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

Principle: B1 Policies, processes and procedures

← Previous Chapter

Objective B - Protecting against cyber attacks and data breaches

Current Chapter

Current chapter – Principle: B1 Policies, processes and procedures

View all

Next Chapter →

Principle: B2 Identity and access control

Page contents

B1.a Policy, process and procedure development

"You have developed and continue to improve a set of information assurance and resilience policies, processes and procedures that manage and mitigate the risk of adverse impact on your essential function(s)."

Overview

This outcome is about ensuring that you have effective cyber security and information governance (IG) policies, processes and procedures in place.

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).

Policies, processes and procedures

Your organisation should have a suite of policies, processes and procedures in place to guide its cyber security and IG activities. You should appropriately scope the policies to cover your people, processes and technology. The policies should be driven by risks and signed off by the Board representative.

You should also review your policies, processes and procedures on a scheduled basis, with a justifiable rationale for time intervals between reviews, and whenever significant changes occur. Your approach should ensure they remain effective at delivering the desired outcomes and that they are appropriate in the context of existing legislation and regulatory guidance.

These policies, processes and procedures should be documented in a central location accessible to all staff who need to refer to them, along with accompanying registers or logs which show how they have been approved, reviewed and managed over time.

Examples of areas your policies, processes and procedures should cover, but not be limited to, include:

- IG-oriented topics such as confidentiality and data protection, data breaches, consent, data protection by design, data protection impact assessments, transparency, data subject rights and information sharing
- cyber security-oriented topics such as information technology (IT) acceptable use policy, data security, asset management, access control, change management, business continuity and disaster recovery, encryption, anti-virus/malware, vulnerability management, patch management, network security, problem management, data backups, remote working and portable devices, IT disposal, configuration management, security logs, events management
- supply chain-oriented topics, such as: procurement, contracts, supplier obligations for data security and protection, incident management support

- risk management and assurance
- incident management
- records management
- data quality
- re-use of public sector information (if applicable)
- freedom of information (FOI) and environmental information regulations (if applicable)

Technical security practice and specific regulatory compliance

Reading through all contributing outcomes of the Cyber Assessment Framework (CAF)-aligned DSPT framework, in conjunction with any regulatory guidance, should give you an overview of the technical and regulatory areas your policies should cover. NHS England and DHSC do not mandate a specific approach for how you should cover them, outside of the specific areas where directive policies have been set which you must comply with to achieve specific CAF-aligned DSPT outcomes.

You should use your professional judgment to determine whether your suite of policies appropriately guides your technical security practices and meets regulatory compliance.

Good reference points for technical security practice and specific regulatory compliance in cyber security and IG include:

- NHS England cyber and data security guidance and resources
- National Cyber Security Centre guidance and resources
- Cyber Associate's Network
- NHS England IG portal
- The national health and care 'strategic information governance network' (SIGN)

National policies and legal frameworks

Ensuring local policies reflect changes at the legal and national level should be part of your policy, process and procedures review process. You can engage with communities of practice, national communications and NHS England and DHSC resources (such as the NHS England IG portal) to ensure that you are aware of changes in the law and national policy directives, and how they impact your local policies.

Each legal entity is fully accountable for all their own legal obligations. The requirements of the DSPT do not represent the entirety of these obligations, and organisations should seek legal assurances separately where necessary to ensure they are complying with the law.

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 groups and meetings
- reports to the board
- policy, process, procedure or strategy documents
- registers, indexes or logs of policies detailing information such as approval dates, last review, approving committee, individuals responsible
- guidance produced for staff to support policies and processes

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 areas of good practice

Indicator(s) of good practice	PA#1 Your policies, processes and procedures document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance.
Term	'policies, processes and procedures'
Interpretation	A 'policy' is a deliberate system of rules to guide decisions and achieve desired outcomes. A policy can be considered as a simple statement of your organisation's position on a chosen topic (the 'why'). 'Processes' or 'procedures' are practical steps to complete a given task, which might contribute towards the implementation of a policy (the 'how'). How you define what constitutes a 'policy', a 'process' or a 'procedure' is not important. What is important is that together, they set out clear, documented expectations for how data security and protection-related activities should be conducted within your organisation.

Indicator(s) of good practice	A#2 Your organisation's policies, processes and procedures are developed to be practical, usable and appropriate for your essential function(s) and your technologies.
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 | B1 Service protection policies, processes and procedures
Information Commissioner's Office | Policies and procedures

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.

B1.b Policy, process and procedure implementation

"You have successfully implemented your information assurance policies, processes and procedures and can demonstrate the benefits achieved."

Overview

This outcome is about ensuring that your organisation's cyber security and information governance (IG) policies and processes are effectively implemented and followed.

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).

Monitoring policies, processes and procedures

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

Spot checks should form part of your policy, process and procedure monitoring activities. Areas could include, but should not be limited to:

- joiner/mover/leaver processes, for example checking that departed staff members have promptly had access rights revoked
- privileged access, for example continuously reviewing staff members with elevated access rights and ensuring they still have a legitimate business need
- change management, for example gathering staff members' feedback on procedural changes
- asset management such as checking whether new assets and data flows are being appropriately registered
- information sharing, such as the recording of ad hoc disclosures for purposes other than direct care
- individual rights, for example checking compliance with administering individual rights requests within statutory time frames
- incident reporting, for example comparing incident reporting numbers or time taken to report incidents across departments

Breaches of policies, processes and procedures

You may become aware of breaches of your policies, process and procedures through alerts, reports and investigations.

You should take a consistent, documented approach to investigating and using these breaches to make improvements. This might mean:

- ensuring policies, processes and procedures, as well as accountability for deliberate or avoidable breaches, are communicated to staff members
- reinforcing policies, processes and procedures through training
- conducting additional spot checks to ensure lessons have been learned
- considering amendments to policies, processes or procedures where these are found to be inadequate or difficult to follow

With an understanding of how and why policies are not being followed, you can undertake trend analysis and take corrective action to address the problem.

See 'D2.b Using incidents and near misses to drive improvements' for additional considerations to be made when the policy, process or procedural breach is associated with an incident or near miss.

Staff awareness

Your training should be designed to make staff members aware of information assurance policies, processes and procedures that are relevant to their role, and ensure they have the skills to implement them.

In addition, all staff with access to confidential patient information should be aware of their obligation to handle information responsibly and the accountability they hold

for deliberate or avoidable breaches.

See 'B6.b Training' for more information.

Integrating policies, processes and procedures across your organisation

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

Under the CAF-aligned DSPT framework, you should demonstrate that you have considered areas of your organisation where business processes should be integrated with cyber security and IG processes to improve overall data protection and security resilience. Some typical examples are:

- procurement – integrating data protection and security considerations into contracting, re-contracting and due diligence procedures (see 'A4.a Supply chain')
- HR – linking joiners, movers and leavers events with identity and access management controls
- HR – reviewing system permissions following disciplinary action
- communications and engagement – ensuring adherence to data protection and security principles in outgoing communications

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 and groups
- monitoring reports
- policy, process, procedure or strategy documents
- communication chains between departments
- training needs analysis and training reports
- details of actions taken to improve levels of policy compliance

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

Most of your policies, processes and procedures are followed and their application is monitored.

Term	'policies, processes and procedures'
Interpretation	A 'policy' is a deliberate system of rules to guide decisions and achieve desired outcomes. A policy can be considered as a simple statement of your organisation's position on a chosen topic (the 'why'). 'Processes' or 'procedures' are practical steps to complete a given task, which might contribute towards the implementation of a policy (the 'how'). How you define what constitutes a 'policy', a 'process' or a 'procedure' is not important. What is important is that together, they set out clear, documented expectations for how data security and protection-related activities should be conducted within your organisation.

Indicator(s) of good practice	PA#4 All breaches of policies, processes and procedures with the potential to adversely impact the essential function(s) are fully investigated. Other breaches are tracked, assessed for trends and action is taken to understand and address.
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 | B1 Service protection policies, processes and procedures
National Cyber Security Centre | You shape security
NHS England | Microsoft Defender for Endpoint service
NHS England | Cyber assurance service
Information Commissioner's Office | Policies and procedures

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 2:34 pm

← **Previous Chapter**

Objective B - Protecting against cyber attacks and data breaches

Next Chapter →

Principle: B2 Identity and access control

Chapters

Legal

Privacy and cookies

Terms and conditions

Looking after your data

Freedom of information

Modern Slavery Act Statement

Accessibility

Change cookie settings

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