Data Security and Protection Toolkit 2024-25

CAF aligned DSPT - Objective A – managing risk

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

NHS England
09 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 2 – Objective A – managing risk

- Overview – what is in the Objective and which teams need to be involved in responding to it?
- Contributing outcomes – A step through A1 and A2
- Half Time Quiz
- Contributing outcomes – A step through A2 and 4
- 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.

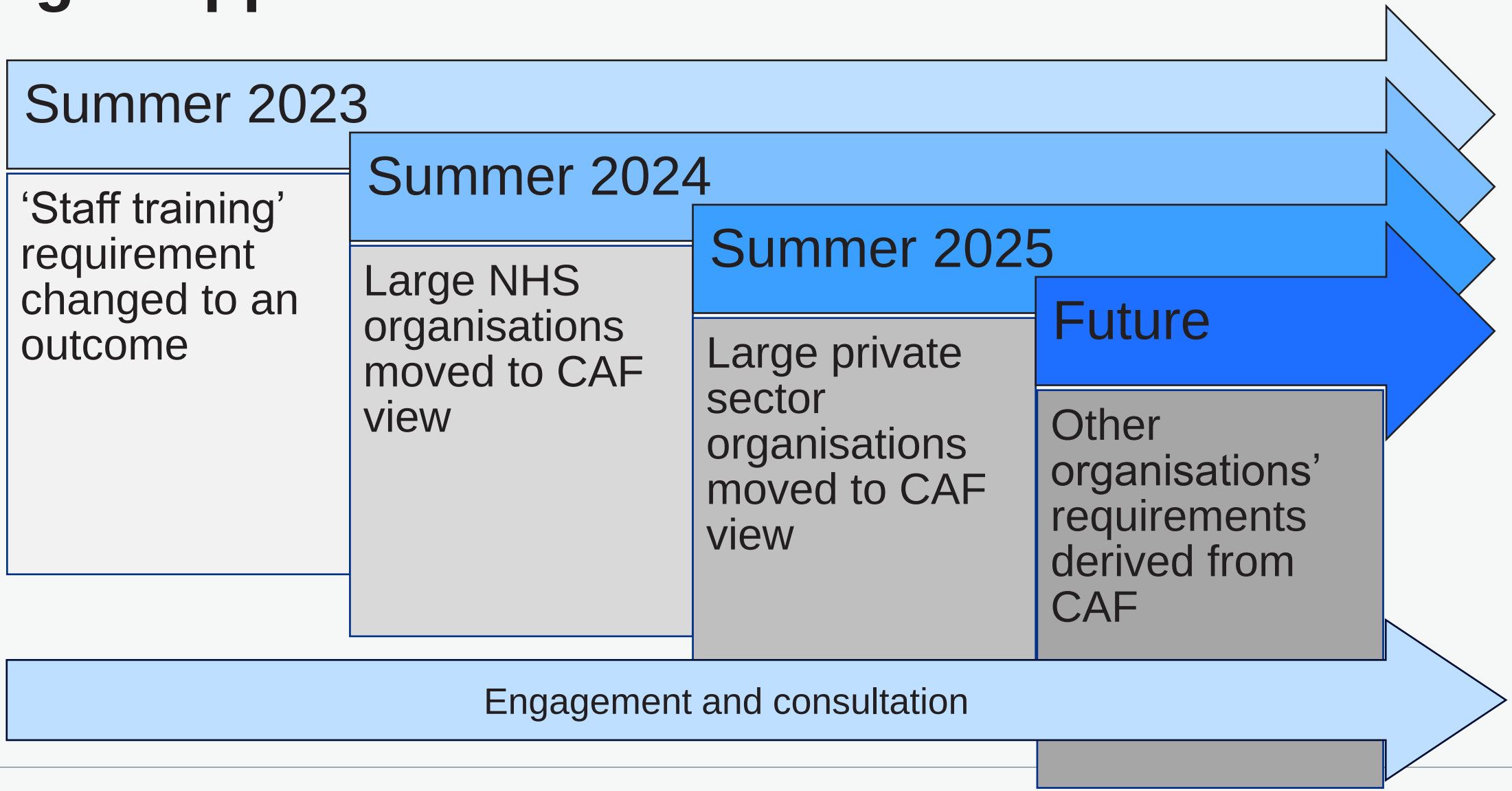
The goals of moving to the CAF-aligned DSPT are to:

- 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



What is staying the same for 24-25?

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

Interim Publication by 31 December 2024

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)

Toolkit for other sectors

IT Suppliers, Universities, Local Authorities, GP

Other sectors

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

Objective A - Managing risk

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	

Principle: A1 Governance

Contributing outcome: A1.a Board direction

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***

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).

Principle: A1 Governance

Contributing outcome:
A1.a Board direction

Mapping, Guidance and Evidence to upload

() indicates mapping onl

Contributing outcome	DSPT V6 *() weak map*
A1.a Board direction: You have effective organisational information assurance management led at board level and articulated clearly in corresponding policies.	1.3.1 1.3.3 1.3.9

Board direction

Your board, or equivalent members of senior management, should take overall accountability for the data protection and security risks your organisation faces. They should provide direction on cyber security and IG, which is then disseminated through your organisation's policies, projects and procedures.

In health and care, these board-level activities are driven by the Senior Information Risk Owner (SIRO) (see A1.b Roles and responsibilities).

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 or groups
- Policy, process, procedure or strategy documents (e.g. accountability)
- Risk management reports
- Accountability structures
- Board member training records

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.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | A1 Governance
National Cyber Security Centre | Risk management – Cyber security governance
Information Commissioner's Office | Leadership and oversight

Principle: A1 Governance

Contributing outcome: A1.a Board direction

Interpretations

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
A#1 Your organisation's approach and policy relating to the security and governance of information, systems and networks supporting the operation of your **essential function(s)** are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.	"essential function(s)"	Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions. For more information, see guidance on scoping essential functions.
A#2 **Regular** board discussions on the security and governance of information, systems and networks supporting the operation of your essential function(s) 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.	"regular"	On a scheduled basis, with enough frequency to ensure there are no key strategic decisions made which the board does not have visibility of.

Principle: A1 Governance

Contributing outcome: A1.b Roles and responsibilities

Contributing outcome A1.b

Roles and responsibilities

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

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 Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis.

NA#2 Staff are assigned security or Information Governance responsibilities but without adequate authority or resources to fulfil them.

NA#3 Staff are unsure what their responsibilities are for the security and governance of the essential function(s).

NA#4 Not all staff contracts clearly set out their responsibilities for the security and governance of information, systems and networks.

Achieved

All the following statements are true.

A#1 Key roles and responsibilities for the security and governance of information, systems and networks supporting your essential function(s) have been identified. These are reviewed regularly to ensure they remain fit for purpose

A#2 Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties.

A#3 There is clarity on who in your organisation has overall accountability for the security and governance of information, systems and networks supporting your essential function(s).

A#4 All staff contracts contain clear clauses confirming their responsibilities for the security and governance of information, systems and networks.

Principle: A1 Governance

Contributing outcome:
A1.b Roles and responsibilities

Mapping and Guidance

Contributing outcome	DSPT V6
	() weak map
A1.b Roles and responsibilities: Your organisation has established roles and responsibilities for the security and governance of information, systems and networks at all levels, with clear and well-understood channels for	1.1.5 1.3.3 1.3.4 2.2.1

Roles and responsibilities

How you structure your cyber security and IG teams and allocate responsibilities is a local decision.

Roles and responsibilities should be well understood to ensure that cyber and IG activities are effectively delivered, and that any gaps in resources are promptly identified and addressed.

You can define roles and responsibilities in a range of ways, including but not limited to:

- documented ownership of actions
- policies and processes
- training
- contracts

Key roles in health and care

Key roles for health and care organisations include:

- Data Protection Officer (DPO)
- Senior Information Risk Owner (SIRO)
- Caldicott Guardian – see guidance produced by the UK Caldicott Guardian Council and the National Data Guardian
- IG lead
- Information Security lead / Cyber Security lead

Staff contracts

Your employment contracts for staff should contain data protection and security requirements.

The NHS terms and conditions of service handbook outlines the following under the 'Governance, confidentiality, data protection' section:

> 35.46 All employees must comply with The General Data Protection Regulation (GDPR) as it applies in the UK, informed by the Data Protection Act 2018.
>
> Policies should set out clear principles and processes. Specifically, home and/or agile/hybrid workers are under a duty to observe security and confidentiality practices in relation to equipment and data in line with GDPR, data protection legislation, and local policies and procedures. Employers need to ensure provisions are in place for the secure storage, use and disposal of confidential information from the home base.

Your organisation may use this, or similar wording, to ensure your contracts cover the appropriate bases.

Principle: A1 Governance

Contributing outcome:
A1.b Roles and responsibilities

Mapping and Evidence to upload

Contributing outcome	DSPT V6 *() weak map*
A1.b Roles and responsibilities: Your organisation has established roles and responsibilities for the security and governance of information, systems and networks at all levels, with clear and well-understood channels for	1.1.5 1.3.3 1.3.4 2.2.1

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 or groups
- Organisational charts
- Lists of roles and responsibilities related to cyber security and IG
- Job specifications
- Policy, process, procedure or strategy documents (e.g. roles and responsibilities)
- Training records
- Staff contract templates
- Performance review templates

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.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | A1 Governance
National Cyber Security Centre | Risk management – Cyber security governance

Principle: A1 Governance

Contributing outcome:
A1.b Roles and responsibilities

Interpretations

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
A#1 Key roles and responsibilities for the security and governance of information, systems and networks supporting your essential function(s) have been identified. These are reviewed **regularly** to ensure they remain fit for purpose.	"regularly"	On a scheduled basis, with enough frequency to ensure there are no critical gaps in cyber security or IG activities.
A#1 Key roles and responsibilities for the security and governance of information, systems and networks supporting your **essential function(s)** have been identified. These are reviewed regularly to ensure they remain fit for purpose.	"essential function(s)"	Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions. For more information, see guidance on scoping essential functions.

Principle: A1 Governance

Contributing outcome: A1.c Decision-making

Contributing outcome A1.c

Decision-making and approval

You have senior-level accountability for the security and governance of information, systems and networks, and delegate decision-making authority appropriately and effectively. Risks to information, systems and networks related to the operation of your essential function(s) are considered in the context of other organisational risks.

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 What should be relatively straightforward risk decisions are constantly referred up the chain, or not made.

NA#2 Risks are resolved informally (or ignored) at a local level when the use of a more formal risk reporting mechanism would be more appropriate.

NA#3 Decision-makers are unsure of what senior management's risk appetite is, or only understand it in vague terms such as "averse" or "cautious".

NA#4 Organisational structure causes risk decisions to be made in isolation. (e.g. engineering and IT don't talk to each other about risk).

NA#5 Risk priorities are too vague to make meaningful distinctions between them. (e.g. almost all risks are rated 'medium' or 'amber').

○ Achieved

All the following statements are true.

A#1 Senior management have visibility of key risk decisions made throughout the organisation.

A#2 Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the essential function(s), as set by senior management.

A#3 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.

A#4 Risk management decisions are regularly reviewed to ensure their continued relevance and validity.

A#5 Risk decisions are joined up between different departments.

Principle: A1 Governance

Contributing outcome: A1.c Decision-making

Mapping and Guidance

Contributing outcome	DSPT V6 *() weak map*
A1.c Decision-making: You have senior-level accountability for the security and governance of information, systems and networks, and delegate decision-making authority appropriately and effectively. Risks to information, systems and networks related to the operation of your essential function(s) are considered in the context of other organisational risks.	1.3.3 1.3.4 1.3.5

Decision making

Your procedures for risk decision making should ensure that:

- appropriate staff members are involved
- staff members operate under direction from senior management
- risk decisions are reviewed in response to changing circumstances

The teams who are directly involved in conducting your cyber security and IG activities are best placed to determine what decisions should be taken in each individual case. However, they should operate from an informed understanding of your board's risk appetite.

Risk appetite

Your organisation should have a board-approved risk appetite which:

- determines acceptable and unacceptable risks
- creates a risk culture and sets risk expectations to be shared across your organisation's teams
- allows staff members to make informed, timely and effective risk management decisions

Your organisation's risk appetite should be continually assessed against current threats and refreshed at suitable intervals.

Principle: A1 Governance

Contributing outcome: A1.c Decision-making

Mapping and Evidence to upload

Contributing outcome	DSPT V6 *() weak map*
A1.c Decision-making: You have senior-level accountability for the security and governance of information, systems and networks, and delegate decision-making authority appropriately and effectively. Risks to information, systems and networks related to the operation of your essential function(s) are considered in the context of other organisational risks.	1.3.3 1.3.4 1.3.5

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:

- Records of decisions made regarding the security of information, networks and systems
- Risk assessment reports
- Risk appetite statements
- Minutes from relevant meetings or groups
- Policy, process, procedure or strategy documents (e.g. risk management)
- Change management records

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.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | A1 Governance
National Cyber Security Centre | Risk management – Cyber security governance

Principle: A1 Governance

Contributing outcome: A1.c Decision-making

Interpretations

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
A#2 Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding this **essential function(s)**, as set by senior management.	"essential function(s)"	Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions. For more information, see guidance on scoping essential functions.
A#4 Risk management decisions are **regularly** reviewed to ensure their continued relevance and validity.	"regularly"	On a scheduled basis, with enough frequency to ensure that the criteria upon which you have made decisions have not changed due to evolving external factors.

Principle: A2 Risk management

Contributing outcome: A2.a Risk management process

Contributing outcome A2.a

Risk management process

Your organisation has effective internal processes for managing risks to the security and governance of information, systems and networks related to the operation of your essential function(s) and communicating associated activities. This includes a process for data protection impact assessments (DPIAs).

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 Risk assessments are not based on a clearly defined set of threat assumptions.

NA#2 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.

NA#3 Risk assessments (including DPIAs) for network and information systems supporting your essential function or high-risk processing activities are a "one-off" activity (or not done at all).

NA#4 The security and IG elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.

NA#5 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.

NA#6 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 operational technology environments, or finance risks and the impact on information governance).

NA#7 Security and IG requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of the essential function(s).

NA#8 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.

Partially achieved

All the following statements are true.

PA#1 Your organisational process ensures that security and wider IG risks to information, systems and networks relevant to essential function(s) are identified, analysed, prioritised, and managed.

PA#2 Your risk assessments are informed by an understanding of the vulnerabilities in the systems and networks supporting your essential function(s), as well as your other data processing activities.

PA#3 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.

PA#4 Significant conclusions reached in the course of your risk management process are communicated to key decision -makers and accountable individuals.

PA#5 You conduct risk assessments (including DPIAs) when significant events potentially affect the essential function(s), such as replacing a system, commencing new or changing high-risk data processing, or a change in the cyber security threat.

PA#6 You perform threat analysis and understand how generic threats apply to your organisation.

PA#7 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.

Achieved

All the following statements are true.

A#1 Your organisational process ensures that security and wider IG risks to information, systems and networks relevant to essential function(s) are identified, analysed, prioritised, and managed effectively. This includes incorporating data protection by design and default into your process.

A#2 Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your information, systems and networks.

A#3 Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function(s) and your sector.

A#4 Your risk assessments are informed by an understanding of the information and vulnerabilities in the systems and networks supporting your essential function(s), 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.

A#5 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.

A#6 Significant conclusions reached in the course of your risk management process are communicated to key decision-makers and accountable individuals.

A#7 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.

A#8 The effectiveness of your information and security risk management process is reviewed periodically, and improvements made as required.

A#9 You perform detailed threat analysis and understand how this applies to your organisation in the context of the threat to your sector and the wider Critical National Infrastructure.

A#10 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.

Principle: A2 Risk management

Contributing outcome:
A2.a Risk management process

DSPT Mapping and Guidance

Contributing outcome	DSPT V6 *() weak map*
A2.a Risk management process: Your organisation has effective internal processes for managing risks to the security and governance of information, systems and networks related to the operation of your essential function(s), and communicating associated activities.	1.3.5 1.3.6 1.3.7* 1.3.8* 7.1.4

Risk assessments

You should conduct risk assessments on a scheduled basis, and whenever significant changes occur to your organisational systems or processes.

The DSPT does not mandate a specific approach to risk assessment, however, it is important to consider:

- your organisation's business priorities and objectives
- who or what those things should be protected from
- any legal and regulatory obligations that apply to your organisation
- the cyber security risk red lines your organisation will and won't cross to complete the things it needs to do

See NCSC guidance on 'A basic risk assessment and management method' for more information on understanding and managing risk.

Linking risk assessment to controls

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

Under the new framework, you should link your cyber security and information governance (IG) controls to your risk assessments. Ways of clearly demonstrating links between controls and risks may include:

- listing controls against each risk in your risk register
- creating a controls catalogue which cross-references each control against individual risks

This should give you confidence that your controls are sufficient and proportionate, and that time and resources are not being wasted on solutions that do not effectively contribute towards the management of cyber security and IG risk.

Principle: A2 Risk management

Contributing outcome:
A2.a Risk management process

DSPT Mapping and Guidance

Contributing outcome	DSPT V6 *() weak map*
A2.a Risk management process: Your organisation has effective internal processes for managing risks to the security and governance of information, systems and networks related to the operation of your essential function(s), and communicating associated activities.	1.3.5 1.3.6 1.3.7* 1.3.8* 7.1.4

Data protection by design and by default

The requirements of data protection by design and by default should be clearly incorporated into your overall approach to cyber security and wider IG risk. Examples of where considerations should be made include:

- developing new IT systems, services and processes that involve processing personal data
- developing organisational policies, processes and strategies that have privacy implications
- embarking on data sharing initiatives
- using personal data for new purposes

See ICO guidance on data protection by design and by default for more information.

Data protection impact assessments (DPIAs)

Conducting data protection impact assessments (DPIAs) is an important pillar of data protection by design and by default.

You should demonstrate that your organisation conducts DPIAs before beginning any type of processing which is "likely to result in a high risk to the rights and freedoms" of individuals. For a detailed list of situations where this applies, see guidance from the Information Commissioner's Office.

See NHS England's universal IG templates page for a template DPIA document which you can use, or reference your own processes against, to ensure all appropriate bases are covered.

Threat analysis

Your risk assessments should be informed by:

- 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

Principle: A2 Risk management

Contributing outcome:
A2.a Risk management process

DSPT Supporting evidence

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:

- Risk registers
- Policy, process, procedure or strategy documents (e.g. risk management)
- Risk assessments reports
- Risk mitigation plans
- Risk acceptance records
- Risk review records
- Data protection impact assessments
- Documents showing follow-up actions taken

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.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | A2 Risk management
National Cyber Security Centre | Risk management
National Cyber Security Centre | Risk management - Introducing system and component driven risk management approaches
Information Commissioner's Office | Risk and data protection impact assessments (DPIAs)
Information Commissioner's Office | Data protection by design and by default

Principle: A2 Risk management

Contributing outcome:
A2.a Risk management process

Interpretations

Interpreting indicators of good practice

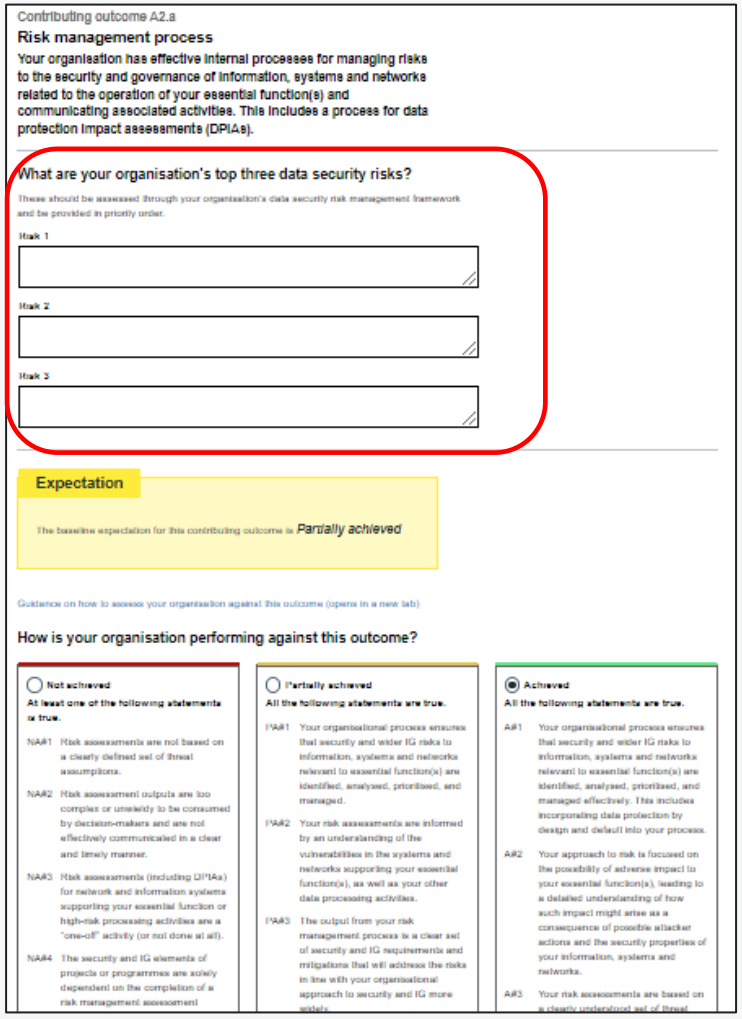
Indicator(s) of good practice	Term	Interpretation
PA#1 Your organisational process ensures that security and wider IG risks to information, systems and networks relevant to **essential function(s)** are identified, analysed, prioritised, and managed.	"essential function(s)"	Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions. For more information, see guidance on scoping essential functions.
PA#7 Your risk process demonstrates how your organisation's processing complies with **data protection principles and relevant legislation**, including the right to a private life.	"data protection principles and relevant legislation"	Principles and legislation which should be considered include: • data protection principles • relevant laws • Caldicott Guardian principles • other legislation, including the common law duty of confidentiality and right to a private life where appropriate
A#2 Your approach to risk is focused on the possibility of **adverse impact** to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your information, systems and networks.	"adverse impact"	This term refers to the wider downstream effects which incidents might have on your organisation's essential functions. For example, your organisation's long-term objectives, its image and reputation.

Principle: A2 Risk management

Contributing outcome:
A2.a Risk management process

Specific Data Collections

You cannot Save as complete until the data collection is complete



Contributing outcome A2.a

Risk management process

Your organisation has effective internal processes for managing risks to the security and governance of information, systems and networks related to the operation of your essential function(s) and communicating associated activities. This includes a process for data protection impact assessments (DPIAs).

What are your organisation's top three data security risks?

These should be assessed through your organisation's data security risk management framework and be provided in priority order.

Risk 1

Risk 2

Risk 3

Expectation

The baseline expectation for this contributing outcome is *Partially 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 Risk assessments are not based on a clearly defined set of threat assumptions.

NA#2 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.

NA#3 Risk assessments (including DPIAs) for network and information systems supporting your essential function or high-risk processing activities are a "one-off" activity (or not done at all).

NA#4 The security and IG elements of projects or programmes are solely dependent on the completion of a risk management assessment

Partially achieved

All the following statements are true.

PA#1 Your organisational process ensures that security and wider IG risks to information, systems and networks relevant to essential function(s) are identified, analysed, prioritised, and managed.

PA#2 Your risk assessments are informed by an understanding of the vulnerabilities in the systems and networks supporting your essential function(s), as well as your other data processing activities.

PA#3 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.

Achieved

All the following statements are true.

A#1 Your organisational process ensures that security and wider IG risks to information, systems and networks relevant to essential function(s) are identified, analysed, prioritised, and managed effectively. This includes incorporating data protection by design and default into your process.

A#2 Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your information, systems and networks.

A#3 Your risk assessments are based on a clearly understood set of threat

Principle: A2 Risk management

Contributing outcome:
A2.a Risk management process

Exceeding Standards met

Exceeding the ‘Standards met’ expectation for 2024-25

Threat analysis

To meet the higher bar of performing detailed threat analysis, the analysis underpinning your risk assessments should be:

- detailed and comprehensive
- specific to your organisation
- underpinned by a robust knowledge base of attacker tactics and techniques

Adverse impacts

To meet the highest achievement benchmark, your risk assessments should consider potential adverse impacts on the delivery of your essential service. Adverse impacts include your organisation’s long-term objectives, its image and reputation.

Your risk assessments should evidence that you have taken measures to control these adverse impacts, informed by your knowledge of specific techniques which an attacker might use.

You should also consider adverse impacts on other health and care services, and conversely, how their risks could impact you where you have dependencies. Again, evidence is required showing the measures you have taken with attacker actions in mind.

The highest assurance benchmark is a broad system-driven approach to risk assessment which shows detailed consideration of how adverse impacts might arise, a system-wide scope for consequences, and pre-emptive implementation of specific measures to mitigate them.

Updating threat assumptions

To meet the higher bar for achievement, you need to have a documented threat assessment where your assumptions cover a wide range of attackers and capabilities.

Your threat assumptions need to be continuously updated in response to changes in the threat landscape. These could include geo-political campaigns, significant data protection and security incidents in health and care, and the discovery of new vulnerabilities.

Your threat assumptions should also be informed by information sharing resources and initiatives. These might include threat intelligence and services provided by NCSC, forums and engagement with professionals in your industry.

Half time Quiz

With thanks to Shaun Van Niekerk at Homerton

A2.a Risk Management Process

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of the essential function(s) and communicating associated activities.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true:	All the following statements are true:	All the following statements are true:
Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.
Risk assessments for network and information systems that support your essential function(s) are a "one-off" activity or not done at all.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).	Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your network and information systems.
The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.	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.	Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function(s) and your sector.
There is no systematic process in place to ensure that identified security risks are managed effectively.	Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).
Systems are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).	You conduct risk assessments when significant events potentially affect the essential function(s), such as replacing a system or a change in the cyber security threat.	Th
Security requirements and mitigations are arbitrary or are	You perform threat analysis and	

Back to top

SCENARIO 1

Is this a **PA** or a **NA**?

RED Frame = FALSE

GREEN Frame = TRUE

Answer

If any of the Indicators listed under Not achieved are true, you should mark yourselves Not achieved.

Rationale

The indicators listed under ‘Not achieved’ list statements which are incompatible with achieving or partially achieving the outcome.

Security chain is only as strong as the weakest link. The best security capabilities in the world aren’t much use if there’s a great big hole in the middle.

A2.a Risk Management Process

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of the essential function(s) and communicating associated activities.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true:	All the following statements are true:	All the following statements are true:
Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.
Risk assessments for network and information systems that support your essential function(s) are a "one-off" activity or not done at all.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).	Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your network and information systems.
The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.	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.	Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function(s) and your sector.
There is no systematic process in place to ensure that identified security risks are managed effectively.	Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).
Systems are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).	You conduct risk assessments when significant events potentially affect the essential function(s), such as replacing a system or a change in the cyber security threat.	Th
Security requirements and mitigations are arbitrary or are	You perform threat analysis and	

Back to top

A2.a Risk Management Process

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of the essential function(s) and communicating associated activities.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true:	All the following statements are true:	All the following statements are true:
Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.
Risk assessments for network and information systems that support your essential function(s) are a "one-off" activity or not done at all.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).	Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your network and information systems.
The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.	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.	Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function(s) and your sector.
There is no systematic process in place to ensure that identified security risks are managed effectively.	Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).
Systems are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).	You conduct risk assessments when significant events potentially affect the essential function(s), such as replacing a system or a change in the cyber security threat.	Th
Security requirements and mitigations are arbitrary or are	You perform threat analysis and	

Back to top

SCENARIO 2

Is this a **PA** or a **NA**?

RED Frame = FALSE
GREEN Frame = TRUE

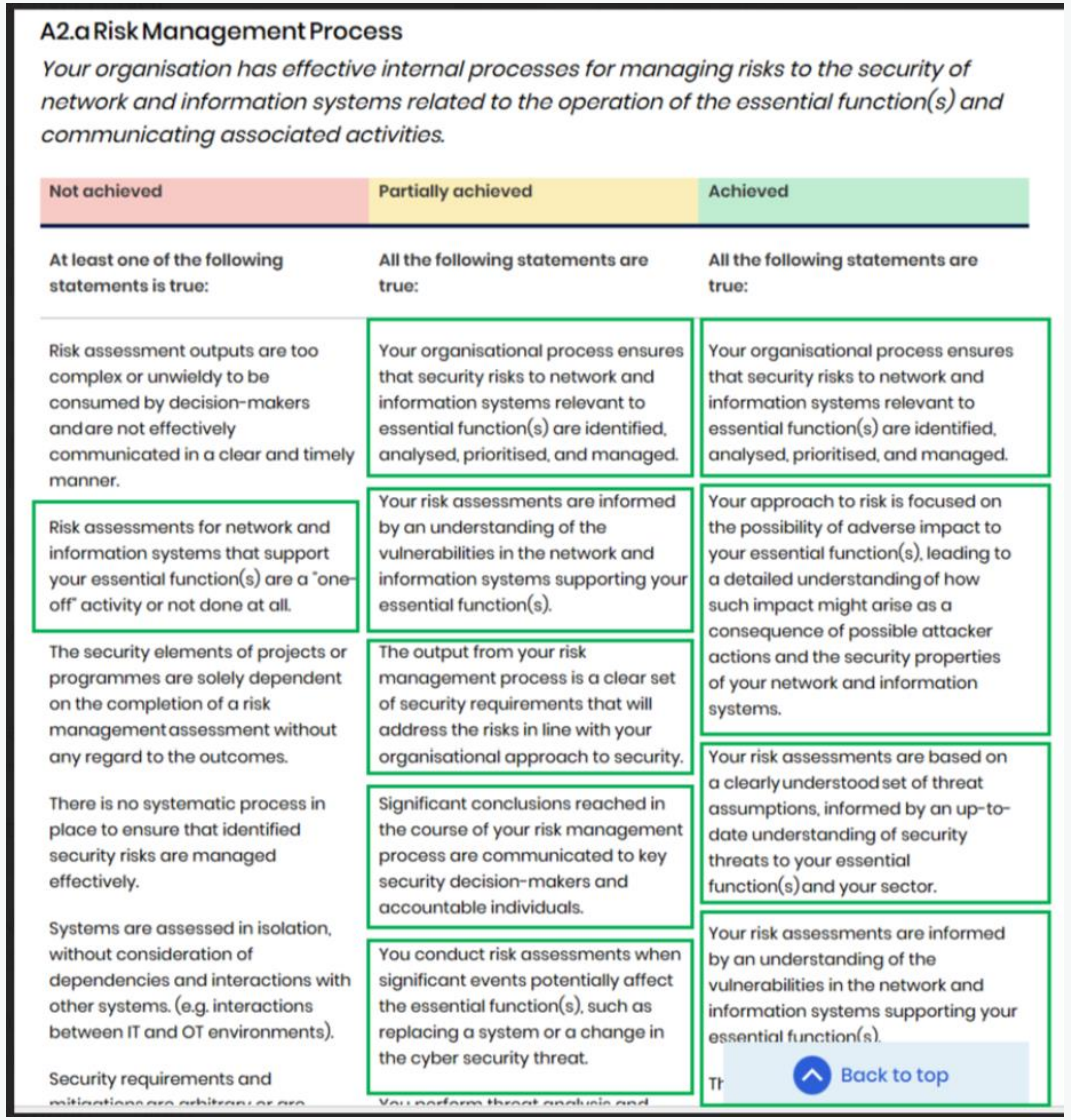
Answer

If any of the Indicators listed under Not achieved are true, you should mark yourselves Not Achieved.

Rationale

The indicators listed under ‘Not achieved’ list statements which are incompatible with achieving or partially achieving the outcome.

Security chain is only as strong as the weakest link. The best security capabilities in the world aren’t much use if there’s a great big hole in the middle.



A2.a Risk Management Process

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of the essential function(s) and communicating associated activities.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true:	All the following statements are true:	All the following statements are true:
Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.
Risk assessments for network and information systems that support your essential function(s) are a "one-off" activity or not done at all.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).	Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your network and information systems.
The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.	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.	Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function(s) and your sector.
There is no systematic process in place to ensure that identified security risks are managed effectively.	Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).
Systems are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).	You conduct risk assessments when significant events potentially affect the essential function(s), such as replacing a system or a change in the cyber security threat.	Th
Security requirements and mitigations are arbitrary or are	You perform threat analysis and	

Back to top

A2.a Risk Management Process

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of the essential function(s) and communicating associated activities.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true:	All the following statements are true:	All the following statements are true:
Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.
Risk assessments for network and information systems that support your essential function(s) are a "one-off" activity or not done at all.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).	Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your network and information systems.
The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.	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.	Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function(s) and your sector.
There is no systematic process in place to ensure that identified security risks are managed effectively.	Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).
Systems are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).	You conduct risk assessments when significant events potentially affect the essential function(s), such as replacing a system or a change in the cyber security threat.	Th
Security requirements and mitigations are arbitrary or are	You perform threat analysis and	

Back to top

SCENARIO 3

Is this a **PA, NA, A**?

RED Frame = FALSE
GREEN Frame = TRUE

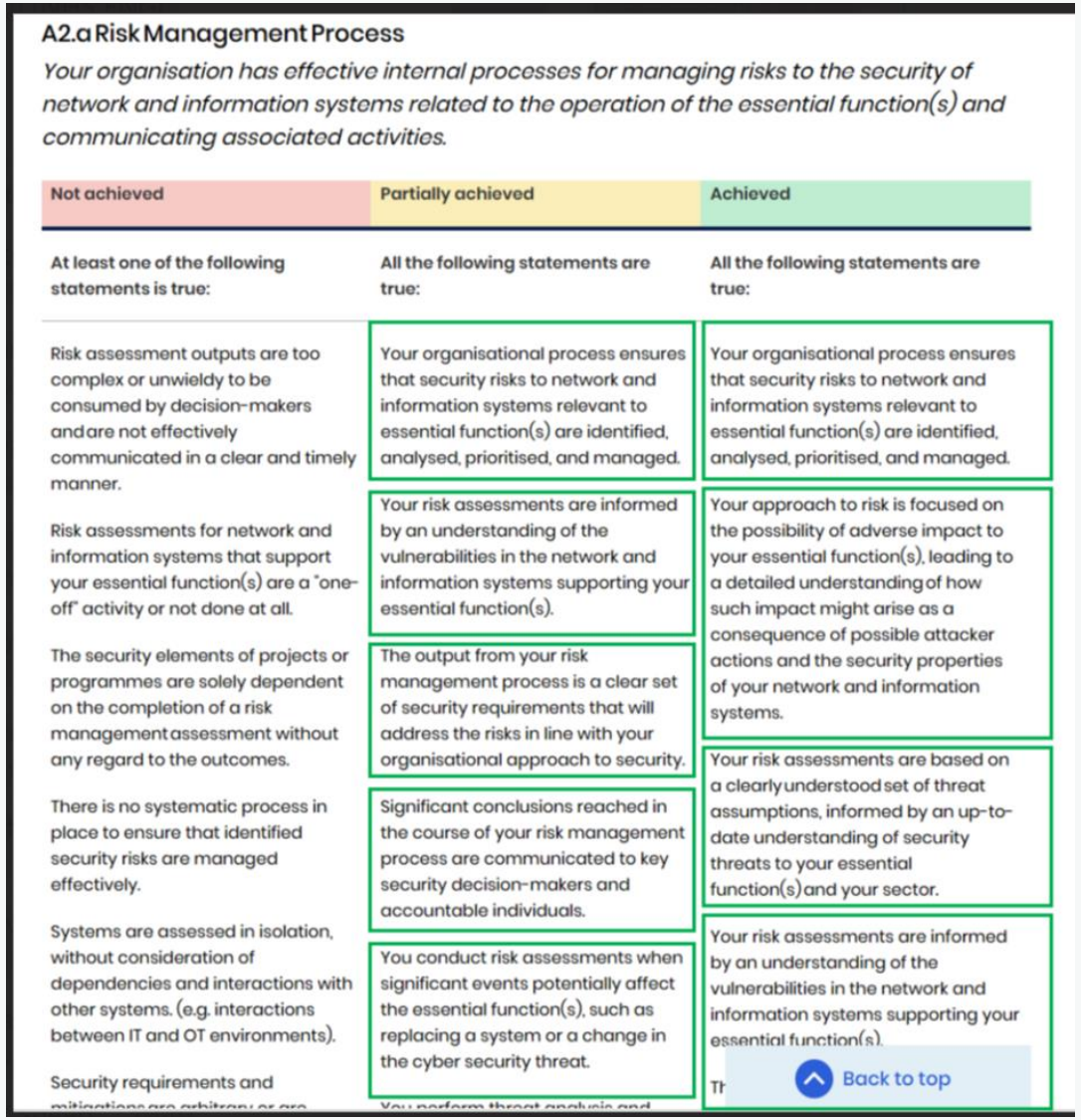
Answer:

If all the Indicators listed under Achieved are true, you should mark yourselves Achieved.

Rationale

In every Contributing Outcome which features a PA column, there are either repetitions of IGPs from the PA to the A column so that PA practices are not lost at the highest level of achievement, or the wording of IGPs under A is changed to represent a strengthening of these same practices.

If the indicators in Achieved are true, this supersedes Partially achieved indicators being true.



A2.a Risk Management Process

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of the essential function(s) and communicating associated activities.

Not achieved	Partially achieved	Achieved
At least one of the following statements is true:	All the following statements are true:	All the following statements are true:
Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.
Risk assessments for network and information systems that support your essential function(s) are a "one-off" activity or not done at all.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).	Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your network and information systems.
The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.	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.	Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function(s) and your sector.
There is no systematic process in place to ensure that identified security risks are managed effectively.	Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).
Systems are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).	You conduct risk assessments when significant events potentially affect the essential function(s), such as replacing a system or a change in the cyber security threat.	
Security requirements and		

Back to top

Principle: A2 Risk management

Contributing outcome: A2.b Assurance

Contributing outcome A2.b

Assurance

You have gained confidence in the effectiveness of the security and governance of your technology, people, and processes relevant to your essential function(s).

Expectation

The baseline expectation for this contributing outcome is ***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 A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value.

NA#2 Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments.

NA#3 Assurance is assumed because there have been no known problems to date.

◯ **Achieved**

All the following statements are true.

A#1 You validate that the security and governance measures in place to protect information, systems and networks are effective and remain effective for the lifetime over which they are needed.

A#2 You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential function(s).

A#3 Your confidence in the security and governance as it relates to your technology, people, and processes can be justified to, and verified by, a third party.

A#4 Security and governance deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.

A#5 The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.

Principle: A2 Risk management

Contributing outcome: A2.b Assurance

DSPT Mapping and Guidance

Contributing outcome	DSPT V6
	() weak map
A2.b Assurance: You have gained confidence in the effectiveness of the security and governance of your technology, people and processes relevant to your essential function(s).	9.2.1 9.2.3 9.4.1 9.4.4 9.4.5

Assurance

Assurance is about gaining confidence that your cyber security and IG controls are working effectively. To achieve this, you should employ an array of techniques to proactively test your people, processes and technology. Any weak points identified through your assurance activities should be documented and followed up on.

You should undertake your assurance activities on a scheduled basis to ensure that the measures you have in place have not been compromised by changing circumstances or new threats.

See NCSC's guidance on how to gain and maintain assurance for more information.

Understanding and reviewing assurance methods

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

Under the CAF-aligned DSPT framework, you should understand the assurance methods that are available and review the ones you use to ensure they remain effective. This might mean, for example, optimising your vulnerability testing process or focussing your spot checks on specific areas identified as weak points.

As part of your review of you may consider whether you are making most effective use of assurance activities such as:

- penetration testing
- behavioural testing (e.g. simulated phishing exercises)
- spot checks of the premises (e.g. physical security of the building, locked cabinets, staff and visitor ID badges, paper waste, computer equipment)

Principle: A2 Risk management

Contributing outcome: A2.b Assurance

DSPT Supporting evidence

Contributing outcome	DSPT V6
	() weak map
A2.b Assurance: You have gained confidence in the effectiveness of the security and governance of your technology, people and processes relevant to your essential function(s).	9.2.1 9.2.3 9.4.1 9.4.4 9.4.5

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 or groups
- Independent penetration testing and vulnerability assessment reports
- Documents showing follow-up actions taken
- DSPT audit reports
- Organisation security certifications i.e. CE, CE+, ISO27001.
- Incident response records

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.

Additional guidance

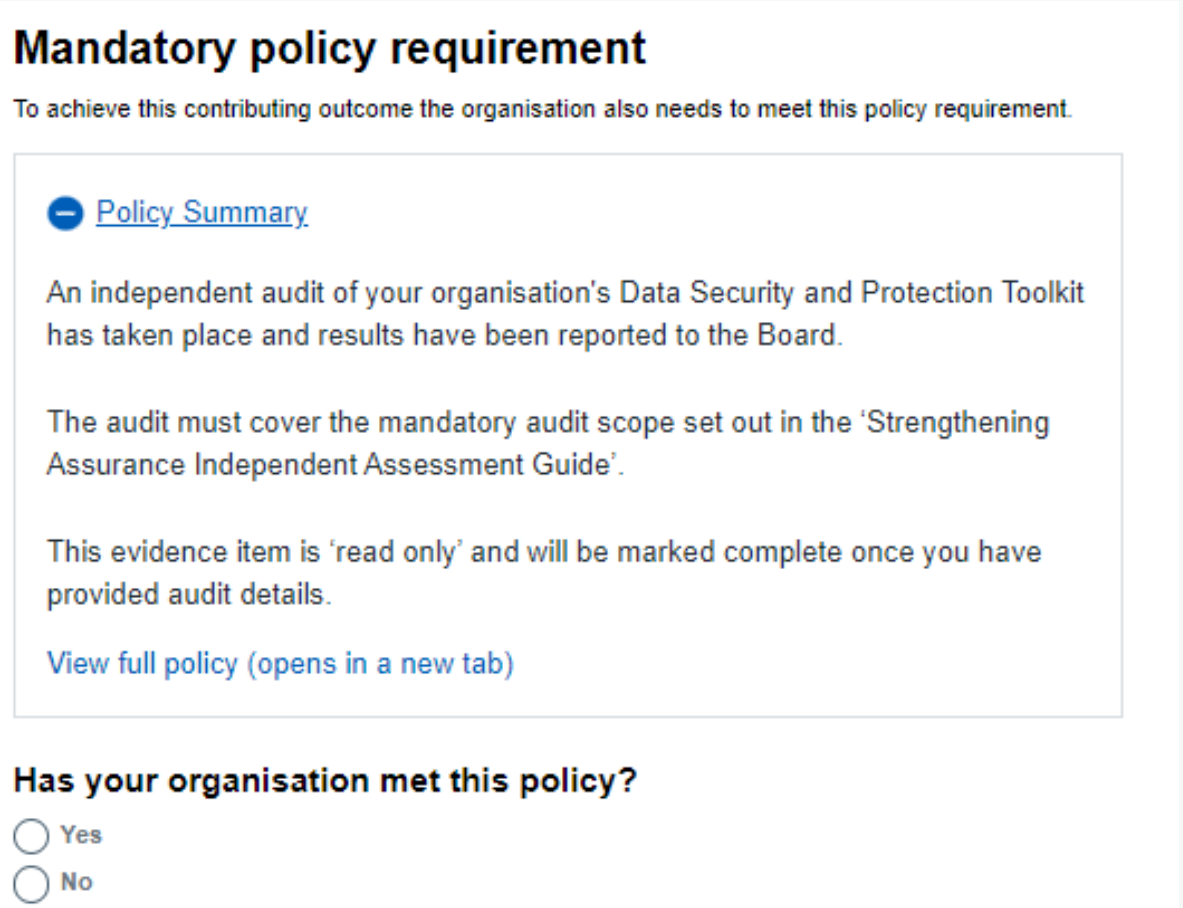
For additional guidance, see:

National Cyber Security Centre CAF guidance | A2 Risk management
National Cyber Security Centre | Risk management - How to gain and maintain assurance
National Cyber Security Centre | Penetration testing

Principle: A2 Risk management

Contributing outcome: A2.b Assurance

Mandatory Policy requirement



Principle: A2 Risk management

Contributing outcome: A2.b Assurance

Interpretations

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
A#2 You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of **essential function(s)**.	"essential function(s)"	Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions. For more information, see guidance on scoping essential functions.

Principle: A3 Asset management

Contributing outcome: A3.a Asset management

Contributing outcome A3.a

Asset management

Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).

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 Inventories of assets relevant to the essential function(s) are incomplete, non-existent, or inadequately detailed.

NA#2 Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT).

NA#3 Information assets, which could include personally identifiable information and / or important / critical data, are stored for long periods of time with no clear business need or retention policy.

NA#4 Knowledge critical to the management, operation, or recovery of essential function(s) is held by one or two key individuals with no succession plan.

NA#5 Asset inventories are neglected and out of date.

◯ **Achieved**

All the following statements are true.

A#1 All assets relevant to the secure operation of essential function(s) are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.

A#2 Dependencies on supporting infrastructure (e.g. power, cooling etc) are recognised and recorded.

A#3 You have prioritised your assets according to their importance to the operation of the essential function(s).

A#4 You have assigned responsibility for managing all assets, including physical assets, relevant to the operation of the essential function(s).

A#5 Assets relevant to essential function(s) are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.

Principle: A3 Risk management

Contributing outcome:
A3.a Asset management

DSPT Mapping and Guidance

Contributing outcome	DSPT V6 *() weak map*
A3.a Asset management	1.1.2 1.1.4 7.1.1 8.1.1 8.1.2 9.3.5 9.3.8 9.3.9 9.5.3

Identifying and documenting assets

All assets which are important to the operation of your essential function should be identified and documented. These include:

- information assets
- hardware assets
- software assets
- connected medical devices
- systems storing personal data
- systems storing business and commercial data

Information asset register (IAR)

Identifying and inventorying information assets is done via your organisation's Information Asset Register (IAR). You should maintain an up-to-date IAR documenting the information assets your organisation holds, 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 IAR with the Record of Processing Activities (ROPA) 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 information governance (IG) document templates and digital platforms that serve an IAR/ROPA purpose.

Maintaining an up to date IAFR gives 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.

Hardware, software, connected medical devices and other assets

For your hardware assets and the software on them, a survey tool will help you catalogue your estate in detail without having to undergo an intensive manual review. You should be aware of the limitations of your chosen tool(s), for example, survey tools may not be able to track installed software.

There is not a singular prescribed method for how assets should be documented. However, at a minimum, your inventory of assets should include details of each asset's:

- type
- location
- software
- owner
- support and maintenance arrangements
- nature and quantity of data
- criticality to the delivery of services
- relevance to the NIS regulations (if appropriate)

Principle: A3 Risk management

Contributing outcome:
A3.a Asset management

DSPT Mapping and Guidance

Contributing outcome	DSPT V6 *() weak map*
A3.a Asset management	1.1.2 1.1.4 7.1.1 8.1.1 8.1.2 9.3.5 9.3.8 9.3.9 9.5.3

Connected medical devices

You should also have a way of cataloguing your organisation's connected medical devices. You can expand an existing register or create a new bespoke register for this purpose, which should include the following details:

- all details you would include in your asset register
- vendor
- support and maintenance arrangements
- any network segmentation in place and whether network access is given to supplier
- network name
- IP address (if static)

For systems holding personal information, it is likely that there will be some overlap between the asset inventory and your information assets and flows register (IAFR).

The registers you hold should ideally be linked or synchronised and enhanced with products such as asset discovery tools.

Asset management

You should have an asset management process which ensures that:

- obsolete devices are identified and managed
- vulnerabilities identified across the sector are cross-referenced against the devices and software on your networks
- suitable controls are applied wherever assets are reused, transferred or disposed of (see B3.e Media / equipment sanitisation)

Assigning responsibility for managing assets

All assets should be assigned to an owner within the organisation who holds ultimate responsibility for managing them.

The owner should understand:

- where the asset is stored
- what the asset is used for
- how access to the asset is controlled
- areas of potential risk – for example, loss of personal data
- how the asset should be transferred or disposed of

Principle: A3 Risk management

Contributing outcome:
A3.a Asset management

DSPT Supporting evidence

Contributing outcome	DSPT V6
	() weak map
A3.a Asset management	1.1.2 1.1.4 7.1.1 8.1.1 8.1.2 9.3.5 9.3.8 9.3.9 9.5.3

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:

- Asset registers
- Inventory audit reports
- Criteria for asset classification
- Risk assessments
- Policy, process, procedure or strategy documents (e.g. asset management, IT disposal, IP address management)
- Data destruction certificates
- High-level network architecture diagrams

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.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | A3 Asset management
National Cyber Security Centre | Asset management

Principle: A3 Risk management

Contributing outcome:
A3.a Asset management

Interpretations

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
A#1 All assets relevant to the secure operation of **essential function(s)** are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date	"essential function(s)"	Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions. For more information, see guidance on scoping essential functions.

Principle: A4 Supply Chain

Contributing outcome: A4.a Supply Chain

Contributing outcome A4.a

Supply chain

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

Expectation

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

◉ Not achieved

At least one of the following statements is true.

NA#1 You do not know what data belonging to you is held by suppliers, or how it is managed.

NA#2 Elements of the supply chain for essential function(s) are subcontracted and you have little or no visibility of the sub-contractors.

NA#3 You have no understanding of which contracts are relevant and / or relevant contracts do not specify appropriate security or IG obligations.

NA#4 Suppliers have access to systems that provide your essential function(s) that is unrestricted, not monitored or bypasses your own security controls.

NA#5 IG is not factored into the procurement process.

NA#6 You are not sure if any data shared with suppliers leaves the UK, or if all international data transfers are covered by a legal protection.

◯ Partially achieved

All the following statements are true.

PA#1 You understand the general risks suppliers may pose to your essential function(s).

PA#2 You know the extent of your supply chain for essential function(s), including sub-contractors.

PA#3 You understand which contracts are relevant and you include appropriate security and data protection obligations in relevant contracts.

PA#4 You are aware of all third-party connections and have assurance that they meet your organisation's security and IG requirements.

PA#5 Your approach to security and data protection incident management considers incidents that might arise in your supply chain.

PA#6 You have confidence that information shared with suppliers that is necessary for the operation of your essential function(s) is appropriately protected from well-known attacks and known vulnerabilities.

PA#7 All international data transfers to suppliers are covered by a legal protection.

◯ Achieved

All the following statements are true.

A#1 You have a deep understanding of your supply chain, including sub-contractors and the wider risks it faces. You consider factors such as IG considerations, due diligence, supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your risk assessment and procurement processes.

A#2 Your approach to supply chain risk management considers the risks to your essential function(s) arising from supply chain subversion by capable and well-resourced attackers.

A#3 You have confidence that information shared with suppliers that is essential to the operation of your function(s) is appropriately protected from sophisticated attacks.

A#4 You understand which contracts are relevant and you include appropriate security and data protection obligations in relevant contracts. You have a proactive approach to contract management which may include a contract management plan for relevant contracts.

A#5 Customer / supplier ownership of responsibilities are laid out in contracts.

A#6 All network connections and data sharing with third parties is managed effectively and proportionately.

A#7 When appropriate, your incident management process and that of your suppliers provide mutual support in the resolution of incidents.

A#8 You routinely liaise with other teams to keep track of changes to services that impact your organisation's agreements.

A#9 All international data transfers to suppliers are covered by a legal protection.

A#10 Your processor has appropriate certification and agree to be audited either by your organisation or an independent auditor.

Principle: A4 Supply Chain

Contributing outcome: A4.a Supply Chain

DSPT Mapping and Guidance

Contributing outcome	DSPT V6 *() weak map*
A4.a Supply chain	1.3.5*
	1.3.7*
	4.5.5
	7.1.1
	9.3.8
	9.3.9
	10.1.1
	10.1.2*
	10.2.1
	10.2.3-5
	10.3.1

* Only maps in health and care

Supply chain

It is your responsibility to understand the risks posed to the operation of your essential function by your supply chain, and to put appropriate controls in place to mitigate those risks.

As part of your scoping exercise, you should have identified the information, systems and networks supporting your essential function which are administered by or require the involvement of suppliers. From here, you can work to understand what controls you need in place to ensure the security of those supplier systems and networks.

Contracts

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

Reviewing contracts with third parties and identifying those with data security contract clauses in place was a non-mandatory requirement in the 23-24 DSPT.

Under the CAF-aligned DSPT framework, it is now essential to conduct a review and ensure that appropriate security and data protection obligations are included in relevant contracts. As part of your review, you should consider all suppliers providing services or systems involved in the delivery of care, and all suppliers with access to confidential patient information.

There may be suppliers whose services would not impact the delivery of care if compromised for a short period of time, such as HR systems. It may still worth factoring these suppliers into your review from a time-bound perspective in case of prolonged disruptions.

Principle: A4 Supply Chain

Contributing outcome: A4.a Supply Chain

DSPT Mapping and Guidance

Contributing outcome	DSPT V6 () weak map
A4.a Supply chain	1.3.5*
	1.3.7*
	4.5.5
	7.1.1
	9.3.8
	9.3.9
	10.1.1
	10.1.2*
	10.2.1
	10.2.3-5
	10.3.1

* Only maps in health and care

Cyber security obligations

You should determine which cyber security obligations you include in supplier contracts based on the service being provided, and the risk to your essential functions if the supplier were to become compromised by an incident.

Examples of cyber security obligations to consider are:

- **Right to audit** – the right to conduct audits of the supplier's infrastructure, systems, services and premises with appropriate notification or in case of an incident
- **Incident management** – the requirement for suppliers to inform your organisation of ongoing incidents and any impacts to your organisation
- **Assurance** – the requirement for the supplier to provide appropriate assurance evidence at the commencement of the contract and regularly throughout the lifetime of the contract (the specific requirements around this will vary depending upon system and data sensitivity)
- **Service Level Agreements (SLAs)** – these should also include security service levels covering out of hours support and reporting, handling and remediation of incidents
- **Vulnerability management** – the requirement for the supplier to keep the system, service or software patched and on up-to-date operating systems
- **Security governance** – the expectations of the organisation around security governance within the supplier including security risk management and signing off residual risks

Organisations are responsible for seeking their own legal advice and ensuring any contracts they sign are fit for purpose.

Data protection obligations

Any contracts or agreements with suppliers must have the appropriate clauses in place to cover the requirements of data protection legislation. If you are using a contract that does not have a section on data protection, you must also have a data processing agreement. See the ICO's guidance on Contracts for more information on data protection requirements.

The NHS universal data sharing and processing agreement (DSPA) template contains all of the necessary clauses needed to comply with UK GDPR and the Common Law Duty of Confidentiality. The NHS standard contract also covers relevant UK GDPR requirements.

Organisations are responsible for seeking their own legal advice and ensuring any contracts they sign are fit for purpose.

Principle: A4 Supply Chain

Contributing outcome: A4.a Supply Chain

DSPT Mapping and Guidance

Contributing outcome	DSPT V6
	() weak map
A4.a Supply chain	1.3.5*
	1.3.7*
	4.5.5
	7.1.1
	9.3.8
	9.3.9
	10.1.1
	10.1.2*
	10.2.1
	10.2.3-5
	10.3.1

* Only maps in health and care

Supplier assurance

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

The CAF-aligned DSPT framework requires you to obtain assurance that all third-party connections to your network meet your security and IG requirements, and that any information you share with suppliers for the delivery of healthcare services is appropriately protected.

This will require engagement with your supply chain. In cases where you encounter obstacles to retrieving the information you need, these should be flagged in your DSPT response along with any mitigating actions you have taken.

Incidents arising in your supply chain

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

The CAF-aligned DSPT framework requires you to consider data security and protection incidents that might arise in your supply chain. This consideration of supply chain incidents may be reflected in a number of documents, including your due diligence processes, your incident response plans, and the contracts and agreements you have in place with suppliers.

Any supplier incidents or near misses that have a data security or data protection implication should be recorded.

Principle: A4 Supply Chain

Contributing outcome: A4.a Supply Chain

DSPT Supporting evidence

Contributing outcome	DSPT V6 () weak map
A4.a Supply chain	1.3.5*
	1.3.7*
	4.5.5
	7.1.1
	9.3.8
	9.3.9
	10.1.1
	10.1.2*
	10.2.1
	10.2.3-5
	10.3.1

* Only maps in health and care

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:

- Overview of contractual agreements in place
- Supplier contracts
- Current data sharing agreements
- Current data processing agreements
- Policy, process, procedure or strategy documents (e.g. third party contracts, procurement)
- Incident response plans
- Supplier's due diligence and assurance procedures
- Supplier's contracts database for services and products

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.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | A4 Supply chain
National Cyber Security Centre | Supply chain
Information Commissioner's Office | Contracts and data sharing

Principle: A4 Supply Chain

Contributing outcome: A4.a Supply Chain

Interpretations

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#1 You understand the general risks suppliers may pose to your **essential function(s)**.	"essential function(s)"	Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions. For more information, see guidance on scoping essential functions.
PA#3 You understand which contracts are relevant and you include appropriate security and data protection obligations in **relevant contracts**.	"relevant contracts"	This applies to all contracts you have that may have a cyber security or data protection impact. This will include, for example, catering services if they handle personal data that includes patient names and dietary requirements, and any supplier whose service includes an IT component.
PA#7 All international data transfers to suppliers are covered by a **legal protection**.	"legal protection"	You must be aware of all countries where data is being processed as part of any supplier-offered service. This should be documented in your Information Assets & Flows register (see A3.a Asset management and B3.a Understanding data). Where data is being processed by suppliers located in countries with no adequacy regulations, you must have an International Data Transfer Agreement in place. You can reference the IDTA documents within other agreements (such as the NHS Data Sharing and Processing Agreement (DSPA) or NHS standard contract) if needed.

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

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