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

Principle: B4 System security

← Previous Chapter

Principle: B3 Data security

Current Chapter

Current chapter – Principle: B4 System security

View all

Next Chapter →

Principle: B5 Resilient networks and systems

Page contents

B4.a Secure by design

> “You design security into the network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential function(s) should not be impacted by the exploitation of any single vulnerability.”

Overview

To achieve this outcome, you need to demonstrate that your system design has been constructed through a secure by design approach, lowering the chance of compromise and enabling more efficient recovery.

Please note that this outcome is focussed on cyber security ‘secure by design’ controls. For information governance (IG) controls required for ‘data protection by design and by default’, please see ‘A2.a Risk management process’.

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).

Designing network and information systems

You must take a secure by design approach to ensure that effective cyber security practices are incorporated into your system design, including systems procured from third parties. This means having informed experts in your organisation who can make judgments on the way networks and systems are constructed that make your essential service less vulnerable to compromise and easier to recover in the event of an incident.

Boundary defences

To design strong boundary defences, you need to identify all the points in your network and systems which external and internal organisations and actors can connect to.

For each point of connection, you should have a technical solution in place (such as a firewall, authentication protocol, intrusion detection or prevention system) which blocks unapproved connections, manages access and validates message format and content.

Data flows

Where you have data flows going between your organisation and external networks, for example when working with a third-party supplier who processes or stores data on your behalf for the provision of services, the data flows should be encrypted end-to-end to ensure the confidentiality of the data.

Simple validation and authentication measures should be implemented for all your data flows to ensure the integrity of the data being transferred.

Designing for system recovery

To show that you have designed for system recovery, you should evidence that you have made deliberate design decisions whilst building your network to simplify recovery processes.

These might include consideration of:

- device naming conventions
- network addressing schemes and registers
- standard builds
- automated deployment
- network segmentation
- configuration management automation
- infrastructure as code

You should be able to rationalise how these build decisions have contributed towards recovery of your systems from potential incidents being simpler, faster or less resource-intensive.

Content-based attacks

To protect against content-based attacks, you should implement solutions at your network boundaries which analyse incoming data and transform, block or filter out harmful content. See NCSC guidance on content based attack protection for more information.

Exceeding the 'Standards met' expectation for 2024-25

Data flows

To meet the highest achievement benchmark, your design and protections of data flows should extend to those between components of your own network and information systems, not only those crossing your network perimeter. Simple and well-understood data flows within your systems will support recovery planning, and enable effective protections and security monitoring within your network.

Content-based attacks

To meet the highest achievement benchmark, your systems should have input controls that effectively mitigate content-based attacks irrespective of source, and not rely only on monitoring or on controls only at your network perimeter.

You should also use appropriate defensive techniques to reduce the likelihood of content-based attacks, which may include:

- rapid patching

- uni-directional flow control
- use of a simple transfer protocol with strong cryptographic algorithms
- message content verification
- message transformation

Security zones

You should design your network with the segregation principle in mind, dividing your networks and systems into zones according to the security requirements of their assets. A risk analysis should determine the level of security required for each zone and guide the technical and physical solutions you put in place.

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:

- network diagrams
- data flows diagrams
- interface control documents
- policy, process, procedure or strategy documents relating to logging and monitoring, physical and network security
- risk registers

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	NA#2 Internet access is available without restriction or business need from network and information systems supporting your essential function(s).
Term	'without restriction or business need'
Interpretation	'Without restriction' would mean that there are no solutions in place to: monitor and analyse incoming and outgoing internet traffic block or filter out harmful content block unapproved connections manage internet access

'Without business need' would mean that there is no documented policy, process or procedure establishing:

acceptable use of the internet

which staff member groups have a legitimate business need to access the internet

how legitimate internet access is managed

Indicator(s) of good practice	PA#5 All inputs to network and information systems supporting your essential function(s) are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.
Term	'inputs'
Interpretation	'Inputs' are all data flows, connections and telemetry traffic coming into your organisation's corporate network or to an organisational device (such as a server).

Indicator(s) of good practice	PA#5 All inputs to network and information systems supporting your essential function(s) are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.
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 | B4 System security

National Cyber Security Centre | Secure design principles

NHS England | Network segmentation - An introduction for health and care organisations

NHS England | Network segmentation for connected medical devices
NHS England | Backups and Office 365
NHS England | Public key infrastructure documentation
NHS England | Public key infrastructure root certification authority information
NHS England | Secure boundary service
NHS England | Vulnerability monitoring service
NHS England | Cyber assurance service
NHS England | Bitsight cyber security ratings service

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.

B4.b Secure configuration

> "You securely configure the network and information systems that support the operation of your essential function(s)."

Overview

This outcome is about the way you configure devices across your estate to guard against a variety of threats.

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).

Configuring assets

Assets which need to be carefully configured to maintain the security of your essential functions should be identified in the documentation you use to catalogue your assets (see 'A3.a Asset management'). This includes network devices such as switches, firewalls and virtual private network (VPN) software.

You should be able to rationalise the way these assets have been configured to reduce the possibility of compromise.

Secure platform and device builds

You should use a collection of base images which are appropriate for your environment to build your end user devices.

Unnecessary services and connectivity should be disabled.

Changes to security configurations

All changes to security configurations should be approved and documented. It will help further down the line to have clear context and a rationalisation for why each change decision was made.

Verifying software

You should implement technical controls on your devices which control the software that can be installed. For example:

- deploying application allow listing technology
- restricting local administrative access rights

See NCSC's guidance on device security for more information.

Exceeding the 'Standards met' expectation for 2024-25

Configuring assets

To meet the highest bar of achievement, you need to demonstrate that you are actively managing the configuration of your assets. This means having detailed policies, processes and procedures to ensure assets are updated with the latest approved patches, keeping a register of any missed updates and documenting all associated risks.

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:

- information assets and flows register/information asset register
- policy, process, procedure or strategy documents relating to device management including information on configurations and patching, changes to security configurations
- baseline builds and build images
- risk registers

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 You have identified and documented the assets that need to be carefully configured to maintain the security of the 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	PA#6 Generic, shared, default name and built in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed.
Term	'Generic, shared default name and built in accounts'
Interpretation	Generic accounts – any user account not tied to a specific employee (includes all of the examples below). Shared accounts – an account shared by multiple employees. Default name accounts – a pre-set account that has standard permissions for basic use of the system or software, commonly named 'admin', 'user', or 'guest'. Built in accounts – the first account created when the operating system (OS) was installed, typically intended to facilitate system setup.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B4 System security

National Cyber Security Centre | Device security guidance

Centre for Internet Security | CIS Benchmarks - prescriptive configuration recommendations
NHS England | Network segmentation for connected medical devices
NHS England | Backups and Office 365
NHS England | Public key infrastructure documentation
NHS England | Public key infrastructure root certification authority information
NHS England | Secure boundary service
NHS England | Vulnerability monitoring service
NHS England | Cyber assurance service
NHS England | Bitsight cyber security ratings service

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.

B4.c Secure management

> "You manage your organisation's network and information systems that support the operation of your essential function(s) to enable and maintain security."

Overview

This outcome relates to you having a robust system management practices which combine technical, procedural and physical measures.

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).

Administration and maintenance of systems and devices

Privileged operations such as system administration should only be carried out from corporately owned and managed devices, with controls in place to separate those privileged operations from normal user activity. Examples of this type of control include:

- issuing users with separate privileged accounts that have no access to the internet, email, or other higher-risk resources used by normal user accounts
- 'browse-up' administration, such as using an ordinary device to access a remote desktop environment for privileged operations - this approach is not recommended (see NCSC guidance on the 'browse-up' anti-pattern) but you may decide the risk is tolerable for a period of time while you implement a better solution
- 'browse-down' administration, such as using a highly-trusted device to access a remote desktop environment for normal user activities - this can include thin clients accessing multiple remote environments separated for privileged and normal user activities
- dedicated privileged access workstations, specifically configured and protected for privileged operations and not used for any other activity

Wherever possible, the administration of a system should be performed from a device that is trusted to at least the same level as that system.

If you have third party suppliers carrying out privileged operations, you should seek assurance (or set requirements) on the devices and architectures used – see NCSC guidance on systems administration architectures for examples and further information.

Preventing, detecting and removing malware and unauthorised software

You should employ a broad range of techniques to protect your networks and systems from malware and unauthorised software.

Technical measures might include:

- technology solutions that prevent users accessing potentially malicious websites such as the UK Public Sector domain name system (DNS) service
- anti-malware software
- automatic file scanning
- email filtering such as domain-based message authentication, reporting and conformance (DMARC)

Procedural measures might include:

- using dedicated privileged systems for administration (see B2.c Privileged user management)
- having policies, processes and procedures in place for acceptable use (B1.a Policy, process and procedure development)
- ensuring staff members know how to identify and report spam messages

Physical measures might include:

- restricting access to facilities and systems
- port locks

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:

- information assets and flows register or information asset register
- network diagrams
- policy, process, procedure or strategy documents relating to network security, configuration procedures, information technology (IT) acceptable use, access management, privileged devices, patch management, network monitoring and anti-malware
- risk registers
- alerts and follow-up actions from network firewalls, intrusion detection system (IDS)/intrusion prevention system (IPS), security information and event management (SIEM) solution, data loss prevention (DLP), web filtering and other network monitoring systems
- vulnerability assessment reports
- action plans for unauthorised or unsupported software detection and removal

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 systems and devices supporting the operation of the essential function(s) are only administered or maintained by authorised privileged users from devices sufficiently separated, using a risk-based approach, from the activities of standard users.
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	PA#1

practice	Your systems and devices supporting the operation of the essential function(s) are only administered or maintained by authorised privileged users from devices sufficiently separated, using a risk-based approach, from the activities of standard users.
Term	'privileged user(s)'
Interpretation	A user that is authorised (and therefore, trusted) to perform privileged operations that standard users are not authorised to perform. Privileged operations are actions that could have a significant impact on the system.

Indicator(s) of good practice	PA#2 Technical knowledge about networks and information systems, such as documentation and network diagrams, is regularly reviewed and updated.
Term	'regularly'
Interpretation	On a scheduled basis, with enough frequency to ensure that any significant changes to your networks and information systems are reflected in your documentation without undue delay.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B4 System security
National Cyber Security Centre | Secure system administration
NHS England | Secure boundary service
NHS England | Cyber assurance service

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.

B4.d Vulnerability management

"You manage known vulnerabilities in your network and information systems to prevent adverse impact on your essential function(s)."

Overview

This outcome relates to the way you identify, prioritise and manage vulnerabilities in your networks and systems.

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).

Publicly-known vulnerabilities

You should have a process for identifying and managing known vulnerabilities. Your knowledge of vulnerabilities should come from, at a minimum:

- software manufacturers' vulnerability publication channels
- cyber alerts issued by NHS England's National Cyber Security Operations Centre (CSOC)
- other public and commercial sources of vulnerability information

Mitigating vulnerabilities

You should be able to rationalise how you safeguard against exploitation of known vulnerabilities through the procedural and technical controls you have in place.

Vulnerabilities should be prioritised according to the risk they pose, and your process should ensure that follow up actions such as patching and system segregation are taken accordingly.

This should be fed into your risk management process (see 'A2.a Risk management process'), resulting in appropriate senior oversight of decisions that have been taken.

Temporary mitigations

In areas where your organisation is using assets with known vulnerabilities that have not been patched or unsupported systems, you should apply temporary mitigations to manage the associated risk. These may include:

- isolating the asset or system from the network
- disabling services on the asset or system
- micropatching
- enhanced monitoring of the asset or system, recognising that this does not reduce the risk of the vulnerability being exploited

You should have an improvement plan with realistic timescales for patching the vulnerabilities (including migrating to supported systems where relevant), and consider any compensating controls you can put in place in the interim.

Vulnerability testing

You should do tests on a periodic basis to understand where your networks and systems have vulnerabilities. These include:

- penetration testing
- vulnerability scans

Exceeding the 'standards met' expectation for 2024-25

Vulnerability testing

To meet the highest achievement benchmark, your understanding of your vulnerabilities should be verified through the commissioning of third-party testing.

Maximising the use of supported software, firmware and hardware

To meet the highest achievement benchmark, you should ensure that supported software, firmware and hardware is used in all cases.

The only exception should be those scenarios where unsupported software, firmware or assets need to be used for specific business reasons. Any instances of this should be recorded, risk-assessed and regularly reviewed by the board or equivalent.

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:

- information assets and flows register or information asset register
- configuration management registers
- policy, process, procedure or strategy documents relating to patching
- risk registers
- vulnerability assessment reports
- improvement plans
- penetration test results
- lists of unsupported software
- 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	PA#1 You maintain a current understanding of the exposure of your essential function(s) to publicly-known vulnerabilities.
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	PA#2 Announced vulnerabilities for all software packages, network and information systems used to support your essential function(s) are tracked and prioritised and externally exposed vulnerabilities are mitigated (by patching, for example) promptly.
Term	'promptly'
Interpretation	As soon as reasonably possible and, for critical vulnerabilities, not later than 14 days after a mitigation being made available.

Indicator(s) of good practice	PA#5 You regularly test to fully understand the vulnerabilities of the networks and information systems that support the operation of your essential function(s).
Term	'regularly'
Interpretation	On a scheduled basis, with enough frequency to ensure that vulnerabilities are identified without undue delay.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B4 System security
National Cyber Security Centre | Vulnerability management
NHS England | Vulnerability monitoring service
NHS England | Threat advice and intelligence
NHS England | Respond to an NHS cyber alert
NHS England | Cyber assurance service
NHS England | Technical remediation service
NHS England | Microsoft Defender for Endpoint service
NHS England | Bitsight cyber security ratings service

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: 29 August 2024 9:10 am

← **Previous Chapter**

Principle: B3 Data security

Next Chapter →

Principle: B5 Resilient networks and systems

Chapters

Legal

Get in touch

Follow us on social media