Data Security and Protection Toolkit 2024-25

CAF aligned DSPT - Overview and background

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

NHS England
04 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 the session
- 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 1 – overview and background

- Introducing the CAF-aligned DSPT, health and care overlay
- Things that stay the same – audits, SIRO sign-off, support inbox for queries
- ‘Essential functions’ scoping exercise
- Explaining the ‘standards met’ profile for year 1
- How to collaborate between teams to manage toolkit submission
- How to write supporting statements
- How to provide evidence
- Demo of the new user interface
- 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.
- The goal of the CAF is to set out broad principles to drive good decision-making, rather than a "compliance checklist" of good practices.
- Expectations for cyber security and IG controls should remain at a reasonably comparable level to the current DSPT, tightening only in areas where NHSE and DHSC believe the higher standard to be a necessary obligation.
- Guidance will be produced and webinars have been stood up to help organisations understand the content, approach and expectations of the CAF-aligned DSPT.

Context

Data Security and Protection Toolkit (DSPT)

- Progress since 2018
- Cohesion
- Forecasting
- Responsiveness
- Adoption of Cyber Assessment Framework (“**CAF**”)

Why is the DSPT changing?

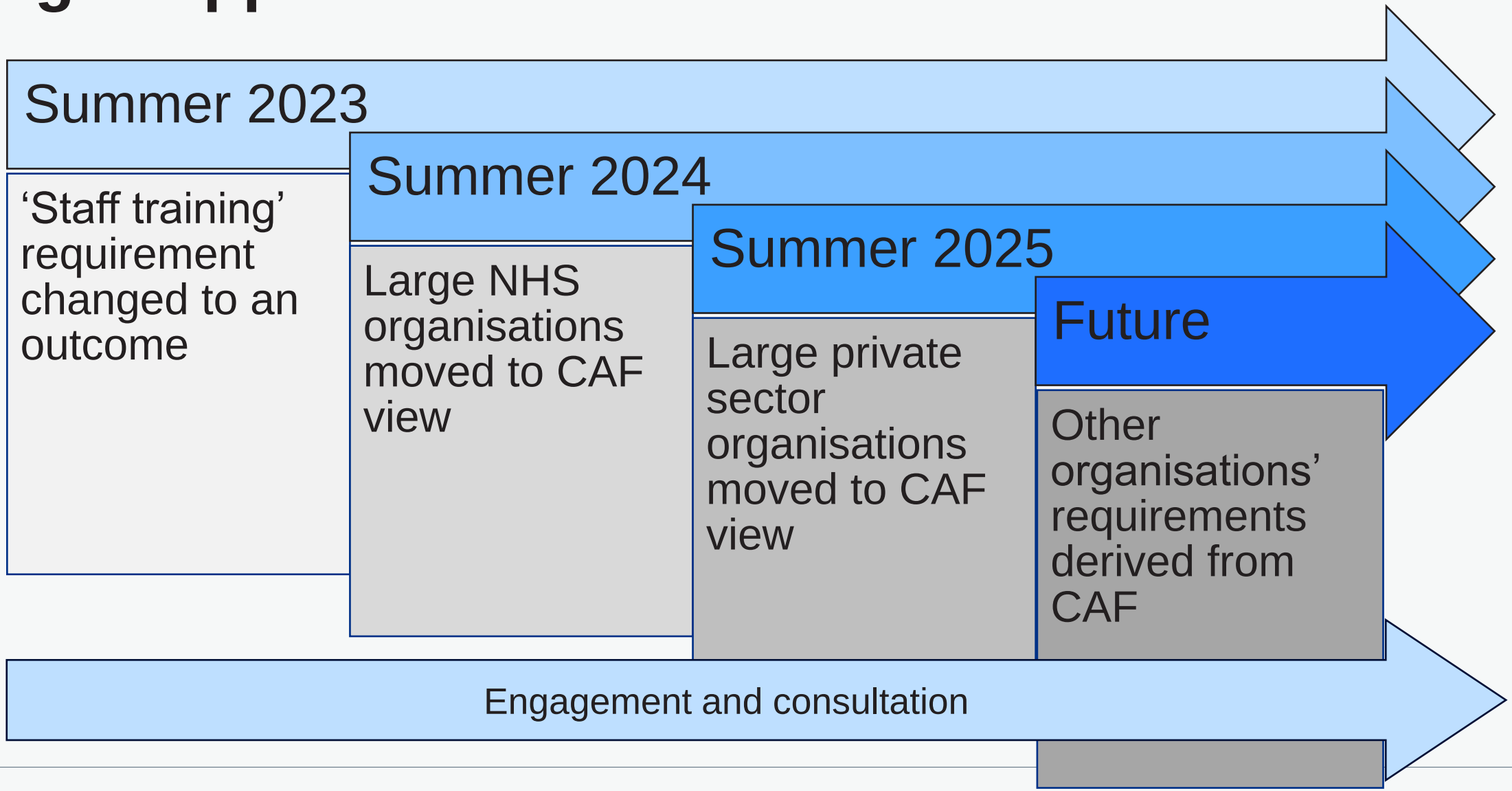
The goals of moving to the CAF-aligned DSPT are to:

- Emphasise good decision-making over compliance, with better understanding and ownership of information risks at the local organisation level where those risks can most effectively be managed

- Support a culture of evaluation and improvement, as organisations will need to understand the effectiveness of their practices at meeting the desired outcomes – and expend effort on what works, not what ticks a compliance box

- Create opportunities for better practice, by prompting and enabling organisations to remain current with new security measures to meet new threats and risks

Staged approach for DSPT



Understanding the CAF

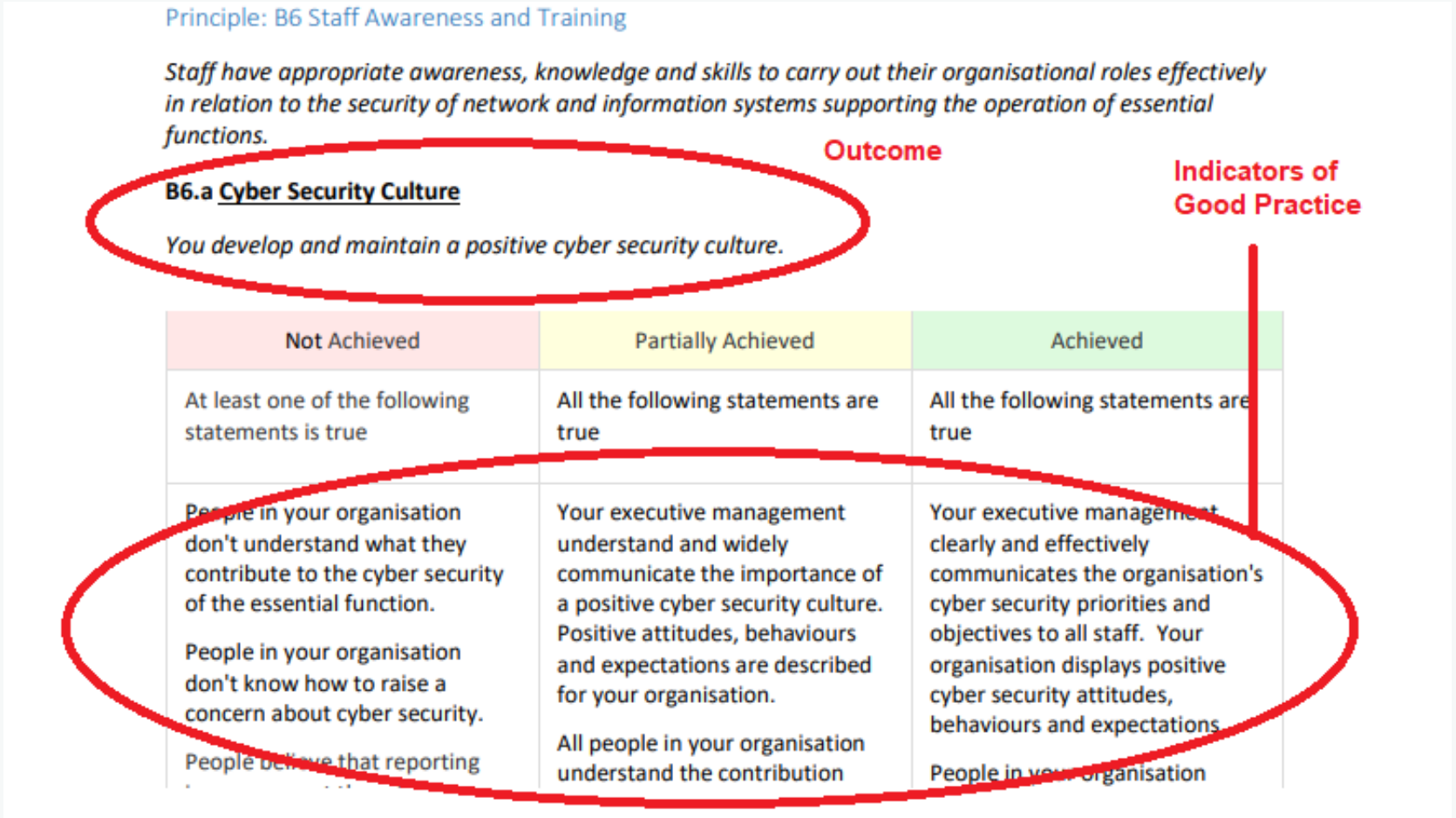
“Pure CAF” structure

Objective A
Managing security risk

Objective B
Protecting against cyber attack

Objective C
Detecting cyber security events

Objective D
Minimising the impact of cyber security incidents



Principle: B6 Staff Awareness and Training

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

Outcome

Indicators of Good Practice

B6.a Cyber Security Culture

You develop and maintain a positive cyber security culture.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
People in your organisation don't understand what they contribute to the cyber security of the essential function. People in your organisation don't know how to raise a concern about cyber security. People believe that reporting	Your executive management understand and widely communicate the importance of a positive cyber security culture. Positive attitudes, behaviours and expectations are described for your organisation. All people in your organisation understand the contribution	Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations People in your organisation

CAF profiles

- Organisations are not expected (ever) to reach ‘Achieved’ on every outcome
- A ‘CAF profile’ sets the expectation for each outcome, for a given year:

Principle	Outcome	NA	PA	A
[…]	[…]			
C2 Proactive Security Event Discovery	C2.a System Abnormalities for Attack Detection	NA		
	C2.b Proactive Attack Discovery	NA		
D1 Response and Recovery Planning	D1.a Response Plan		PA	
	D1.b Response and Recovery Capability			A
	D1.c Testing and Exercising			A
[…]	[…]			

The role of ‘Partially Achieved’

B2.b Device Management

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

Not Achieved	Partially Achieved	Achieved
[…] NA#3 You have not gained assurance in the the security of any third-party devices or networks connected to your systems. […]	[…] 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. […]	[…] A#2 You… obtain independent and professional assurance of the security of third-party devices or networks before they connect to your systems… […]

Implementing the CAF in health and care

Health and care ‘CAF overlay’ (1)

Objective A
Managing risk

Objective B
Protecting against cyber attack and data breaches

Objective C
Detecting cyber security events

Objective D
Minimising the impact of incidents

Objective E
Using and sharing information appropriately

Health and care ‘CAF overlay’ (2)

Objective	Principle	Contributing outcome
A - Managing security risk: Appropriate organisational structures, policies and processes in place to understand, assess and systematically manage security risks to ~~the network and information systems~~ information, systems and networks supporting essential functions.	**A1 Governance:** The organisation has appropriate management policies and processes in place to govern its approach to the security of information, systems and networks ~~network and information systems~~.	**A1.a Board Direction and accountability:** You have effective ~~organisational security~~ information assurance management led at board level and articulated clearly in corresponding policies.
		A1.b Roles and Responsibilities: Your organisation has established roles and responsibilities for the security and governance of information, systems and networks ~~of network and information systems~~ at all levels, with clear and well-understood channels for communicating and escalating risks.
		A1.c Decision-making: You have senior-level accountability for the security and governance of information, systems and networks ~~of networks and information systems~~, and delegate decision-making authority appropriately and effectively. Risks to information, systems and networks ~~network and information systems~~ related to the operation of essential functions are considered in the context of other organisational risks.
	A2 Risk Management: The organisation takes appropriate steps to identify, assess and understand security risks to the security and governance of information, systems and networks ~~network and information systems supporting the operation of essential functions~~. This includes an overall organisational approach to risk management.	**A2.a Risk Management Process:** Your organisation has effective internal processes for managing risks to the security and governance of information, systems and networks ~~of network and information systems related to the operation of essential functions~~ and communicating associated activities. This includes a process for data protection impact assessments (DPIAs).
		A2.b Assurance: You have gained confidence in the effectiveness of the security of your technology, people and processes relevant to essential functions.

Health and care ‘CAF overlay’ (3)

E - **Using and sharing information appropriately:** The organisation ensures that information is used and shared lawfully and appropriately.	**E1 Transparency:** The organisation is transparent about how it collects, uses, shares and stores information. Privacy notices are clear and easy for members of the public to access.	**E1.a Privacy information:** Your organisation follows best practice for the drafting and publication of its privacy information to ensure that all individuals have a reasonable understanding of their rights and how their information is being used.
	E2 Upholding the rights of individuals: The organisation respects and supports individuals in exercising their information rights	**E2.a Managing data subject rights under UK GDPR:** Your organisation appropriately assesses and manages information rights requests.
		E2.b Consent: Your organisation has a good understanding of the common law duty of confidentiality and uses it to manage consent.
		E2.c National data opt-out policy: A robust policy and system is in place to ensure opt-outs are correctly applied to the information being used and shared by your organisation.
	E3 Sharing information: Your organisation shares information appropriately.	**E3.a Information sharing for direct care:** Your organisation facilitates lawful and appropriate sharing of information for direct care.
		E3.b Information sharing for other purposes: Your organisation facilitates lawful and appropriate sharing of information for purposes outside of direct care.
	E4 Records management: Your organisation manages records in accordance with its professional responsibilities and the law.	**E4.a Managing records**
		E4.b Clinical coding: Your organisation is committed to regularly evaluating and improving its coded clinical data.

What is staying the same?

DSPT functionality - not changing (1/2)

Name and URL

Data Security and Protection Toolkit

Web address unchanged
https://www.dsptoolkit.nhs.uk/

Deadlines

Final Publication 30 June 2025

Standards Met

Organisation has met expectations

Requirement for Audit

Audit Guidance being updated

Launch with DSPT

SIRO sign off

Requires formal sign off

SIRO level for 24-25.

DSPT functionality - not changing (2/2)

Interim Assessment

Interim Publication by 31 December 2024

Improvement Plan

Organisations not meeting expectation complete Improvement plan

Access to history

Previous years DSPT assessments can be accessed

Not transferred over though

Organisation Search

DSPT Status in public domain

Search for other organisations DSPT Status

Support

Exeter Helpdesk

Webinars

Guidance

What is Changing?

DSPT functionality - what's changing

Exemptions

No exemptions for NHS Mail or Cyber Essentials + certification

Data Security Standards

Cyber Assessment framework replacing the 10 Data Security Standards

Evidence

Ability to upload any evidence type to any outcome

Respond at Outcome

Higher level than evidence item

Likely to need input from Cyber, IT operations and IG

Standards Exceeded

Not available for 24-25

To be considered for 25-26

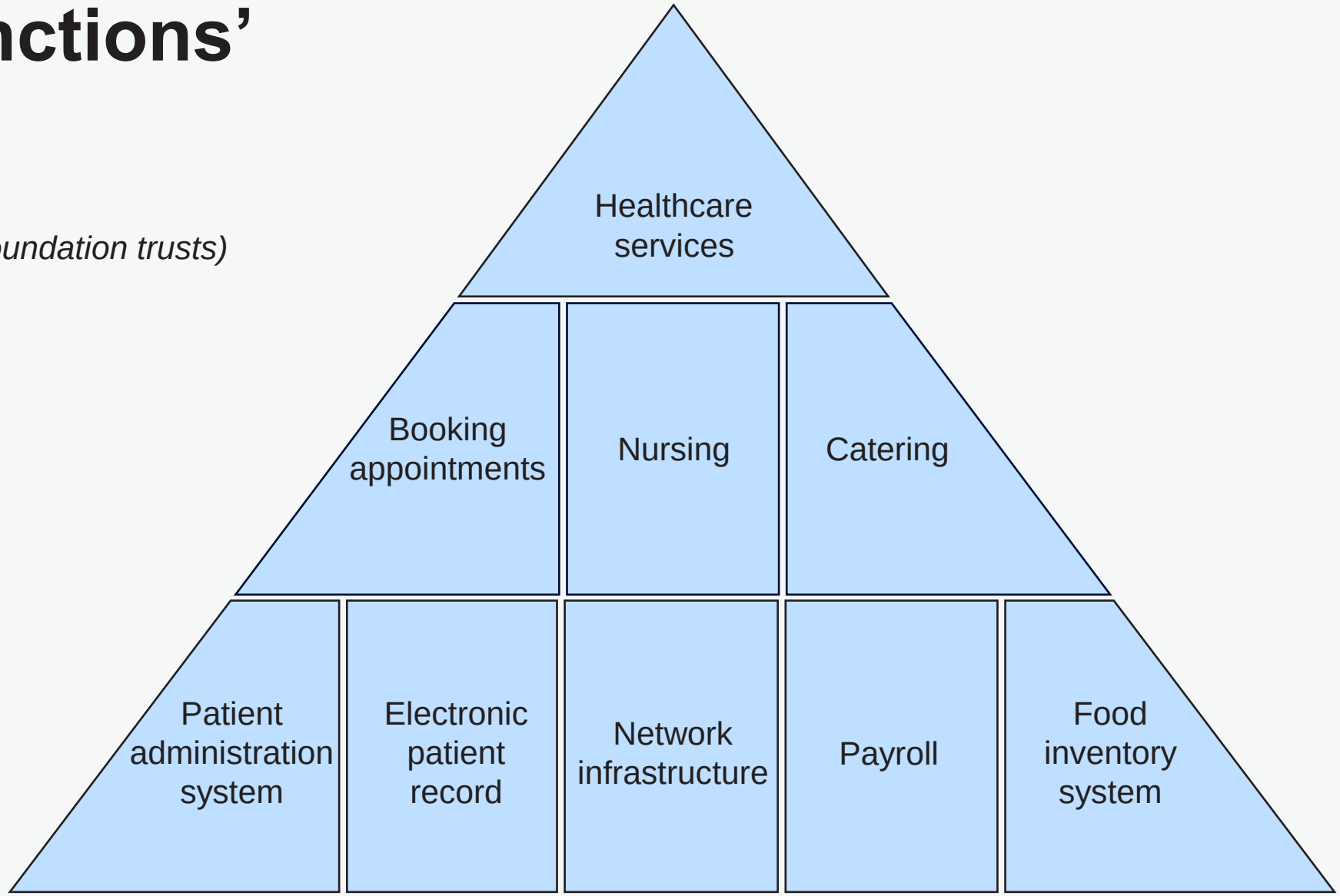
‘Essential functions’

‘Essential functions’

Essential service
(example for NHS trusts and foundation trusts)

Essential functions

Systems that support the operation of essential functions



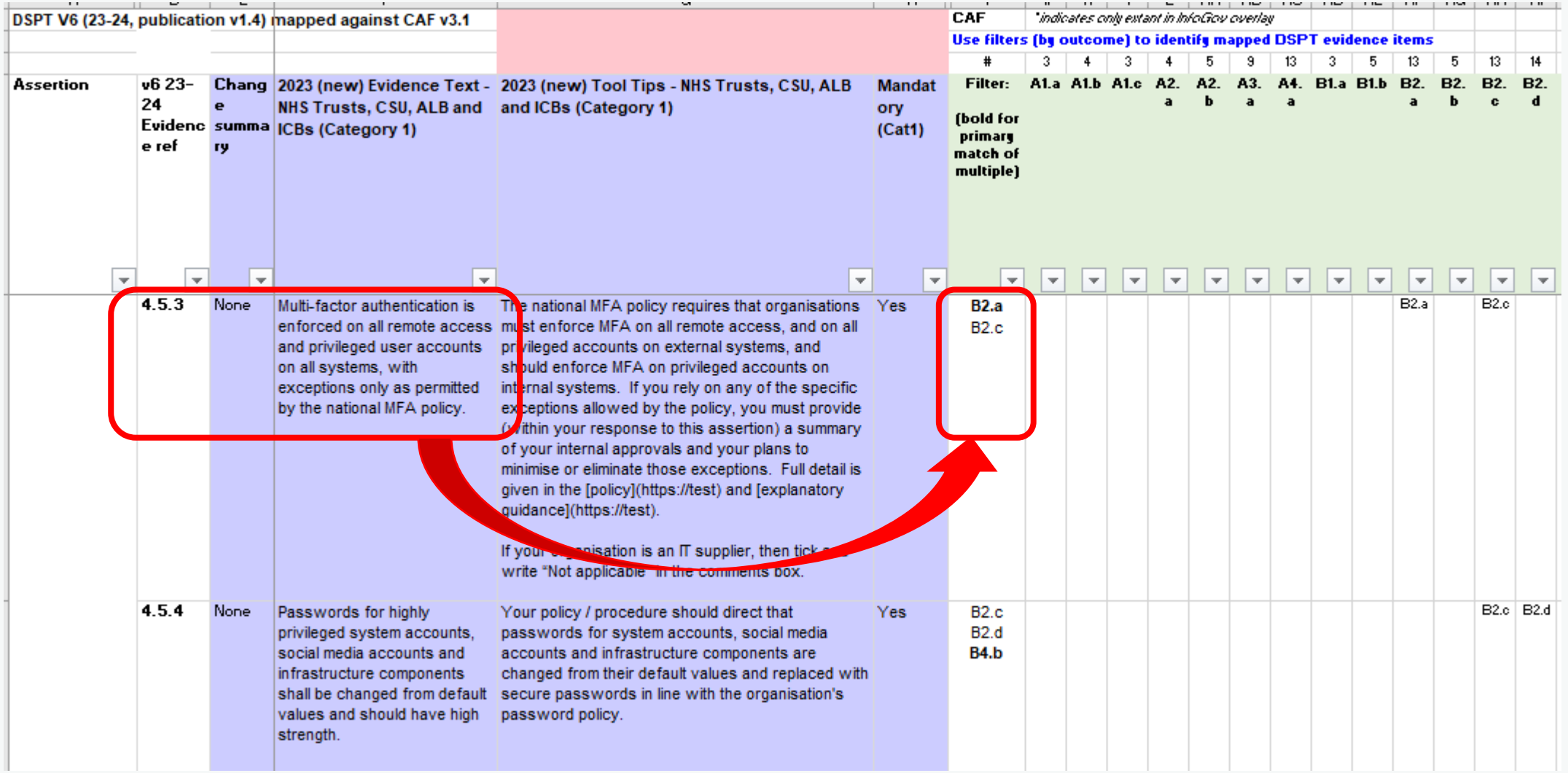
Standards Met in 2024-25

Continuity of expectations

1. DSPT evidence items mapped to CAF outcomes
2. Coverage for each CAF outcome
3. ‘Legacy’ CAF profile *(right)*
4. Proposed ‘year 1’ profile, intended to be ***no less stringent than current DSPT***

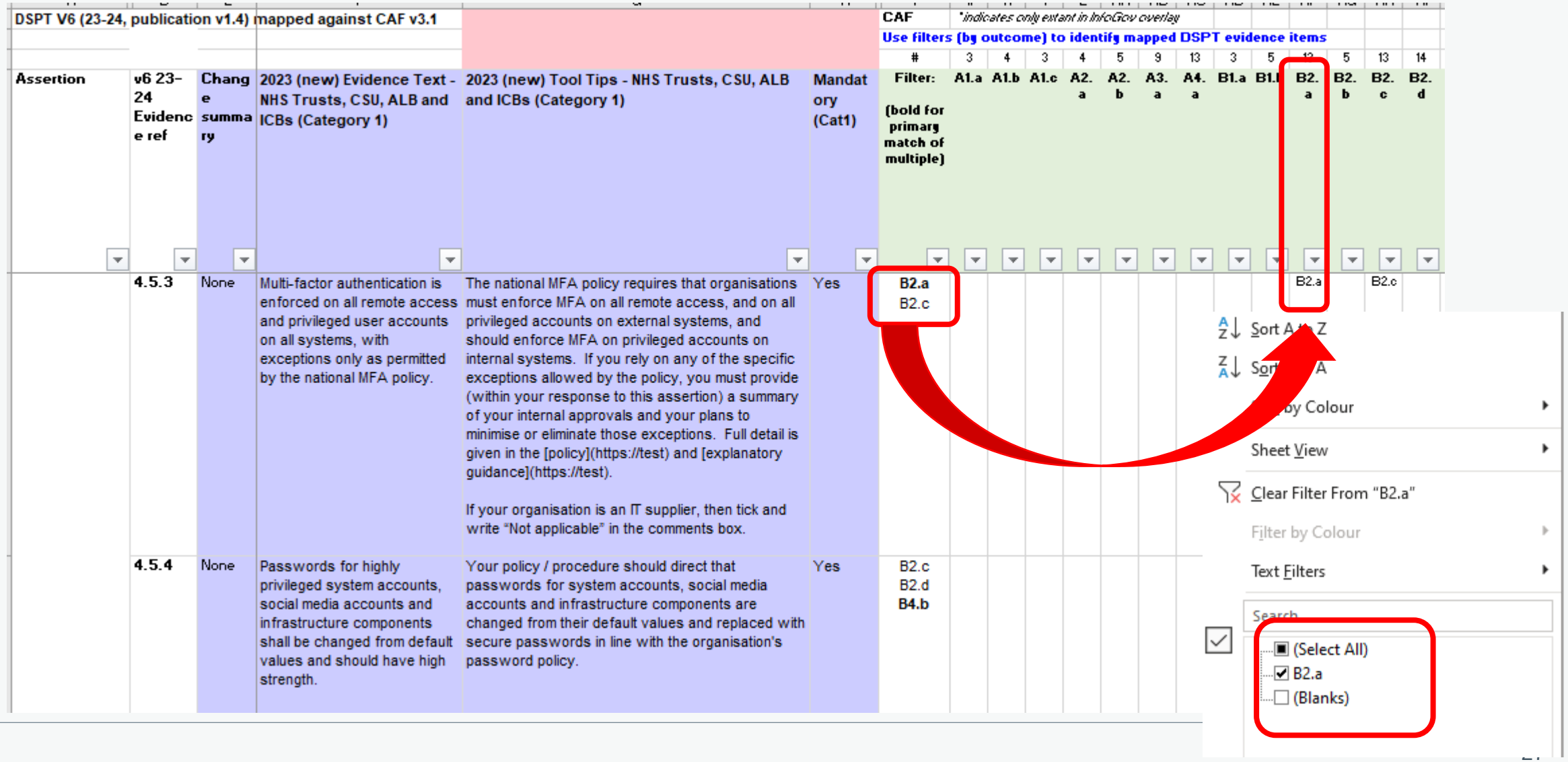
DSPT/CAF outcome		Legacy profile (DSPT v6 'Cat1' mapping)		
Principle	**Outcome**	**NA**	**PA**	**A**
Objective A - Managing risk				
Governance	A1.a Board Direction			
	A1.b Roles and Responsibilities			
	A1.c Decision-making			
Risk Management	A2.a Risk Management Process		<	
	A2.b Assurance			<
Asset Management	A3.a Asset Management			
Supply Chain	A4.a Supply Chain	m	m< nm	

Step 1 – DSPT to CAF mapping



DSPT V6 (23-24, publication v1.4) mapped against CAF v3.1						CAF	*indicates only extant in IoTCoGov overlay											
						Use filters (by outcome) to identify mapped DSPT evidence items												
						#	3	4	3	4	5	9	13	3	5	13	5	13	14
Assertion	v6 23-24 Evidence ref	Change summary	2023 (new) Evidence Text - NHS Trusts, CSU, ALB and ICBs (Category 1)	2023 (new) Tool Tips - NHS Trusts, CSU, ALB and ICBs (Category 1)	Mandatory (Cat1)	Filter: (bold for primary match of multiple)	A1.a	A1.b	A1.c	A2.a	A2.b	A3.a	A4.a	B1.a	B1.b	B2.a	B2.b	B2.c	B2.d
	4.5.3	None	Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.	The national MFA policy requires that organisations must enforce MFA on all remote access, and on all privileged accounts on external systems, and should enforce MFA on privileged accounts on internal systems. If you rely on any of the specific exceptions allowed by the policy, you must provide (within your response to this assertion) a summary of your internal approvals and your plans to minimise or eliminate those exceptions. Full detail is given in the [policy](https://test) and [explanatory guidance](https://test). If your organisation is an IT supplier, then tick and write "Not applicable" in the comments box.	Yes	**B2.a** B2.c										B2.a		B2.c	
	4.5.4	None	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.	Your policy / procedure should direct that passwords for system accounts, social media accounts and infrastructure components are changed from their default values and replaced with secure passwords in line with the organisation's password policy.	Yes	B2.c B2.d **B4.b**												B2.c	B2.d

Step 1 – DSPT to CAF mapping



DSPT V6 (23-24, publication v1.4) mapped against CAF v3.1

CAF — *indicates only extant in IoTCoG overlay

Use filters (by outcome) to identify mapped DSPT evidence items

Assertion	v6 23-24 Evidence ref	Change summary	2023 (new) Evidence Text - NHS Trusts, CSU, ALB and ICBs (Category 1)	2023 (new) Tool Tips - NHS Trusts, CSU, ALB and ICBs (Category 1)	Mandatory (Cat1)	Filter: (bold for primary match of multiple)	A1.a	A1.b	A1.c	A2.a	A2.b	A3.a	A4.a	B1.a	B1.b	B2.a	B2.b	B2.c	B2.d
						#	3	4	3	4	5	9	13	3	5	13	5	13	14
	4.5.3	None	Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.	The national MFA policy requires that organisations must enforce MFA on all remote access, and on all privileged accounts on external systems, and should enforce MFA on privileged accounts on internal systems. If you rely on any of the specific exceptions allowed by the policy, you must provide (within your response to this assertion) a summary of your internal approvals and your plans to minimise or eliminate those exceptions. Full detail is given in the [policy](https://test) and [explanatory guidance](https://test). If your organisation is an IT supplier, then tick and write "Not applicable" in the comments box.	Yes	B2.a B2.c										B2.a		B2.c	
	4.5.4	None	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.	Your policy / procedure should direct that passwords for system accounts, social media accounts and infrastructure components are changed from their default values and replaced with secure passwords in line with the organisation's password policy.	Yes	B2.c B2.d **B4.b**													

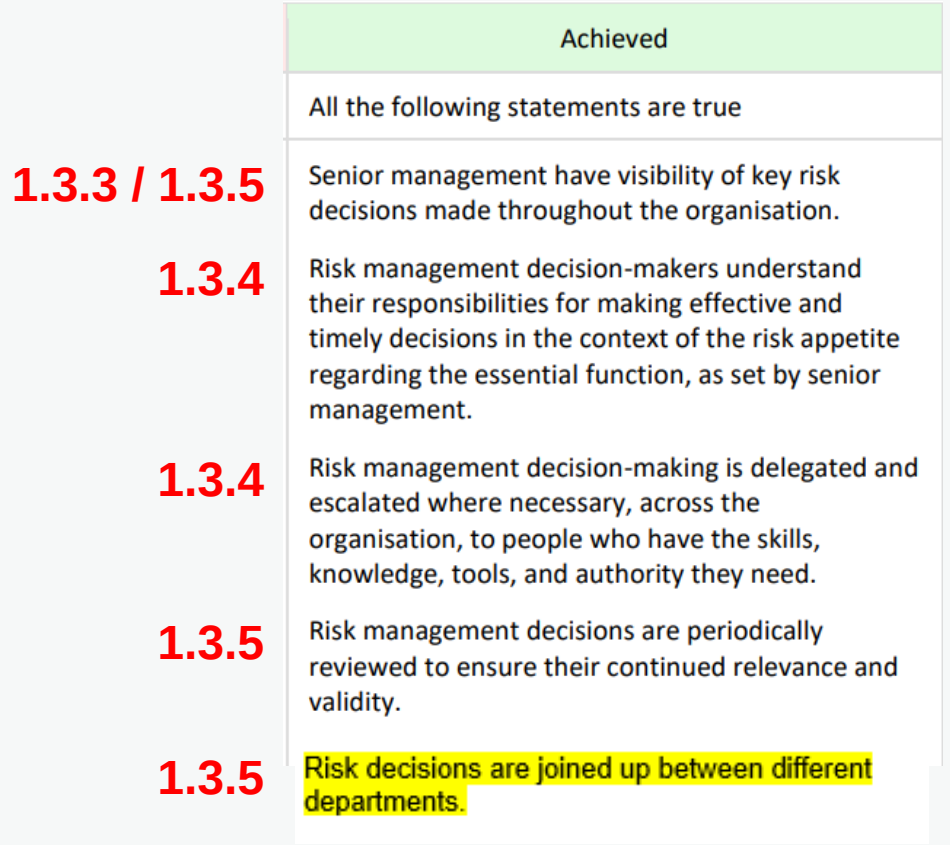
Step 1 example – A1.c Decision-making

DSPT assertions

1.3.3
SIRO responsibility for data security has been assigned.

1.3.4
There are clear documented lines of responsibility and accountability to named individuals for data security and data protection.

1.3.5
Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility.



	Achieved
	All the following statements are true
1.3.3 / 1.3.5	Senior management have visibility of key risk decisions made throughout the organisation.
1.3.4	Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the essential function, as set by senior management.
1.3.4	Risk management decision-making is delegated and escalated where necessary, across the organisation, to people who have the skills, knowledge, tools, and authority they need.
1.3.5	Risk management decisions are periodically reviewed to ensure their continued relevance and validity.
1.3.5	Risk decisions are joined up between different departments.

Step 2 – CAF to DSPT mapping

CAF v3.1 mapped against DSPT V6 (23-24, publication v1.4)

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

Red text indicates proposed additions/amendments to the CAF as part of the DSPT 'information governance CAF overlay' (taken as at 26 Sep 2023; updated for likely clinical coding outcome).

** indicates mapping only extant in InfoGov overlay*

Objective	Principle	Contributing outcome	Indicators	DSPT V6 (() weak ma	Likely coverage of CAF outcome
B - Protecting against cyber attack and data breaches: Proportionate security measures are in place to protect information, systems and networks ~~the networks and information systems~~ supporting essential functions from cyber attack and data breaches.	**B1 ~~Service Protection~~ Policies and Processes:** The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing informationn, systems and data that support operation of essential functions.	**B1.a Policy and Process Development:** You have developed and continue to improve a set of information assurance ~~cyber security~~ and resilience policies and processes that manage and mitigate the risk of adverse impact on the essential function.	RAG	1.3.1 1.3.2 1.3.7*	PA fully met (no non-mand)
		B1.b Policy and Process Implementation: You have successfully implemented your information assurance ~~security~~ policies and processes and can demonstrate the ~~security~~ benefits achieved.	RAG	1.3.1 1.3.2 3.2.2 5.1.1 5.2.1	PA partially met (key issues is PA#2 integration with other organisational policies) (no non-mand)
	B2 Identity and Access Control: The organisation understands, documents and manages access to information, systems and networks ~~network and information systems~~ supporting the operation of essential services. Individuals ~~Users~~ (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.	**B2.a Identity Verification, Authentication and Authorisation:** You robustly verify, authenticate and authorise access to the information, systems and networks ~~networks and information systems~~ supporting your essential function.	RAG	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	PA fully met (no change for non-mand)
		B2.b Device Management: You fully know and have trust in the devices that are used to access your information, systems and networks ~~networks, information systems and data~~ that support your essential function.	RAG	4.3.2 4.4.2 4.4.3 9.3.8 9.3.9	PA partially met (key issue is PA#2 requiring dedicated mgt devices; also PA#1 corporate managed EUDs if non-mand not met) (no change for non-mand)
		B2.c Privileged User Management: You closely manage privileged user access to networks and information systems supporting the essential function.	RAG	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	PA partially met (key issue is PA#3 monitoring and PA#4 permissions) (A partially met with non-mand, except for PA#3 monitoring)

Step 3 – DSPT coverage of CAF outcome

CAF v3.1 mapped against DSPT V6 (23-24, publication v1.4)

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

Red text indicates proposed additions/amendments to the CAF as part of the DSPT 'information governance CAF overlay' (taken as at 26 Sep 2023; updated for likely clinical coding outcome).

** indicates mapping only extant in InfoGov overlay*

Objective	Principle	Contributing outcome	Indicators	DSPT V6	Likely coverage of CAF outcome
B - Protecting against cyber attack and data breaches: Proportionate security measures are in place to protect information, systems and networks ~~the networks and information systems~~ supporting essential functions from cyber attack and data breaches.	**B1 ~~Service Protection~~ Policies and Processes:** The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing informationn, systems and data that support operation of essential functions.	**B1.a Policy and Process Development:** You have developed and continue to improve a set of information assurance ~~cyber security~~ and resilience policies and processes that manage and mitigate the risk of adverse impact on the essential function.	RAG	1.3.1 1.3.2 1.3.7*	PA fully met (no non-mand)
		B1.b Policy and Process Implementation: You have successfully implemented your information assurance ~~security~~ policies and processes and can demonstrate the ~~security~~ benefits achieved.	RAG	1.3.1 1.3.2 3.2.2 5.1.1 5.2.1	PA partially met (key issues is PA#2 integration with other organisational policies) (no non-mand)
	B2 Identity and Access Control: The organisation understands, documents and manages access to information, systems and networks ~~network and information systems~~ supporting the operation of essential services. Individuals ~~Users~~ (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.	**B2.a Identity Verification, Authentication and Authorisation:** You robustly verify, authenticate and authorise access to the information, systems and networks ~~networks and information systems~~ supporting your essential function.	RAG	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	PA fully met (no change for non-mand)
		B2.b Device Management: You fully know and have trust in the devices that are used to access your information, systems and networks ~~networks, information systems and data~~ that support your essential function.	RAG	4.3.2 4.4.2 4.4.3 9.3.8 9.3.9	PA partially met (key issue is PA#2 requiring dedicated mgt devices; also PA#1 corporate managed EUDs if non-mand not met) (no change for non-mand)
		B2.c Privileged User Management: You closely manage privileged user access to networks and information systems supporting the essential function.	RAG	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	PA partially met (key issue is PA#3 monitoring and PA#4 permissions) (A partially met with non-mand, except for PA#3 monitoring)

Step 4 – ‘Legacy’ CAF profile from DSPT

DSPT/CAF outcome		Legacy profile (DSPT v6 'Cat1' mapping)		
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			
	B1.b Policy and Process Implementation		<	
Identity and Access Control	B2.a Identity Verification, Authentication and Authorisation			<
	B2.b Device Management		<	
	B2.c Privileged User Management		<	<
	B2.d Identity and Access Management (IdAM)	m	m< nm	

< means level partially met

m means DSPT mandatory items

nm means DSPT non-mandatory items

Step 5 – increased outcomes and gap analysis

DSPT/CAF outcome		Legacy profile (DSPT v6 'Cat1' mapping)			Proposed 'Year 1' profile for larger NHS organisations and non-CNI-operating arm's length bodies *(NHS trusts and foundation trusts, integrated care boards, commissioning support units, and non-CNI arm's length bodies)*			
Principle	**Outcome**	**NA**	**PA**	**A**	**Level**	**Remarks**	**Gap analysis (to increase to at least PA)**	**Challenge**
Objective B - Protecting against cyber attack and data breaches								
Service Protection Policies and Processes	B1.a Policy and Process Development				(as legacy)		-	-
	B1.b Policy and Process Implementation		<		PA	**Why increase:** gap analysis (right) shows low challenge to increase to PA.	Integration with other organisational policies (PA#2)	Low
Identity and Access Control	B2.a Identity Verification, Authentication and Authorisation			<	(as legacy)		-	-
	B2.b Device Management		<		(as legacy)	Gap analysis (right) shows significant challenge to increase to PA.	Corporately managed EUDs (PA#1 - for discussion; views welcomed re. BYOD and cf. PA#3) and dedicated devices for management functions (PA#2)	Moderate
	B2.c Privileged User Management		<	<	(as legacy)	Gap analysis (right) shows significant challenge to increase to PA.	Monitoring (PA#3) and specific permissions (PA#4)	Moderate
	B2.d Identity and Access Management (IdAM)	m	m< nm		PA	**Why increase:** gap analysis (right) shows low challenge to increase to PA.	Least privilege (PA#1)	Low

Proposed increase over legacy profile

No proposed change over legacy profile (reasons vary)

Step 5 example – A2.a Risk Management Process

Legacy:
NA (some PA)

Proposal:
PA

Gap analysis:
Link from risk assessment to controls (PA#1,3)

Challenge:
Low

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Risk assessments are not based on a clearly defined set of threat assumptions. Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner. Risk assessments for critical systems are a "one-off" activity or not done at all. The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes. There is no systematic process in place to ensure that identified security risks are managed effectively.	Your organisational process ensures that security risks to networks and information systems relevant to essential functions are identified, analysed, prioritised, and managed. Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential function. The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security. Significant conclusions	Your organisational process ensures that security risks to networks and information systems relevant to essential functions are identified, analysed, prioritised, and managed. Your approach to risk is focused on the possibility of adverse impact to your essential function, leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your networks and information systems. Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function and your sector. Your risk assessments are

Step 5 example – A4.a Supply Chain

Legacy:
Mandatory: NA
Non-mandatory: PA

Proposal:
PA

Gap analysis:
Contracts (PA#3), assurances (PA#4,6) and consideration of incidents (PA#5)

Challenge:
Moderate

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You do not know what data belonging to you is held by suppliers, or how it is managed. Elements of the supply chain for essential functions are subcontracted and you have little or no visibility of the sub-contractors. You have no understanding of which contracts are relevant and / or relevant contracts do not specify appropriate security obligations. Suppliers have access to systems that provide your essential function that is unrestricted, not monitored or bypasses your own security controls.	You understand the general risks suppliers may pose to your essential functions. You know the extent of your supply chain for essential functions, including sub-contractors. You understand which contracts are relevant and you include appropriate security obligations in relevant contracts. You are aware of all third-party connections and have assurance that they meet your organisation's security requirements. Your approach to security incident management considers incidents that might arise in your supply chain. You have confidence that information shared with suppliers that is necessary for the operation of your essential function is appropriately protected from well-known attacks and known vulnerabilities.	You have a deep understanding of your supply chain, including sub-contractors and the wider risks it faces. You consider factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your risk assessment and procurement processes. Your approach to supply chain risk management considers the risks to your essential functions arising from supply chain subversion by capable and well-resourced attackers. You have confidence that information shared with suppliers that is essential to the operation of your function is appropriately protected from sophisticated attacks. You understand which contracts are relevant and you include appropriate security obligations in relevant contracts. You have a proactive approach to contract management which may include a contract management plan for relevant contracts.

Expectations for Standards met:

Objective A - Managing risk

CAF element		Profile		
Principle	**Outcome**	**NA**	**PA**	**A**
Objective A - Managing risk				
Governance	A1.a Board Direction			A
	A1.b Roles and Responsibilities			A
	A1.c Decision-making			A
Risk Management	A2.a Risk Management Process		PA	
	A2.b Assurance			A
Asset Management	A3.a Asset Management			A
Supply Chain	A4.a Supply Chain		PA	

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

Expectations for Standards met:

Objective C - Detecting cyber security events

CAF element		Profile		
Principle	Outcome	NA	PA	A
Objective C - Detecting cyber security events				
Security Monitoring	C1.a Monitoring Coverage		PA	
	C1.b Securing Logs		PA	
	C1.c Generating Alerts		PA	
	C1.d Identifying Security Incidents		PA	
	C1.e Monitoring Tools and Skills	NA		
Proactive Security Event Discovery	C2.a System Abnormalities for Attack Detection	NA		
	C2.b Proactive Attack Discovery	NA		

Expectations for Standards met:

Objective D - Minimising the impact of incidents

CAF element		Profile		
Principle	**Outcome**	**NA**	**PA**	**A**
Objective D - Minimising the impact of incidents				
Response and Recovery Planning	D1.a Response Plan		PA	
	D1.b Response and Recovery Capability			A
	D1.c Testing and Exercising			A
Lessons Learned	D2.a Incident Root Cause Analysis			A
	D2.b Using Incidents to Drive Improvements			A

Expectations for Standards met:

Objective E - Using and sharing information appropriately

CAF element		Profile		
Principle	**Outcome**	**Not Achieved (NA)**	**Partially Achieved (PA)**	**Achieved (A)**
Objective E - Using and sharing information appropriately				
Transparency	E1.a Privacy and transparency information		PA	
Upholding the rights of individuals	E2.a Managing data subject rights under UK GDPR			A
	E2.b Consent			A
	E2.c National data opt-out policy			A
Using and sharing information	E3.a Using and sharing information for direct care			A
	E3.b Using and sharing information for other purposes			A
Records management	E4.a Managing records			A
	E4.b Clinical coding			A

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.

Planning for DSPT in 2024-25

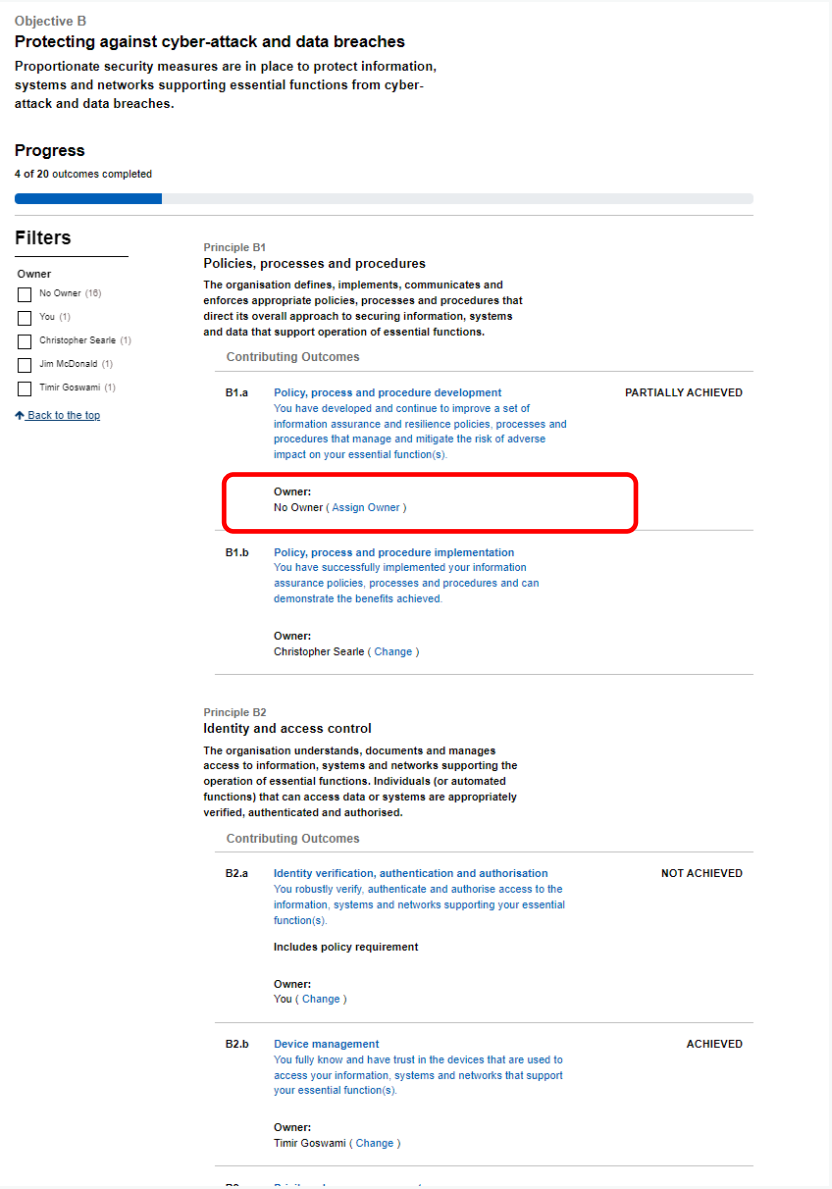
Allocating Owners

Each Outcome can be allocated an owner

Owner must be a user on the DSPT

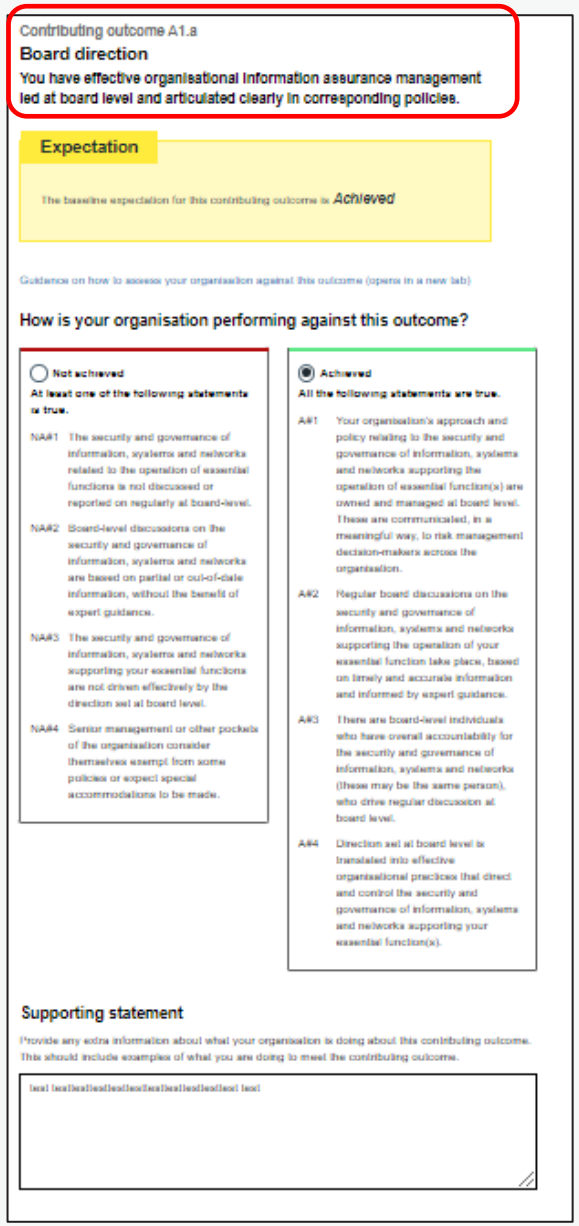
This links to the filters

Owners and admins can Save as complete



Completing the assessment

Each Outcome has a reference number and a separate page



Contributing outcome A1.a

Board direction

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

Expectation

The baseline expectation for this contributing outcome is *Achieved*

Guidance on how to assess your organisation against this outcome (opens in a new tab)

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

NA#1 The security and governance of information, systems and networks related to the operation of essential functions is not discussed or reported on regularly at board-level.

NA#2 Board-level discussions on the security and governance of information, systems and networks are based on partial or out-of-date information, without the benefit of expert guidance.

NA#3 The security and governance of information, systems and networks supporting your essential functions are not driven effectively by the direction set at board level.

NA#4 Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.

Achieved

All the following statements are true.

A#1 Your organisation's approach and policy relating to the security and governance of information, systems and networks supporting the operation of essential function(s) are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.

A#2 Regular board discussions on the security and governance of information, systems and networks supporting the operation of your essential function take place, based on timely and accurate information and informed by expert guidance.

A#3 There are board-level individuals who have overall accountability for the security and governance of information, systems and networks (these may be the same person), who drive regular discussion at board level.

A#4 Direction set at board level is translated into effective organisational practices that direct and control the security and governance of information, systems and networks supporting your essential function(s).

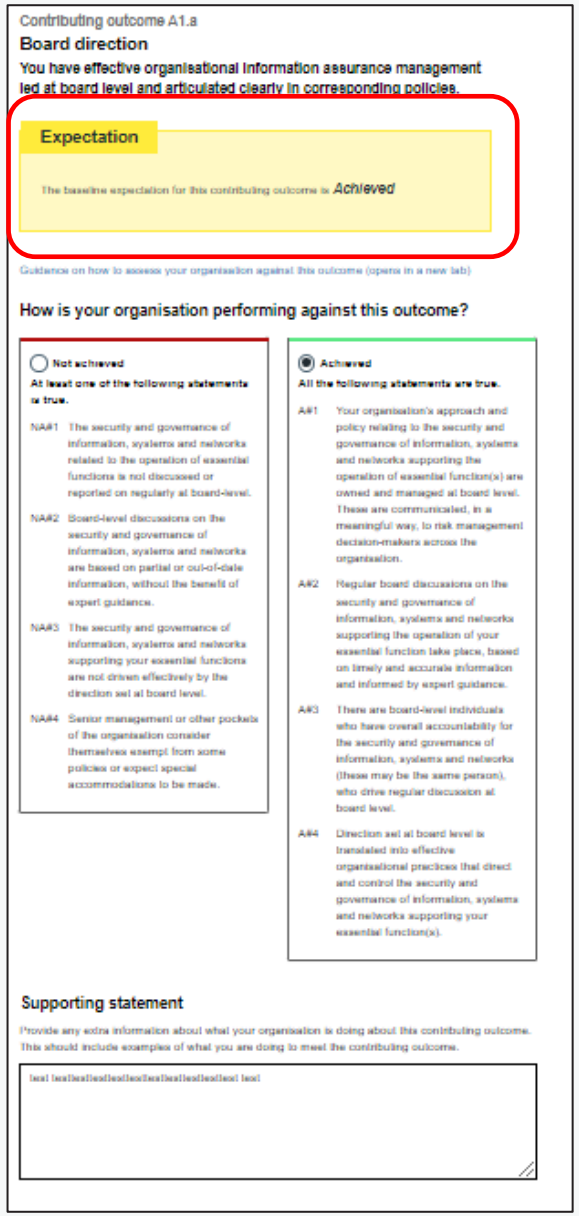
Supporting statement

Provide any extra information about what your organisation is doing about this contributing outcome. This should include examples of what you are doing to meet the contributing outcome.

Completing the assessment

Each Outcome has a reference number and a separate page

The expected achievement level is emphasised


Contributing outcome A1.a

Board direction

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

Expectation

The baseline expectation for this contributing outcome is *Achieved*

Guidance on how to assess your organisation against this outcome (opens in a new tab)

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

NA#1 The security and governance of information, systems and networks related to the operation of essential functions is not discussed or reported on regularly at board-level.

NA#2 Board-level discussions on the security and governance of information, systems and networks are based on partial or out-of-date information, without the benefit of expert guidance.

NA#3 The security and governance of information, systems and networks supporting your essential functions are not driven effectively by the direction set at board level.

NA#4 Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.

Achieved

All the following statements are true.

A#1 Your organisation's approach and policy relating to the security and governance of information, systems and networks supporting the operation of essential function(s) are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.

A#2 Regular board discussions on the security and governance of information, systems and networks supporting the operation of your essential function take place, based on timely and accurate information and informed by expert guidance.

A#3 There are board-level individuals who have overall accountability for the security and governance of information, systems and networks (these may be the same person), who drive regular discussion at board level.

A#4 Direction set at board level is translated into effective organisational practices that direct and control the security and governance of information, systems and networks supporting your essential function(s).

Supporting statement

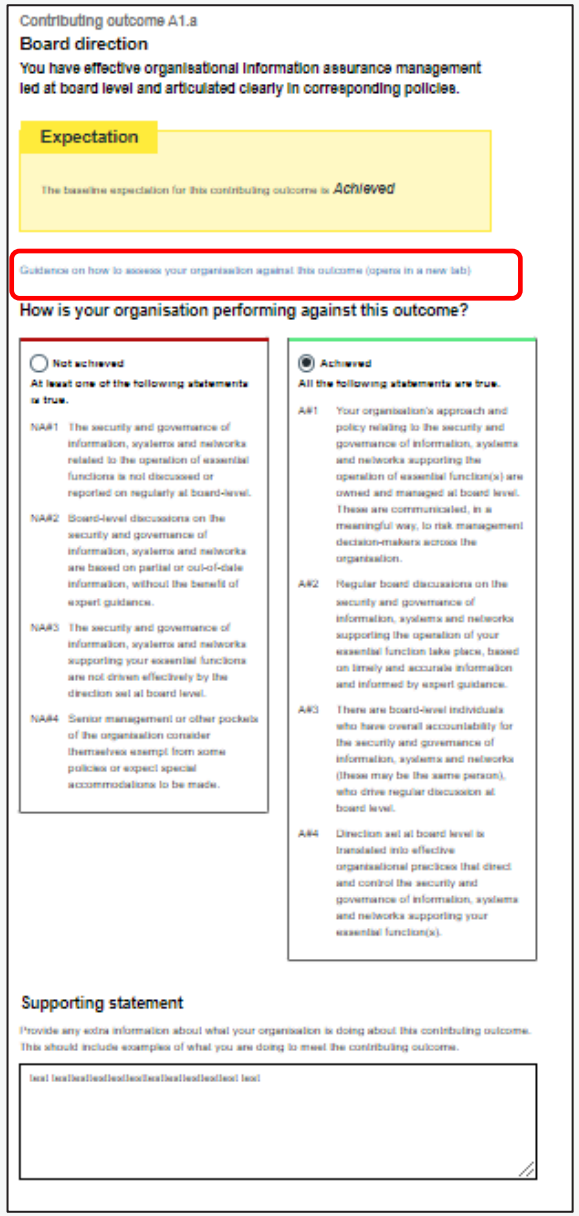
Provide any extra information about what your organisation is doing about this contributing outcome. This should include examples of what you are doing to meet the contributing outcome.

Completing the assessment

Each Outcome has a reference number and a separate page

The expected achievement level is emphasised

Each Outcome has a link to the guidance


Contributing outcome A1.a

Board direction

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

Expectation

The baseline expectation for this contributing outcome is *Achieved*

Guidance on how to assess your organisation against this outcome (opens in a new tab)

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

NA#1 The security and governance of information, systems and networks related to the operation of essential functions is not discussed or reported on regularly at board-level.

NA#2 Board-level discussions on the security and governance of information, systems and networks are based on partial or out-of-date information, without the benefit of expert guidance.

NA#3 The security and governance of information, systems and networks supporting your essential functions are not driven effectively by the direction set at board level.

NA#4 Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.

Achieved

All the following statements are true.

A#1 Your organisation's approach and policy relating to the security and governance of information, systems and networks supporting the operation of essential function(s) are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.

A#2 Regular board discussions on the security and governance of information, systems and networks supporting the operation of your essential function take place, based on timely and accurate information and informed by expert guidance.

A#3 There are board-level individuals who have overall accountability for the security and governance of information, systems and networks (these may be the same person), who drive regular discussion at board level.

A#4 Direction set at board level is translated into effective organisational practices that direct and control the security and governance of information, systems and networks supporting your essential function(s).

Supporting statement

Provide any extra information about what your organisation is doing about this contributing outcome. This should include examples of what you are doing to meet the contributing outcome.

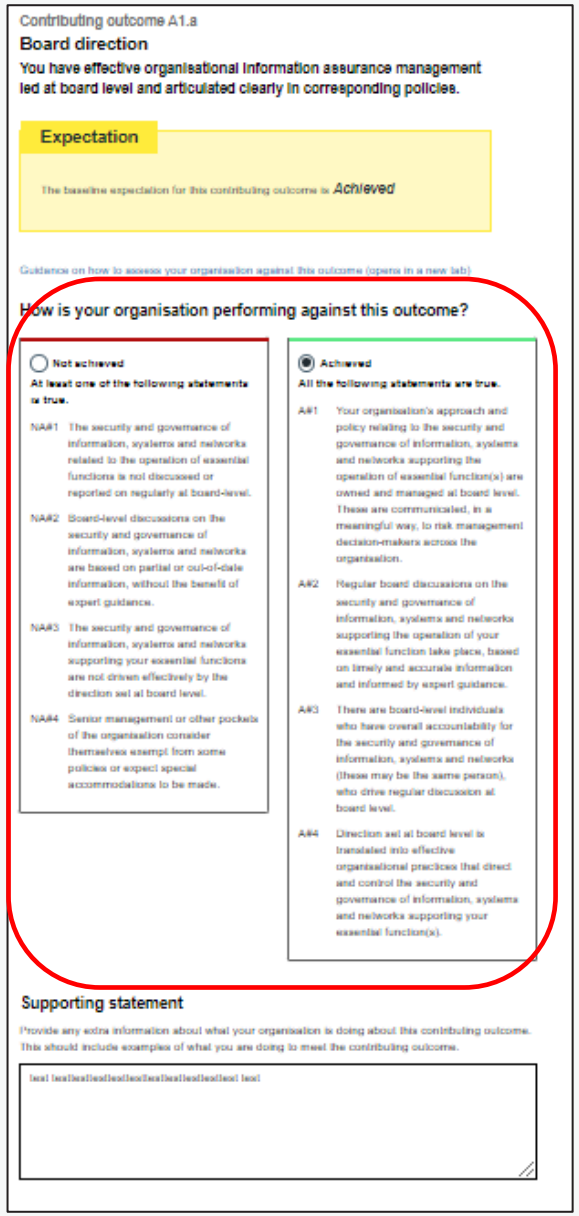
Completing the assessment

Each Outcome has a reference number and a separate page

The expected achievement level is emphasised

Each Outcome has a link to the guidance

The achievement level has indicators of good practice with reference numbers


Contributing outcome A1.a

Board direction

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

Expectation

The baseline expectation for this contributing outcome is *Achieved*

Guidance on how to assess your organisation against this outcome (opens in a new tab)

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

NA#1 The security and governance of information, systems and networks related to the operation of essential functions is not discussed or reported on regularly at board-level.

NA#2 Board-level discussions on the security and governance of information, systems and networks are based on partial or out-of-date information, without the benefit of expert guidance.

NA#3 The security and governance of information, systems and networks supporting your essential functions are not driven effectively by the direction set at board level.

NA#4 Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.

Achieved

All the following statements are true.

A#1 Your organisation's approach and policy relating to the security and governance of information, systems and networks supporting the operation of essential function(s) are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.

A#2 Regular board discussions on the security and governance of information, systems and networks supporting the operation of your essential function take place, based on timely and accurate information and informed by expert guidance.

A#3 There are board-level individuals who have overall accountability for the security and governance of information, systems and networks (these may be the same person), who drive regular discussion at board level.

A#4 Direction set at board level is translated into effective organisational practices that direct and control the security and governance of information, systems and networks supporting your essential function(s).

Supporting statement

Provide any extra information about what your organisation is doing about this contributing outcome. This should include examples of what you are doing to meet the contributing outcome.

Completing the assessment

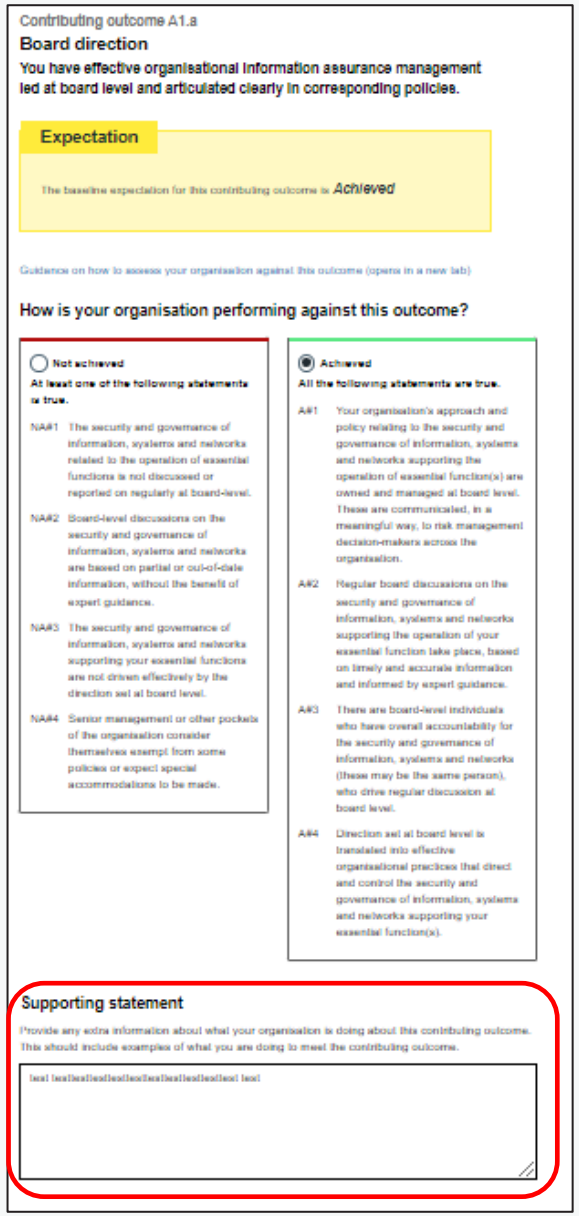
Each Outcome has a reference number and a separate page

The expected achievement level is emphasised

Each Outcome has a link to the guidance

The achievement level has indicators of good practice with reference numbers

The outcome must have a Supporting Statement


Contributing outcome A1.a

Board direction

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

Expectation

The baseline expectation for this contributing outcome is *Achieved*

Guidance on how to assess your organisation against this outcome (opens in a new tab)

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

NA#1 The security and governance of information, systems and networks related to the operation of essential functions is not discussed or reported on regularly at board-level.

NA#2 Board-level discussions on the security and governance of information, systems and networks are based on partial or out-of-date information, without the benefit of expert guidance.

NA#3 The security and governance of information, systems and networks supporting your essential functions are not driven effectively by the direction set at board level.

NA#4 Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.

Achieved

All the following statements are true.

A#1 Your organisation's approach and policy relating to the security and governance of information, systems and networks supporting the operation of essential function(s) are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.

A#2 Regular board discussions on the security and governance of information, systems and networks supporting the operation of your essential function take place, based on timely and accurate information and informed by expert guidance.

A#3 There are board-level individuals who have overall accountability for the security and governance of information, systems and networks (these may be the same person), who drive regular discussion at board level.

A#4 Direction set at board level is translated into effective organisational practices that direct and control the security and governance of information, systems and networks supporting your essential function(s).

Supporting statement

Provide any extra information about what your organisation is doing about this contributing outcome. This should include examples of what you are doing to meet the contributing outcome.

Supporting Statement

Each Outcome requires a supporting statement to enable you to Save as Complete

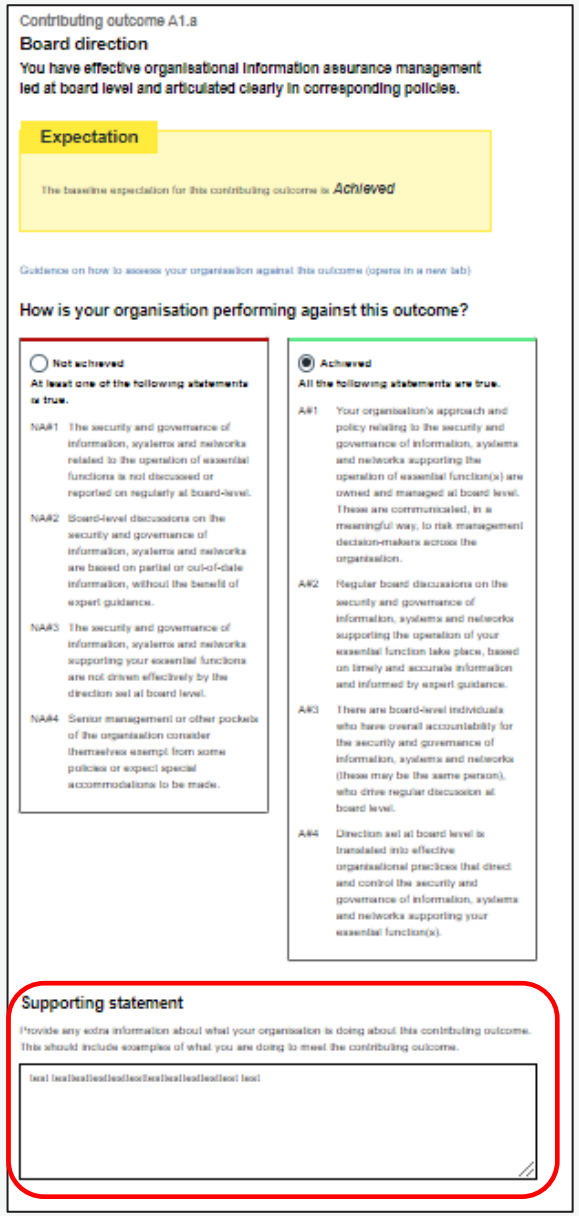
Should justify your decision on achievement level

Should help your SIRO, an auditor, DHSC/NHS England or your team understand the decision

Cross reference to evidence and include details of decision makers

The achievement level has indicators of good practice with reference numbers

Example supporting statements will form part of guidance materials

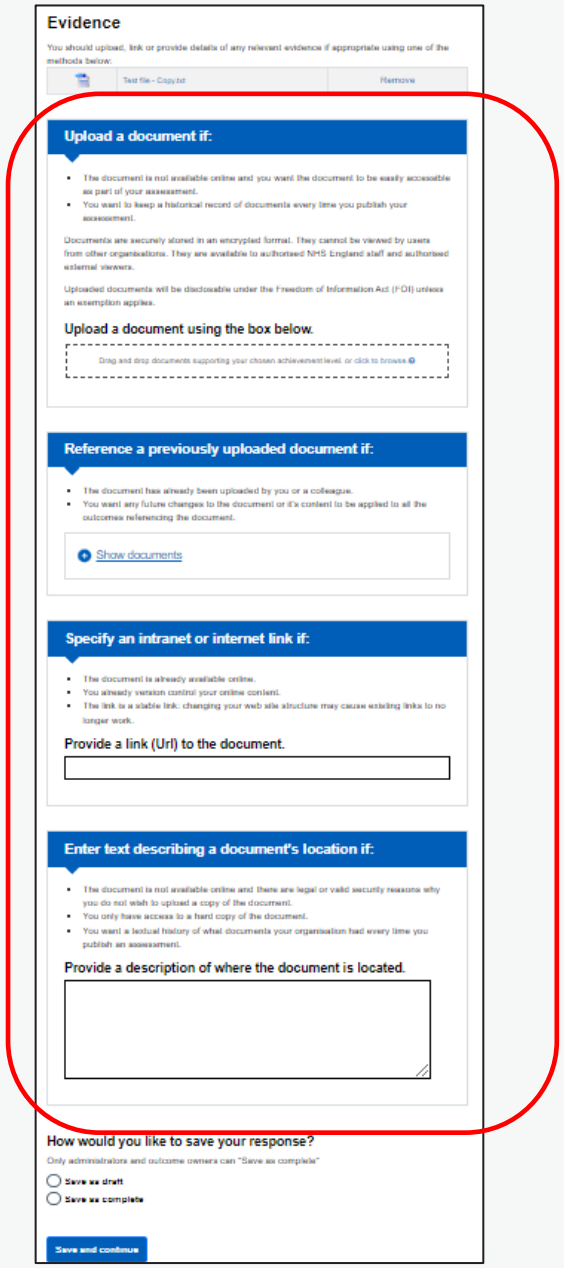


Evidence the assessment

For every outcome you can include:

Uploaded documents
Internet/Intranet links
Text

Uploading documents is optional and you can Save as complete without uploading any documents

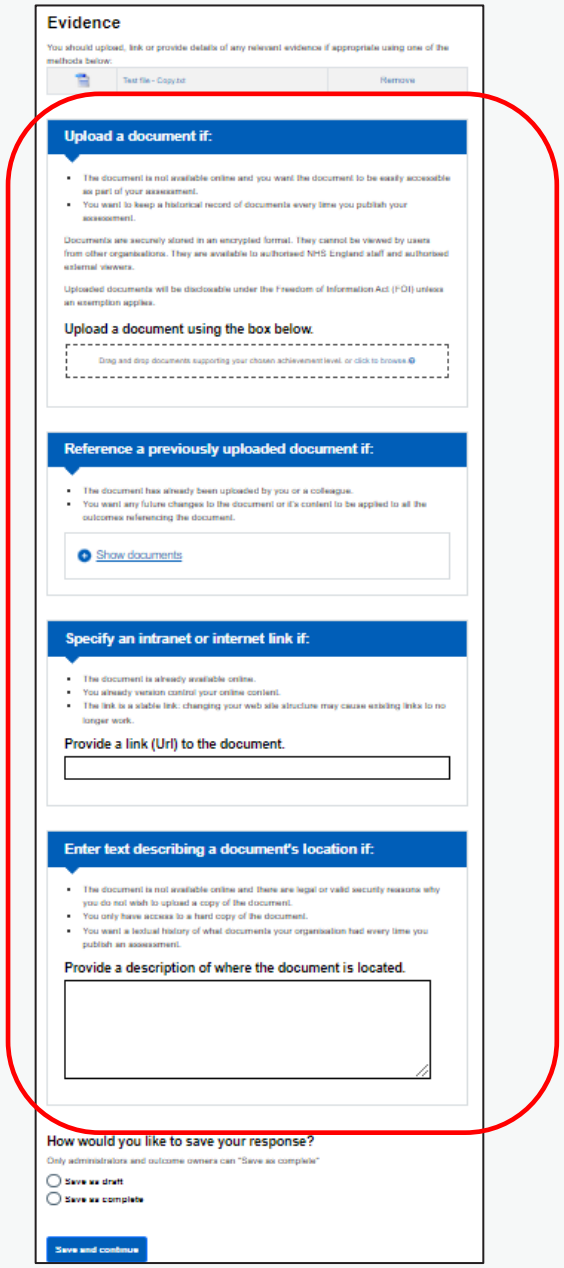


Evidence the assessment

Use evidence to justify your decision on achievement level

Should help your SIRO, an auditor, DHSC/NHS England or your team understand the decision

Securely stored and NOT releasable under Freedom of Information

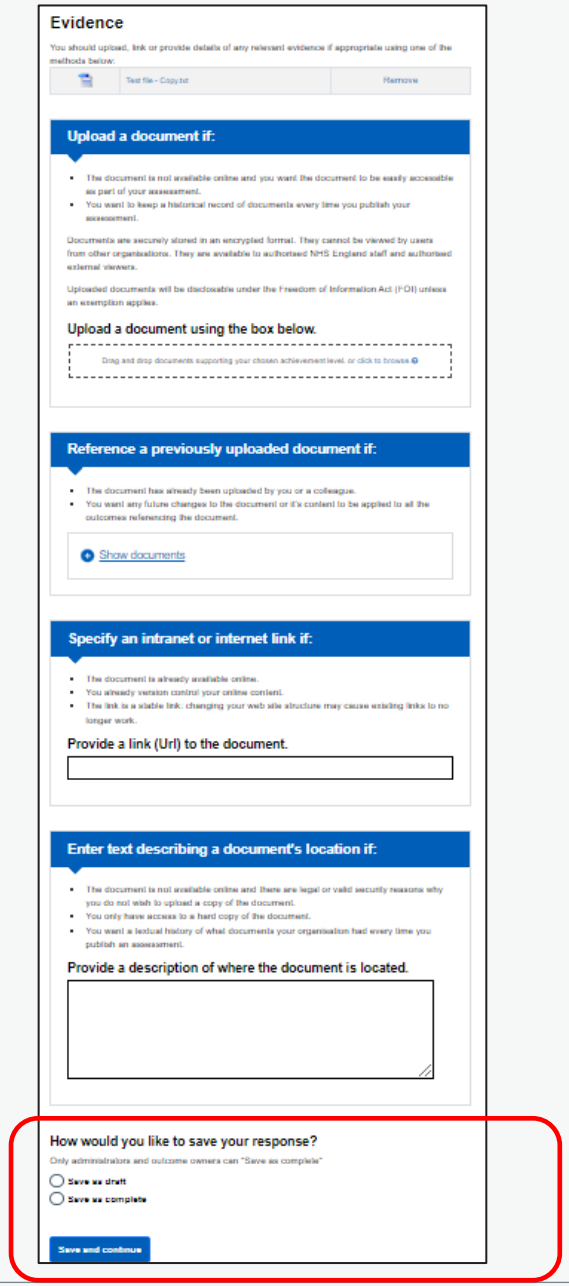


Saving the assessment as you go

For each outcome you can :

Save as draft
or
Save as complete

You cannot publish until all outcomes are marked as Save as complete



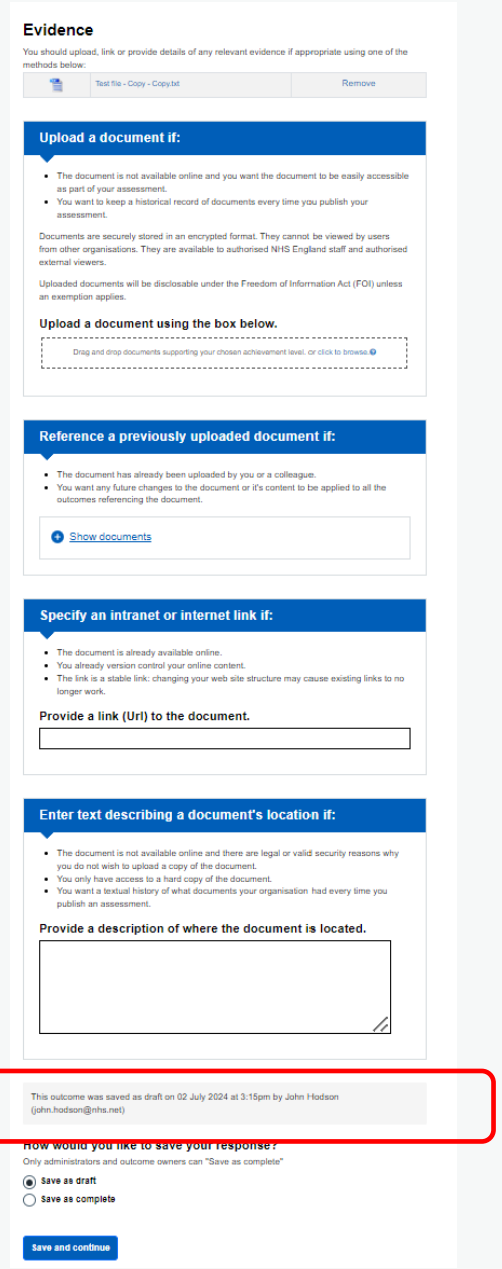
Seeing who last updated the outcome

For each outcome you can :

See who last updated it

And

When it was last updated

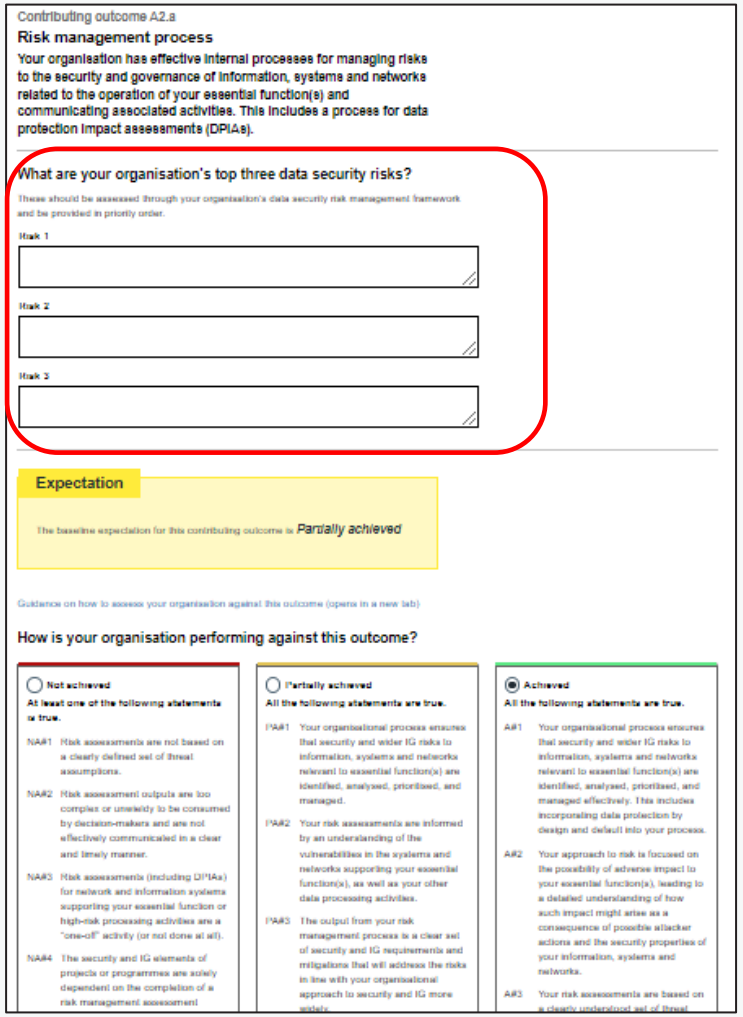


Specific Data Collections

In a few specific areas, the CAF will be bolstered by explicitly-worded data collections which users will need to provide to meet an outcome

These are in Unsupported systems, and Top 3 Data Security Risks

You cannot Save as complete until the data collection is complete



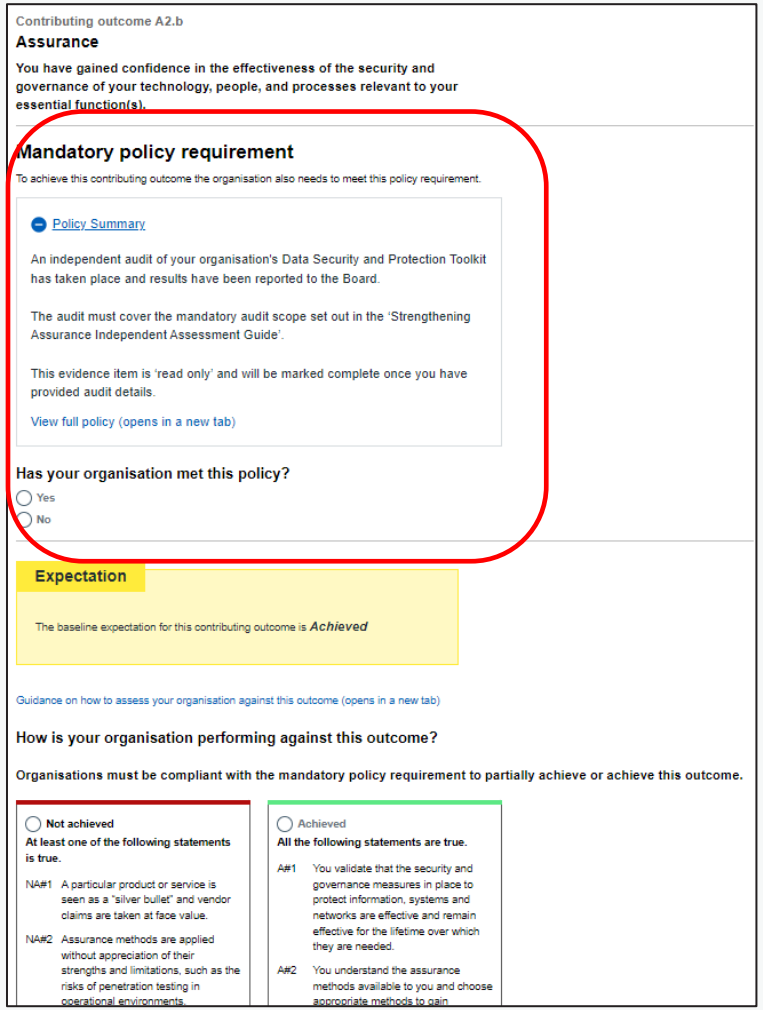
Policy Collections

In a few specific outcomes, the DSPT will be bolstered by explicitly-worded policy requirements

These are in Audit, Multi-Factor Authentication and Responding to a cyber alert

You cannot meet the outcome achievement level without meeting the policy requirement

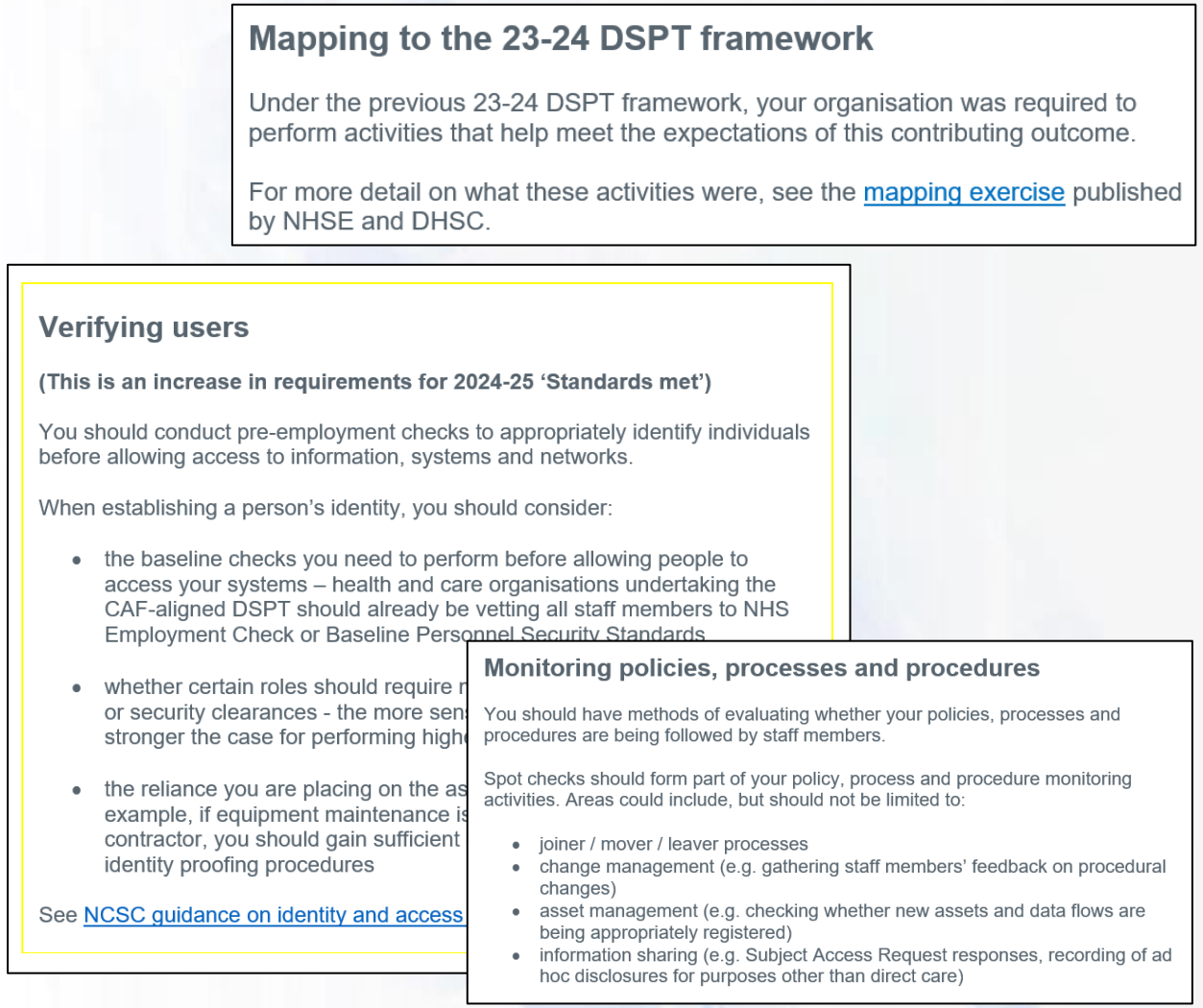
You cannot Save as complete until the policy requirement is answered



Guidance

Approach (1/2)

- pointing toolkit users to practices they are already doing under the current DSPT regime, highlighting where those practices fall in the new CAF-based framework
- highlighting areas where the CAF-based requirements go beyond the current DSPT regime
- providing brief summaries of key concepts where relevant, such as risk assessments, key data protection and security roles (but not going into great detail, ensuring specific decisions are left to judgment of organisations)



Mapping to the 23-24 DSPT framework

Under the previous 23-24 DSPT framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHSE and DHSC.

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
or security clearances - the more sen
stronger the case for performing high
- the reliance you are placing on the as
example, if equipment maintenance is
contractor, you should gain sufficient
identity proofing procedures

See NCSC guidance on identity and access

Monitoring policies, processes and procedures

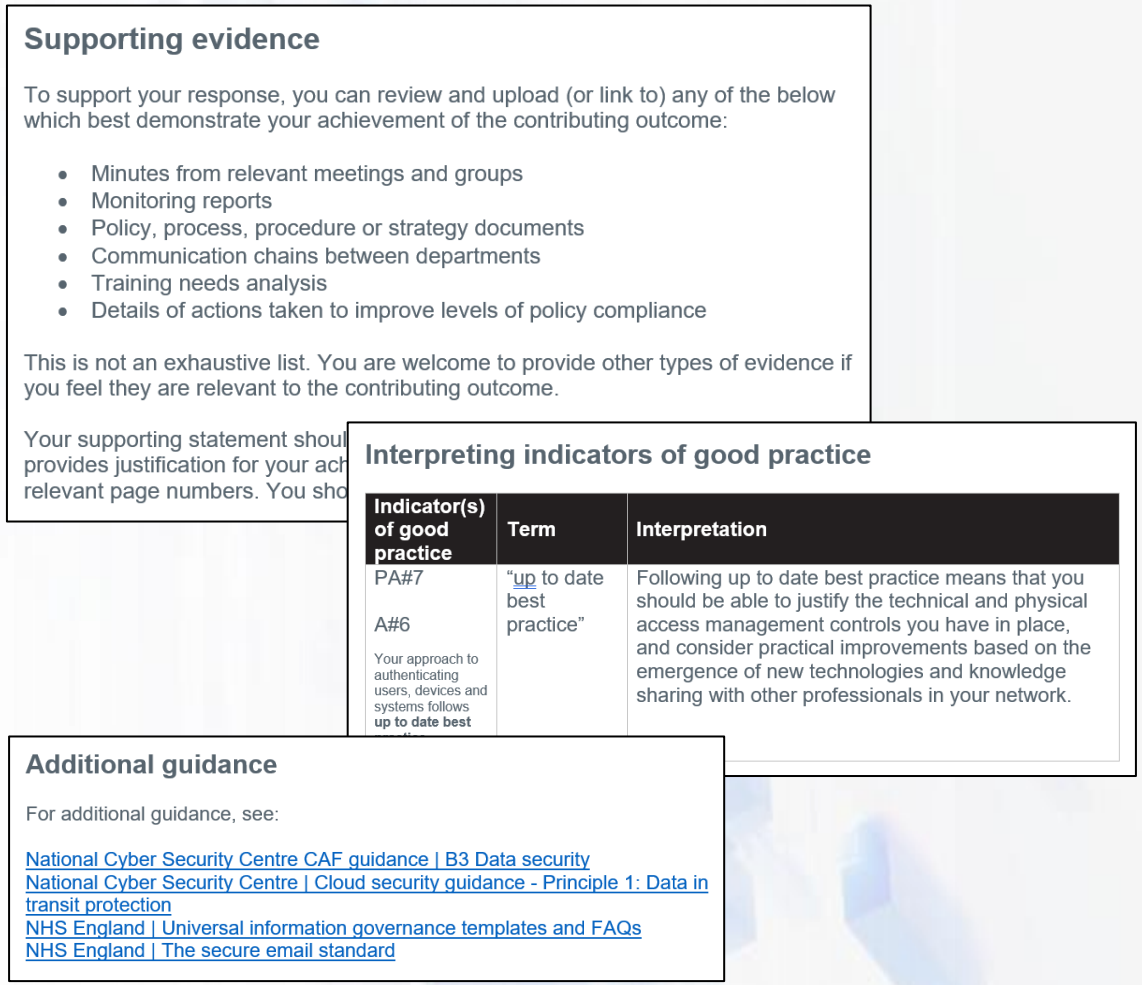
You should have methods of evaluating whether your policies, processes and procedures are being followed by staff members.

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)

Approach (2/2)

- suggesting evidence for toolkit users to upload to support their responses
- giving interpretations of specific terms within the indicators of practice
- linking to external guidance from authoritative sources such as NCSC and ICO



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 shoul
provides justification for your ach
relevant page numbers. You sho

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**	"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.

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

Stakeholder review (A Big Thank You)

Group: Frontline professionals, wider NHS & external stakeholders
Consulted on: Clarity and overall approach of the CAF-aligned DSPT guidance
Result: Sections added, clarification on key concepts & terms

Stakeholders involved:

National Data Guardian	Information Commissioner's Office	Health Research Authority	Care Quality Commission	NHS Privacy, Transparency, Trust team	National Cyber Security Centre	NHS Counter Fraud Authority
Meds & Hlthcare Products Reg Agency	Human Fert'tion and Embryology Authority	National Institute for Health & Care Excellence	NHS Business Services Authority	DSPT Working Group	UK Health Security Agency	Human Tissue Authority
NHS Resolution	NHS Blood & Transplant	T&F frontline professionals				

Demonstration

Question and answer session

Next webinars

Date and time	Topics to be covered
Tuesday 9th July 10:00 – 11:30	**Objective A – managing risk**
Thursday 18th July 10:00 – 11:30	Objective B – Protecting against cyber attack and data breaches
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

Thank You

@nhsengland

company/nhsengland

england.nhs.uk