Part of Objective D - Minimising the impact of incidents

Principle: D1 Response and recovery planning

← Previous Chapter

Objective D - Minimising the impact of incidents

Current Chapter

Current chapter – Principle: D1 Response and recovery planning

View all

Next Chapter →

Principle: D2 Lessons learned

Page contents

D1.a Response plan

> “You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function(s) and covers a range of incident scenarios.”

Overview

This contributing outcome relates to you having an incident response plan, or a suite of plans, covering an appropriate range of scenarios, informed by an understanding of your organisation’s risks.

In the scope of the Cyber Assessment Framework (CAF)-aligned Data Security Protection Toolkit (DSPT), 'incidents' refers to personal data breaches, breaches of confidence relating to other confidential health information, and events which have an actual adverse effect on the security of network and information systems (NIS).

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 the Department of Health and Social Care (DHSC).

Incidents

In the scope of the CAF-aligned DSPT, 'incidents' refers to:

- personal data breaches – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.
- breaches of confidence relating to other confidential health information – such as belonging to deceased people or the organisation
- events which have an actual adverse effect on the security of network and information systems

As such, 'incidents' under the CAF-aligned DSPT comprise adverse events from across the domains of information governance (IG), cyber security, emergency preparedness, Resilience and Response (EPRR) and business continuity, bringing them under one assurance umbrella.

You may have separate mechanisms, and separate teams, for dealing with these incidents within your organisation. You're free to categorise and allocate responsibilities for incident response in whatever way works best, provided it's clear how the indicators of good practice of the CAF-aligned DSPT framework have been implemented.

Incident response plan

Your incident response plans should support your incident management process. Plans should include, but not be limited to:

- **Key contacts** - covering anyone who would need to be involved in the incident response process - for example, data protection officer, IT managers, senior information risk owner (SIROs) and senior management, legal teams, HR, comms, system partners. Consider the risk of people being unavailable and include back up contacts.
- **Roles and responsibilities** - defining which groups or individuals are responsible for different elements of an incident response.
- **Escalation criteria** - covering appropriate escalation routes along with a process for escalation and making critical decisions.
- **Flowchart or process** - this should cover the full lifecycle of the incident (such as preparation, detection and analysis, containment, eradication and recovery, post-event activity).
- **Guidance on regulatory requirements** - including the appropriate thresholds for external reporting and notifying impacted individuals.

This is a basic plan. For more information on creating an incident response plan from a cyber security perspective, see NCSC guidance. For more information on incident response from a data protection perspective, see guidance from NHS England on personal data breaches.

Known and well-understood incidents and attacks

Your response plan(s) should be shaped with known and well-understood incident and attack scenarios in mind. Examples include:

- **Data breaches** - incidents resulting in the confidentiality, integrity or availability of information being compromised. Data breaches are often a component of other incidents such as:
  - **confidentiality breach -** emailing files in error, failing to redact personal information from public disclosures, unauthorised access to information, devices being lost or stolen
  - **integrity breach -** editing a patient record in error, misfiling test results
  - **availability breach -** deleting information in error, being unable to access information in the aftermath of a cyber attack
- **Phishing** - emails attempting to convince someone to trust a link or attachment
- **Malicious code** - malware infection on the network, including ransomware
- **Denial of service** - typically a flood of traffic taking down a website, can apply to phone lines, other web facing systems, and in some cases internal systems
- **Targeted attack** - an attack specifically targeted at the business - usually by a sophisticated attacker (often encompassing several of the above categories)

You should also use knowledge you have gained from previous incidents, your organisation's known risks, trusted professionals and open-source reporting to establish known and well-understood threats to the confidentiality, integrity and availability of data upon which your essential function depends, and shape your response plan(s) accordingly.

Suppliers and system partners

It is likely for third parties to be involved in the operation or maintenance of some of your essential systems. For example, suppliers who process data on your behalf, or system partners who share access to repositories owned by you for providing care.

Mounting a response to any incident where third-party supplied systems are affected, or where an incident originates with a supplier, will entail your incident response team working closely with those third parties to contain the impact and put appropriate mitigations in place. Your incident response plan(s) should show that you have appropriate measures in place to facilitate this, including requesting important information from the supplier where necessary such as log files.

Incident reporting

It is a contractual requirement of the standard NHS contract to notify incidents in accordance with the DSPT Incident Reporting Guidance via the DSPT incident reporting tool. This does not change with the adoption of the CAF-aligned DSPT.

If the incident meets the necessary thresholds, details will be sent to the Information Commissioner's Office (ICO) as the supervisory authority and, depending on impact and nature (such as a network and information systems incident), the DHSC or NHS England.

Your board (or equivalent) should be notified of the incident including any associated action plan, which should encompass dealing with the risks and impact of the incident and lessons learned.

Obligations as a controller or processor

As a controller, you're legally obliged to notify personal data breaches to the ICO within 72 hours where the breach is likely to result in a risk to the rights and freedoms of individuals. This should be done via the DSPT reporting tool. You also have a legal obligation to inform the data subjects (such as patients or staff) who have been impacted by a breach which is likely to result in a risk to their rights and freedoms.

Processors also have a legal obligation to promptly notify controllers in the event of a data breach.

For more information, see NHS England guidance on personal data breaches.

Obligations as an Operator of Essential Services (OES) under NIS

Under the network and information systems regulations, operators of essential services (OES) have a legal duty to report any incident which has an adverse effect on the security of network and information systems and which has a significant impact on the continuity of an essential service within 72 hours. This should be done via the DSPT reporting tool.

For more information, see DHSC guidance on network and information systems regulations.

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:

- incident response plans
- business continuity and disaster recovery plans
- business impact assessments
- evidence of workflow management for incident reporting
- training needs analysis
- minutes and terms of reference from relevant meetings or groups
- policy, process, procedure or strategy documents (such as business continuity and disaster recovery, or incident management)
- risk management reports

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 response plan covers your essential functions.
Term	'essential functions'
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 Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks and incidents only.

Term	'likely impacts'
Interpretation	Scenarios could be focussed on likely impacts to the operation of your essential function, for example: systems going offline back-up systems being deployed staff resources being diverted to deal with the incident Scenarios could also be focussed on likely impacts to patients, for example: publication of patient data threat actors actively misusing patient data unrelated threat actors claiming to have access to the patient data Your response plan should aim to minimise the impacts of these scenarios, both on the delivery of your essential service and on patients.

Indicator(s) of good practice	PA#4 Your response plan is documented and shared with all relevant stakeholders.
Term	'relevant stakeholders'
Interpretation	Identifying which stakeholders are relevant to your response plan is a local decision, and you should document your rationale. These should include your SIRO and members of senior management who formally sign off your suggested approach, and members of staff who would be the first line of defence in reporting concerns. You should consider the best format for sharing your response plan depending on your audience. This may include formal training, guidance, workshops, and testing exercises.

Additional guidance

For additional guidance, see:

National Cyber Security Centre | D1 Response and recovery planning
National Cyber Security Centre | Incident management
NHS England | Personal data breaches

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.

D1.b Response and recovery capability

> "You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function(s). During an incident, you have access to timely information on which to base your response decisions."

Overview

To meet this contributing outcome, you need to ensure you have the capability to enact your incident response plan.

In the scope of the Cyber Assessment Framework (CAF)-aligned Data Security and Protection Toolkit (DSPT), 'incidents' refers to personal data breaches, breaches of confidence relating to other confidential health information, and events which have an actual adverse effect on the security of network and information systems (see 'D1.a Response plan' for more information).

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).

Resources for response activities

As part of your planning for foreseeable incidents, you should designate clear roles and responsibilities. Formation of a capable incident response team with the necessary skills, tools, and reach within the organisation to mitigate the effects of incidents is critical.

Given the unpredictable nature of incidents, you also need to make appropriate arrangements for how response activities should be coordinated out-of-hours.

With advanced planning of the activities which fall under each person's remit, your organisation should be able to practically assess its capability for responding to potential incidents.

Necessary information for response teams

Your response team may require access to several types of information during an incident, which include but are not limited to:

- incident response plans and supporting procedures
- contact details for other supporting teams and external stakeholders
- monitoring and alert information
- detailed hardware and software engineering information, network diagrams, system descriptions and functional specifications
- asset registers with lists of critical sites and systems
- authorisation requirements
- communication plans
- evidence of post incident activities such as 'root cause analysis' and 'lessons learned'

You should consider how this information would be made available to your incident response team, including contingency plans if business-as-usual methods of communication and transferring files are compromised.

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

Skills and knowledge

Your training needs analysis should identify any competency gaps within your teams which might impact:

- your ability to limit harm during an incident
- the operation and recovery of your essential function during an incident

Your training needs analysis should show how you plan to address these.

For more information, see NCSC's guidance on building a response team. Please note that NCSC guidance is written from a cyber security perspective. Your organisation's response team should also include information governance specialists who know how to manage personal data breaches in line with ICO guidance.

Sharing knowledge

Under the CAF-aligned DSPT, you must share knowledge across your incident response team, and duplicate key roles. For your organisation's purposes, you should assure that your incident response team can perform its role with a reliable degree of confidence, regardless of whether key members of the team are unavailable (due to annual leave for example).

Back-up/fallback mechanisms

It is possible for your systems to fail during an incident, or for them to be intentionally restricted to contain the impact. This could be one system, several systems, or all of them (such as in the event of a power outage). Your risk assessments should evaluate the resilience of your existing systems under such conditions, and identify any back-up/fallback mechanisms that would be needed to deliver your essential service. These

could be temporary solutions which keep your operations functioning at a reduced level.

The impact of network and system compromise should be considered from a time-bound perspective. If systems can be down for a significant time period without causing unacceptable consequences, or mitigations you already have in place mean that systems would be recovered before any unacceptable consequences could occur, you could rationalise a judgment that additional back-up/fallback mechanisms are not needed.

Augmenting incident response capabilities

You should identify sources of external support in your incident response plans such as NHS England central teams, specialist suppliers and law enforcement, and establish when, how and under what conditions they would be engaged. Where external specialists may be used, appropriate contractual arrangements should be in place.

You should also have arrangements pre-agreed with suppliers, vendors and any third parties on which your essential functions depend to ensure they are committed to providing support during times of incident response.

Given the nature of incidents, your arrangements should cover out-of-hours scenarios as well as those that can be responded to within business-as-usual hours.

Supporting evidence

To support your response, you can review and upload (or link to) evidence below which best demonstrates your achievement of the contributing outcome. Examples include:

- incident response plans
- policy, process, procedure or strategy documents (such as business continuity and disaster recovery, or incident management)
- business impact assessments
- minutes and terms of reference from relevant meetings or groups
- risk assessments
- training needs analysis
- reports of procedures that have been conducted to challenge response and recovery capabilities
- exemplar job roles referencing responsibilities for incident response

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	A#5 Back-up mechanisms are available that can be readily activated to allow continued operation of your essential function (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.
Term	'back-up mechanisms'
Interpretation	In this context, 'back-up mechanisms' refer to additional systems, networks, means of communication and equipment that could be used during an incident if primary ones were compromised. Examples of back-up/fallback mechanisms include: an offline record repository and redundant networks to support availability and resilience for an electronic patient records system an alternative messaging system that could be used if your main system was compromised other recovery site options such as hot sites, disaster recovery as a service (DRaaS) and reciprocal agreements

Additional guidance

For additional guidance, see:

National Cyber Security Centre | D1 Response and recovery planning
National Cyber Security Centre | Incident management
NHS England | Personal data breaches

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.

D1.c Testing and exercising

"Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment."

Overview

This contributing outcome relates to your implementation of tests and exercises to assess the readiness of your people, processes and technologies for responding to incidents.

In the scope of the Cyber Assessment Framework (CAF)-aligned Data Security and Protection Toolkit (DSPT), 'incidents' refers to personal data breaches, breaches of confidence relating to other confidential health information, and events which have an actual adverse effect on the security of network and information systems (see 'D1.a Response plan' for more information).

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).

Incident response and recovery testing

Your organisation can conduct exercises to assess its readiness to respond to an incident, and improve its policies and procedures. Exercises could include:

- orientation/walkthroughs
- table-top exercises (TTX)
- live exercises
- functional testing of sections of your response plan
- full scale test of all elements of your response plan
- activation of disaster recovery plans
- communications tests – suppliers, emergency services, media, the public for example

The aim of these exercises is to test your communications channels, decision making, your incident response team's composition and their technical capabilities to use tools and data in the event of an incident. The activity should help you identify any barriers to sustaining your normal business operations and minimising negative impacts.

Findings should be used to:

- reinforce roles and responsibilities
- identify gaps in your response plan
- agree and assign specific time-bound actions to address the gaps

For more information, see NCSC's guidance on cyber exercise creation.

Additionally, see NHS England's cyber incident response exercises for pre-made practical scenarios which can be used to test your organisation's response functions.

Using threat intelligence to design exercises

The tests and exercises you conduct should be informed by your knowledge of previous incidents, your organisation's risk profile, and available intelligence from external sources on threats and threat actors in the health and care sector. As a result, you should be able to design your exercises to be practical, appropriately challenging to meet the complexity of threats you face and relevant to your operating environment.

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 support your designing of tests and exercises.

Testing all parts of the response cycle

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

Under the previous DSPT framework, you were required to test your incident response plan to ensure that relevant team members understood their roles and responsibilities. Under the CAF-aligned DSPT framework, your testing should meet a higher bar, testing all parts of your incident response plan to ensure you would be able to restore business operations in the event of an incident.

You'll need to consider how to design exercises to ensure your people, processes and technologies have been tested. You do not have to test everything at once – it's sufficient to target specific areas with different exercises – but the overall result should be you having confidence in your organisation's array of competencies, governance and tools for responding to incidents.

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:

- reports of testing exercises conducted
- minutes and terms of reference from relevant meetings and groups
- documented exercise scenarios with details of the contextual factors that informed the approach (such as threat intelligence and security events)
- updates to incident response plans which were made as a result of testing exercises

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	A#2 Exercise scenarios are documented, regularly reviewed, and validated.
Term	'regularly reviewed'
Interpretation	On a scheduled basis, at sufficient frequency to ensure the form your exercise scenarios take is up-to-date with your operating environment, the intelligence available to you and your organisation's risks.

Indicator(s) of good practice	A#2 Exercise scenarios are documented, regularly reviewed, and validated.
Term	'validated'
Interpretation	There is no prescribed method for validating your exercise scenarios, and there is no prescription for who performs the validation. What's important is that your organisation evaluates your exercise scenarios to determine: whether the exercise scenario is plausible for your organisation's circumstances and the threats you face whether the scenario is suitably designed to test all your organisation's response functions, not just the ones you already have a high level of confidence in

Indicator(s) of good practice	A#3 Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned.
Term	'routinely run'
Interpretation	Exercises should be run on a scheduled basis. How often they occur is a local decision, but it should be enough to respond to emerging threats, and keep your team's knowledge of incident response policies, processes and procedures sufficient to effectively deploy them when they are called upon.

Additional guidance

For additional guidance, see:

National Cyber Security Centre | D1 Response and recovery planning
National Cyber Security Centre | Effective steps to cyber exercise creation

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 3:37 pm

← **Previous Chapter**

Objective D - Minimising the impact of incidents

Next Chapter →

Principle: D2 Lessons learned

Chapters

Press office

Tell us what you think of our website

RSS feeds

Follow us on social media

Twitter

Facebook

LinkedIn

YouTube