Part of Objective B - Protecting against cyber attacks and data breaches

Principle: B6 Staff awareness and training

Previous Chapter

Principle: B5 Resilient networks and systems

Current Chapter

Current chapter – Principle: B6 Staff awareness and training

View all

Page contents

B6.a Culture

"You develop and maintain a positive culture around information assurance."

Overview

To achieve this outcome, you need to demonstrate that your organisation actively promotes a positive culture around 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 that 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).

Positive information assurance culture

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

This is why you must have a positive information assurance culture underpinning your policies, processes and procedures. It should be a 'just' culture, and emphasise the importance of recognising and reporting near misses, breaches and incidents.

This is key to building on improvements in your security posture and ensuring you have the support of staff members in protecting your essential service.

Executive management

All senior leaders on the board, including clinical leaders, must take an active interest in cyber security and IG matters, and act as role models for positive attitudes, behaviours and expectations around information assurance.

Examples of this include:

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

Staff members

All staff members should understand the contribution they make to the security and governance of your information, systems and networks, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

In relation to your information assurance policies, processes and procedures, staff members should understand:

- why they have a duty to follow them

- who they can speak to for direction (for example, your IT team or Caldicott Guardian)
- where they can find relevant documentation (for example, the location on your intranet where all policies, processes and procedures are stored)

Raising issues

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

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

Exceeding the 'Standards met' expectation for 2024-25

Raising issues

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

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

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

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:

- policy, process, procedure or strategy documents relating to reporting concerns
- records documenting reports received from staff members regarding phishing emails and data protection incidents
- minutes and terms of reference from relevant meetings and groups
- training and engagement materials

This is not an exhaustive list. You're 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(s) of good practice	PA#1 Your executive management understand and widely communicate the importance of a positive culture around information assurance. Positive attitudes, behaviours and expectations are described for your organisation.
Term	'information assurance'
Interpretation	For the purposes of the CAF-aligned DSPT, the phrase 'information assurance' should be interpreted as a collective term that encompasses cyber security, IG and confidentiality.

Indicator(s) of good practice	PA#2 All people in your organisation understand the contribution they make to the security and governance of information, systems and networks supporting your essential function(s).
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(s) of good practice	A#3 Individuals at all levels in your organisation routinely report concerns or issues about information assurance and are recognised for their contribution to keeping the organisation and its information secure.
Term	'routinely'
Interpretation	This should not be interpreted to mean that you are receiving frequent reports of concerns or issues, but rather that your staff

reliably report issues when they arise.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B6 Staff awareness and training
Information Commissioner's Office | Training and awareness

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.

B6.b Training

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

Overview

This outcome is about ensuring that a range of approaches to information assurance training, awareness and communications are employed to equip staff members with an appropriate level of understanding and awareness.

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 that 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).

Information assurance training paths

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

All staff working in a health and care organisation need some understanding of confidentiality, information governance (IG) and cyber security. They need to understand their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

The level of training will vary depending on the staff member’s role, for example:

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

Training needs analysis

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

Your TNA (or equivalent document) should:

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

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

Tracking and refreshing training activities

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

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

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

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

Information and good practice guidance

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

These include:

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

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:

- policy, process, procedure or strategy documents relating to staff training
- training needs analysis
- training material/s used for staff training
- minutes and terms of reference from relevant meetings and groups

This is not an exhaustive list. You're 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(s) of good practice	All people in your organisation, from the most senior to the most junior, follow appropriate information assurance training paths.
Term	'information assurance'
Interpretation	For the purposes of the CAF-aligned DSPT, the phrase 'information assurance' should be interpreted as a collective term that encompasses cyber security, IG and confidentiality.

Additional guidance

For additional guidance, see:

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

National Cyber Security Centre | Guidance and resources

NHS England | NCSC assured training

NHS England | NCSC assured cyber security for SIROs

NHS England | Simulated phishing service

NHS England | Cyber incident response exercise (CIRE)

NHS England | Immersive labs online cyber security e-learning

NHS England | IG portal

NHS England | Cyber and data security services and resources

Information Commissioner’s Office | Guidance and resources

Information Commissioner’s Office | Training and awareness

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: 19 September 2024 2:47 pm

← **Previous Chapter**

Principle: B5 Resilient networks and systems

Chapters

Legal

Get in touch

Contact us

Press office

Tell us what you think of our website

RSS feeds

Follow us on social media

Twitter

Facebook

LinkedIn

YouTube