Part of Objective A - Managing risk

Principle: A1 Governance

← Previous Chapter

Objective A - Managing risk

Current Chapter

Current chapter – Principle: A1 Governance

View all

Next Chapter →

Principle A2 Risk management

Page contents

A1.a Board direction

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

Overview

To meet this contributing outcome, you need to assure that your board is appropriately sighted and involved in your organisation's cyber security and information governance (IG) activities.

Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities which help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

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) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- minutes and terms of reference from relevant meetings or groups
- policy, process, procedure or strategy documents (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.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Interpreting indicators of good practice

Indicator of good practice	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.
Term	'essential function(s)'
Interpretation	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.

Indicator of good practice	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.
Term	'regular'
Interpretation	On a scheduled basis, with enough frequency to ensure there are no key strategic decisions made which the board does not have visibility of.

Indicator of good practice	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.
Term	'regular'
Interpretation	On a scheduled basis, with enough frequency to ensure there are no key strategic decisions made which the board does not have visibility of.

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

Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

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."

Overview

This contributing outcome relates to your organisation's cyber security and information governance (IG) activities being directed, delivered and followed by a team of appropriately knowledgeable and capable staff.

Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities which help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

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
- documented role descriptions
- 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.

Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- minutes and terms of reference 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 (such as 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.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Interpreting indicators of good practice

Indicator of good practice	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.
Term	'regularly'
Interpretation	On a scheduled basis, with enough frequency to ensure there are no critical gaps in cyber security or IG activities.

Indicator of good practice	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.
Term	'essential function(s)'
Interpretation	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.

Additional guidance

For additional guidance, see:

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

Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

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."

Overview

This contributing outcome relates to your organisational procedures for making decisions relating to cyber security and information governance (IG).

Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities which help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

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 and escalating where appropriate. 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.

Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- records of decisions made regarding the security of information, networks and systems
- risk assessment reports
- risk appetite statements
- minutes and terms of reference from relevant meetings or groups
- policy, process, procedure or strategy documents (such as 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.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

Interpreting indicators of good practice

Indicator of good practice	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.
Term	'essential function(s)'
Interpretation	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.

Indicator of good practice	A#4 Risk management decisions are regularly reviewed to ensure their continued relevance and validity.
Term	'regularly'
Interpretation	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.

Additional guidance

For additional guidance, see:

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

Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

Last edited: 13 September 2024 4:36 pm

← Previous Chapter

Objective A - Managing risk

Next Chapter →

Principle A2 Risk management

Chapters

Legal

Get in touch

Follow us on social media