Data Security and Protection Toolkit

DSPT 2023-24 and a bit of 24-25

15 May 2024

John Hodson

DSPT 2023-24

DSP Toolkit 23-24

Fully Incorporated in DSPT.
Big Picture Guides
Minor Changes overall

Biggest change is to the Data Security Awareness requirement

Update Tooltips based on feedback

Final Publication 30th June 2024

There will be an improvement plan process released today

Additional requirements for key IT Suppliers and Operators of Essential Service under NIS who are not NHS organisations

Training

To meet the DSP Toolkit

3.1.1 Training and awareness activities form part of organisational mandatory training requirements, with a training and awareness needs analysis (covering all staff roles) that is formally endorsed and resourced by senior leadership

Step 1 Mandatory requirement

- Information governance and Cyber training must form part of organisations mandatory training
- A TNA saying the organisation does not require staff to complete any training or awareness activities would not meet the requirement.

Step 2 – Documented Training Needs Analysis

- Covering all staff groups and roles within the organisation
- Should show different methods used (e.g., formal training, eLearning, awareness campaigns etc.,)
- Specimen TNA available
- **Organisation controls frequency and type of training and awareness**
- Can utilise local and central resources
- Reference historic training

Step 3 – Endorsed and resourced by senior leadership

- Should not be developed by the IG and Cyber teams in isolation.
- May take some time to agree
- Organisations take on more responsibility for deciding levels of training
- You will be accountable to the Board for delivering so ensure you can answer the how are we going to be able to deliver this question.

To meet the DSP Toolkit

3.1.2 Your organisation's defined training and awareness activities are implemented for and followed by all staff.

Step 1 Implement TNA

- Tracking achievement of TNA may be more challenging
- Resource required to calculate it and report to the organisation

Step 2 – If it is your TNA, it needs measuring.

- Document initial training and refresher training
- All staff roles and training
- Specimen TNA and guidance available: https://www.dsptoolkit.nhs.uk/News/Training

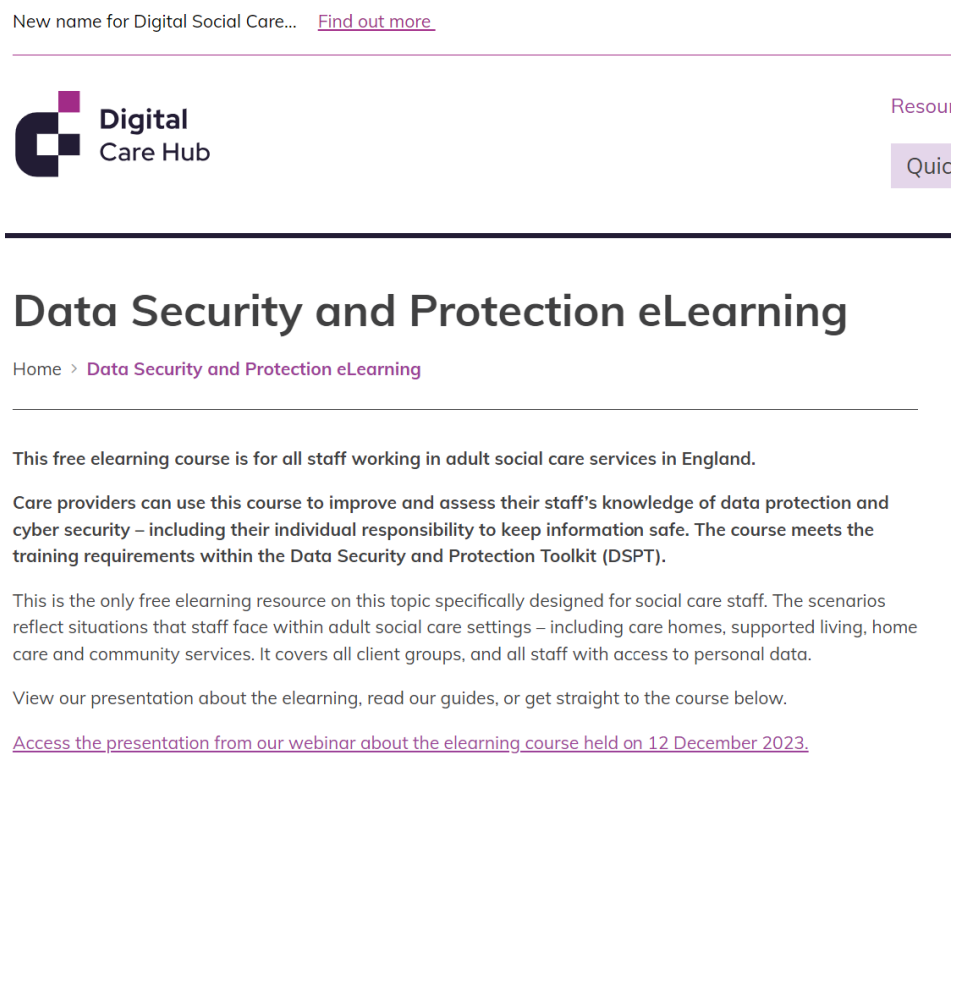
Step 3 – Plan reporting

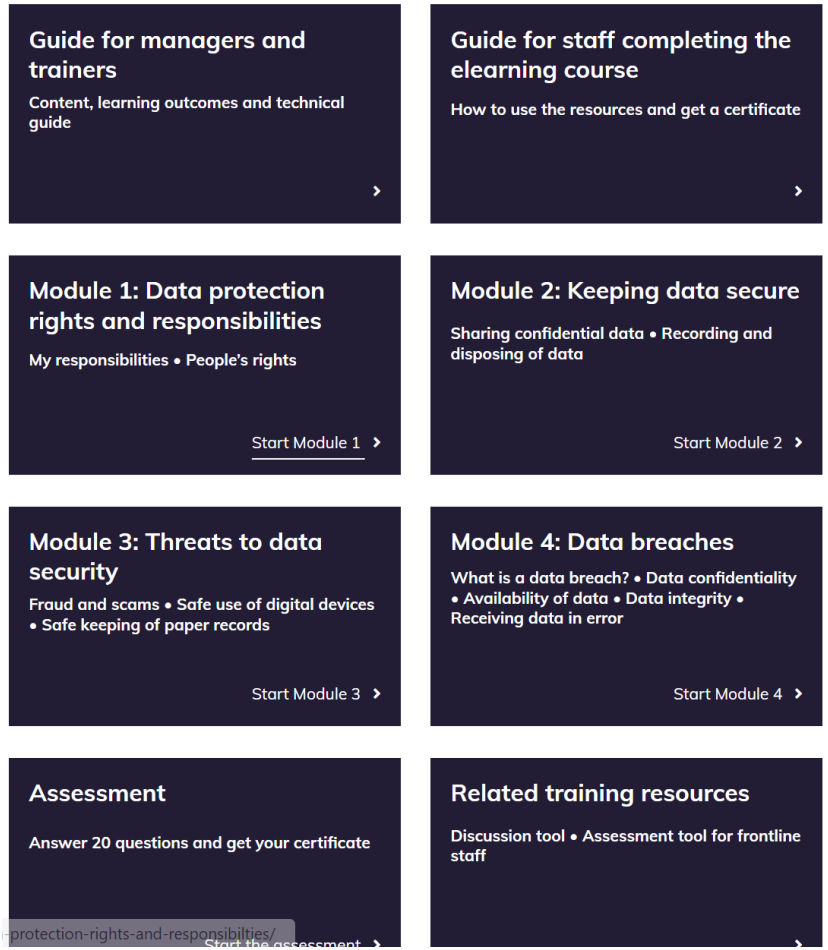
- Who are you going to report progress to?
- Who signs off at year end?
- Audit would pick a sample of staff and check they had received the training that the TNA set out for them.

Help and Support

- From Big Picture guides on training https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-3---staff-training
- Deep Dive webinar recording and copy of the slides https://www.dsptoolkit.nhs.uk/News/Webinar-Slides

Free training resources: https://www.digitalcarehub.co.uk/elearning/





Individual changes

Updated wording

6.1.1	Update Wording update Guidance	Data security and protection incidents are reported appropriately and by a full range of staff groups.	You should confirm that a functioning data security and protection breach reporting and management mechanism is in place including use of the DSP Toolkit incident reporting tool. You should include in the comments the number of incidents and near misses reported per staff group in your organisation, as a proportion of the number of people in each group.
4.5.3	Updated Wording and Guidance	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 and explanatory guidance If your organisation is an IT supplier, then tick and write “Not applicable” in the comments box.

DSPT Audit

Audit –

Read the audit guidance and scope

Watch out for 1.1 covering ROPAs and Privacy notice

Also 8.4 it drags in many of the evidence items across Standard 8.

Make sure your Auditors are set up with Audit access to DSPT

Work with auditor to agree audit report

Auditors to upload details to DSPT

New publication not required

If your audit is not final on 30th June, upload a draft report and then update after the deadline

What will the Audit Cover for 23-24

13 assertions:

1.1 The organisation has a framework in place to support Lawfulness, Fairness and Transparency
2.2 Staff contracts set out responsibilities for data security
3.1 Staff have appropriate understanding of information governance and cyber security, with an effective range of approaches taken to training and awareness
3.2 Your organisation engages proactively and widely to improve data security, and has an open and just culture for data security incidents
4.4 You closely manage privileged user access to networks and information systems supporting the essential service
5.1 Process reviews are held at least once per year where data security is put at risk and following DS incidents
6.2 All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway
7.1 Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services
8.4 You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service
9.2 A penetration test has been scoped and undertaken
9.5 You securely configure the network and information systems that support the delivery of essential services
9.6 The organisation is protected by a well-managed firewall
10.2 Basic due diligence has been undertaken against each supplier that handles personal information

https://www.dsptoolkit.nhs.uk/News/auditnews

Improvement plans 23-24

DSP Toolkit Improvement plan 23-24

What are they

- Designed to support those organisations who have not quite achieved Standards Met and only have a few outstanding evidence items to meet.
- Available to:
  NHS Trusts, Integrated Care Boards, CSUs, Independent Providers who are Operators of Essential Services under NIS, Key IT Suppliers, Local Authorities and DHSC Arm's Length Bodies

How to prepare

- Have a read of the guidance available on the DSPT News page: To generate an Improvement plan, click the publish button on the assessment page,
- NHS Trusts, CSU, ICBs speak to Regional Security leads
- ALBS speak to DHSC
- LAs speak to Exeter helpdesk
- Develop your plan and get it signed off by SIRO

Submission of the plan

- Improvement plan submitted with publication
- Publish a Standards not met DSPT
- Plan will come through to DSPT team to review. This will be supported by Regional Security leads, DHSC and Exeter helpdesk.
- Once agreed Status amends to Approaching Standards.
- Updates quarterly
- Once complete status is amended to Standards met.

DSP Toolkit Improvement plan

Very similar to last year

Removed columns for COVID

Additional information required on plans to show robustness

Additional fields on the template covering dependencies and any internal references

More explicit link to DSPT Audit. I.e. if audit has agreed management action to meet requirement, is it in the Improvement plan

Regional Security Leads help and support NHS orgs.

DHSC/JCU can support ALBs.

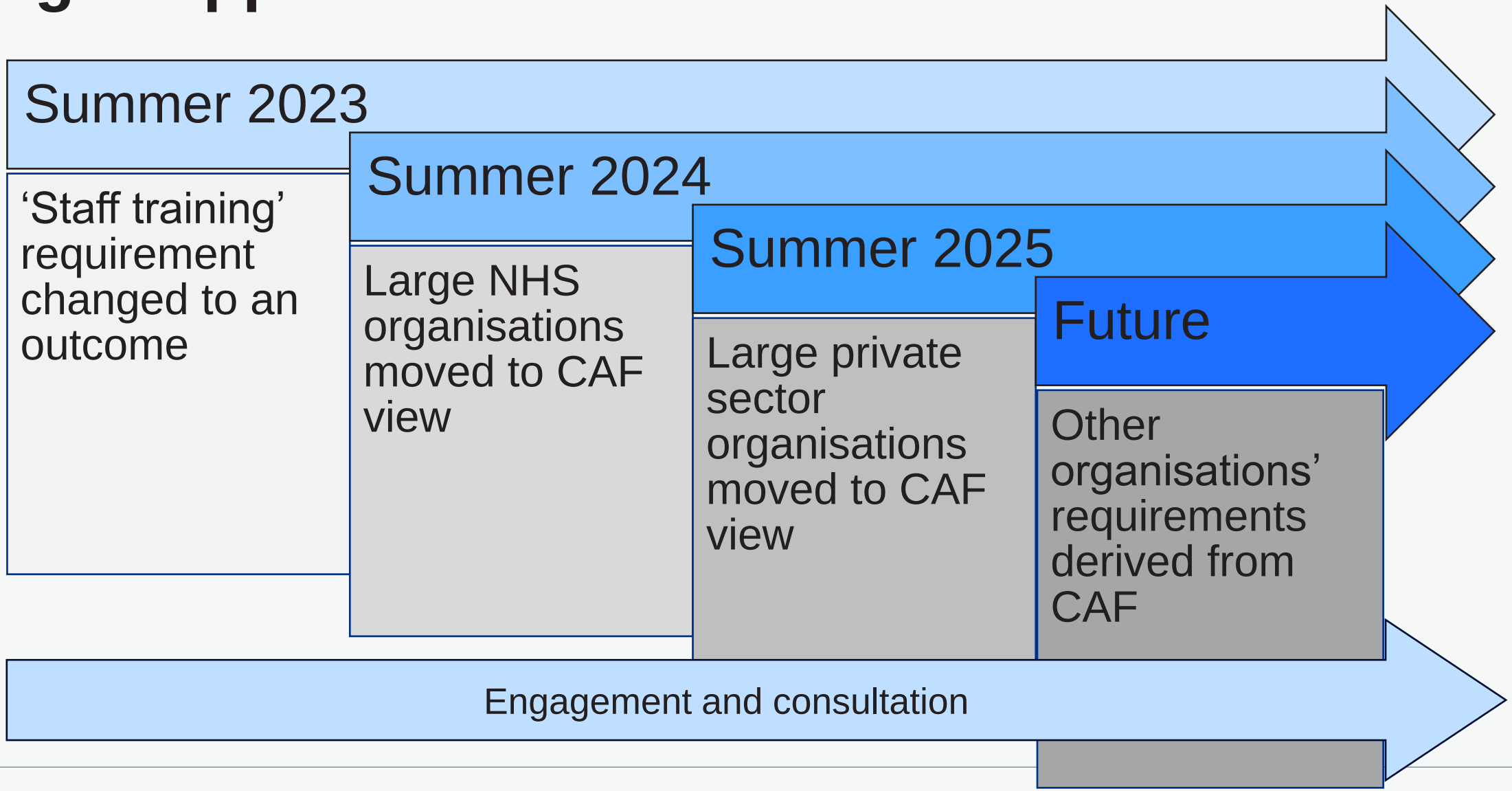
DSPT team support OES and LA

CAF for 24-25

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 Cat 1 organisations (NHS Trusts, CSU, ALB 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 will be stood up to help organisations understand the content, approach and expectations of the CAF-aligned DSPT.

Staged approach for DSPT



Health and care ‘CAF overlay’ (1)

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’ (2)

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.

“CAF-led DSPT” framework

		Not achieved	Partially achieved	Achieved
A2 Risk management The organisation takes appropriate steps to identify, assess and understand risks to the security and governance of information, systems and networks. 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, and communicating associated activities. This includes a process for data protection impact assessments (DPIAs).	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 (including DPIAs) for critical systems or high-risk processing activities 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 identify risks, and then ensure that identified risks are managed effectively, which includes incorporating data protection by design and default. Systems and risks are assessed in isolation, without consideration of dependencies and interactions with other systems or risks in other areas of the business. (e.g. interactions between IT and OT environments, or finance risks and the impact on IG). Security requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of the essential function. Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve. These risks may be out of date or incomplete.	Your organisational process ensures that security and wider IG risks to information, systems and networks relevant to essential functions are identified, analysed, prioritised, and managed. Your risk assessments are informed by an understanding of the information and vulnerabilities in the systems and networks supporting your essential function, as well as your other data processing activities. The output from your risk management process is a clear set of security and IG requirements and mitigations that will address the risks in line with your organisational approach to security and IG more widely. Significant conclusions reached in the course of your risk management process are communicated to key information risk decision-makers and accountable individuals. You conduct risk assessments (including DPIAs) when significant events potentially affect the essential function, such as replacing a system, commencing new or changing high-risk data processing, or a change in the cyber security threat. Your risk process clearly demonstrates how your organisation’s processing complies with data protection principles and relevant legislation, including the right to a private life. You perform threat analysis and understand how generic threats apply to your organisation.	Your organisational process ensures that security and wider IG risks to information, systems and networks relevant to essential functions are identified, analysed, prioritised, and managed effectively. This includes incorporating data protection by design and default into your process. 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 information, systems and networks. 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 process clearly demonstrates how your organisation’s processing complies with data protection principles and relevant legislation, including the right to a private life. Your risk assessments are informed by an understanding of the information and vulnerabilities in the systems and networks supporting your essential function, as well as a good understanding of your data processing activities in all areas of your organisation. This includes evaluation of repeated or significant near misses. The output from your risk management process is a clear set of requirements that will address the risks in line with your organisational approach to security and IG more widely. Significant conclusions reached in the course of your risk management process are communicated to key decision-makers and accountable individuals. Your risk assessments (including DPIAs) are dynamic and updated in the light of relevant changes which may include technical changes to networks and information systems, change of use or processing, and new threat information.

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	

TEST This is a new service - your feedback will help us to improve it.

NHS England **Data Security and Protection Toolkit**

My account Logout

This is a test site and is not intended for live use.

Test CAF organisation Change organisation

Organisation search News Help

Assessment Provide audit details Report an incident Admin

Complete your assessment for YYYY-YY (version N)

The Cyber Assessment Framework provides a systematic and comprehensive approach to assessing the extent to which cyber and data security risks to essential functions are being managed.

Completing this self-assessment will demonstrate that your organisation is working towards or meeting the required standard.

Objectives

Select an objective to assess your organisation against each principle associated with it.

A. Managing risk

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

B. Protecting against cyber attack and data breaches

Proportionate security measures are in place to protect information, systems and networks supporting essential functions from cyber attack and data breaches.

C. Detecting cyber security events

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

D. Minimising the impact of incidents

Capabilities exist to minimise the adverse impact of an incident on the operation of essential functions, including the restoration of those functions where necessary, and to uphold the rights of impacted individuals.

E. Using and sharing information appropriately

The organisation ensures that information is used and shared lawfully and appropriately.

© 2024 NHS Digital

Build: 717_7442cf54

TEST This is a new service - your feedback will help us to improve it.

NHS England **Data Security and Protection Toolkit**

My account Logout

This is a test site and is not intended for live use.

Test CAF organisation Change organisation

Organisation search News Help

Assessment Provide audit details Report an incident Admin

Complete your assessment for yyyy-yy (Version Z)

The Cyber Assessment Framework provides a systematic and comprehensive approach to assessing the extent to which cyber and data security risks to essential functions are being managed.

Completing this self-assessment will demonstrate that your organisation is working towards or meeting the required standard.

Back to objectives

Objective B

Protecting against cyber attack and data breaches

Proportionate security measures are in place to protect information, systems and networks supporting essential functions from cyber attack and data breaches.

Progress

3 of 20 outcomes completed

Principle B1

Policies and processes

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

Contributing Outcomes

B1.a	**Policy and process development** You have developed and continue to improve a set of information assurance and resilience policies and processes that manage and mitigate the risk of adverse impact on the essential function. **Owner:** No Owner (Assign Owner)	**PARTIALLY ACHIEVED**
B1.b	**Policy and process implementation** You have successfully implemented your information assurance policies and processes and can demonstrate the benefits achieved. **Owner:** No Owner (Assign Owner)	**NOT COMPLETED**

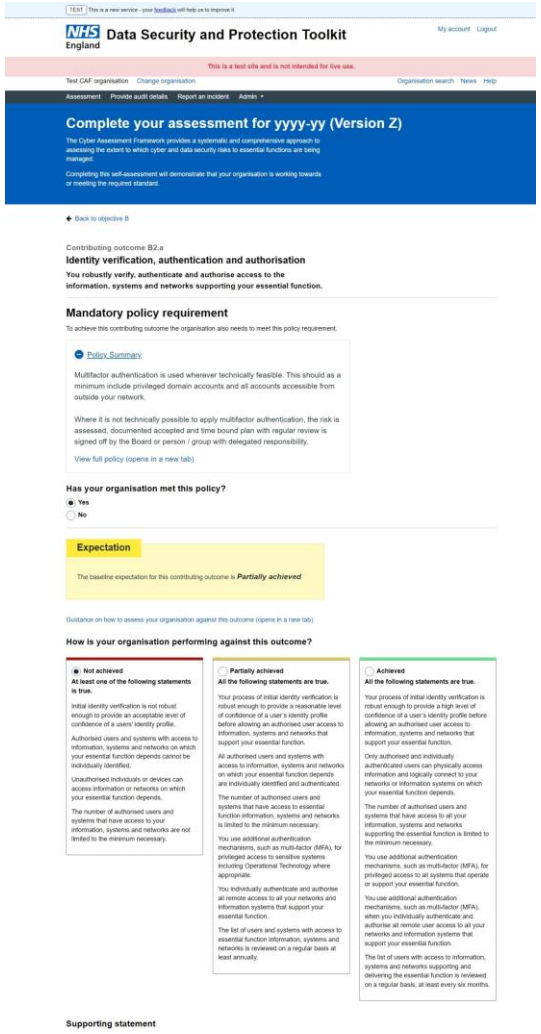
Principle B2

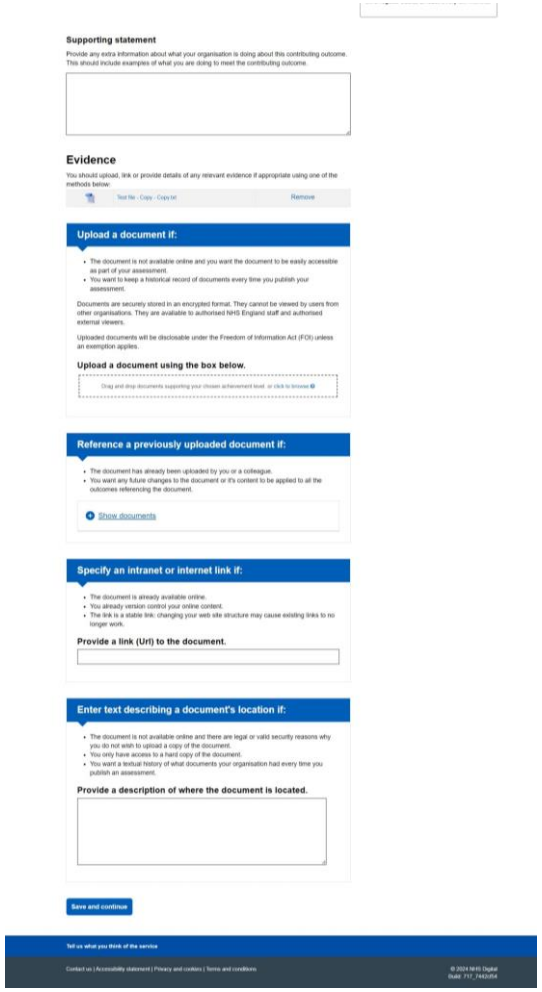
Identity and access control

The organisation understands, documents and manages access to information, systems and networks supporting the operation of essential functions. Individuals (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.

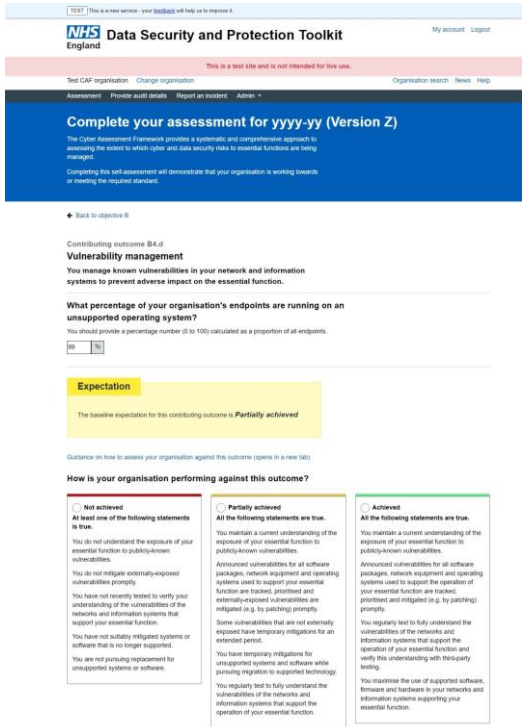
Contributing Outcomes

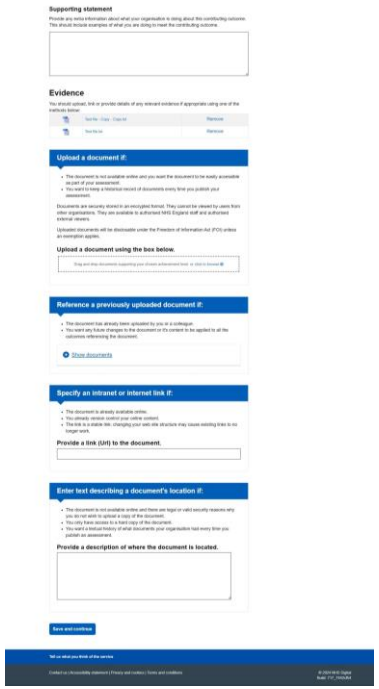
B2.a	**Identity verification, authentication and authorisation** You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function. **Includes policy requirement** **Owner:** No Owner (Assign Owner)	**NOT ACHIEVED**
B2.b	**Device management** You fully know and have trust in the devices that are used to access your information, systems and networks that support your essential function. **Owner:** No Owner (Assign Owner)	**ACHIEVED**
B2.c	**Privileged user management** You closely manage privileged user access to networks and information systems supporting the essential function. **Owner:** No Owner (Assign Owner)	**NOT COMPLETED**
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 the essential function. **Owner:** No Owner (Assign Owner)	**NOT COMPLETED**





- In a few specific areas, the CAF will be bolstered by explicitly-worded policy requirements which users will need to comply with to meet an outcome
- This is for areas where outcomes need to be interpreted less broadly by organisations to reduce risk
- The goal is to keep CAF-aligned “policy requirements” to a minimum
- MFA, DSPT Audit, Responding to a cyber alert,





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, Privileged access and Top 3 Data Security Risks

Monthly breakdown of activity

Draft timescale – subject to change.

- Dates for webinars to be communicated in May/early June 2024.
- Option for users to raise queries via MS form in June on the new DSPT v7 ahead of the webinars.
- Messaging will be repeated again in September, once the system has been updated and the new interface is up and running.

June 2024

Complete current DSPT v6 by 30 June.

DSPT v7 standards and assertions to be published with guidance. Users can log queries via MS form.

July 2024

Series of webinars to be delivered over a 6 week period – covering each section of the new DSPT requirements and an introduction webinar.

August 2024

Reminder comms about the new changes and link to webinar recordings.

September 2024

New DSPT v7 launched / available on the system.

Signpost to webinar recordings.

Deliver updated webinar if needed.

Webinars content – Introduction and then aligned to the 5 sections of DSPT

Week 1	Week 2
A - Managing risk	B - Protecting against cyber attack and data breaches

Week 3	Week 4	Week 5
C - Detecting cyber security events	D - Minimising the impact of incidents	E - Using and sharing information appropriately

How can you help

- Interested in participating in User research sessions for the move to CAF
- Email: england.cyberresearch@nhs.net

- Webinar programme https://www.dsptoolkit.nhs.uk/News/webinars
- Extra Webinars in June covering Improvement plans etc.,

- Caf Webinars will begin in July 2024.
- Regional Briefing on-going watch out for your local SIGN group

- Watch out for an email from Network and Information Systems regulation (NIS) team coming out about Independent providers who are operators of essential service and warning that some of them will be Approaching Standards as it is their first year at Catergory1.

Thank You

@nhsengland

company/nhsengland

england.nhs.uk