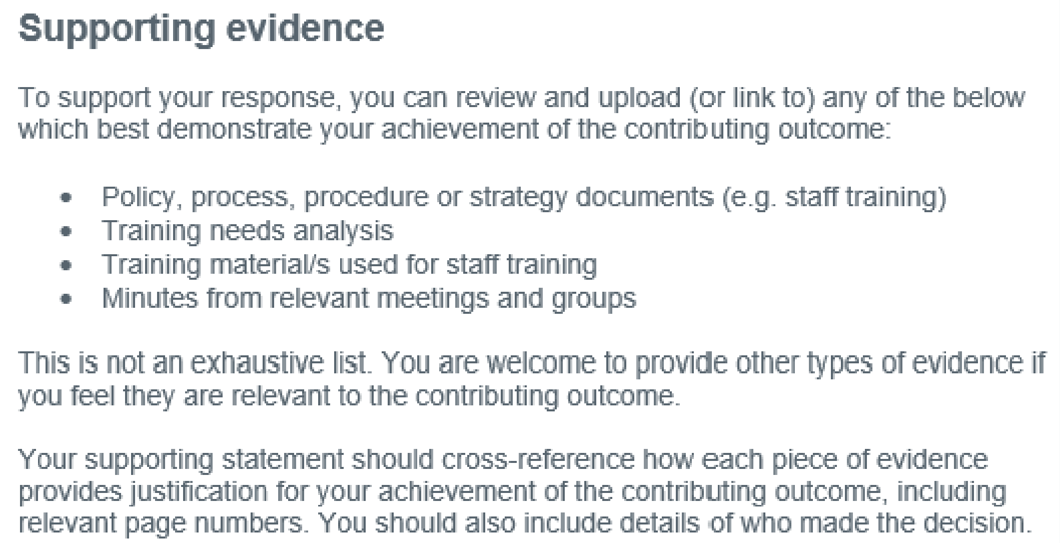
Contributing outcome B6.b

Training

The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.



Contributing outcome	DSPT V6
B6.b Training: The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.	3.1.1 3.1.2 3.1.3



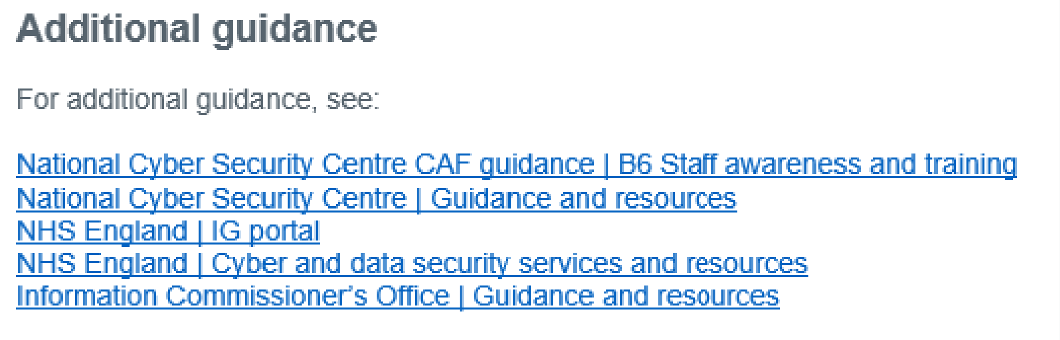
Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Policy, process, procedure or strategy documents (e.g. staff training)
- Training needs analysis
- Training material/s used for staff training
- Minutes from relevant meetings and groups

This is not an exhaustive list. You are welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers. You should also include details of who made the decision.



Additional guidance

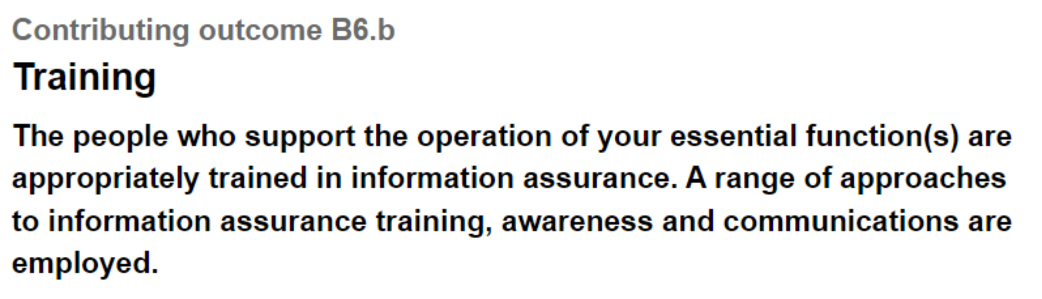
For additional guidance, see:

National Cyber Security Centre CAF guidance | B6 Staff awareness and training
National Cyber Security Centre | Guidance and resources
NHS England | IG portal
NHS England | Cyber and data security services and resources
Information Commissioner's Office | Guidance and resources

Principle: B6 Staff awareness and training

Contributing outcome:
B6.b Training

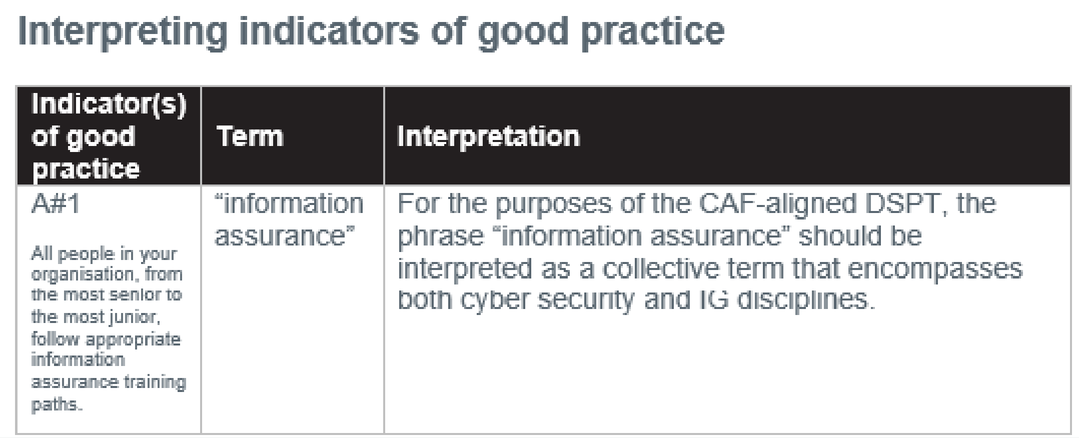
Interpretations



Contributing outcome B6.b

Training

The people who support the operation of your essential function(s) are appropriately trained in information assurance. A range of approaches to information assurance training, awareness and communications are employed.

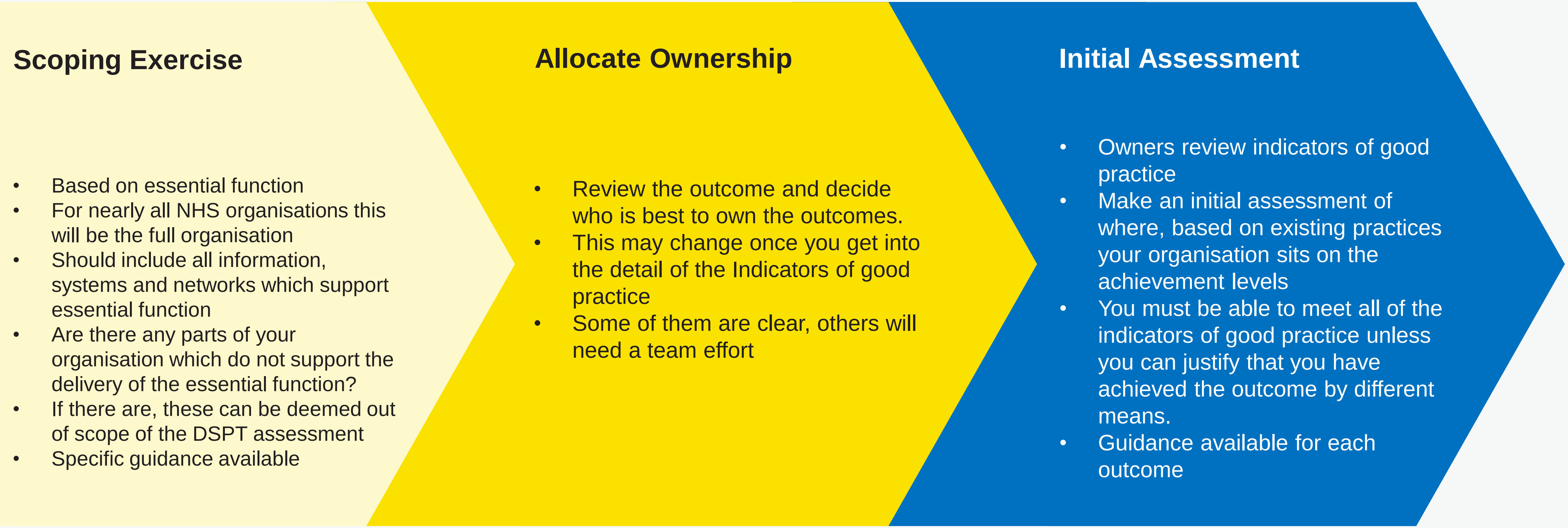


Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
A#1 All people in your organisation, from the most senior to the most junior, follow appropriate information assurance training paths.	“information assurance”	For the purposes of the CAF-aligned DSPT, the phrase “information assurance” should be interpreted as a collective term that encompasses both cyber security and IG disciplines.

Planning for DSPT in 24-25

Completing the DSPT 24-25 – Initial Review



Scoping Exercise

- Based on essential function
- For nearly all NHS organisations this will be the full organisation
- Should include all information, systems and networks which support essential function
- Are there any parts of your organisation which do not support the delivery of the essential function?
- If there are, these can be deemed out of scope of the DSPT assessment
- Specific guidance available

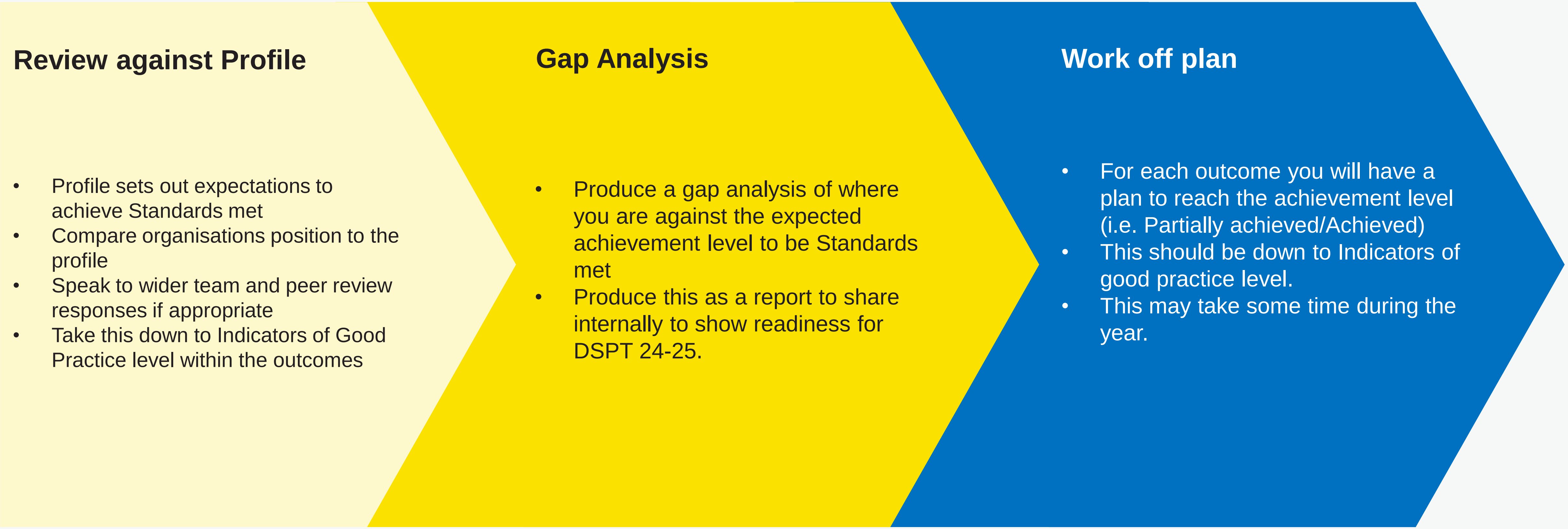
Allocate Ownership

- Review the outcome and decide who is best to own the outcomes.
- This may change once you get into the detail of the Indicators of good practice
- Some of them are clear, others will need a team effort

Initial Assessment

- Owners review indicators of good practice
- Make an initial assessment of where, based on existing practices your organisation sits on the achievement levels
- You must be able to meet all of the indicators of good practice unless you can justify that you have achieved the outcome by different means.
- Guidance available for each outcome

Completing the DSPT 24-25 – Planning to deliver



Review against Profile

- Profile sets out expectations to achieve Standards met
- Compare organisations position to the profile
- Speak to wider team and peer review responses if appropriate
- Take this down to Indicators of Good Practice level within the outcomes

Gap Analysis

- Produce a gap analysis of where you are against the expected achievement level to be Standards met
- Produce this as a report to share internally to show readiness for DSPT 24-25.

Work off plan

- For each outcome you will have a plan to reach the achievement level (i.e. Partially achieved/Achieved)
- This should be down to Indicators of good practice level.
- This may take some time during the year.

Demonstration

Question and answer session

Next Webinars

Date and time	Topics to be covered
Wednesday 31st July 10:00 – 11:30	**Objective E – Using and sharing information appropriately and update on DSPT audits**
Thursday 8th August 14:00 – 15:30	Objective D – Minimising the impact of incidents
Wednesday 14th August 14:00 – 15:30	Objective C – Detecting cyber security events

Please use the link below to register for the webinar series:
CAF-aligned DSPT 2024-25 webinar series | NHS England Events
You can ask any questions in advance of the webinar using this form.
If you are interested

NHS England

Thank You

@nhsengland

company/nhsengland

england.nhs.uk