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

Principle: B5 Resilient networks and systems

← Previous Chapter

Principle: B4 System security

Current Chapter

Current chapter – Principle: B5 Resilient networks and systems

View all

Next Chapter →

Principle: B6 Staff awareness and training

Page contents

B5.a Resilience preparation

"You are prepared to restore the operation of your essential function(s) following adverse impact."

Overview

To achieve this outcome, you need to be prepared to withstand an incident, maintain your essential functions, and restore the full operation of your essential functions in the event of an incident.

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).

Restoring the operation of the essential function

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

You should understand the information, networks and systems that are necessary to restore the operation of the essential function in the event of an incident.

The scoping exercise at the outset of your DSPT assessment which determines the information, networks and systems which support your essential functions provides such an overview.

You should understand:

- business importance – the systems which are most important to bring back online for the operation of the essential function from a time-bound perspective
- dependencies – the order in which systems can technically be brought back online given the interdependencies between them

Business continuity and disaster recovery plans

See 'D1.a Response plan' and 'D1.c Testing and exercising'.

Threat intelligence sources

You should use threat intelligence sources to identify new or heightened levels of risk. Sources include:

- current and emerging threats described in DHSC/NHS England's Cyber Security Strategy for Health and Care to 2030
- any threats which you have been contacted about directly by DHSC/NHS England
- threat intelligence and alerts received from NHS England's National Cyber Security Operations Centre (CSOC), including via Microsoft Defender for Endpoint

Keeping a record of the information sources you use for intelligence gathering, as well as your engagement with professionals in your wider network, will better enable you to demonstrate how you acquire and use intelligence to identify new or heightened levels of risk.

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
- DSPT scoping documentation
- business continuity and disaster recovery plans
- sources of threat intelligence
- 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 know all network and information systems, and underlying technologies, that are necessary to restore the operation of the essential function(s) and understand their interdependence.
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 | B5 Resilient networks and systems
NHS England | Cyber incident response service (CIRE)
NHS England | NHS simulated phishing 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.

B5.b Design for resilience

> "You design the network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated."

For this contributing outcome, there is no minimum expected level of achievement for 'Standards met'. You are still required to assess your achievement level and provide a response, showing you have considered the implications of the contributing outcome for your organisation's cyber security and information governance (IG) activities. The Data Security and Protection Toolkit (DSPT) 'Standards met' expectation should be regarded as a minimum compliance level, not the end goal of your organisation's cyber security and IG activities.

Overview

To achieve this outcome, you should be able to demonstrate that your networks and systems are designed to be resilient to incidents.

Mapping to the 23-24 DSPT framework

Under the previous 23-24 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).

Resource limitations

You should conduct a review of your network and systems to identify single points of failure, which risk causing major disruption to your essential service if compromised. You should document, review and accept the associated risks. You should have an improvement plan in place to upgrade your networks and systems where the risk they pose exceeds the risk appetite of your organisation.

To meet the highest bar for achievement, you should have also taken appropriate follow-up action to resolve or mitigate all single points of failure which have been identified.

Segregation

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.

Networks and systems which you have identified as being critical to your essential functions should be segregated from your enterprise systems, placed in a highly trusted and secure zone.

Geographical constraints and weaknesses

When designing your networks and systems, you should also consider geographical constraints. If all your servers, or all your suppliers' servers, are in the same geographical area, one serious security event localised to that area could cause system-wide consequences with little chance of an efficient recovery.

For this reason, to meet the highest achievement benchmark, your documentation should reflect the mitigations you have in place to prevent adverse impact.

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
- risk registers
- improvement plans
- assessments of dependencies
- policy, process, procedure or strategy documents relating to network security

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 services, such as browsing and email, are accessible without restriction or business need from network and information systems supporting the 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#1 Network and information systems supporting the operation of your essential function(s) are logically separated from your business systems (that is, they reside on the same network as the rest of the organisation but within a demilitarised zone (DMZ)). Internet services are not accessible from network and information systems supporting the essential function(s) unless there is a clear business need and with appropriate restrictions.
Term	'unless there is a clear business need and with appropriate restrictions'
Interpretation	A 'clear business need' means you must have a 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 'with appropriate restrictions' means that you have solutions in place to: monitor and analyse incoming and outgoing internet traffic block or filter out harmful content block unapproved connections manage internet access

Indicator(s) of good practice	PA#1

	Network and information systems supporting the operation of your essential function(s) are logically separated from your business systems (that is, they reside on the same network as the rest of the organisation but within a demilitarised zone (DMZ)). Internet services are not accessible from network and information systems supporting the essential function(s) unless there is a clear business need and with appropriate restrictions.
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 | B5 Resilient networks and systems
National Cyber Security Centre | Secure design principles
NHS England | Cyber assurance service
NHS England | Technical remediation 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.

B5.c Backups

"You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s)."

Overview

This outcome relates to you having a robust system for backups which ensures you can efficiently restore your essential functions in the event of an incident.

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).

Backups

You should maintain backups of the most important electronic information supporting your essential functions (see 'B3.c Stored data'). These should be deployed following an incident or event to restore your essential service.

The frequency of backup operations should also be agreed, documented and adhered to. It is up to you to decide what intervals are appropriate. However, you should make and justify your decision based on:

- the agreed length of time your organisation could be disrupted by loss of access to data before unacceptable consequences would arise
- the frequency of backup operations which would enable you to restore your essential functions to an acceptable level within the timeframe

Your recovery point objective (RPO) and recovery time objective (RTO) need to be formally agreed and tested to ensure they can be met. Where services cannot be returned within the timeframe, this should be documented and managed as a risk.

Appropriately securing backups

You should appropriately secure your backups to ensure they are accessible and the data within them is recoverable at critical times.

Rules outlined by NCSC which serve as effective guidelines for backup protection are:

- the offline rule – at any given time, one or more backups should be offline and therefore unaffected by incidents impacting the live environment
- the 3-2-1 rule – keep at least 3 logically separated backup copies, on 2 devices, with 1 being offsite, to ensure that if one is compromised the other remains

For more detail, and other rules see NCSC guidance on offline backups in an online world.

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.

Testing backups

It is important that you are confident you can recover the data which is required to maintain your essential service from your backups. To gain this confidence, you should test your backups on a scheduled basis, or after significant changes have been made to your networks and systems.

Things to look out for include:

- overused or old media
- corrupt backup catalogue
- bad backup image files
- multiple complex restores required
- backup didn’t occur or backed up the wrong system
- nowhere to store the restore
- networked disk-based storage being unavailable due to the nature of the incident

The testing should be representative of the service or system in focus and not based on routine smaller scale requests or an old live incident. For example, a routine restore of single mailbox for a returning member of staff would not be considered as enough confidence to restore a whole email system.

You should decide whether to use live systems or test systems based on your judgment of the risk and whether the test system is sufficiently representative of the live system to make the testing valid.

You should also know the process for restoring the system, as well as documenting any issues found during the test and the plan to rectify them.

Documenting backup procedures

Your backup activities should be supported by documentation which outlines:

- frequency of backups
- how you ensure the ongoing security and maintenance of your backups
- which business events trigger backups to be made or used
- how you have automated your backups processes (in areas where it is appropriate to do so)
- how your testing regime ensures you are ready to efficiently recover the essential function 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:

- policy, process, procedure or strategy documents relating to backups
- records of back-up activity and back-ups testing activity
- improvement 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#2 You routinely test backups to ensure that the backup process functions correctly and the backups are usable.
Term	'routinely'
Interpretation	On a scheduled basis, with enough frequency to give you confidence that your backups are usable.

Indicator(s) of good practice	A#2 Backups of all important data and information needed to recover the essential function(s) are made, tested, documented and routinely reviewed.
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 | B5 Resilient networks and systems
National Cyber Security Centre | Cloud security guidance - Principle 2: Asset protection and resilience
NHS England | Backups and Office 365 guidance
NHS England | Technical remediation 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: 19 September 2024 2:45 pm

← Previous Chapter

Principle: B4 System security

Next Chapter →

Principle: B6 Staff awareness and training

Chapters