

[NHS Digital](#) >  > [Objective B - Protecting against cyber attacks and data breaches](#) >

Principle: B3 Data security

Part of [Objective B - Protecting against cyber attacks and data breaches](#)

Principle: B3 Data security

[← Previous Chapter](#)

[Principle: B2 Identity and access control](#)

Current Chapter

Current chapter – Principle: B3 Data security

[View all](#)

[Next Chapter →](#)

[Principle: B4 System security](#)

Page contents

[B3.a Understanding data](#)

[B3.b Data in transit](#)

[B3.c Stored data](#)

[B3.d Mobile data](#)

[B3.e Media/equipment sanitation](#)

B3.a Understanding data

“You have a good understanding of data important to the operation of your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).”

Overview

This outcome is about understanding the data which supports your organisation’s essential functions, and assessing the potential risks and real world impacts from compromise or loss.

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).

Data important to the operation of essential functions

For the purpose of cataloguing data important to the operation of essential functions for the Cyber Assessment Framework (CAF)-aligned DSPT, there are two types of data supporting the operation of your essential functions which you should consider:

- personal data – belonging to staff members and patients
- other data – all data supporting your essential functions which is not personal data

To meet contributing outcome ‘B3.a Understanding data’, both types of data need to be understood and documented.

Personal data

When processing personal data, to be legally compliant with UK General Data Protection Regulation (GDPR) you must maintain a record of processing activities (ROPA). This is a document which sets out where the personal data your organisation processes is flowing to and from, the types of information involved and a description of the safeguards you have in place.

You should also maintain an up-to-date information asset register documenting the information assets you hold, where they are located, how long they will be retained

for and who holds responsibility. For more information about what an information asset is, see [‘A3.a Asset management’](#).

The [template information assets and flows register](#) produced by NHS England combines the ROPA and information asset register 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 a ROPA/information asset register purpose.

Maintaining an up-to-date information assets and flows register will give 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.

Other data

Other types of data which support the operation of your essential functions may include operational data (such as finance data), technical data, or security impacting data (such as network and information system designs).

Either as an addition to your organisation’s information assets and flows register (or equivalent document), or as a separate document, you should catalogue where these other types of data are stored and how they are protected.

Identifying and cataloguing access to data

You should know which staff members have access to which types of personal data and other data you have catalogued.

This can be recorded at staff group level, for example, 'clinicians' and 'Information Technology (IT) personnel'. Clinicians are likely to need access to your Electronic Patient Record (EPR) system but are unlikely to require access your network configurations. By contrast, IT personnel are likely to need access to network and information system designs but are unlikely to require access to your appointment booking system.

Documenting the impact of scenarios such as unauthorised data access, modification or deletion

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

You should document the impact of compromise for the personal and other data you have catalogued. This means understanding the real world impacts if the data were:

- lost
- modified
- deleted
- accessed without authorisation

- inaccessible to staff members

This should be expressed in terms of the effects on clinical activities or other business operations that you have identified as essential functions. You may have organisational risk assessment processes that define how you should express impact, but the result should be a meaningful way of understanding the real world consequences of compromise – informing your risk assessments (A2.a) to determine the security requirements and protective controls that should be in place.

Examples of where this could be documented are your information assets and flows register (or equivalent document), or business continuity plans.

Your impact statements should be reviewed periodically or following major organisational changes to ensure they remain accurate and proportionate.

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 and record of processing activities
- assets inventories
- associated documents for cataloguing technical data
- business continuity plans
- 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 have identified and catalogued all the data important to the operation of the essential function(s) or that would assist an attacker. This includes maintaining a record of processing activities and an information asset register (IAR) which are updated whenever significant changes occur.

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#3

You regularly review location, transmission, quantity and quality of data important to the operation of the essential function(s).

Term

'location, transmission, quantity and quality of data'

Interpretation

Location – covered within your information assets and flows register and associated documentation.

Transmission – covered within your information assets and flows register and associated documentation.

Quantity – understanding approximate data volumes, such as the amount of data held on different servers or the number of patient records your organisation holds,.

Quality – you have processes for assuring the integrity of information which supports your essential functions. In the case of personal data, this may be through routine checks such as synchronising with the Personal Demographics Service (PDS) and conducting data quality audits. In the case of other data, this would likely be through periodic review, for example, checking that configuration data used by a third-party IT supplier is up to date.

Additional guidance

For additional guidance, see:

[National Cyber Security Centre CAF guidance | B3 Data security](#)

[National Cyber Security Centre | 10 steps to cyber security – Data security](#)

[NHS England | Technical remediation service](#)

[NHS England | Universal information governance templates and FAQs](#)

[Information Commissioner's Office | Records of processing and lawful basis](#)

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.

B3.b Data in transit

“You have protected the transit of data important to the operation of your essential function(s). This includes the transfer of data to third parties.”

Overview

To achieve this outcome, you need to demonstrate that you have suitable controls in place to protect your organisation’s internal and external data flows. This includes electronic and physical information.

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).

Identifying and protecting data links

You need to identify the data flows that are critical to your organisation’s provision of essential services. These are likely to include physical communications (such as sending confidential patient information by mail), electronic information transfers (such as email and automated transmissions), and network traffic between end user devices, infrastructure devices and servers. Data flows within your organisation as well as those entering and leaving your organisation will all be relevant.

You should be able to demonstrate that you have taken reasonable steps to protect the data.

You should use your judgment to decide the best way to document this. It could be a combination of:

- a spreadsheet-based document, as part of or similar to an information assets and flows register or record of processing activities (ROPA), taking note that you may also need to document non-personal data such as operational data and configurations
- data flow diagrams, or similar, which are sufficiently detailed to show individual data links and the means of protection
- interface control documents that specify the nature of the data links used for each interface

Protecting electronic information in transit

For electronic communications, you should apply appropriate technical means to protect the data in transit through some combination of encryption, network

protection and authentication.

Meeting the [Secure Email standard \(DCB1596\)](#) is a requirement for health and care organisations. You can evidence activities you have undertaken to meet the Secure Email standard as part of your assessment of your organisation's performance against this contributing outcome.

See [NCSC guidance on protecting data in transit](#) for more information.

Protecting physical information in transit

Physical information includes:

- paper records and reports
- ID cards
- paper invoices
- correspondence letters
- case notes

When sending physical information, you should take reasonable steps to ensure data is protected. Some examples are:

- securely packaging post
- ensuring that physical post is signed for where appropriate
- correctly addressing post
- delivering information in-person by hand where appropriate
- using a trusted mail service which has been reviewed and approved at organisational level

Exceeding the 'Standards met' expectation for 2024-25

Protecting electronic information in transit

To obtain justified confidence in the technical means you are using, you should carry out assurance activities such as penetration tests and integrity checking. The results should confirm whether protective measures are working as intended.

Protecting physical information in transit

To obtain justified confidence in the way you protect physical information in transit, you should undertake activities to assure that delivery protocols are being followed and use knowledge of incidents and near misses both in your organisation and partner organisations to guide your approach.

Alternative transmission paths

For all data flows which are critical to your essential functions, you should evaluate the impact of transmission paths being compromised.

If the transmission paths are likely to be compromised by known attack or data breach scenarios, you should carry out integrity checks on data travelling

through them. This will enable you to understand what data you can rely on and detect attacks more reliably.

If the transmission paths are likely to be compromised, you should also have documented maintenance plans and alternative solutions to ensure communications can continue in the event of an incident.

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/record of processing activities (ROPA)
- policy, process, procedure or strategy documents relating to data encryption, transfer of records and physical information
- standard accreditations, for example DCB1596 compliance standard
- data flow diagrams
- interface control documents

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 protected (effectively and proportionately) all the data links that carry data important to the operation of your essential function(s).

Term

'data links'

Interpretation

Data links are the route data takes when moving from a source to a destination. For example, if the source was a remote support laptop and the destination was a server, the 'data link' could be a journey through a VPN, the cloud, and a series of firewalls.

**Indicator(s)
of good
practice**

PA#1

You have identified and protected (effectively and proportionately) all the data links that carry data important to the operation of 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**

PA#2

You apply appropriate technical means (such as cryptography) to protect data that travels over non-trusted or openly accessible carriers, but you have limited or no confidence in the robustness of the protection applied.

Term

'data'

Interpretation For the purposes of the DSPT, 'data' applies to both electronic and physical information (such as paper records, ID cards and case notes).

**Indicator(s)
of good
practice**

PA#2

You apply appropriate technical means (such as cryptography) to protect data that travels over non-trusted or openly accessible carriers, but you have limited or no confidence in the robustness of the protection applied.

Term

'non-trusted [...]carriers'

Interpretation Any network outside of your own, would be a non-trusted carrier. For example, public internet.

**Indicator(s)
of good**

PA#2

practice You apply appropriate technical means (such as cryptography) to protect data that travels over non-trusted or openly accessible carriers, but you have limited or no confidence in the robustness of the protection applied.

Term 'openly accessible carriers'

Interpretation These would be any networks that people outside of your organisation can connect to. For example:

- internet
- public wireless network
- Health and Social Care Network (HSCN)
- cellular (mobile) networks

Additional guidance

For additional guidance, see:

[National Cyber Security Centre CAF guidance | B3 Data security](#)

[National Cyber Security Centre | Cloud security guidance - Principle 1: Data in transit protection](#)

[NHS England | Secure boundary service](#)

[NHS England | Cyber assurance service](#)

[NHS England | Public key infrastructure documentation](#)

[NHS England | Universal information governance templates and FAQs](#)

[NHS England | The secure email standard](#)

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.

B3.c Stored data

“You have protected stored soft and hard copy data important to the operation of your essential function(s).”

Overview

This outcome relates to the way your organisation protects stored data, in both electronic and paper form, from unauthorised access, modification or deletion.

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).

Stored data supporting your essential functions

Your stored data which is important to your essential functions should be identified and catalogued.

You have achieved this if you have met or performed activities equivalent to data cataloguing requirements (PA#1) under contributing outcome '[B3.a Understanding data](#)'.

Protecting stored data

Your information, networks and systems should be maintained in a way which protects stored data from unauthorised access, modification or deletion. Both electronic and physical information (such as paper records, ID cards and case notes) should be protected.

For all types of data, limiting the quantity and detail held to the minimum necessary for business purposes, especially in devices, media and areas that are more vulnerable to unauthorised access, is a practice that should be embedded in your policies, processes and procedures.

Electronic information

You can apply a number of physical and technical means to protect the confidentiality, integrity and availability of your stored electronic information. Some examples are:

- applying [pseudonymisation](#)
- minimising the number of copies of data stored on your systems
- providing read-only copies of data
- retaining operationally sensitive data on segregated systems
- restricting access (see '[B2.d Identity and access management \(IAM\)](#)')
- encrypting data at rest using well-tested cryptographic suites
- providing multiple network paths for traffic (see '[B3.b Data in transit](#)')
- testing automatic backup systems (see '[B5.c Backups](#)')
- having a plan for retaining access to essential electronic information in the event of an incident (see '[D1.b Response and recovery capability](#)')

Where cryptographic mechanisms are used, consideration should be given to how to manage keys appropriately.

You should use your judgment to assure that your organisation's electronic information is suitably protected from unauthorised access, modification and deletion through implementing some combination of the above and associated activities.

The [NCSC guidance on protecting bulk personal data](#) gives a practical model to follow to ensure your system is designed, implemented and operated to help protect stored data.

Physical information

Where you hold stored data in physical form which supports your essential function, you should take reasonable steps to appropriately secure it. Examples include:

- granting different levels of access according to role
- locking cupboards and cabinets
- restricting access to key areas
- disposing of confidential waste appropriately

You should use your judgment to assure that your organisation's physical information is suitably protected from unauthorised access, modification and removal through implementing some combination of the above and associated activities.

If your organisation uses physical archives, you should seek assurances that the controls which the supplier has implemented are as robust as your organisation's controls for protecting physical information.

Backups

You should maintain backups of all stored electronic information which supports your essential functions (see '[B5.c Backups](#)'). These should be deployed in the event of an incident or event to restore your essential service.

For cloud backup services, see [NCSC cloud security principle 2 on asset protection and resilience](#) for things you should consider when working with a cloud service provider.

Exceeding the 'Standards met' expectation for 2024-25

Cryptographic protections

To obtain justified confidence in the cryptographic protections you have applied, you should carry out assurance activities such as penetration tests. The results should confirm whether encryption functions are working as intended.

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/record of processing activities (ROPA)
- policy, process, procedure or strategy documents relating to access control, data encryption, records management and retention, backups
- business continuity and disaster recovery plans

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

All copies of data important to the operation of your essential function(s) are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy.

Term

'data'

Interpretation

For the purposes of the DSPT, 'data' applies to both electronic and physical information (such as paper records, ID cards and case notes).

Indicator(s) of good practice

PA#1

All copies of data important to the operation of your essential function(s) are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy.

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 | B3 Data security](#)

[National Cyber Security Centre | Protecting bulk personal data](#)

[National Cyber Security Centre | Cloud security guidance](#)

[NHS England | Cyber assurance service](#)

[NHS England | Technical remediation service](#)

[NHS England | Backups and Office 365](#)

[Information Commissioner's Office | Encryption and data storage](#)

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.

B3.d Mobile data

“You have protected data important to the operation of your essential function(s) on mobile devices.”

Overview

To achieve this outcome, you need to show how your organisation keeps track of its mobile devices and applies technical controls to protect the data they hold.

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).

Mobile devices holding data important to the operation of the essential function

Mobile devices should be accounted for in the documentation you use to catalogue your assets (see '[A3.a Asset management](#)'), and any data held on mobile devices which supports your essential functions should be accounted for in your information assets and flows register or equivalent document (see '[A3.a Asset management](#)'/'[B3.a Understanding data](#)').

Mobile device security

Any mobile devices which hold or access data supporting your essential functions should be subject to similar physical and technical controls to the ones outlined in [‘B3.c Stored data’](#) to ensure the data is suitably protected from unauthorised access, modification and deletion.

Exceeding the ‘Standards met’ expectation for 2024-25

Best practice mobile device configuration

To meet the highest achievement benchmark, you should demonstrate that you have assessed each category of mobile device individually, and optimally configured technical controls in a way which reflects best practice for their relative platforms. This should also be reflected in your policies, processes and procedural documentation.

Minimising data on mobile devices

To meet the highest bar for achievement, you should have an evidence-backed rationalisation for the data held on each category of mobile device, showing how you maintain the minimum which is necessary and reasonable to deliver your essential functions. Where practical, you have also implemented technical controls that ensure data is deleted when no longer needed.

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:

- asset registers
- information assets and flows register/information asset register/record of processing activities (ROPA)
- policy, process, procedure or strategy documents relating to removable media, lost/stolen devices and device-specific policies
- reports and analysis from Mobile Device Management (MDM) systems

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 know which mobile devices hold data important to the operation of the essential function(s).

Term 'mobile devices'

Interpretation Mobile devices are any devices that are portable in nature which your organisation uses to perform specific functions. They include, but are not limited to:

mobile phones
tablets
laptops and notebooks
removable media (such as USBs, external hard drives)
connected medical devices

Indicator(s) of good practice PA#1

You know which mobile devices hold data important to the operation 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 A#1

Mobile devices that hold data that is important to the operation of the essential function(s) are catalogued, are under your organisation's control and configured according to best practice for the platform, with appropriate technical and procedural policies in place.

Term 'according to best practice'

Interpretation You should be able to justify the configurations you have in place on your chosen platform, and show that you consider practical improvements based on the development of the technology and knowledge sharing with other professionals in your network.

Additional guidance

For additional guidance, see:

[National Cyber Security Centre CAF guidance | B3 Data security](#)

[National Cyber Security Centre | Device security guidance](#)

[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.

B3.e Media/equipment sanitation

“Before reuse and/or disposal you appropriately sanitise devices, equipment and removable media holding data important to the operation of your essential function(s).”

Overview

This outcome is about ensuring devices, equipment and removable media are appropriately sanitised before reuse, repair, disposal or destruction.

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).

Removing data before reuse and/or disposal

You should have procedures in place which ensure that storage media is sanitised before:

- re-use
- repair
- disposal
- destruction

In all cases, outside of your operating environment the media will be subject to greater risk from different users, third parties, or less trusted organisations.

See NCSC guidance on [secure sanitisation of storage media](#) for more information.

Third party disposal services

You may contract third party services to dispose of your devices.

The nature of the devices you are reusing or disposing of, and the devices themselves (such as hard drives, USB memory sticks, CDs), may change over the course of your contract with a supplier. You therefore need to review contracts with suppliers periodically.

The contract with the supplier should also contain a provision allowing you, or a contracted third party auditor, to periodically audit them. The type of items that should be included in that audit are:

- onsite inspection of the contractor disposal site ensuring sufficient physical segregation of different customer disposal items
- observing the disposal journey from asset receipt to disposal and certification
- tracing a recently collected disposed of item(s) to track where they are in the disposal journey and how they are secured (especially if mid journey)
- if the items are to be recycled, examining a finalised refurbished asset for any data remnants
- verifying the employment checks on a dip sample of employees from the disposal company
- tracing a dip sample of assets' chain of custody documentation from collection to destruction and certification
- observing physical destruction of media

Exceeding the 'standards met' expectation for 24-25

Removing data before reuse and/or disposal

To meet the highest achievement benchmark, you need to conduct media sanitisation through an assured product or service.

Examples of assurance are NCSC's [Assured Service \(Sanitisation\) scheme \(CAS\(S\)\)](#), NPSA's [Secure Destruction of Sensitive Items standard](#), and [ADISA Certification](#).

Tracking all devices with data important to the operation of essential functions

To meet the highest achievement benchmark, it is expected that you take all practical steps to track devices holding data important to the operation of your essential functions. This includes removable media assets, such as USB sticks, which can be more difficult to manage and control.

Devices should be accounted for in the documentation you use to catalogue your assets (see '[A3.a Asset management](#)'), and any data which supports your essential functions should be accounted for in your information assets and flows register or equivalent document (see '[A3.a Asset management](#)'/'[B3.a Understanding data](#)').

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:

- asset registers
- information assets and flows register, information asset register or record of processing activities (ROPA)
- policy, process, procedure or strategy documents relating to IT equipment disposal and removable media devices
- data destruction certificates
- 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

PA#1

practice Data important to the operation of the essential function(s) is removed from all devices, equipment and removable media before reuse and/or disposal.

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 | B3 Data security](#)

[National Cyber Security Centre | Secure sanitisation of storage media](#)

[National Cyber Security Centre | Assured Service \(Sanitisation\) scheme \(CAS\(S\)\)](#)

[National Protective Security Authority | Secure Destruction](#)

[ADISA | Certification](#)

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 2:39 pm

← **Previous Chapter**

[Principle: B2 Identity and access control](#)

Next Chapter →

[Principle: B4 System security](#)

Chapters

1. [Objective B - Protecting against cyber attacks and data breaches](#)
2. [Principle: B1 Policies, processes and procedures](#)

3. [Principle: B2 Identity and access control](#)

7. [Principle: B6 Staff awareness and training](#)

4. **[Principle: B3 Data security](#)**

5. [Principle: B4 System security](#)

6. [Principle: B5 Resilient networks and systems](#)

Legal

[Privacy and cookies](#)

[Terms and conditions](#)

[Looking after your data](#)

[Freedom of information](#)

[Modern Slavery Act Statement](#)

[Accessibility](#)

[Change cookie settings](#)

[Copyright \(c\) NHS Digital](#)

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](#)