NHS England

# Data Security and Protection Toolkit 2024-25

CAF aligned DSPT - Objective D – Minimising the impacts of incidents

**This session is being recorded and will be uploaded to the CAN workspace**

NHS England
08 August 2024

# Welcome and agenda for today

**Housekeeping**

- The session is being recorded and is a one-way broadcast, please use the Q&A function to ask any questions
- The slides and recording will be uploaded to the CAN workspace after there will be a link to the recordings for non-CAN members
- The first three webinars have been uploaded to YouTube (unlisted) and can be accessed here:

  Webinar 1 Background and overview: https://www.youtube.com/watch?v=BG6YE1h4W40

  Webinar 2 Section A - Managing risk: https://www.youtube.com/watch?v=2aZ6TyEkUgc

  Webinar 3 Section B - Protecting against cyber attack and data breaches: https://youtu.be/IP0Fs1iX1WU

  Webinar 4 Section E - Using and sharing information appropriately https://youtu.be/JvJhxen6aEg

- If you experience any technical issues, please leave and re-join the call

# Webinar content

## Session 2 – Objective D – minimising the impacts of incidents

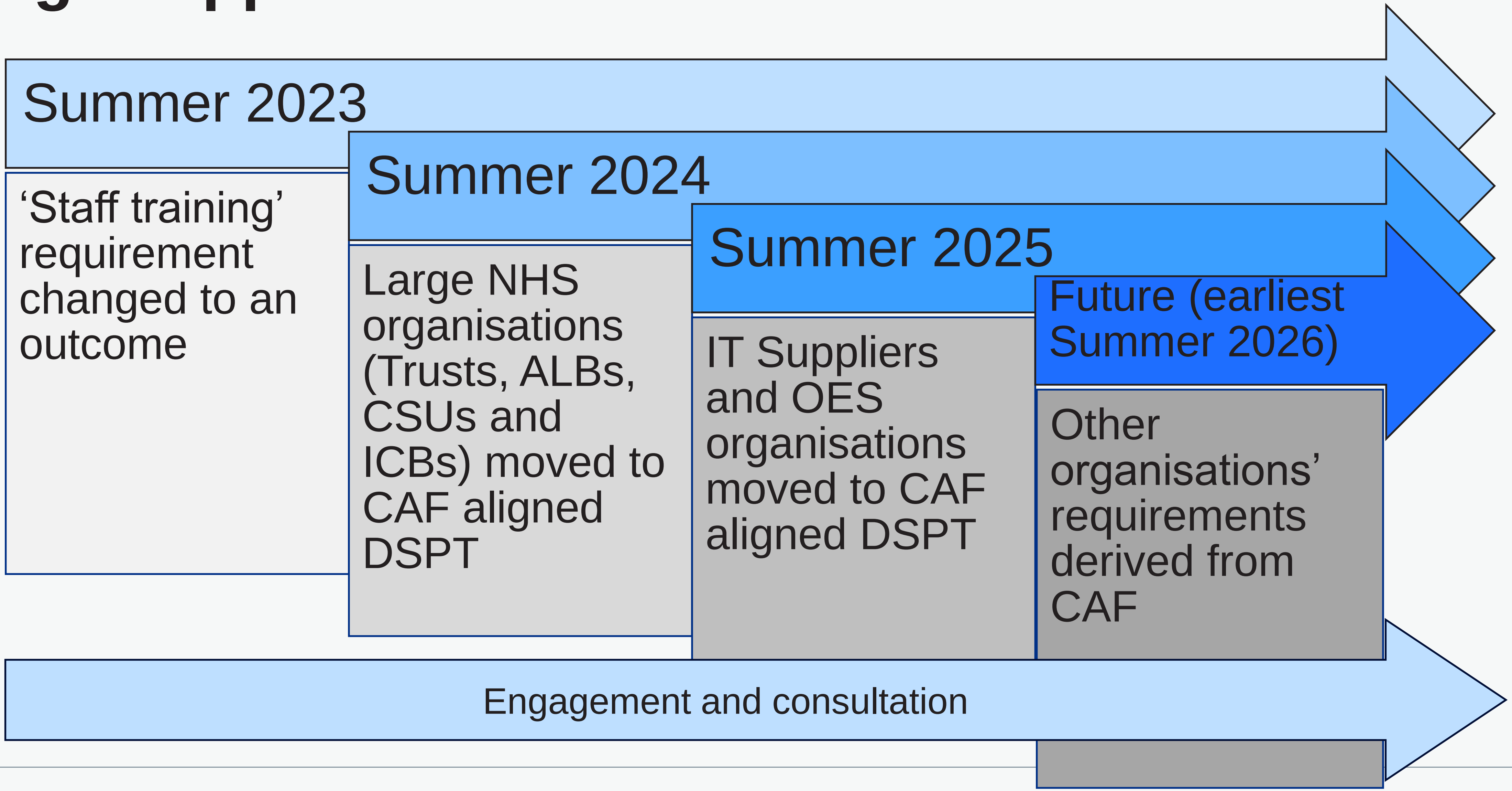
- ➢ Overview – what is in the Objective and which teams need to be involved in responding to it?
- ➢ Contributing outcomes – A step through D1
- ➢ Demonstration
- ➢ Contributing outcomes – A step through D2
- ➢ Q&A session

# What is happening and why?

# What you need to know

- In September 2024 the DSPT will be changing to adopt the National Cyber Security Centre’s Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance.
- This change will lead to NHS Trusts, CSUs, ALBs and ICBs seeing a different interface when they log in, which sets out CAF-aligned requirements in terms of Objectives, Principles and Outcomes.
- The goal of the CAF is to set out broad principles to drive good decision-making, rather than a “compliance checklist” of good practices.
- Expectations for cyber security and IG controls should remain at a reasonably comparable level to the current DSPT, tightening only in areas where NHSE and DHSC believe the higher standard to be a necessary obligation.
- Guidance is being be produced to help understand the content, approach and expectations of the CAF-aligned DSPT.

# Staged approach for DSPT



Summer 2023

‘Staff training’ requirement changed to an outcome

Summer 2024

Large NHS organisations (Trusts, ALBs, CSUs and ICBs) moved to CAF aligned DSPT

Summer 2025

IT Suppliers and OES organisations moved to CAF aligned DSPT

Future (earliest Summer 2026)

Other organisations’ requirements derived from CAF

Engagement and consultation

# What is staying the same for 24-25?

# DSPT functionality - not changing (1/2)

### Name and URL

Data Security and Protection Toolkit

Web address unchanged https://www.dsptoolkit.nhs.uk/

### Deadlines

Final Publication 30 June 2025

Interim Publication by 31 December 2024

### Standards Met

Organisation has met expectations

### Requirement for Audit

Audit Guidance being updated

Aligned with guidance and Indicators of good practice

### SIRO sign off

Requires formal sign off

SIRO level for 24-25.

# DSPT functionality - not changing (2/2)

### Toolkit for other sectors

IT Suppliers, Universities, Local Authorities, GP

Other sectors

### Improvement Plan

Organisations not meeting expectation complete Improvement plan

### Access to history

Previous years DSPT assessments can be accessed

Not transferred over though

### Organisation Search

DSPT Status in public domain

Search for other organisations DSPT Status

### Support

Exeter Helpdesk

Webinars

Guidance

# What is Changing?

# DSPT functionality - what's changing

### Exemptions

No exemptions for NHS Mail or Cyber Essentials + certification

### Data Security Standards

Cyber Assessment framework replacing the 10 Data Security Standards

### Evidence

Ability to upload any evidence type to any outcome

### Respond at Outcome

Higher level than evidence item

Likely to need input from Cyber, IT operations and IG

### Standards Exceeded

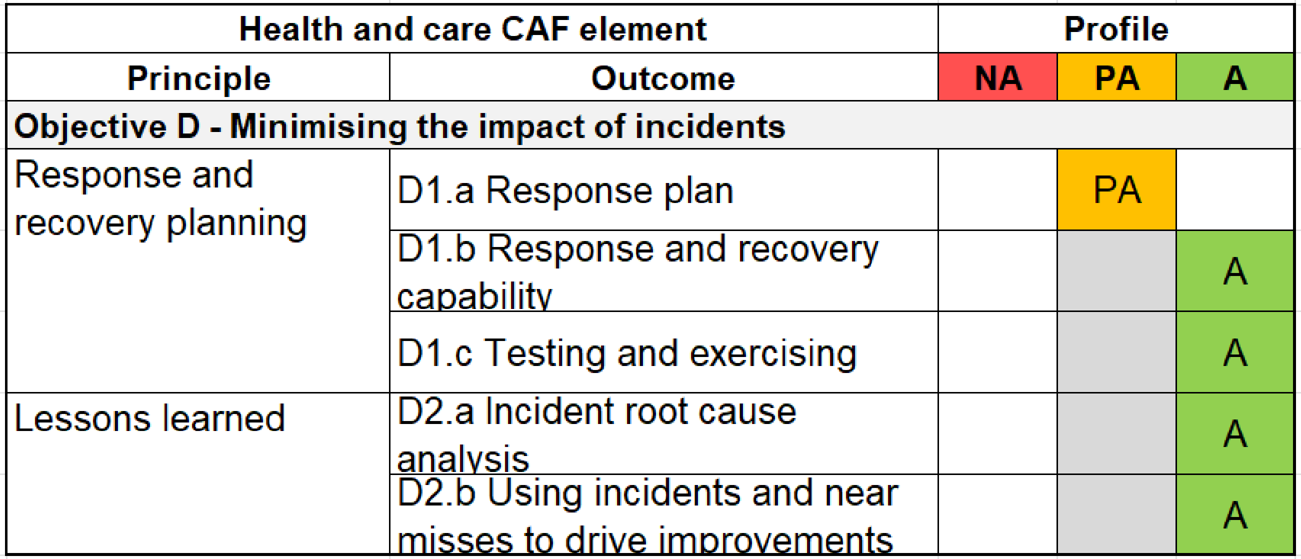
Not available for 24-25

To be considered for 25-26

# **Objective D** – Minimising the impacts of incidents

# Expectations for Standards met:

# Objective D – Minimising the impacts of incidents



| Health and care CAF element | | Profile | | |
|---|---|---|---|---|
| **Principle** | **Outcome** | **NA** | **PA** | **A** |
| **Objective D - Minimising the impact of incidents** | | | | |
| Response and recovery planning | D1.a Response plan | | PA | |
| | D1.b Response and recovery capability | | | A |
| | D1.c Testing and exercising | | | A |
| Lessons learned | D2.a Incident root cause analysis | | | A |
| | D2.b Using incidents and near misses to drive improvements | | | A |

# Principle: D1 Response and recovery planning

# Contributing outcome:
# D1.a Response Plan

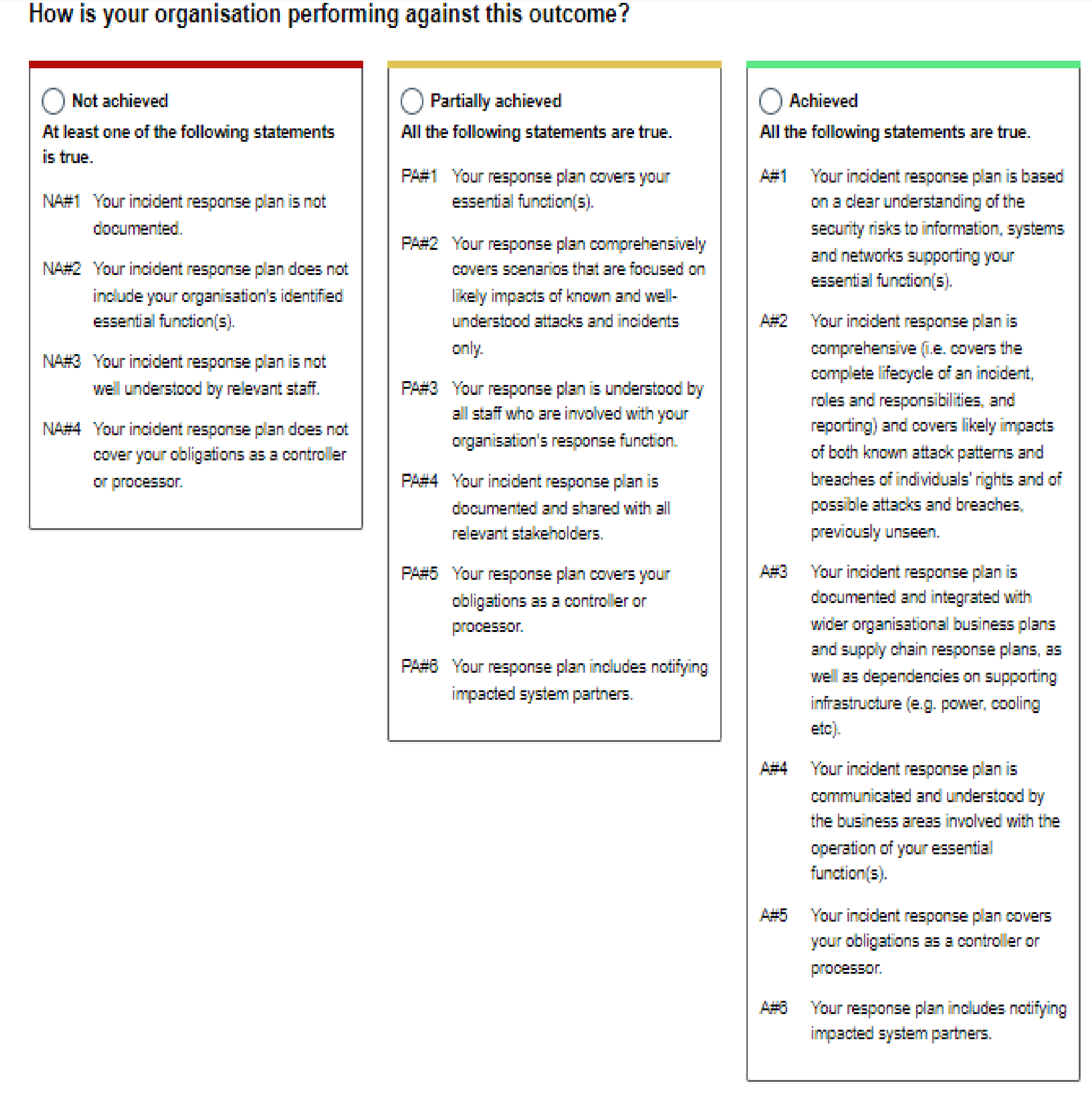
Contributing outcome D1.a

## 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.**

### Expectation

The baseline expectation for this contributing outcome is ***Partially achieved***



How is your organisation performing against this outcome?

○ Not achieved

At least one of the following statements is true.

NA#1 Your incident response plan is not documented.

NA#2 Your incident response plan does not include your organisation's identified essential function(s).

NA#3 Your incident response plan is not well understood by relevant staff.

NA#4 Your incident response plan does not cover your obligations as a controller or processor.

○ Partially achieved

All the following statements are true.

PA#1 Your response plan covers your essential function(s).

PA#2 Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks and incidents only.

PA#3 Your response plan is understood by all staff who are involved with your organisation's response function.

PA#4 Your incident response plan is documented and shared with all relevant stakeholders.

PA#5 Your response plan covers your obligations as a controller or processor.

PA#6 Your response plan includes notifying impacted system partners.

○ Achieved

All the following statements are true.

A#1 Your incident response plan is based on a clear understanding of the security risks to information, systems and networks supporting your essential function(s).

A#2 Your incident response plan is comprehensive (i.e. covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely impacts of both known attack patterns and breaches of individuals' rights and of possible attacks and breaches, previously unseen.

A#3 Your incident response plan is documented and integrated with wider organisational business plans and supply chain response plans, as well as dependencies on supporting infrastructure (e.g. power, cooling etc).

A#4 Your incident response plan is communicated and understood by the business areas involved with the operation of your essential function(s).

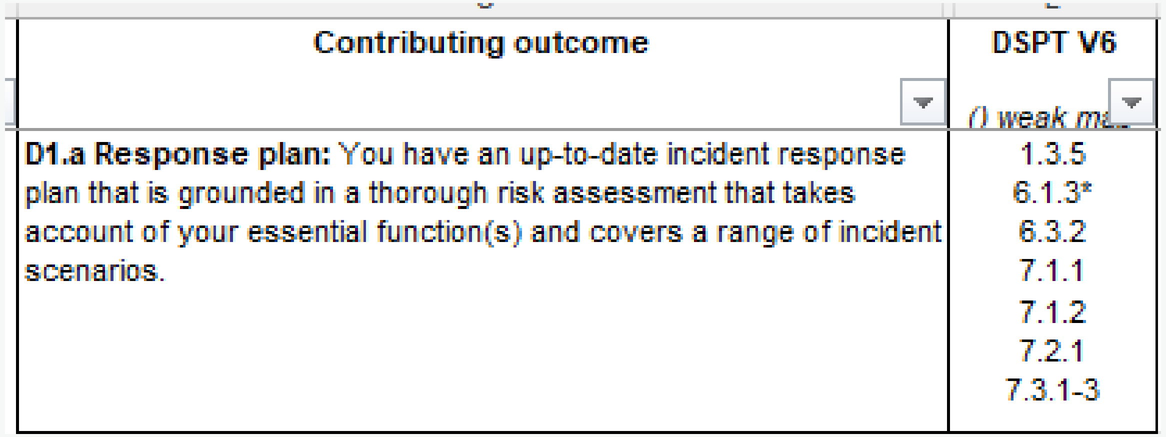
A#5 Your incident response plan covers your obligations as a controller or processor.

A#6 Your response plan includes notifying impacted system partners.

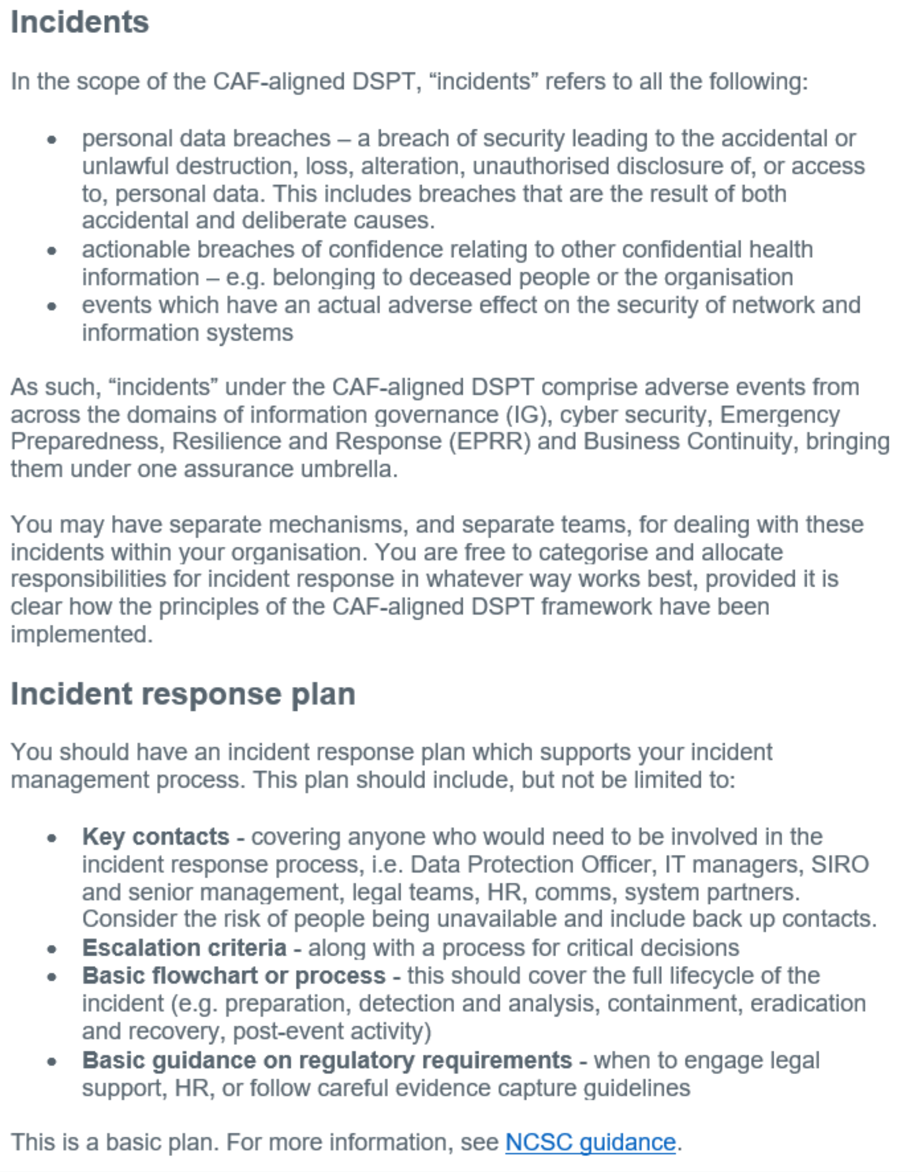
# Principle: D1 Response and recovery planning

# Contributing outcome:
# D1.a Response Plan

# Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **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. | 1.3.5<br>6.1.3*<br>6.3.2<br>7.1.1<br>7.1.2<br>7.2.1<br>7.3.1-3 |



## Incidents

In the scope of the CAF-aligned DSPT, “incidents” refers to all the following:

- 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.
- actionable breaches of confidence relating to other confidential health information – e.g. 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 are free to categorise and allocate responsibilities for incident response in whatever way works best, provided it is clear how the principles of the CAF-aligned DSPT framework have been implemented.

## Incident response plan

You should have an incident response plan which supports your incident management process. This plan should include, but not be limited to:

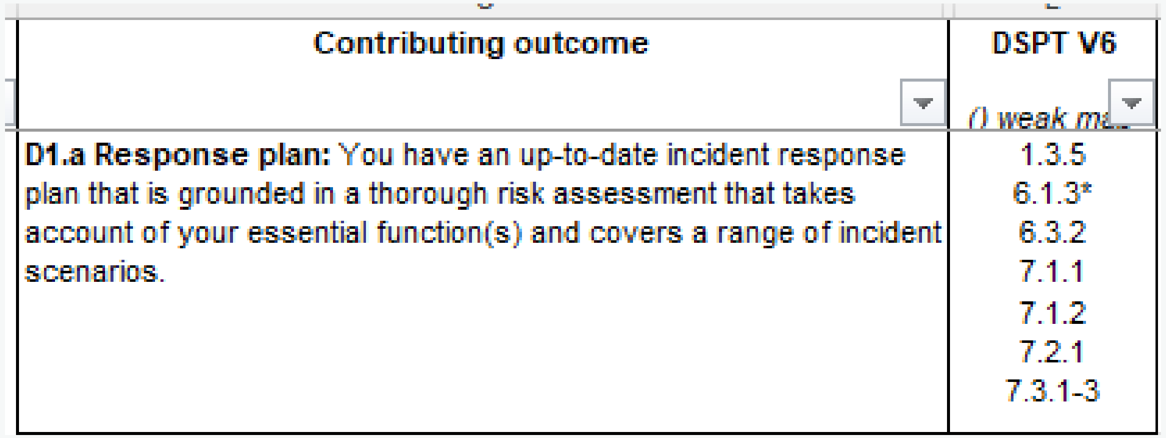
- **Key contacts** - covering anyone who would need to be involved in the incident response process, i.e. Data Protection Officer, IT managers, SIRO and senior management, legal teams, HR, comms, system partners. Consider the risk of people being unavailable and include back up contacts.
- **Escalation criteria** - along with a process for critical decisions
- **Basic flowchart or process** - this should cover the full lifecycle of the incident (e.g. preparation, detection and analysis, containment, eradication and recovery, post-event activity)
- **Basic guidance on regulatory requirements** - when to engage legal support, HR, or follow careful evidence capture guidelines

This is a basic plan. For more information, see NCSC guidance.

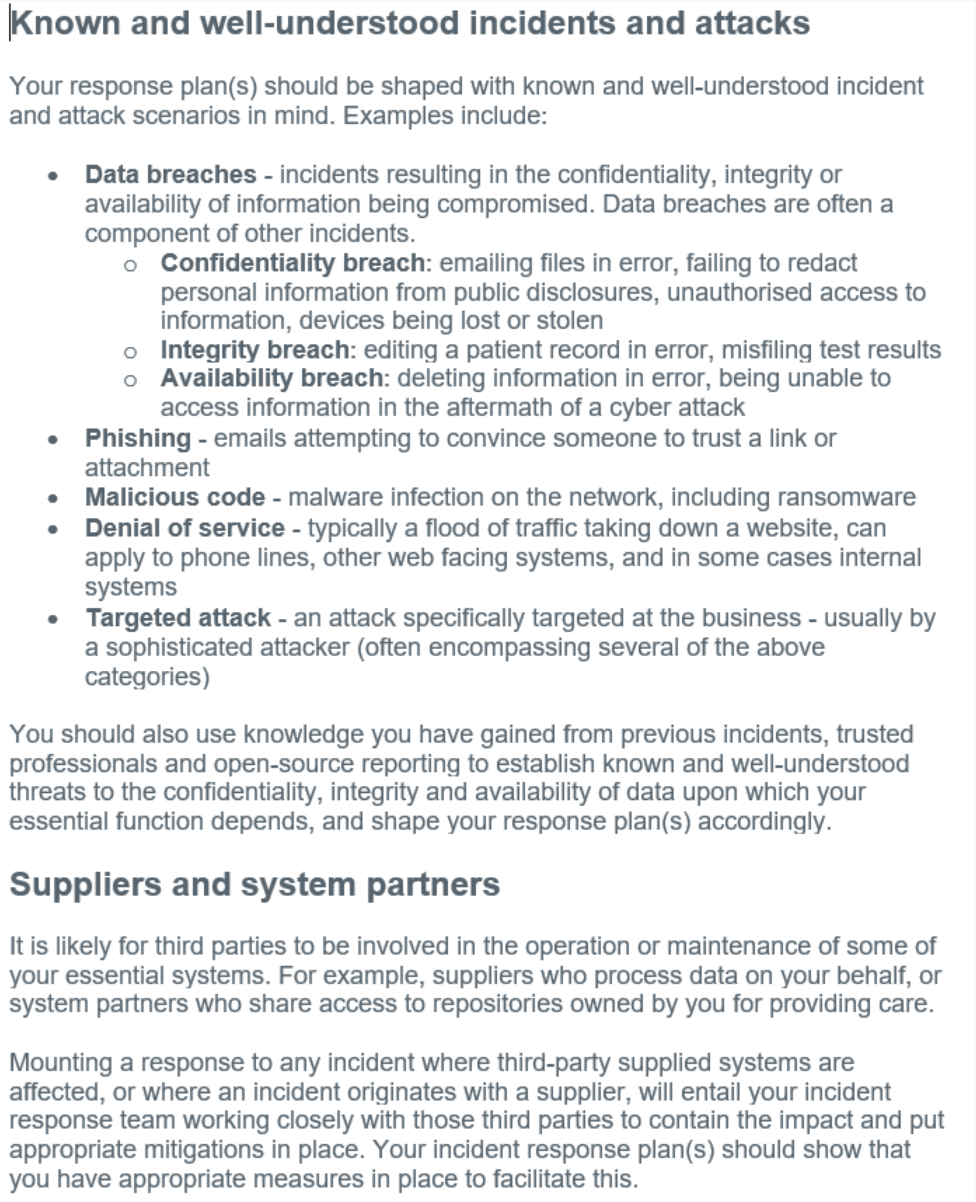
# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.a Response Plan

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **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. | 1.3.5<br>6.1.3*<br>6.3.2<br>7.1.1<br>7.1.2<br>7.2.1<br>7.3.1-3 |



### 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.
  - **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, 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

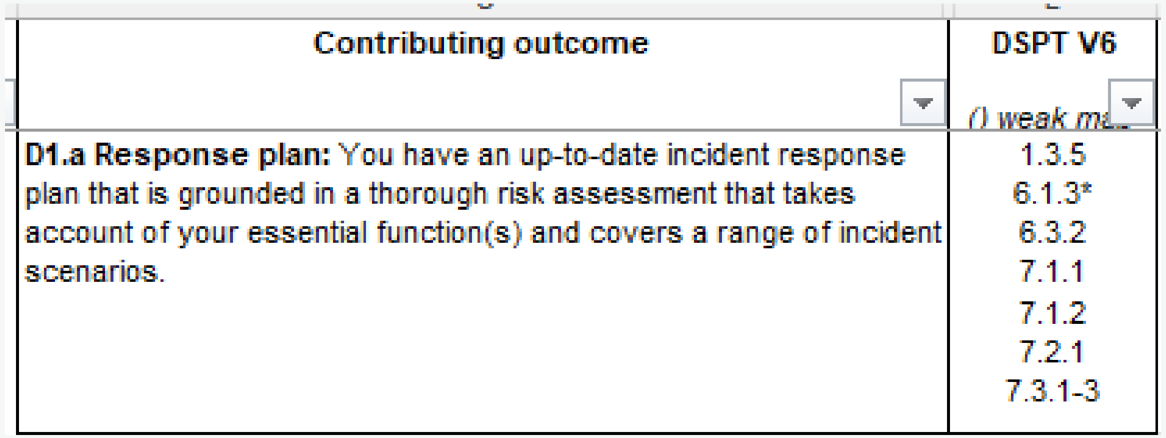
It is likely for third parties to be involved in the operation or maintenance of some of your essential systems. For example, suppliers who process data on your behalf, or system partners who share access to repositories owned by you for providing care.

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.

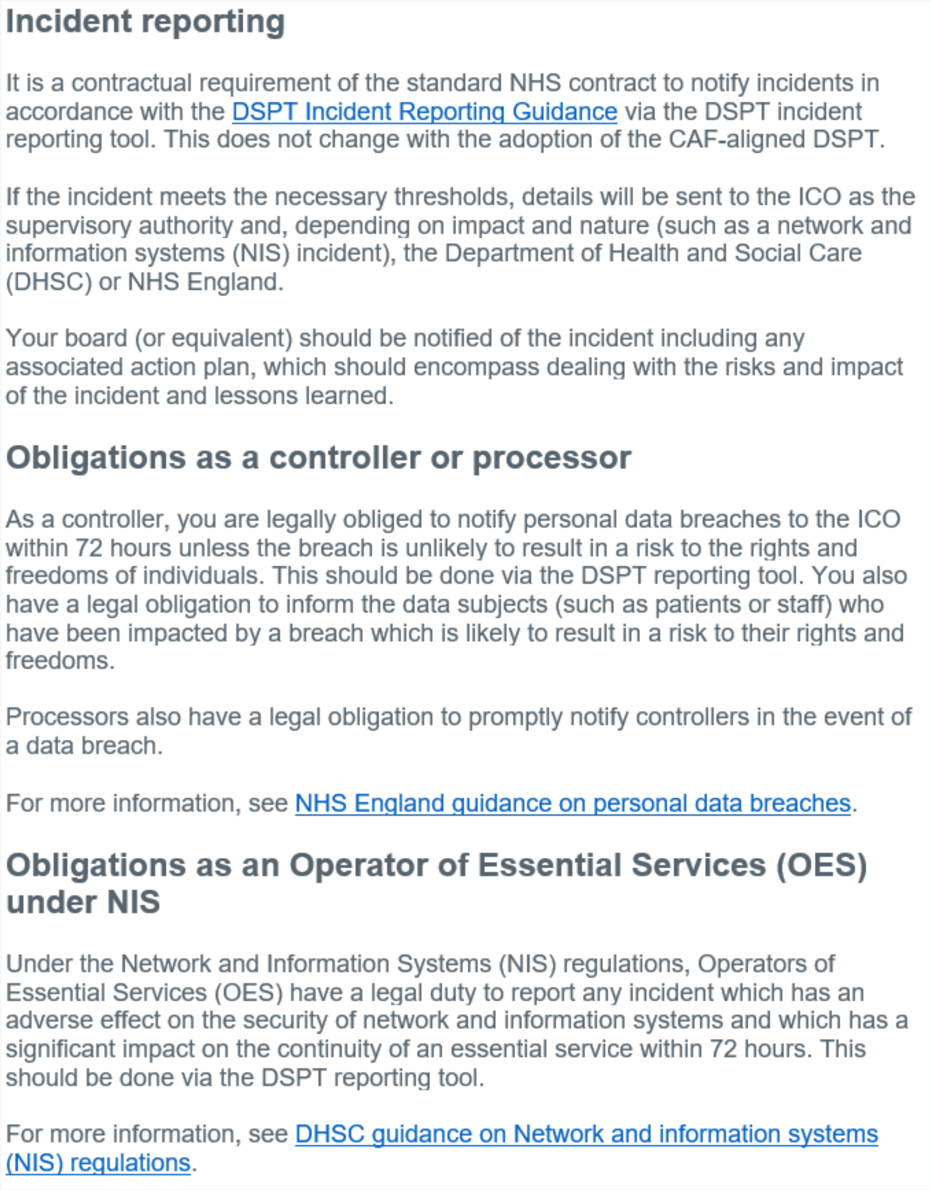
# Principle: D1 Response and recovery planning

# Contributing outcome:
# D1.a Response Plan

# Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak m |
|---|---|
| **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. | 1.3.5<br>6.1.3*<br>6.3.2<br>7.1.1<br>7.1.2<br>7.2.1<br>7.3.1-3 |



## 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 ICO as the supervisory authority and, depending on impact and nature (such as a network and information systems (NIS) incident), the Department of Health and Social Care (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 are legally obliged to notify personal data breaches to the ICO within 72 hours unless the breach is unlikely 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

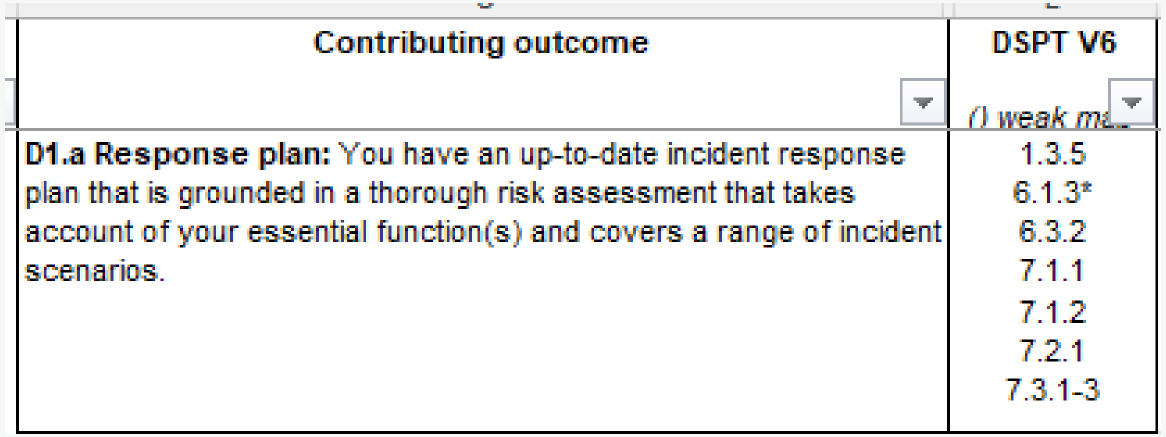
Under the Network and Information Systems (NIS) regulations, Operators of Essential Services (OES) have a legal duty to report any incident which has an adverse effect on the security of network and information systems and which has a significant impact on the continuity of an essential service within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

For more information, see DHSC guidance on Network and information systems (NIS) regulations.

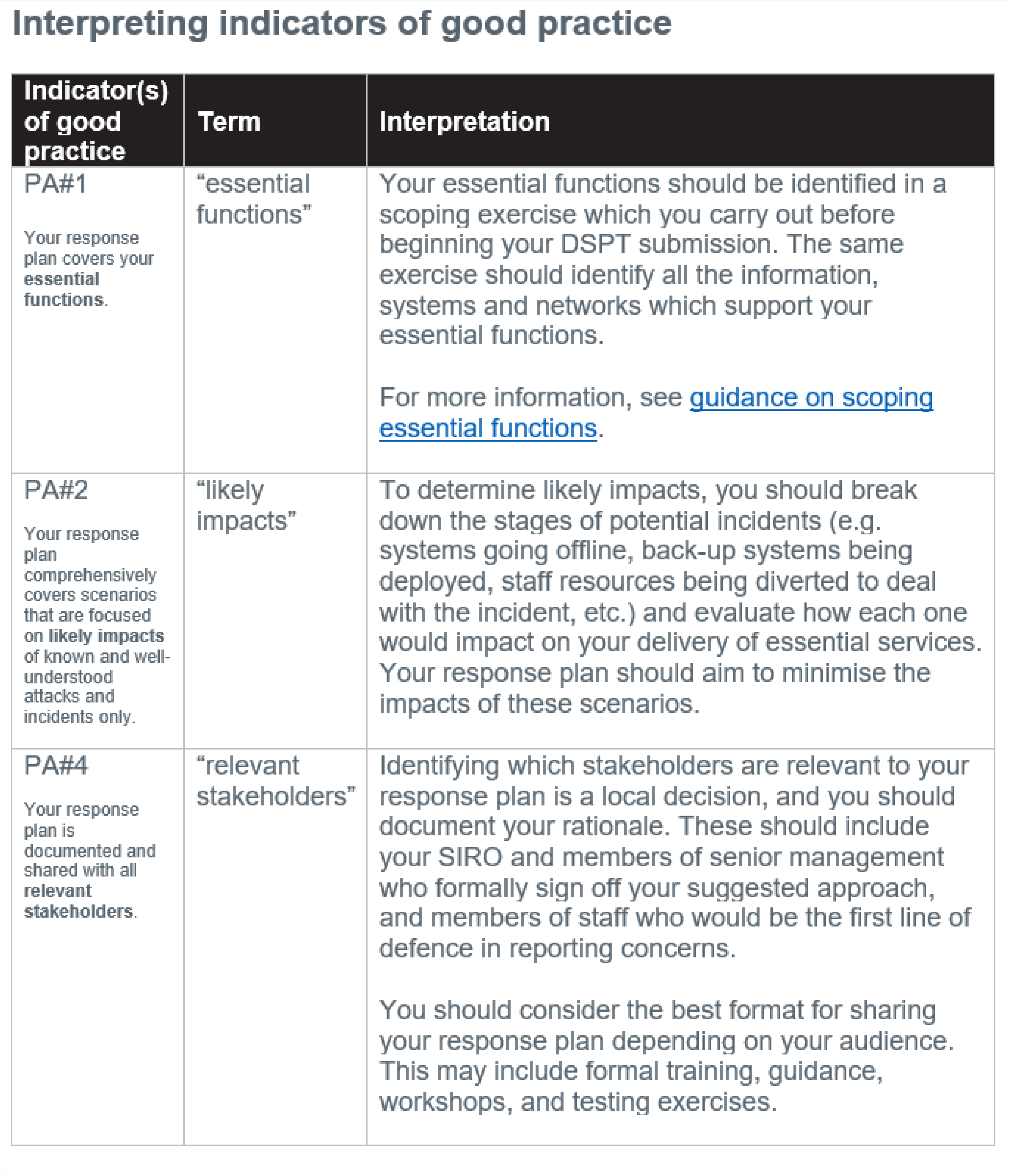
# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.a Response Plan

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **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. | 1.3.5<br>6.1.3*<br>6.3.2<br>7.1.1<br>7.1.2<br>7.2.1<br>7.3.1-3 |



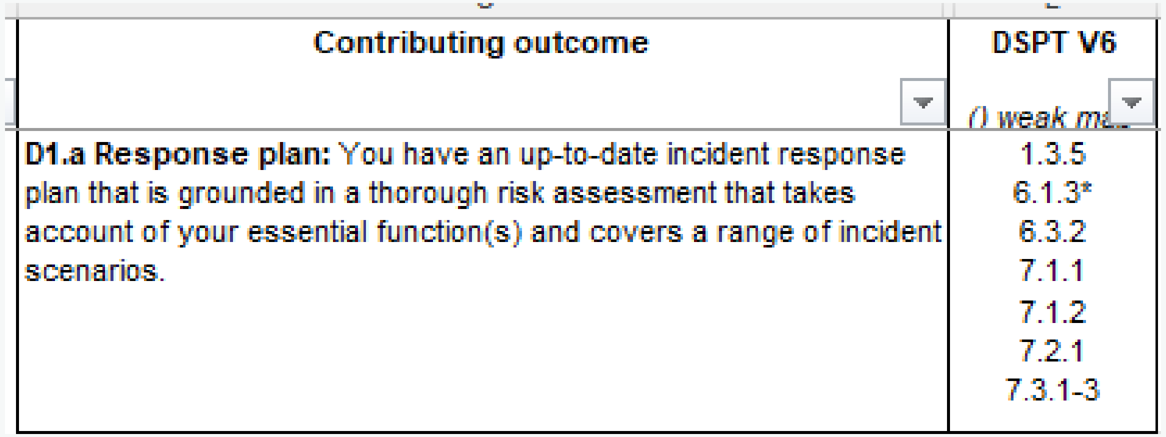
### Interpreting indicators of good practice

| Indicator(s) of good practice | Term | Interpretation |
|---|---|---|
| PA#1<br>Your response plan covers your **essential functions**. | "essential functions" | 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.<br>For more information, see guidance on scoping essential functions. |
| PA#2<br>Your response plan comprehensively covers scenarios that are focused on **likely impacts** of known and well-understood attacks and incidents only. | "likely impacts" | To determine likely impacts, you should break down the stages of potential incidents (e.g. systems going offline, back-up systems being deployed, staff resources being diverted to deal with the incident, etc.) and evaluate how each one would impact on your delivery of essential services. Your response plan should aim to minimise the impacts of these scenarios. |
| PA#4<br>Your response plan is documented and shared with all **relevant stakeholders**. | "relevant stakeholders" | 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.<br>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. |

# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.a Response Plan

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **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. | 1.3.5<br>6.1.3*<br>6.3.2<br>7.1.1<br>7.1.2<br>7.2.1<br>7.3.1-3 |

### Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- 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 (e.g. business continuity and disaster recovery, incident management)
- Risk management reports

This is not an exhaustive list. You are 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.

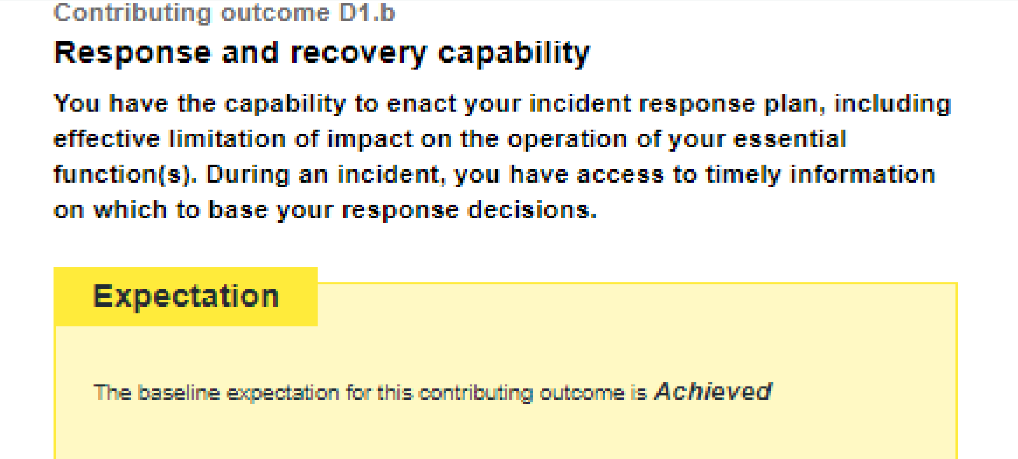
### Additional guidance

For additional guidance, see:

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

# Principle: D1 Response and recovery planning

# Contributing outcome:
# D1.b Response and recovery capability



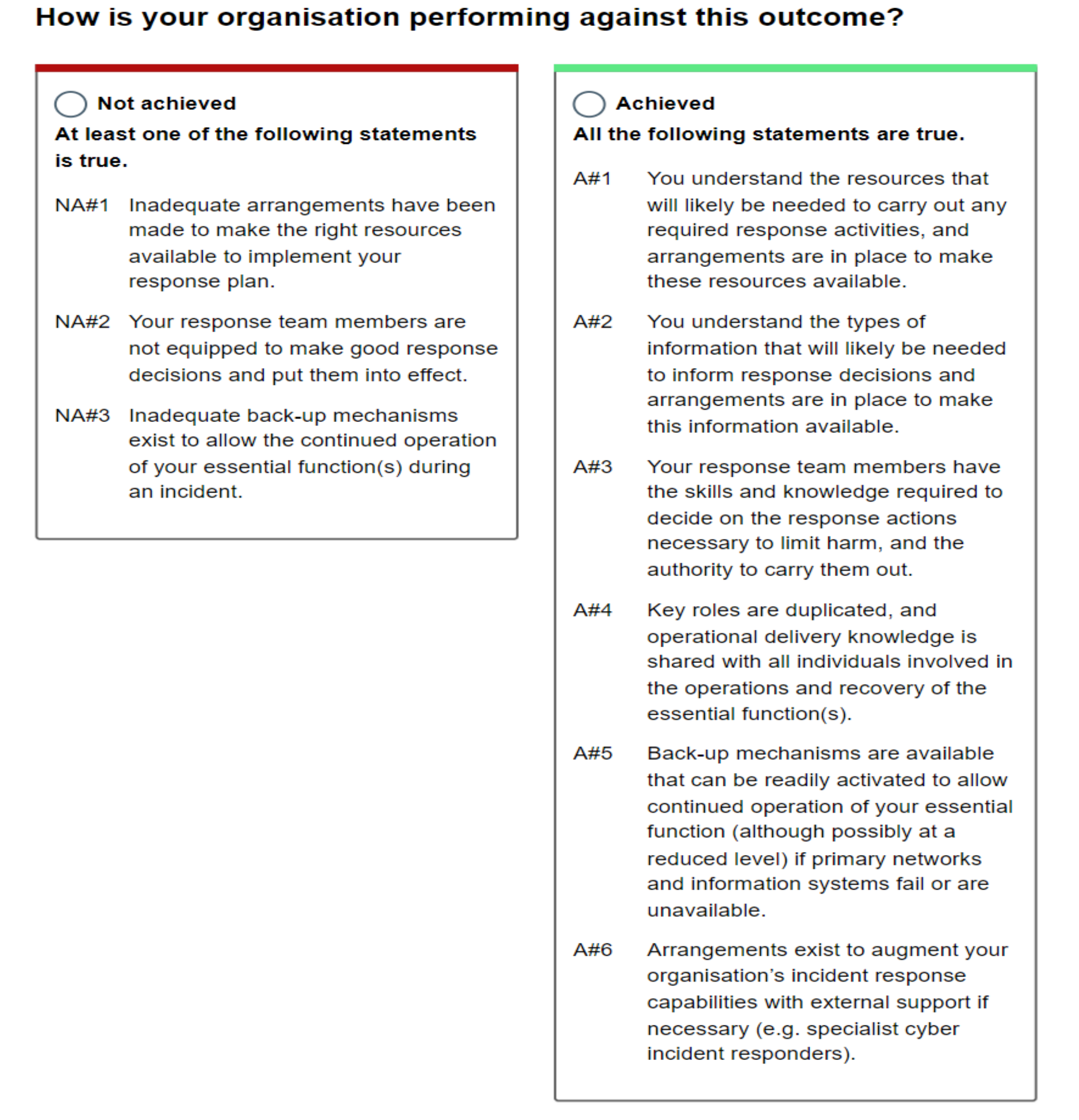
Contributing outcome D1.b

## 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.

**Expectation**

The baseline expectation for this contributing outcome is *Achieved*



**How is your organisation performing against this outcome?**

○ **Not achieved**

**At least one of the following statements is true.**

NA#1 Inadequate arrangements have been made to make the right resources available to implement your response plan.

NA#2 Your response team members are not equipped to make good response decisions and put them into effect.

NA#3 Inadequate back-up mechanisms exist to allow the continued operation of your essential function(s) during an incident.

○ **Achieved**

**All the following statements are true.**

A#1 You understand the resources that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.

A#2 You understand the types of information that will likely be needed to inform response decisions and arrangements are in place to make this information available.

A#3 Your response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and the authority to carry them out.

A#4 Key roles are duplicated, and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential function(s).

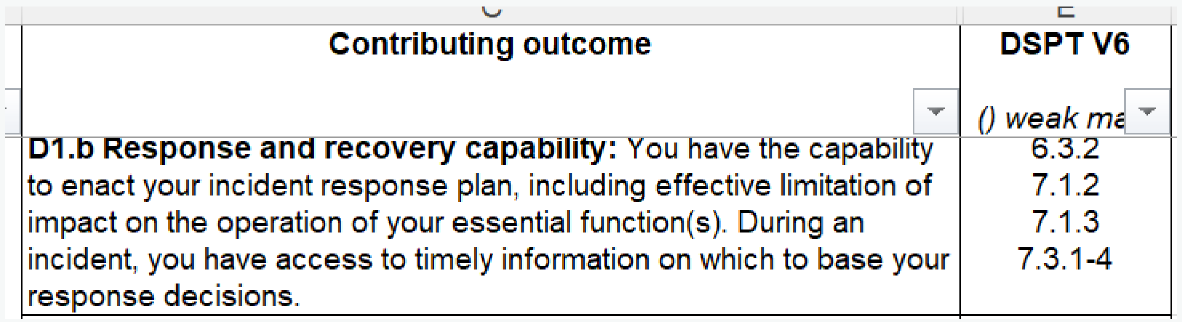
A#5 Back-up mechanisms are available that can be readily activated to allow continued operation of your essential function (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.

A#6 Arrangements exist to augment your organisation’s incident response capabilities with external support if necessary (e.g. specialist cyber incident responders).

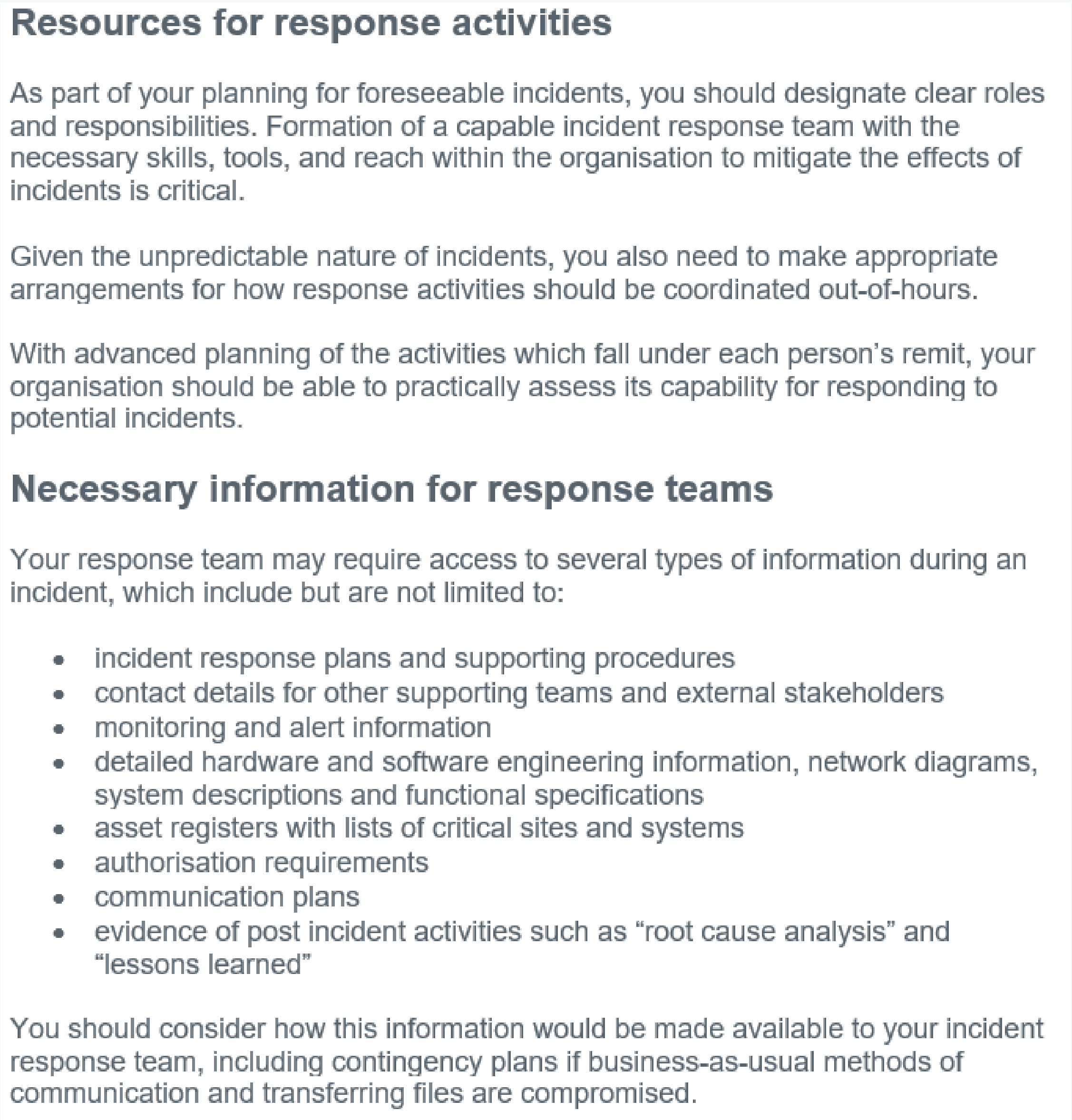
# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.b Response and recovery capability

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6 |
|---|---|
| | *() weak ma* |
| **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. | 6.3.2<br>7.1.2<br>7.1.3<br>7.3.1-4 |



### 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:

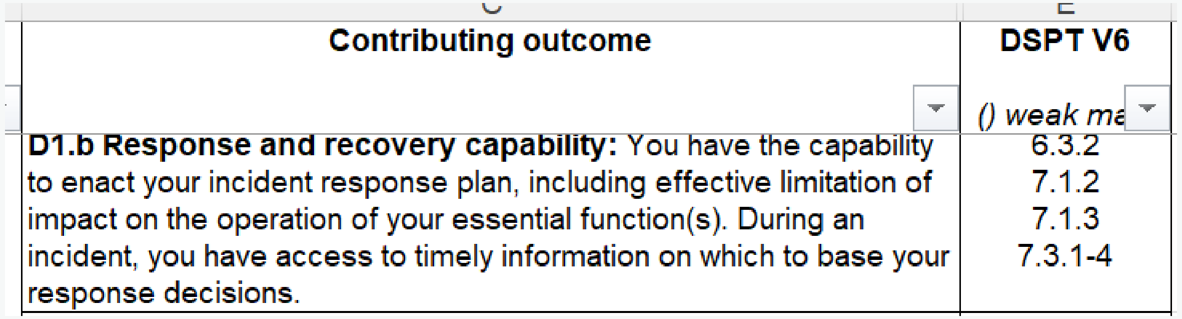
- incident response plans and supporting procedures
- contact details for other supporting teams and external stakeholders
- monitoring and alert information
- detailed hardware and software engineering information, network diagrams, system descriptions and functional specifications
- asset registers 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.

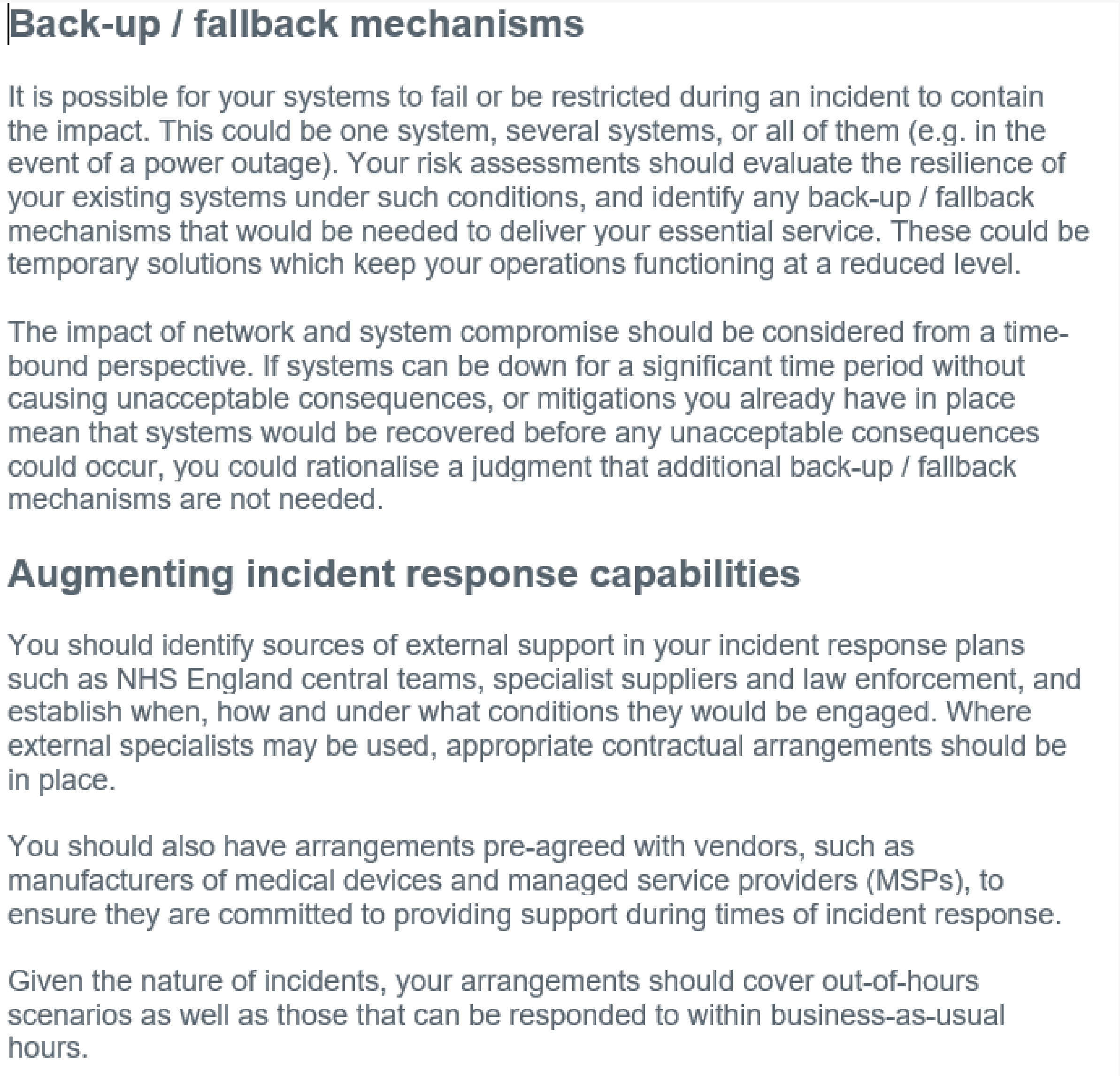
# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.b Response and recovery capability

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6 |
|---|---|
| | () weak ma |
| **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. | 6.3.2<br>7.1.2<br>7.1.3<br>7.3.1-4 |



### Back-up / fallback mechanisms

It is possible for your systems to fail or be restricted during an incident to contain the impact. This could be one system, several systems, or all of them (e.g. 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.

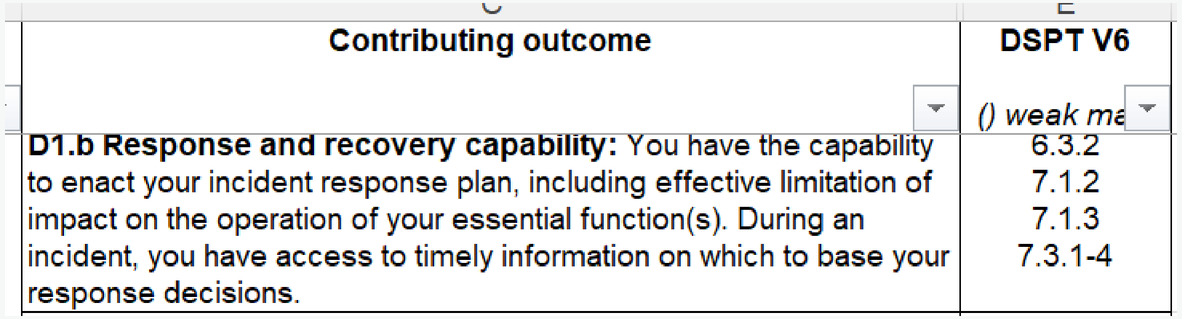
You should also have arrangements pre-agreed with vendors, such as manufacturers of medical devices and managed service providers (MSPs), to ensure they are committed to providing support during times of incident response.

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.

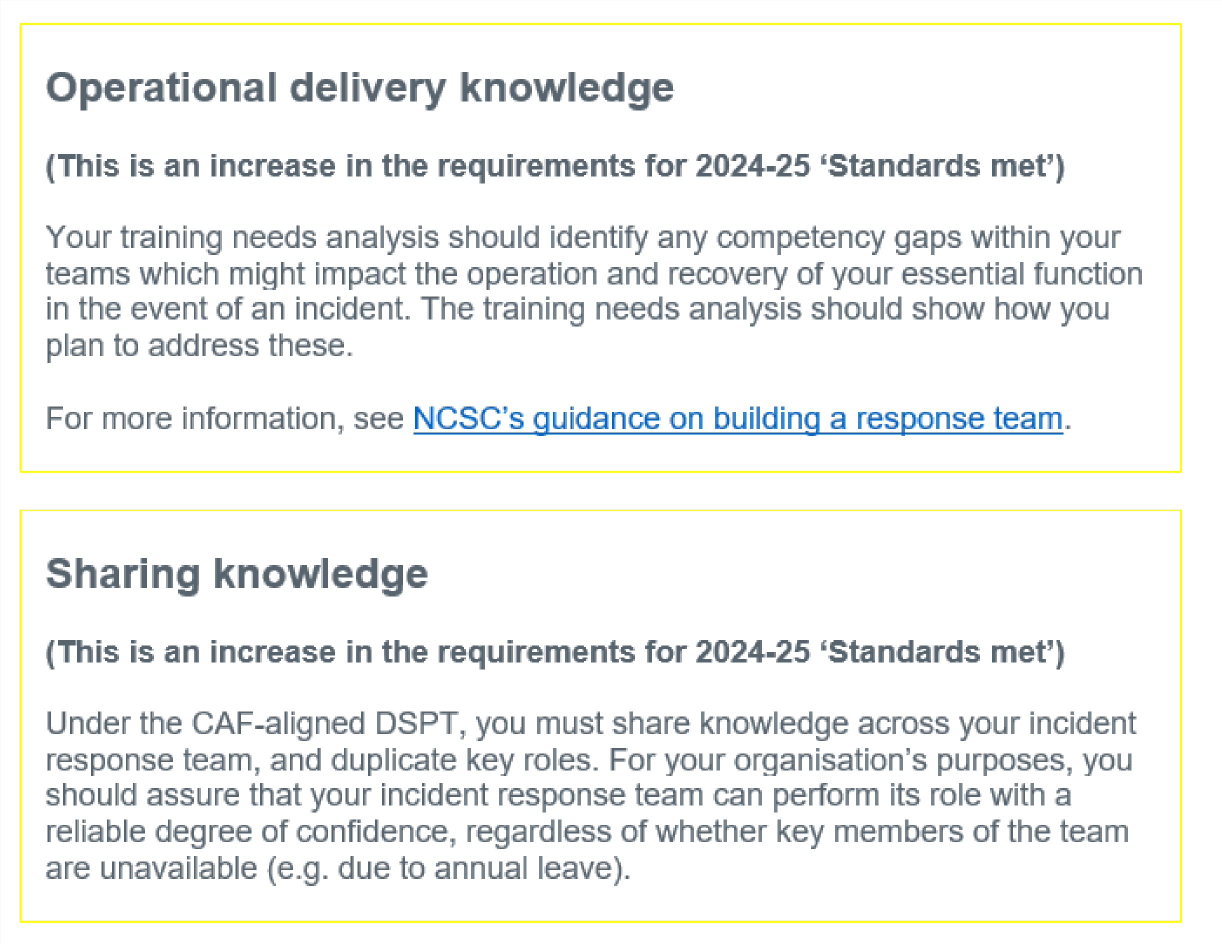
# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.b Response and recovery capability

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **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. | 6.3.2<br>7.1.2<br>7.1.3<br>7.3.1-4 |



### Operational delivery knowledge

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

Your training needs analysis should identify any competency gaps within your teams which might impact the operation and recovery of your essential function in the event of an incident. The training needs analysis should show how you plan to address these.

For more information, see NCSC’s guidance on building a response team.

### Sharing knowledge

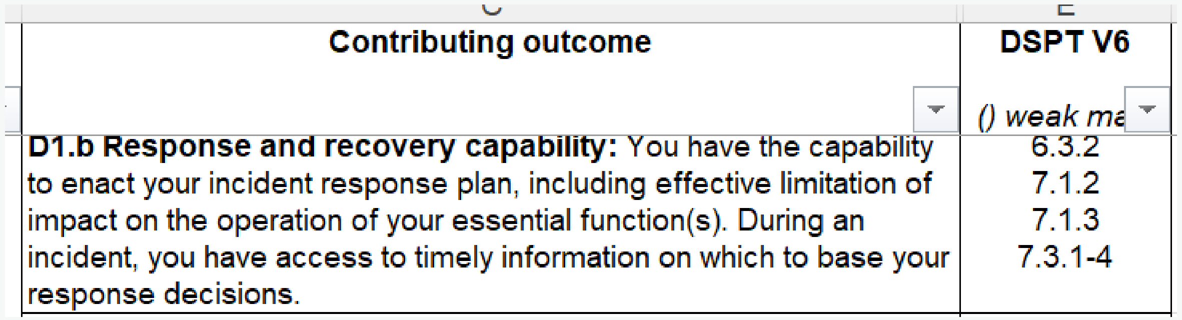
**(This is an increase in the requirements for 2024-25 ‘Standards met’)**

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 (e.g. due to annual leave).

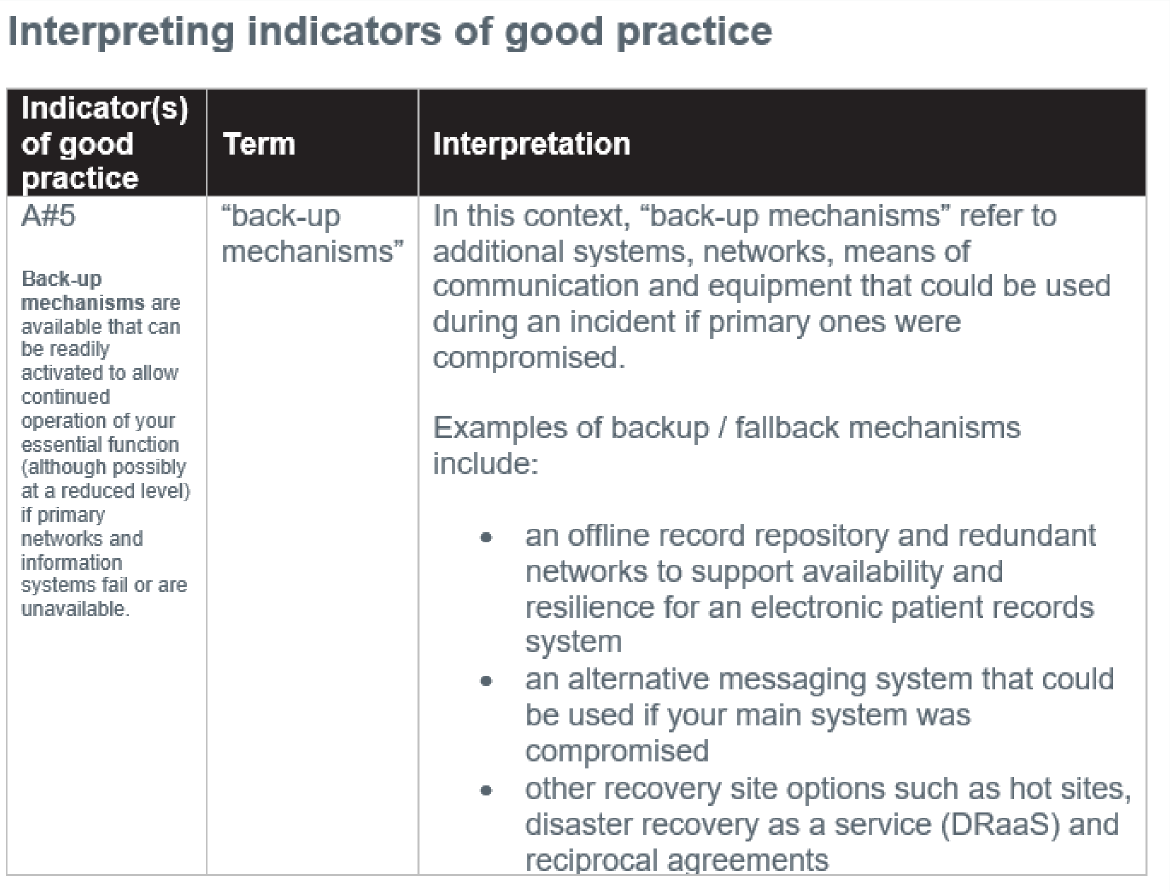
# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.b Response and recovery capability

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **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. | 6.3.2<br>7.1.2<br>7.1.3<br>7.3.1-4 |



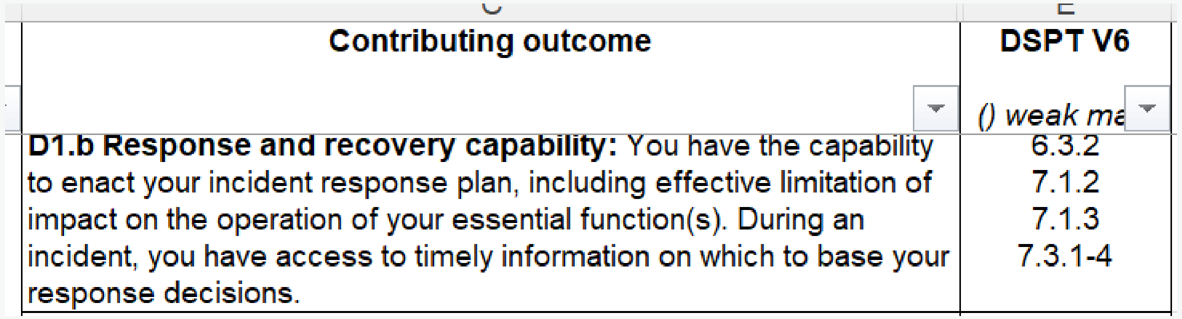
### Interpreting indicators of good practice

| Indicator(s) of good practice | Term | Interpretation |
|---|---|---|
| A#5<br>**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. | "back-up mechanisms" | 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.<br>Examples of backup / fallback mechanisms include:<br>• an offline record repository and redundant networks to support availability and resilience for an electronic patient records system<br>• an alternative messaging system that could be used if your main system was compromised<br>• other recovery site options such as hot sites, disaster recovery as a service (DRaaS) and reciprocal agreements |

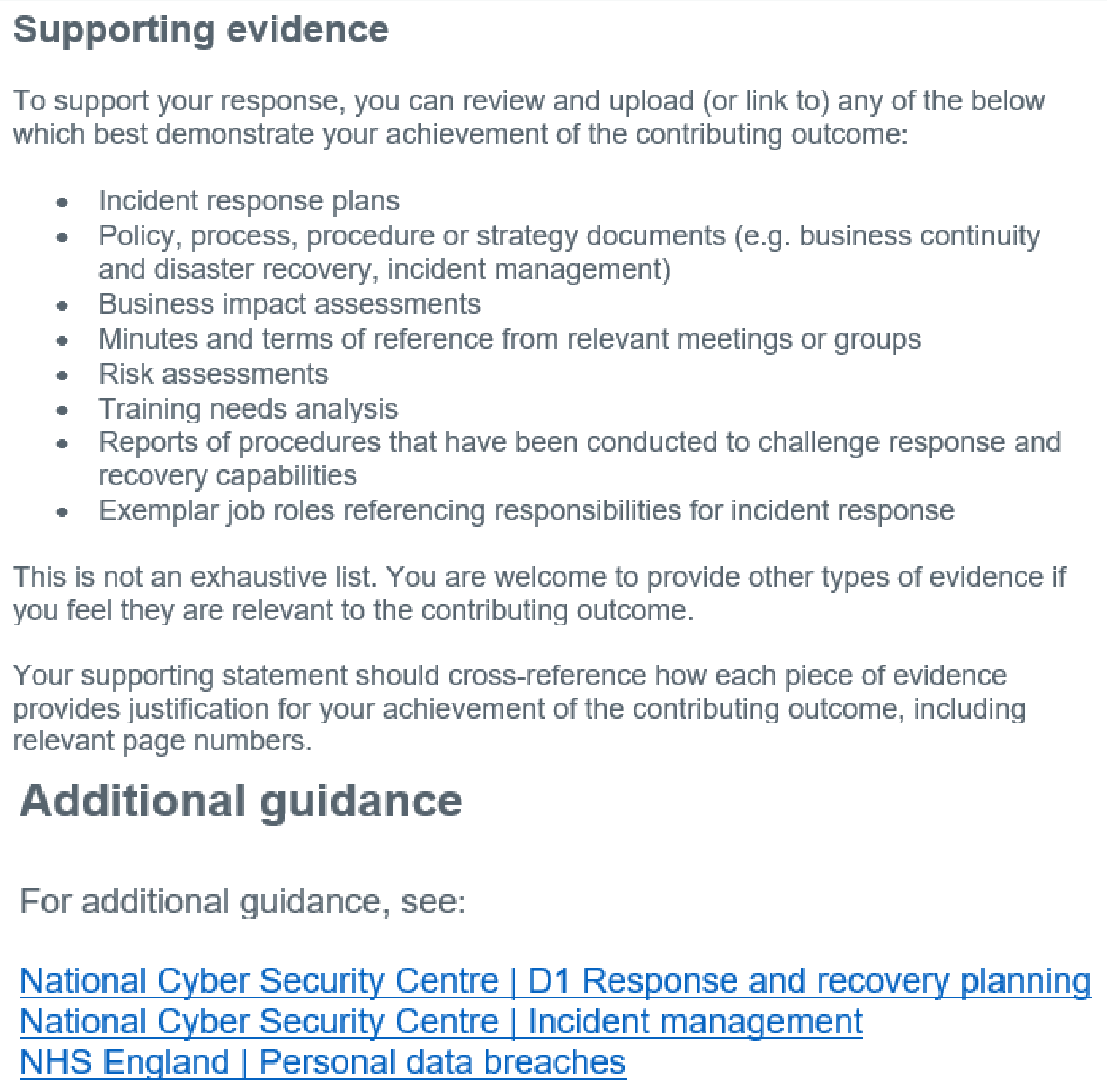
# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.b Response and recovery capability

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **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. | 6.3.2<br>7.1.2<br>7.1.3<br>7.3.1-4 |



### Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Incident response plans
- Policy, process, procedure or strategy documents (e.g. business continuity and disaster recovery, 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 are 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.

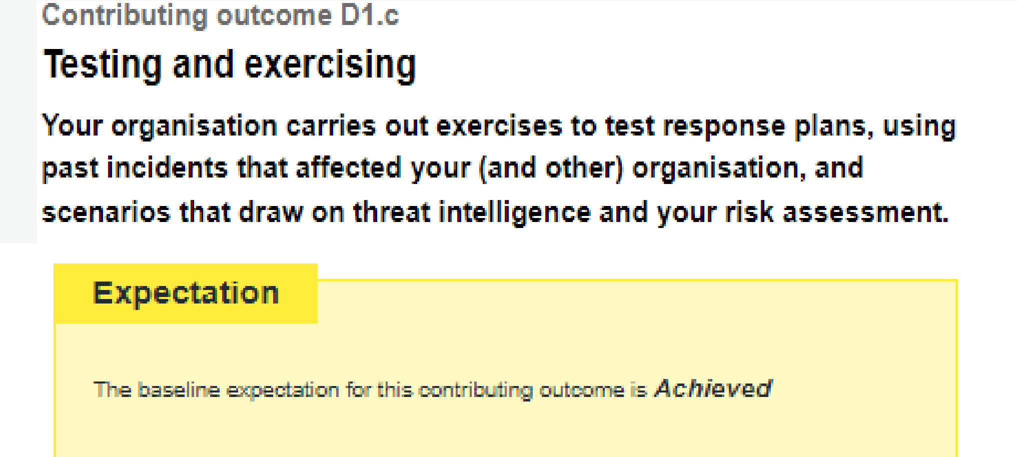
### Additional guidance

For additional guidance, see:

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

# Principle: D1 Response and recovery planning

# Contributing outcome:
# D1.c Testing and exercising



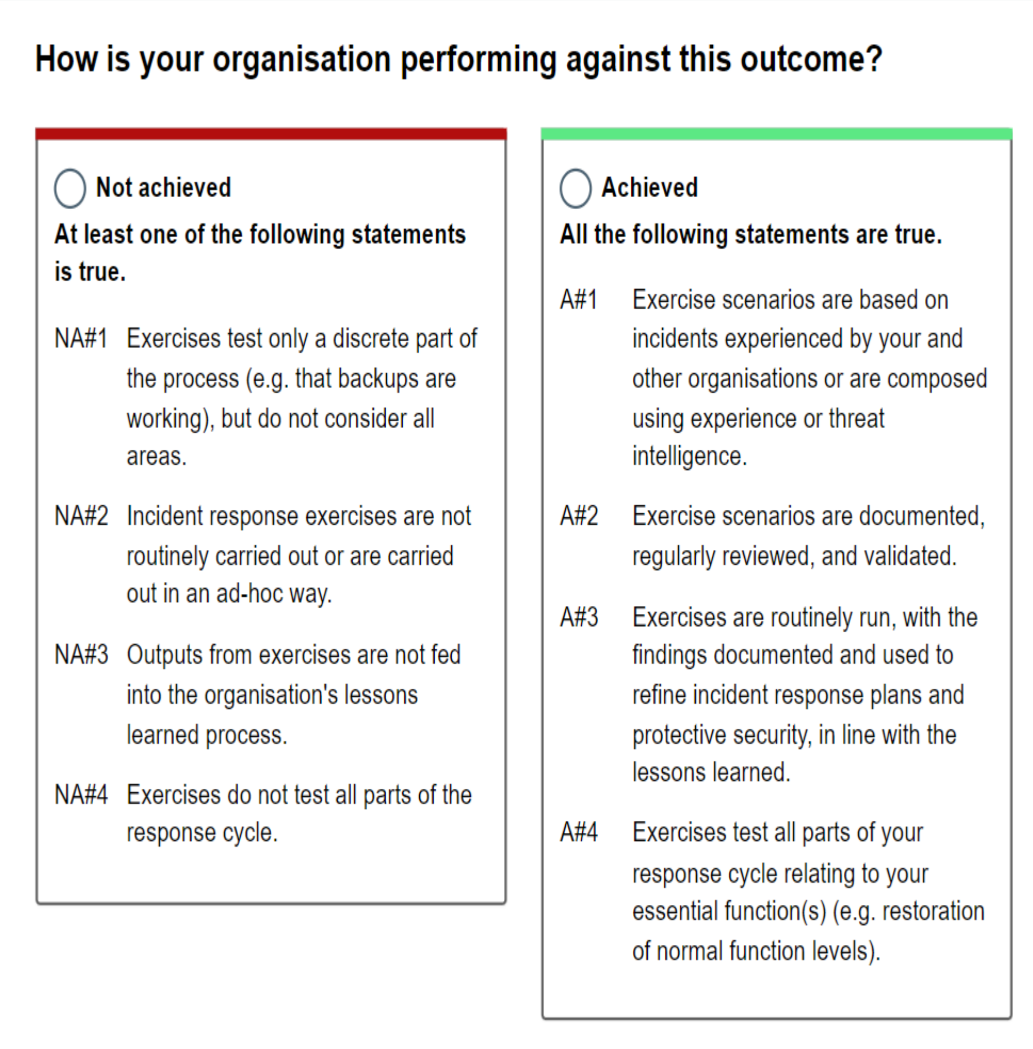
Contributing outcome D1.c

## 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.**

**Expectation**

The baseline expectation for this contributing outcome is ***Achieved***



**How is your organisation performing against this outcome?**

○ **Not achieved**

**At least one of the following statements is true.**

NA#1 Exercises test only a discrete part of the process (e.g. that backups are working), but do not consider all areas.

NA#2 Incident response exercises are not routinely carried out or are carried out in an ad-hoc way.

NA#3 Outputs from exercises are not fed into the organisation's lessons learned process.

NA#4 Exercises do not test all parts of the response cycle.

○ **Achieved**

**All the following statements are true.**

A#1 Exercise scenarios are based on incidents experienced by your and other organisations or are composed using experience or threat intelligence.

A#2 Exercise scenarios are documented, regularly reviewed, and validated.

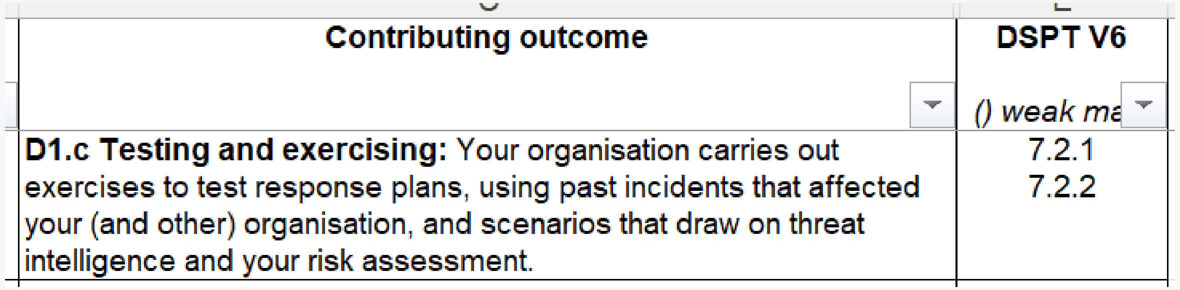
A#3 Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned.

A#4 Exercises test all parts of your response cycle relating to your essential function(s) (e.g. restoration of normal function levels).

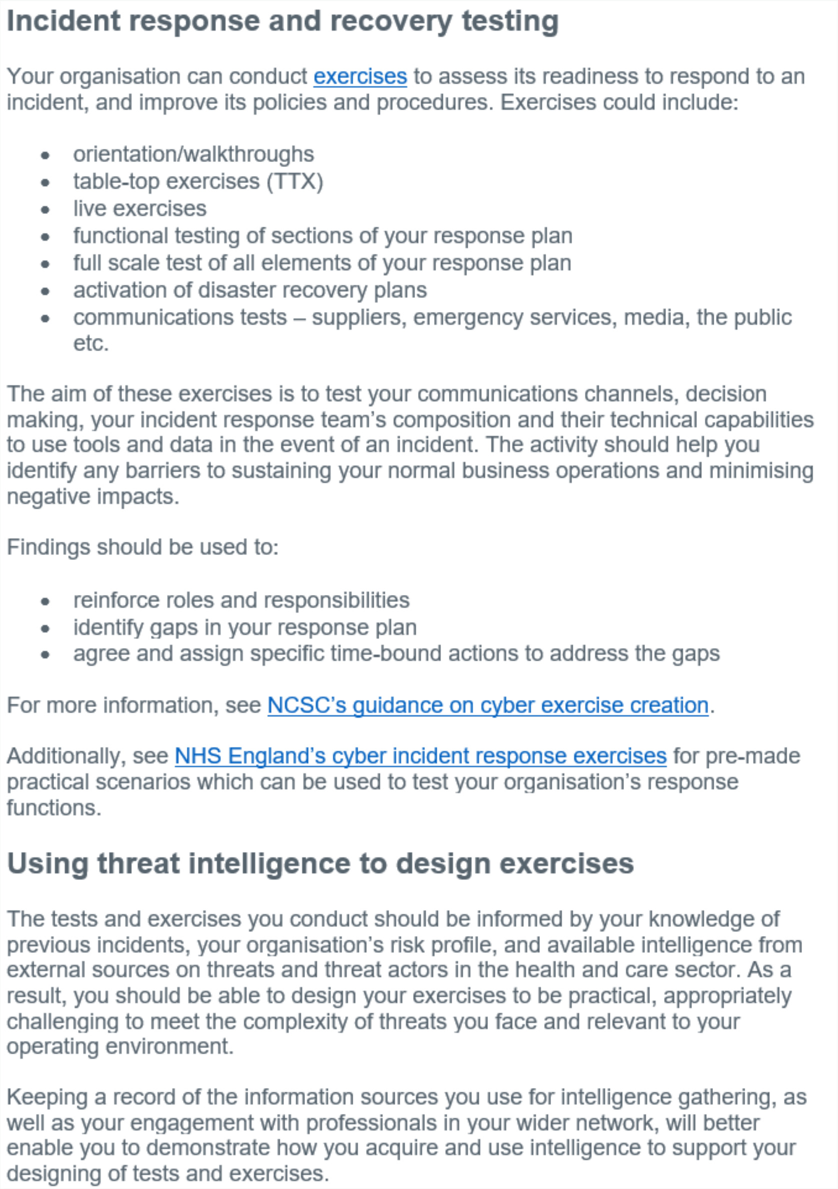
# Principle: D1 Response and recovery planning

# Contributing outcome:
# D1.c Testing and exercising

# Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **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. | 7.2.1<br>7.2.2 |



## 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 etc.

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

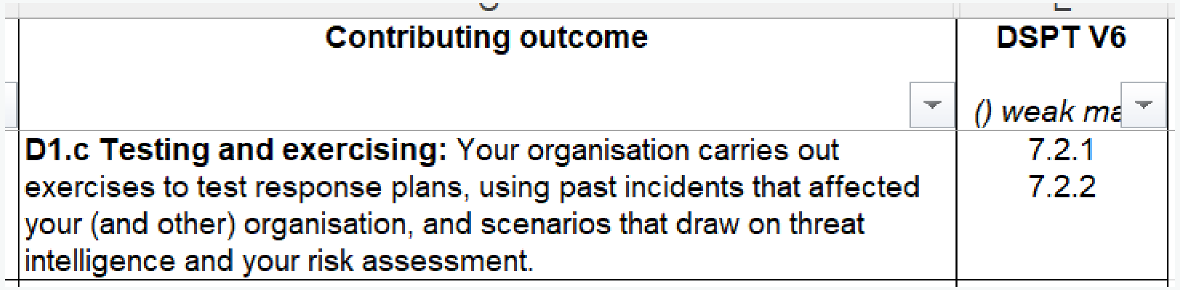
The tests and exercises you conduct should be informed by your knowledge of previous incidents, your organisation's risk profile, and available intelligence from external sources on threats and threat actors in the health and care sector. As a result, you should be able to design your exercises to be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

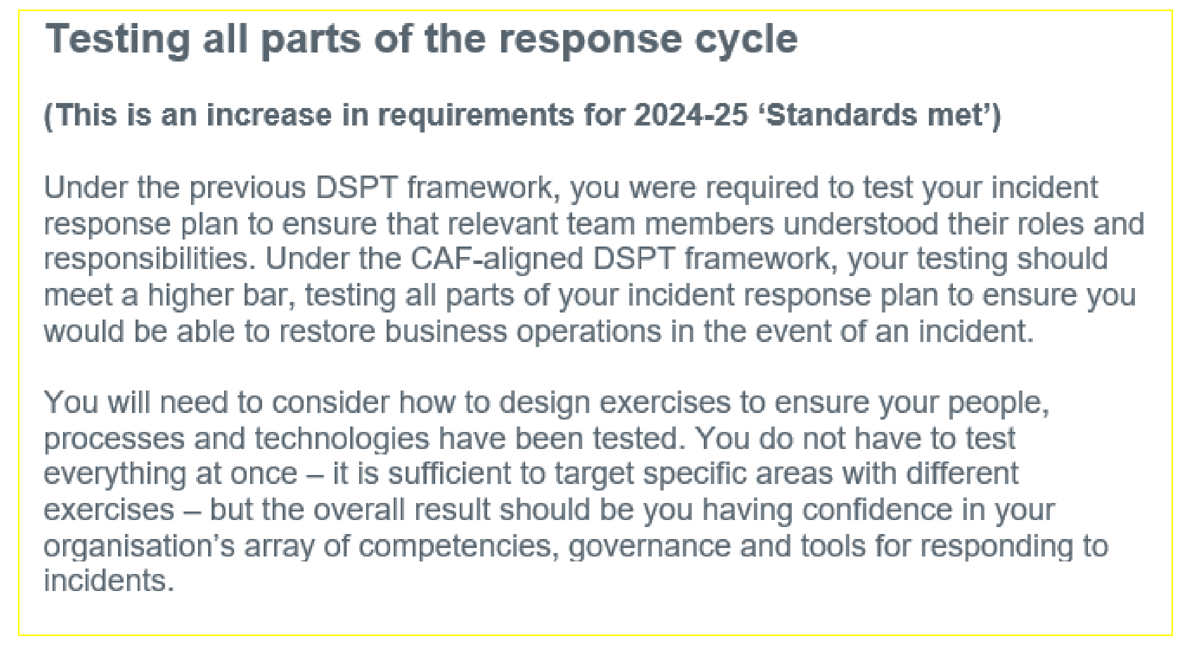
# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.c Testing and exercising

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>*() weak ma* |
|---|---|
| **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. | 7.2.1<br>7.2.2 |



### Testing all parts of the response cycle

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

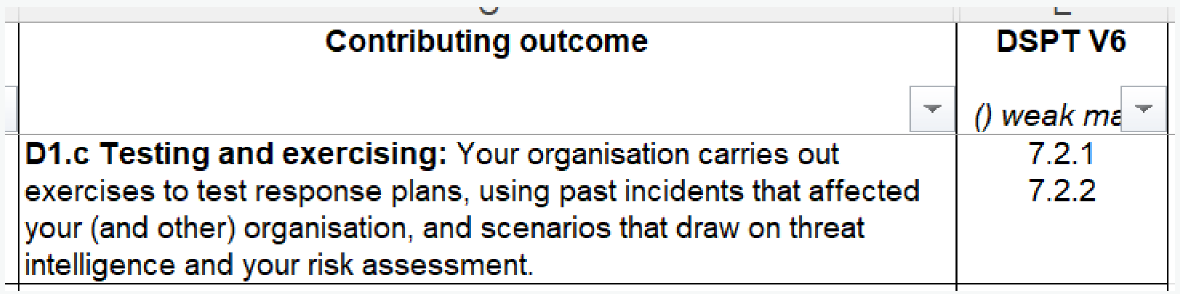
Under the previous DSPT framework, you were required to test your incident response plan to ensure that relevant team members understood their roles and responsibilities. Under the CAF-aligned DSPT framework, your testing should meet a higher bar, testing all parts of your incident response plan to ensure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

You will 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 is 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.

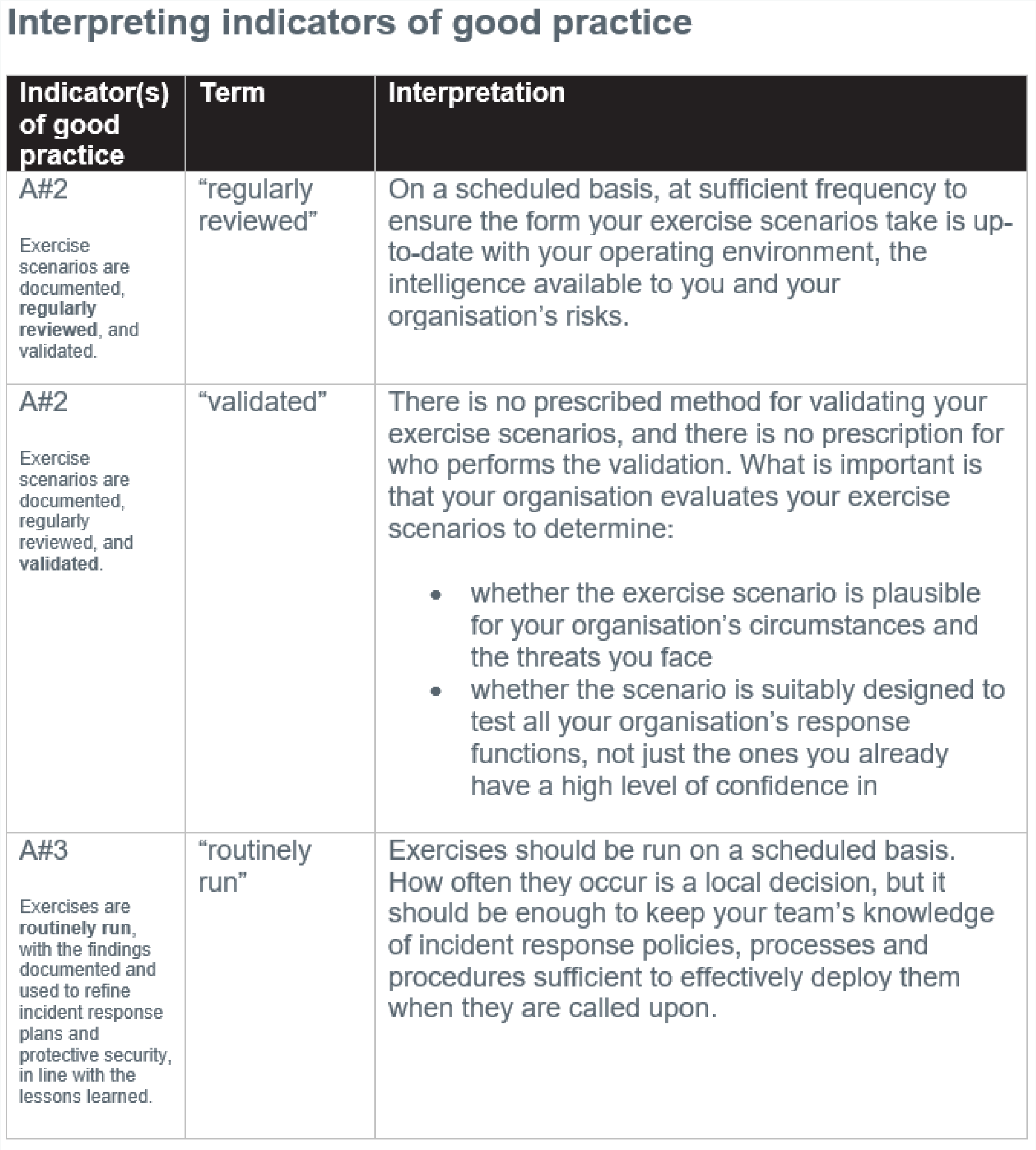
# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.c Testing and exercising

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **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. | 7.2.1<br>7.2.2 |



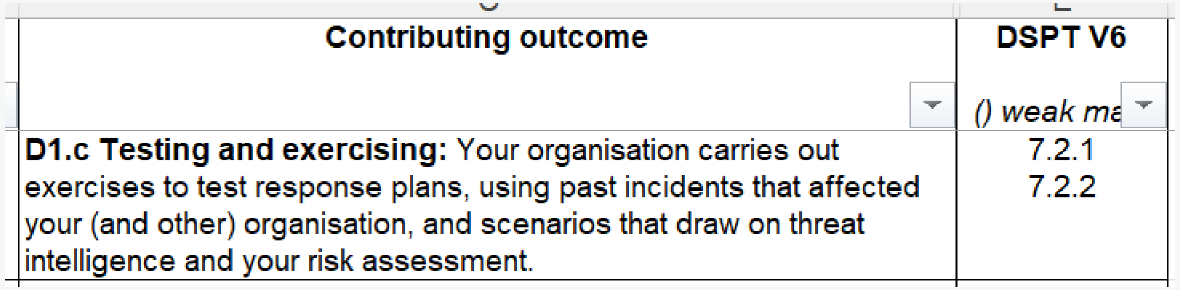
### Interpreting indicators of good practice

| Indicator(s) of good practice | Term | Interpretation |
|---|---|---|
| A#2<br>Exercise scenarios are documented, **regularly reviewed**, and validated. | "regularly reviewed" | 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. |
| A#2<br>Exercise scenarios are documented, regularly reviewed, and **validated**. | "validated" | There is no prescribed method for validating your exercise scenarios, and there is no prescription for who performs the validation. What is important is that your organisation evaluates your exercise scenarios to determine:<br>• whether the exercise scenario is plausible for your organisation's circumstances and the threats you face<br>• 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 |
| A#3<br>Exercises are **routinely run**, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned. | "routinely run" | Exercises should be run on a scheduled basis. How often they occur is a local decision, but it should be enough to keep your team's knowledge of incident response policies, processes and procedures sufficient to effectively deploy them when they are called upon. |

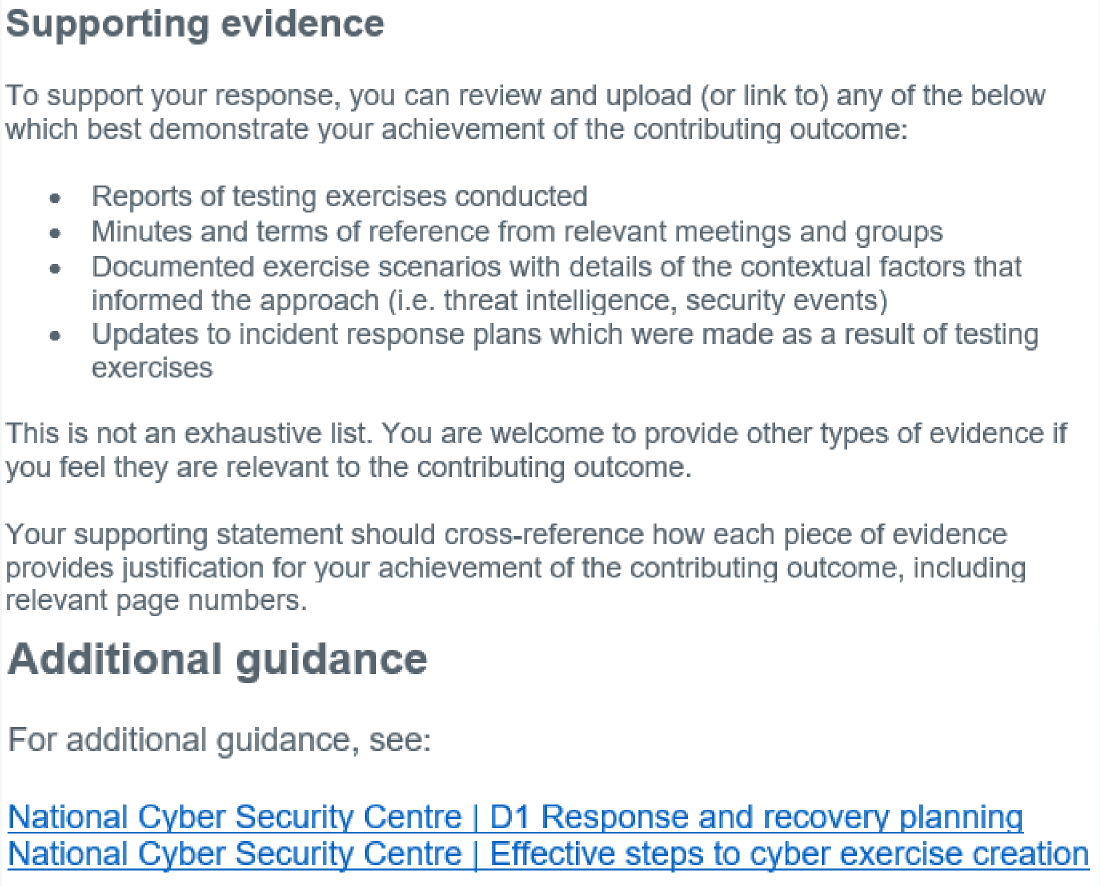
# Principle: D1 Response and recovery planning

## Contributing outcome:
## D1.c Testing and exercising

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6 |
|---|---|
| | () weak ma |
| **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. | 7.2.1<br>7.2.2 |



### Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- 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 (i.e. threat intelligence, security events)
- Updates to incident response plans which were made as a result of testing exercises

This is not an exhaustive list. You are 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.

### Additional guidance

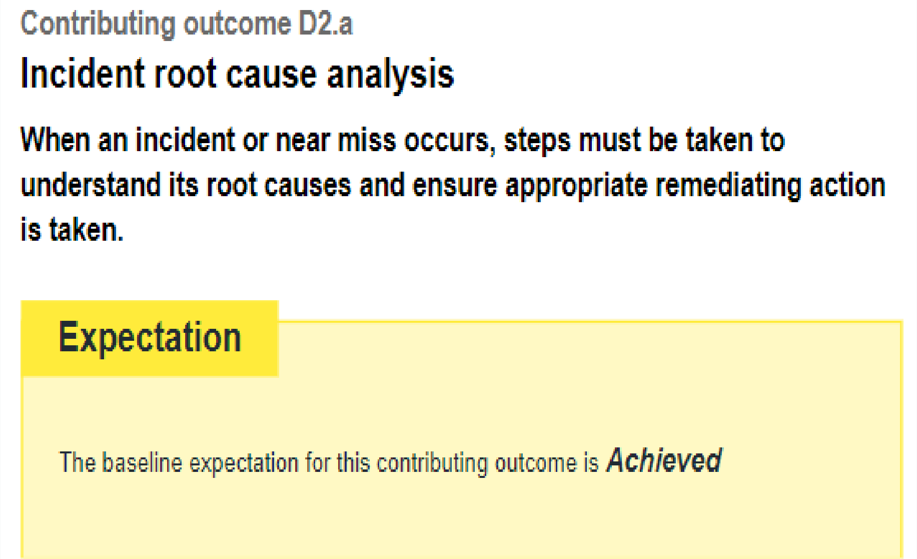
For additional guidance, see:

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

# Demonstration

# Principle: D2 Lessons Learned

# Contributing outcome:
# D2.a Incident root cause analysis



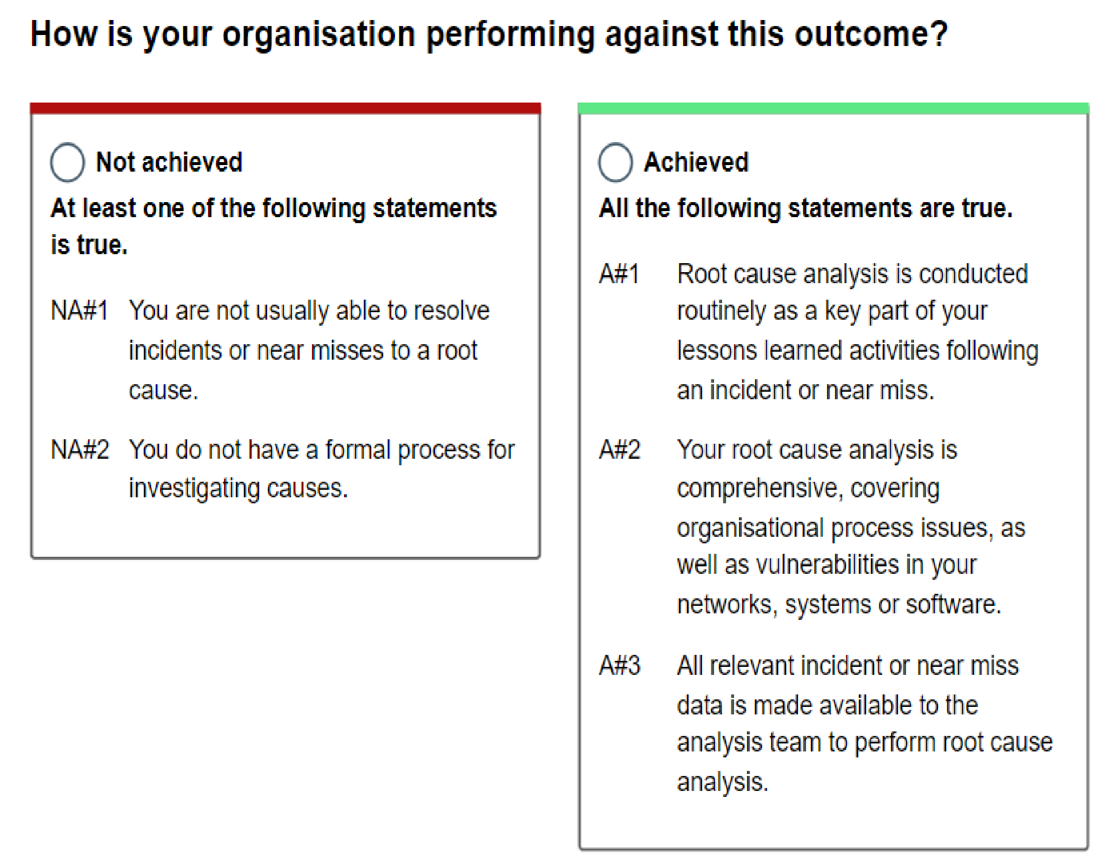
Contributing outcome D2.a

## Incident root cause analysis

**When an incident or near miss occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.**

### Expectation

The baseline expectation for this contributing outcome is ***Achieved***



**How is your organisation performing against this outcome?**

○ **Not achieved**

**At least one of the following statements is true.**

NA#1 You are not usually able to resolve incidents or near misses to a root cause.

NA#2 You do not have a formal process for investigating causes.

○ **Achieved**

**All the following statements are true.**

A#1 Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident or near miss.

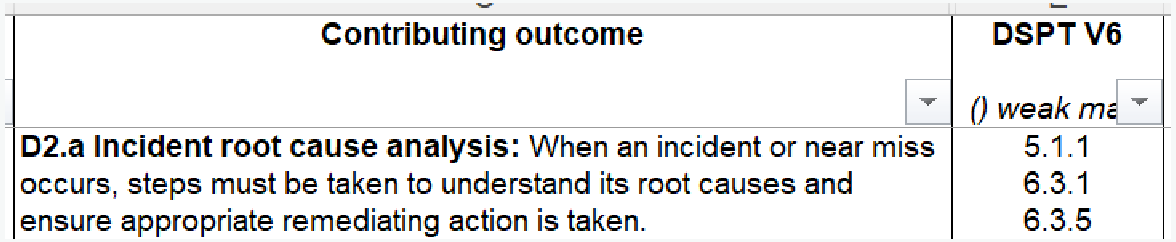
A#2 Your root cause analysis is comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software.

A#3 All relevant incident or near miss data is made available to the analysis team to perform root cause analysis.

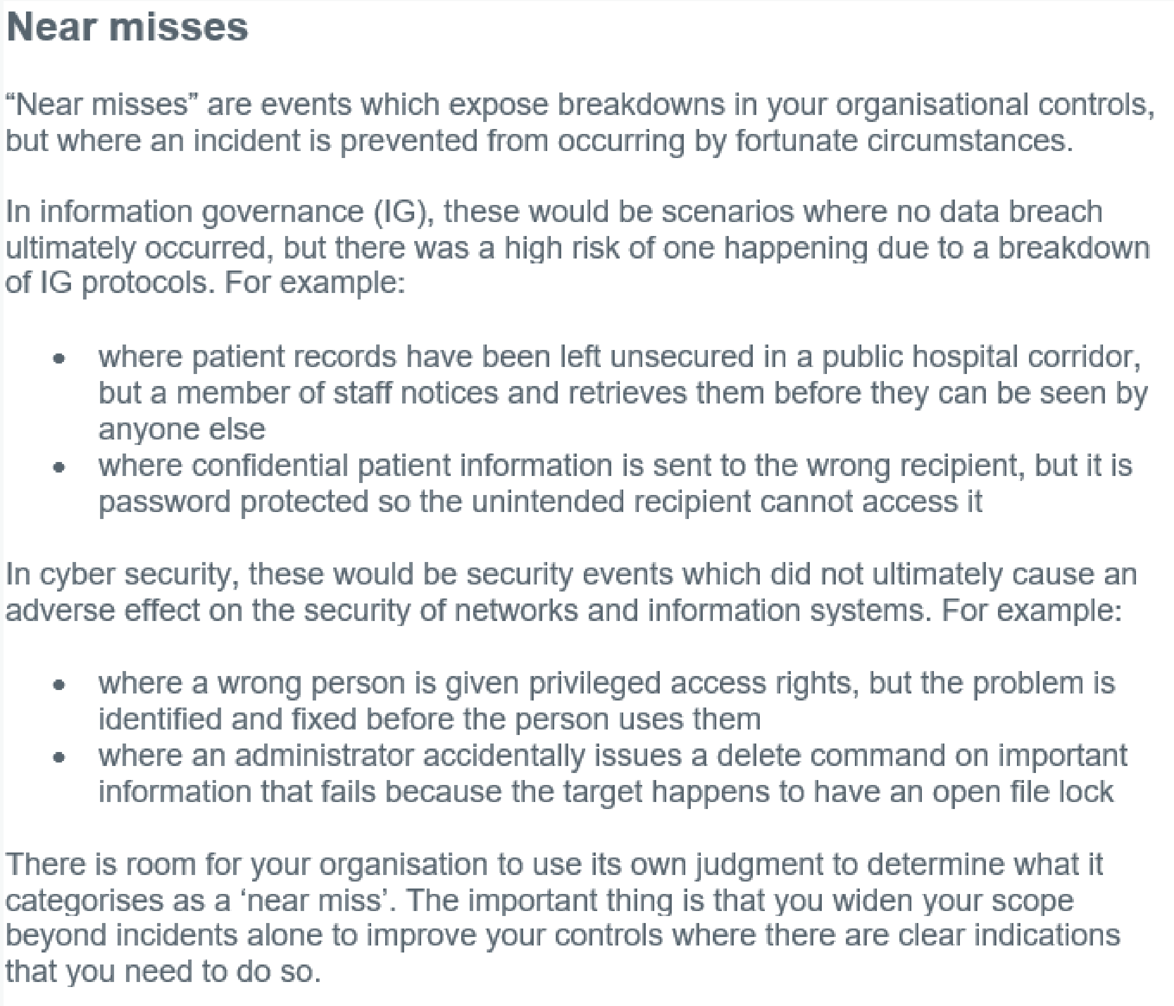
# Principle: D2 Lessons Learned

## Contributing outcome:
## D2.a Incident root cause analysis

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **D2.a Incident root cause analysis:** When an incident or near miss occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken. | 5.1.1<br>6.3.1<br>6.3.5 |



### Near misses

“Near misses” are events which expose breakdowns in your organisational controls, but where an incident is prevented from occurring by fortunate circumstances.

In information governance (IG), these would be scenarios where no data breach ultimately occurred, but there was a high risk of one happening due to a breakdown of IG protocols. For example:

- where patient records have been left unsecured in a public hospital corridor, but a member of staff notices and retrieves them before they can be seen by anyone else
- where confidential patient information is sent to the wrong recipient, but it is password protected so the unintended recipient cannot access it

In cyber security, these would be security events which did not ultimately cause an adverse effect on the security of networks and information systems. For example:

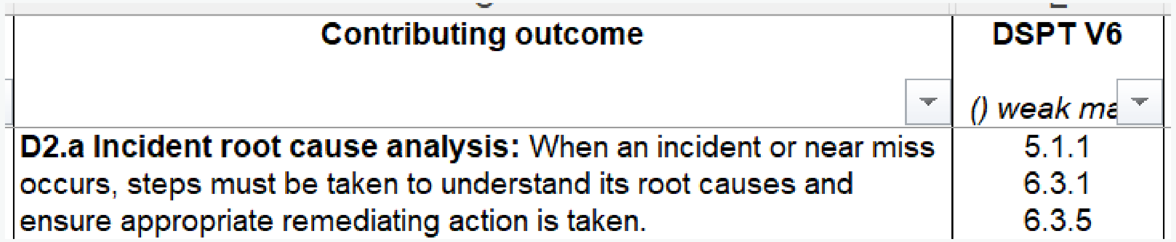
- where a wrong person is given privileged access rights, but the problem is identified and fixed before the person uses them
- where an administrator accidentally issues a delete command on important information that fails because the target happens to have an open file lock

There is room for your organisation to use its own judgment to determine what it categorises as a ‘near miss’. The important thing is that you widen your scope beyond incidents alone to improve your controls where there are clear indications that you need to do so.

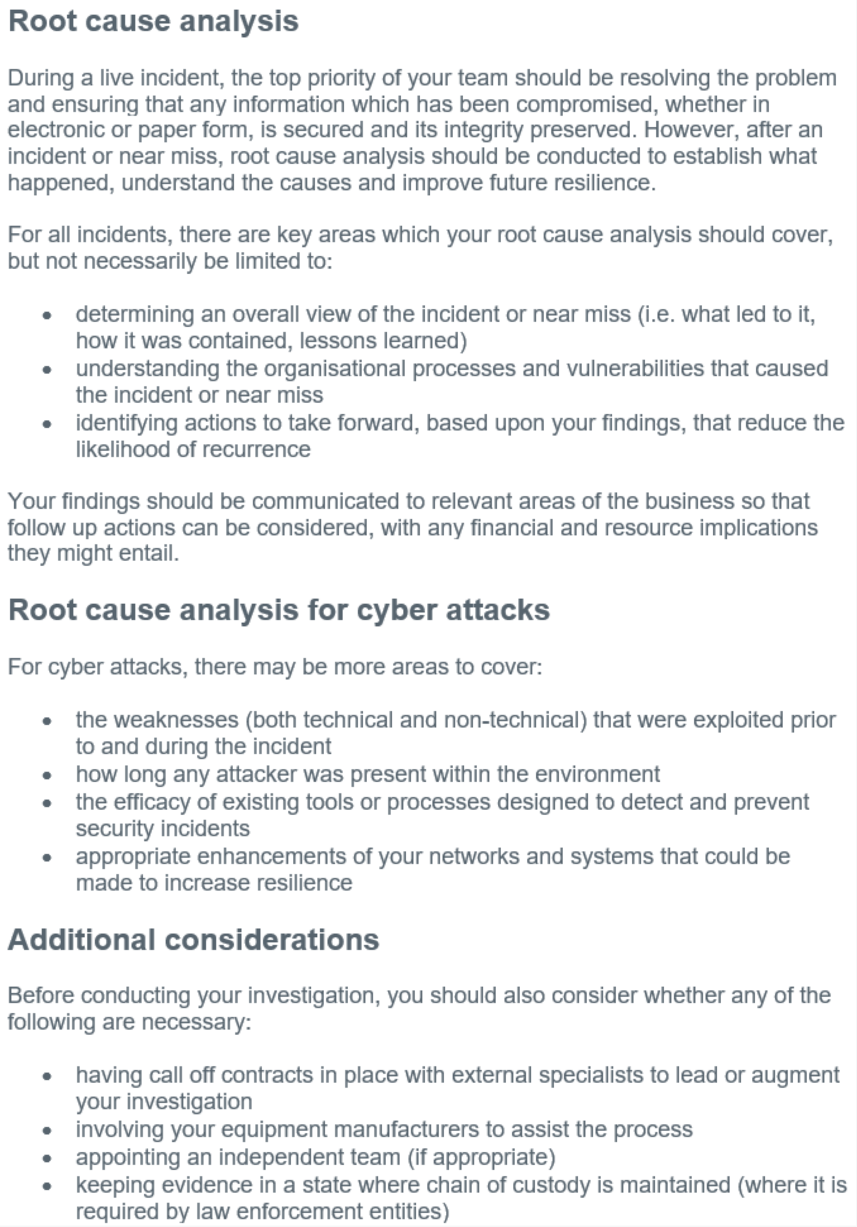
# Principle: D2 Lessons Learned

## Contributing outcome:
## D2.a Incident root cause analysis

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>*() weak ma* |
|---|---|
| **D2.a Incident root cause analysis:** When an incident or near miss occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken. | 5.1.1<br>6.3.1<br>6.3.5 |



### Root cause analysis

During a live incident, the top priority of your team should be resolving the problem and ensuring that any information which has been compromised, whether in electronic or paper form, is secured and its integrity preserved. However, after an incident or near miss, root cause analysis should be conducted to establish what happened, understand the causes and improve future resilience.

For all incidents, there are key areas which your root cause analysis should cover, but not necessarily be limited to:

- determining an overall view of the incident or near miss (i.e. what led to it, how it was contained, lessons learned)
- understanding the organisational processes and vulnerabilities that caused the incident or near miss
- identifying actions to take forward, based upon your findings, that reduce the likelihood of recurrence

Your findings should be communicated to relevant areas of the business so that follow up actions can be considered, with any financial and resource implications they might entail.

### Root cause analysis for cyber attacks

For cyber attacks, there may be more areas to cover:

- the weaknesses (both technical and non-technical) that were exploited prior to and during the incident
- how long any attacker was present within the environment
- the efficacy of existing tools or processes designed to detect and prevent security incidents
- appropriate enhancements of your networks and systems that could be made to increase resilience

### Additional considerations

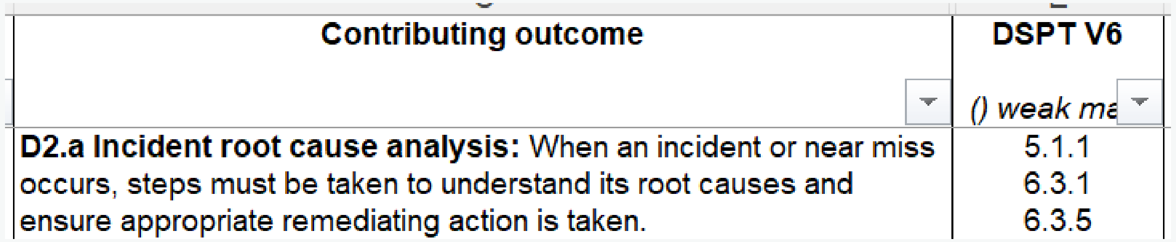
Before conducting your investigation, you should also consider whether any of the following are necessary:

- having call off contracts in place with external specialists to lead or augment your investigation
- involving your equipment manufacturers to assist the process
- appointing an independent team (if appropriate)
- keeping evidence in a state where chain of custody is maintained (where it is required by law enforcement entities)

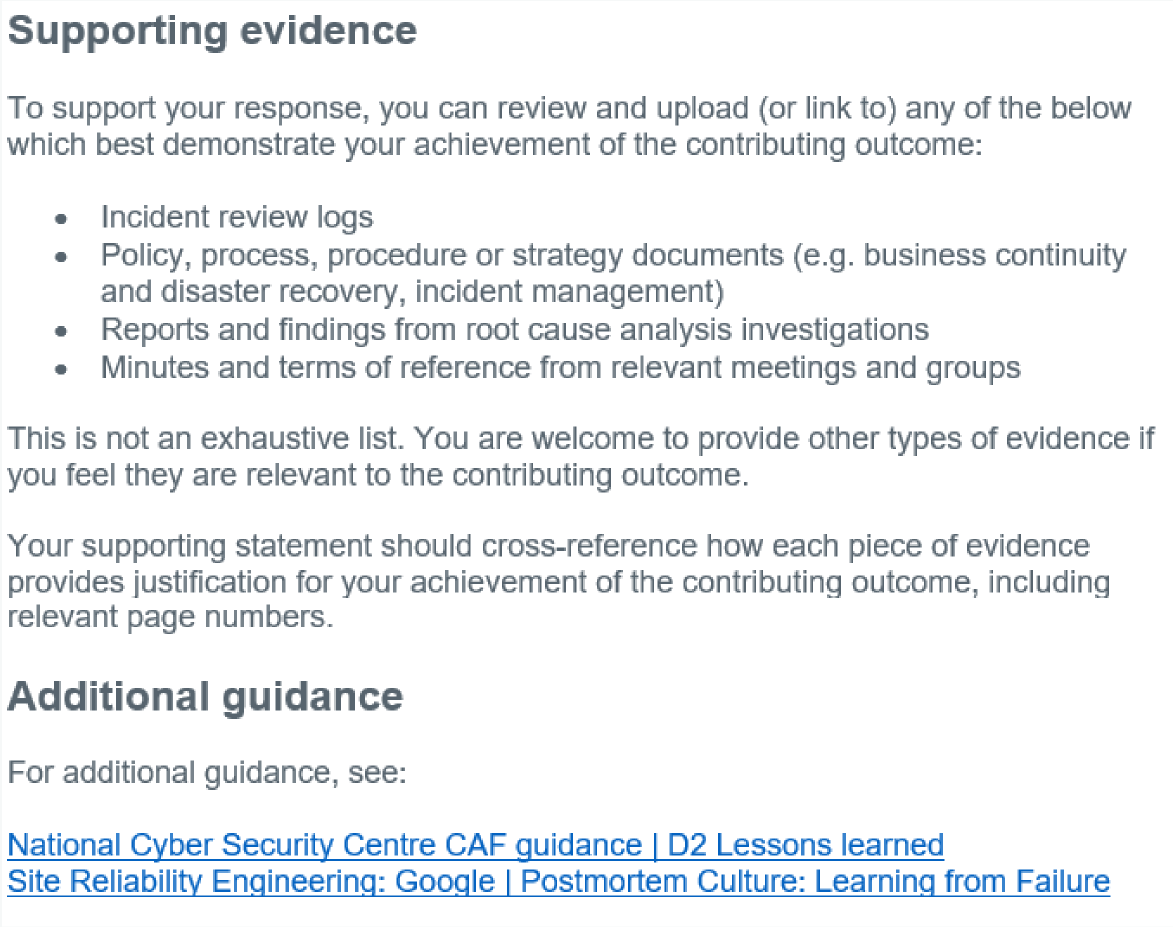
# Principle: D2 Lessons Learned

## Contributing outcome:
## D2.a Incident root cause analysis

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **D2.a Incident root cause analysis:** When an incident or near miss occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken. | 5.1.1<br>6.3.1<br>6.3.5 |



### Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Incident review logs
- Policy, process, procedure or strategy documents (e.g. business continuity and disaster recovery, incident management)
- Reports and findings from root cause analysis investigations
- Minutes and terms of reference from relevant meetings and groups

This is not an exhaustive list. You are 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.

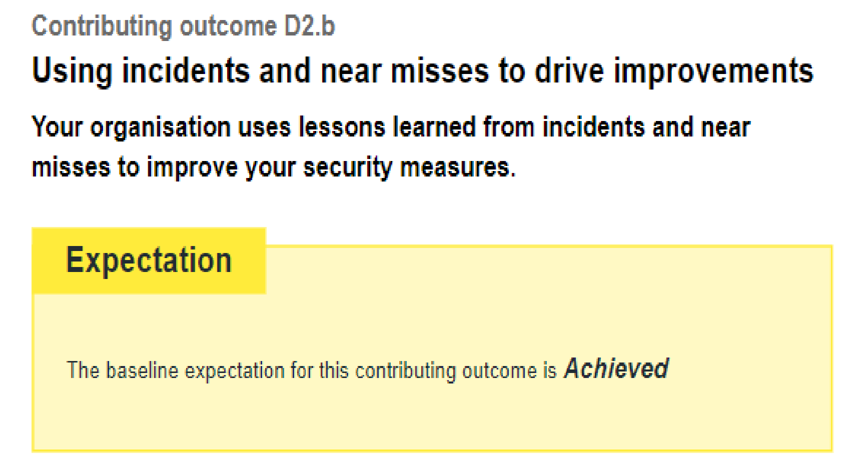
### Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | D2 Lessons learned
Site Reliability Engineering: Google | Postmortem Culture: Learning from Failure

# Principle: D2 Lessons Learned

# Contributing outcome: D2.b Using incidents and near misses to drive improvements



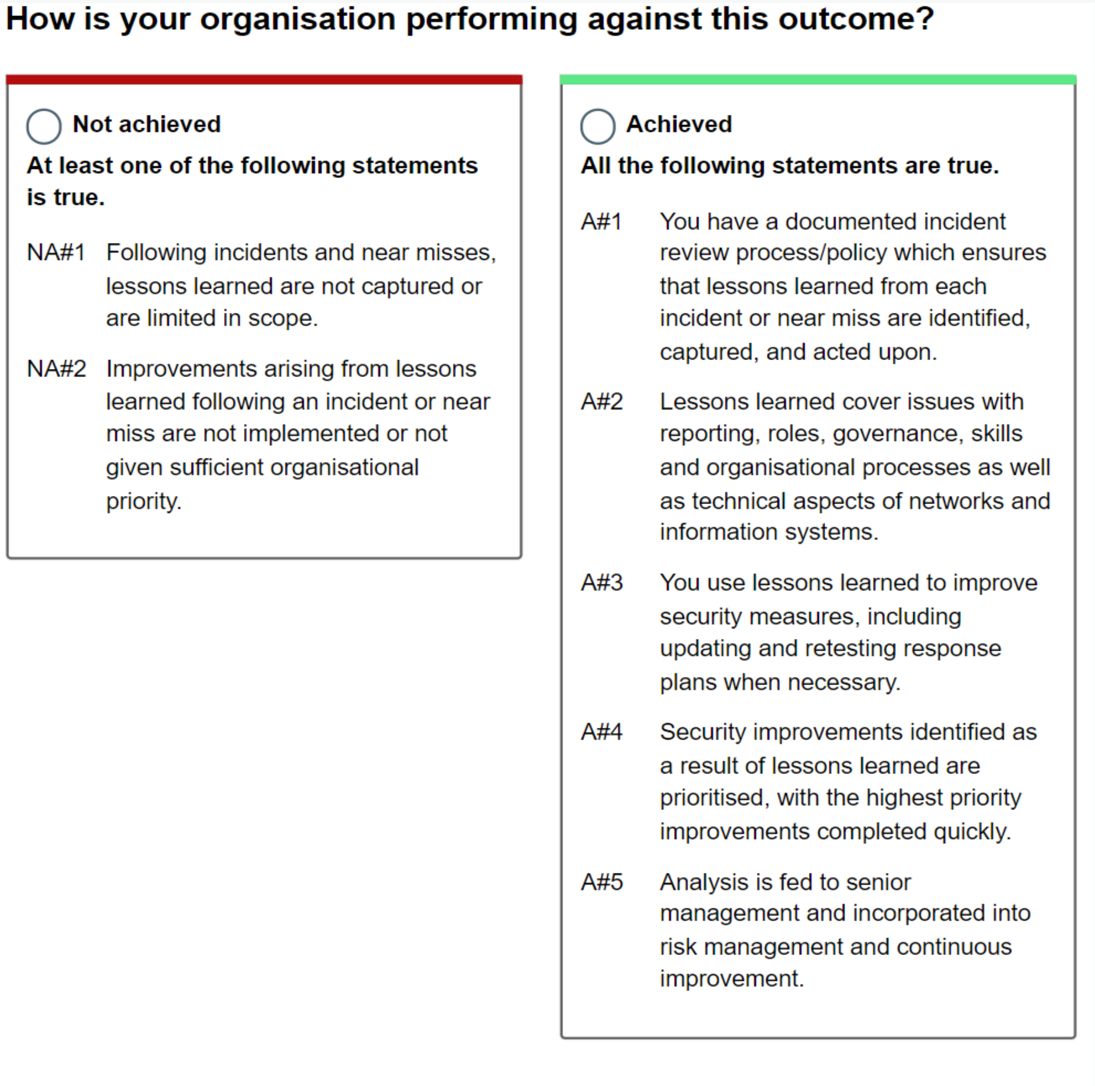
Contributing outcome D2.b

## Using incidents and near misses to drive improvements

**Your organisation uses lessons learned from incidents and near misses to improve your security measures.**

**Expectation**

The baseline expectation for this contributing outcome is ***Achieved***



**How is your organisation performing against this outcome?**

○ **Not achieved**

**At least one of the following statements is true.**

NA#1 Following incidents and near misses, lessons learned are not captured or are limited in scope.

NA#2 Improvements arising from lessons learned following an incident or near miss are not implemented or not given sufficient organisational priority.

○ **Achieved**

**All the following statements are true.**

A#1 You have a documented incident review process/policy which ensures that lessons learned from each incident or near miss are identified, captured, and acted upon.

A#2 Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems.

A#3 You use lessons learned to improve security measures, including updating and retesting response plans when necessary.

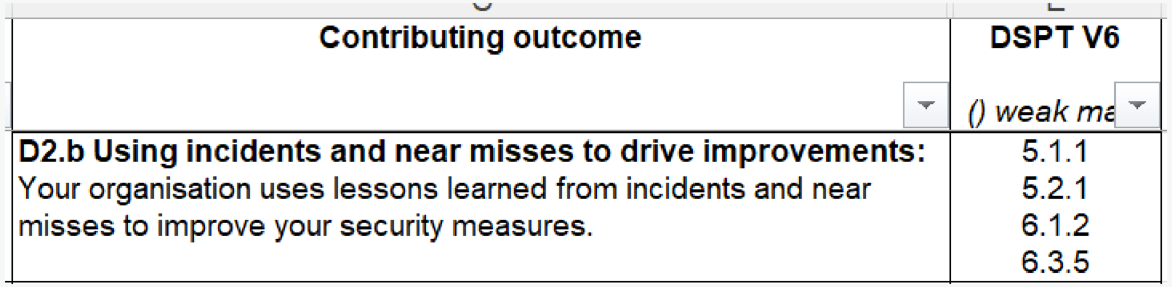
A#4 Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.

A#5 Analysis is fed to senior management and incorporated into risk management and continuous improvement.

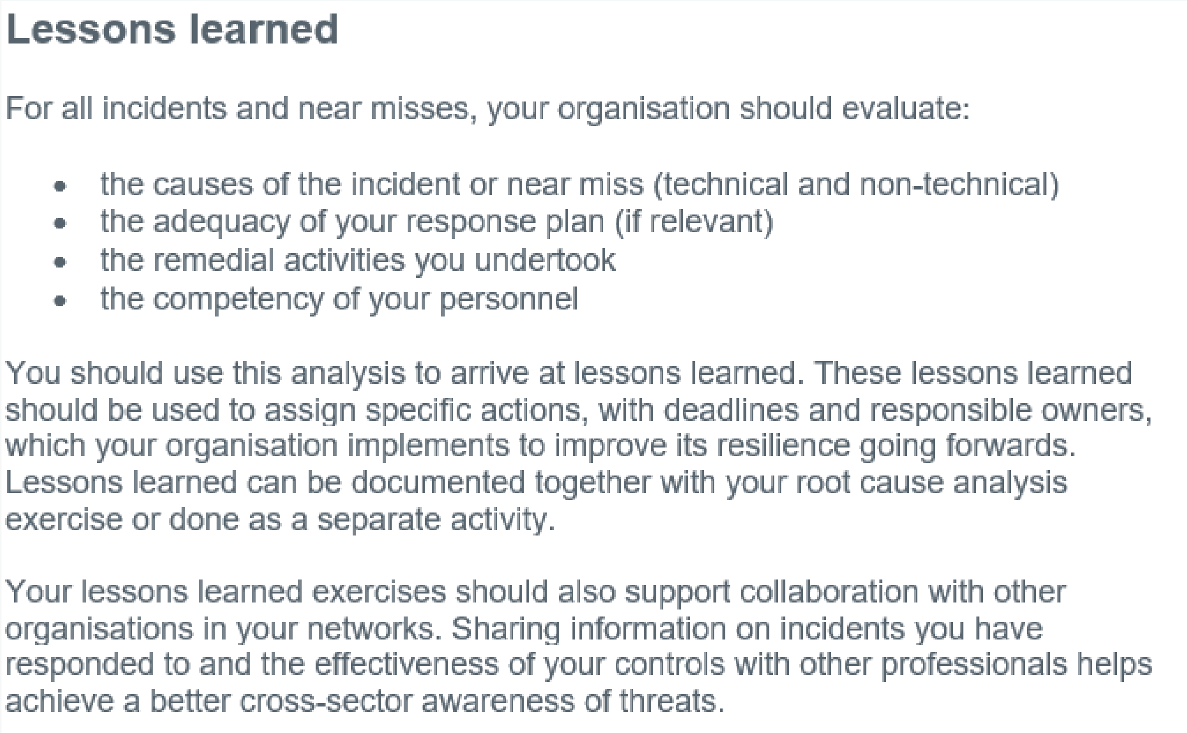
# Principle: D2 Lessons Learned

## Contributing outcome:
## D2.b Using incidents and near misses to drive improvements

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>*() weak ma* |
|---|---|
| **D2.b Using incidents and near misses to drive improvements:** Your organisation uses lessons learned from incidents and near misses to improve your security measures. | 5.1.1<br>5.2.1<br>6.1.2<br>6.3.5 |



### Lessons learned

For all incidents and near misses, your organisation should evaluate:

- the causes of the incident or near miss (technical and non-technical)
- the adequacy of your response plan (if relevant)
- the remedial activities you undertook
- the competency of your personnel

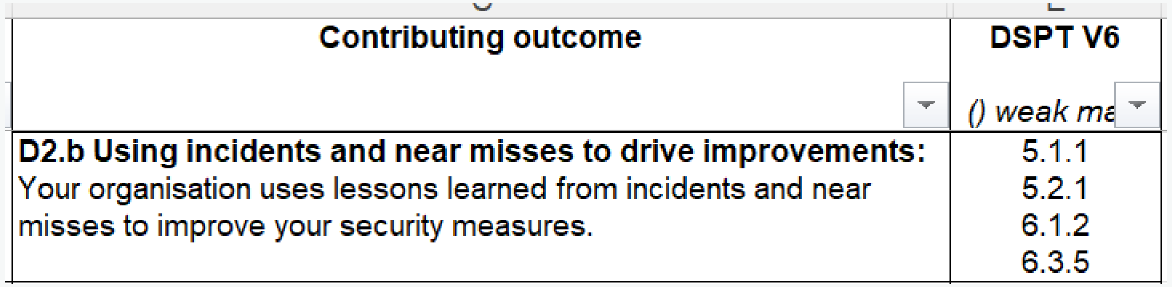
You should use this analysis to arrive at lessons learned. These lessons learned should be used to assign specific actions, with deadlines and responsible owners, which your organisation implements to improve its resilience going forwards. Lessons learned can be documented together with your root cause analysis exercise or done as a separate activity.

Your lessons learned exercises should also support collaboration with other organisations in your networks. Sharing information on incidents you have responded to and the effectiveness of your controls with other professionals helps achieve a better cross-sector awareness of threats.

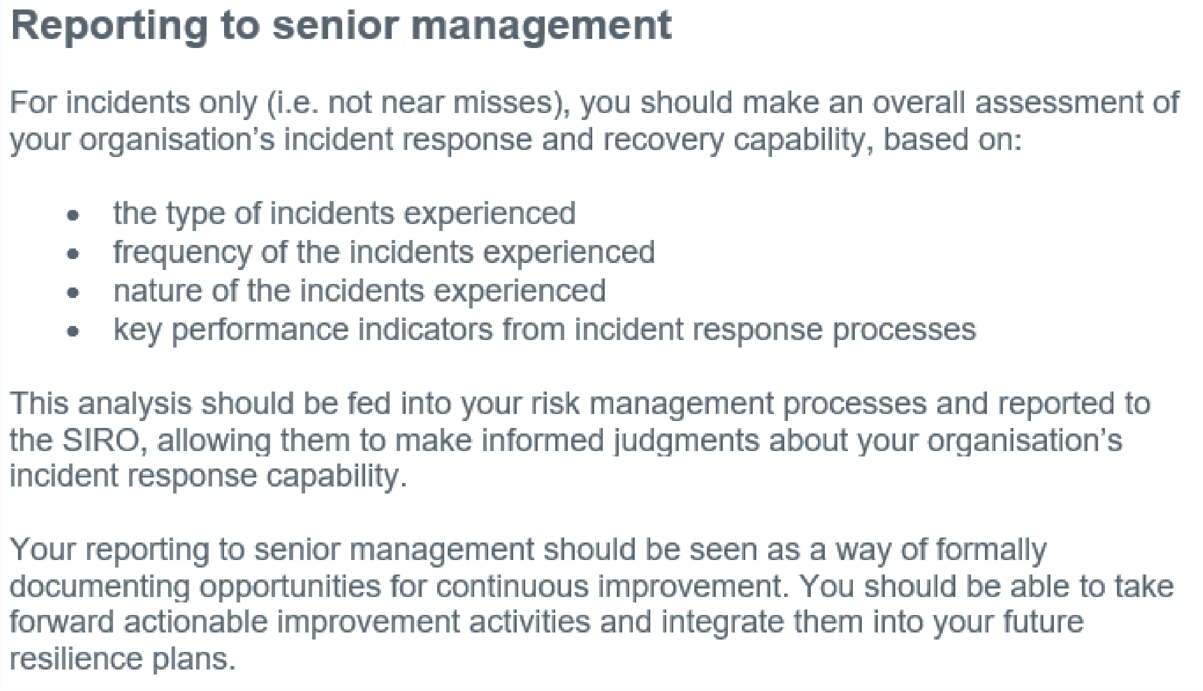
# Principle: D2 Lessons Learned

## Contributing outcome:
## D2.b Using incidents and near misses to drive improvements

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **D2.b Using incidents and near misses to drive improvements:** Your organisation uses lessons learned from incidents and near misses to improve your security measures. | 5.1.1<br>5.2.1<br>6.1.2<br>6.3.5 |



### Reporting to senior management

For incidents only (i.e. not near misses), you should make an overall assessment of your organisation's incident response and recovery capability, based on:

- the type of incidents experienced
- frequency of the incidents experienced
- nature of the incidents experienced
- key performance indicators from incident response processes

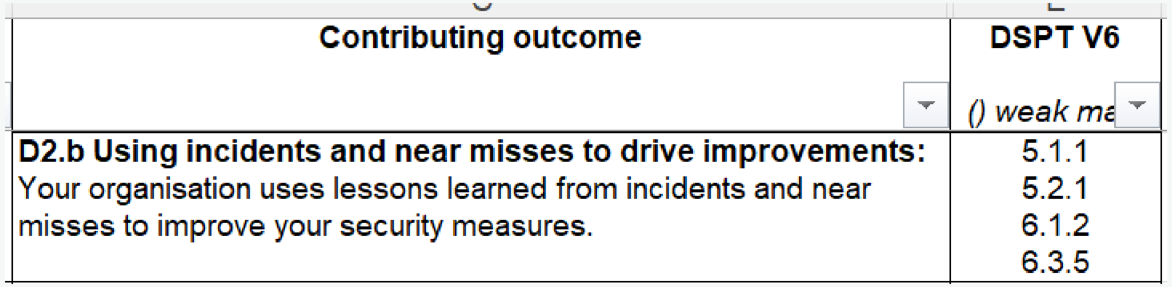
This analysis should be fed into your risk management processes and reported to the SIRO, allowing them to make informed judgments about your organisation's incident response capability.

Your reporting to senior management should be seen as a way of formally documenting opportunities for continuous improvement. You should be able to take forward actionable improvement activities and integrate them into your future resilience plans.

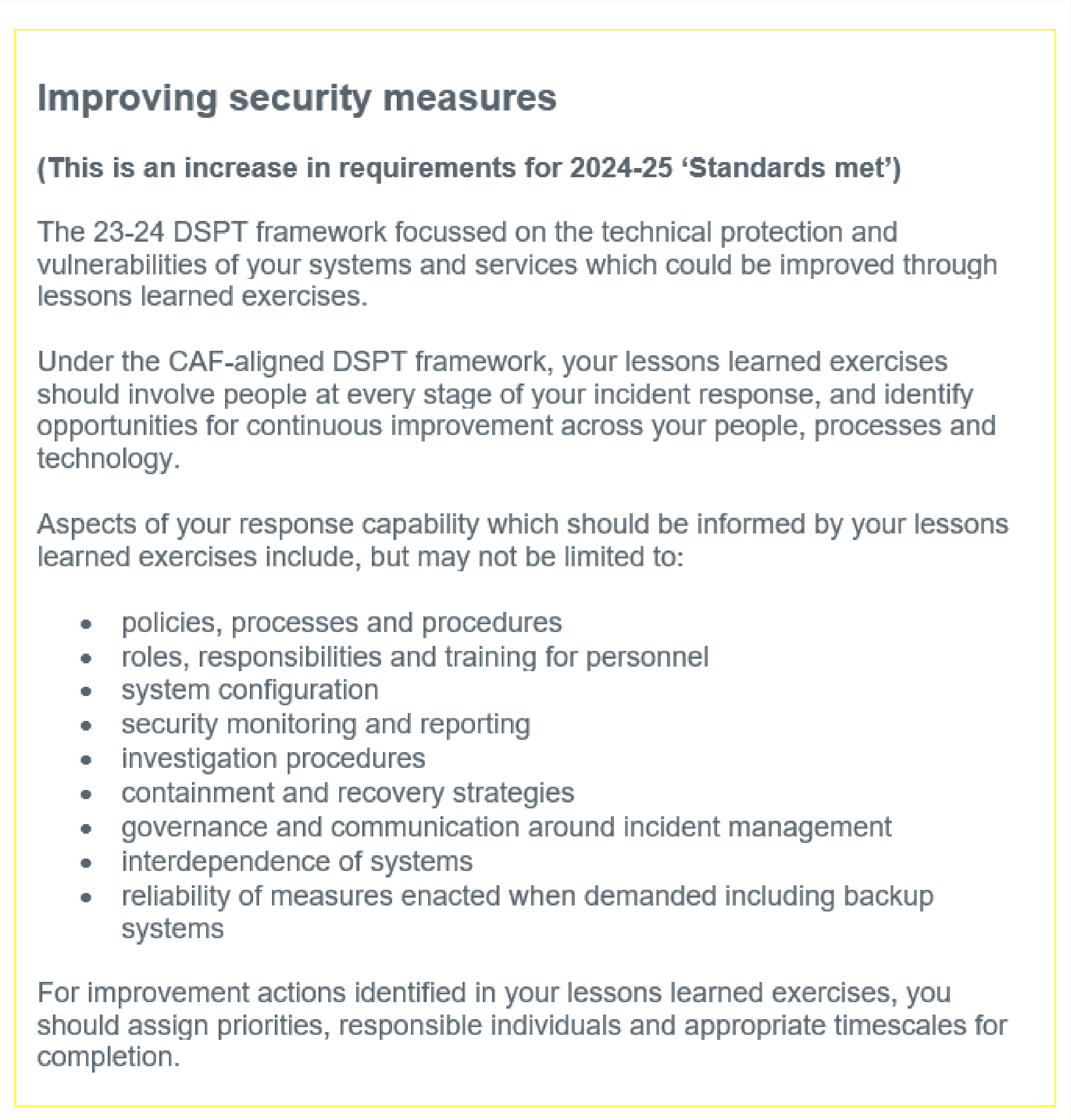
# Principle: D2 Lessons Learned

## Contributing outcome:
## D2.b Using incidents and near misses to drive improvements

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **D2.b Using incidents and near misses to drive improvements:** Your organisation uses lessons learned from incidents and near misses to improve your security measures. | 5.1.1<br>5.2.1<br>6.1.2<br>6.3.5 |



### Improving security measures

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

The 23-24 DSPT framework focussed on the technical protection and vulnerabilities of your systems and services which could be improved through lessons learned exercises.

Under the CAF-aligned DSPT framework, your lessons learned exercises should involve people at every stage of your incident response, and identify opportunities for continuous improvement across your people, processes and technology.

Aspects of your response capability which should be informed by your lessons learned exercises include, but may not be limited to:

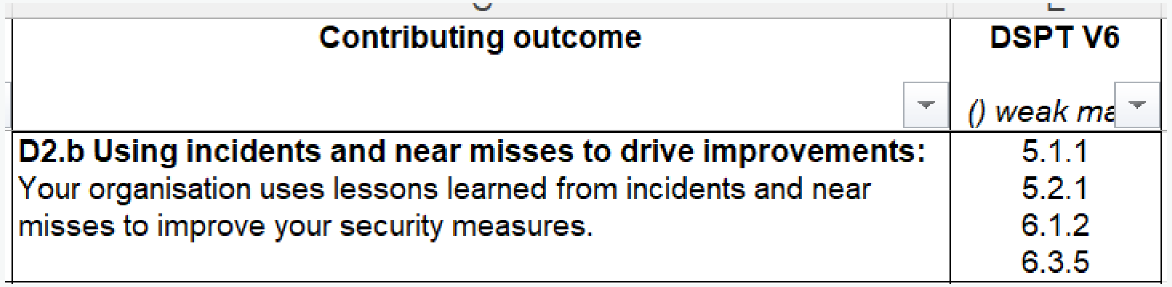
- policies, processes and procedures
- roles, responsibilities and training for personnel
- system configuration
- security monitoring and reporting
- investigation procedures
- containment and recovery strategies
- governance and communication around incident management
- interdependence of systems
- reliability of measures enacted when demanded including backup systems

For improvement actions identified in your lessons learned exercises, you should assign priorities, responsible individuals and appropriate timescales for completion.

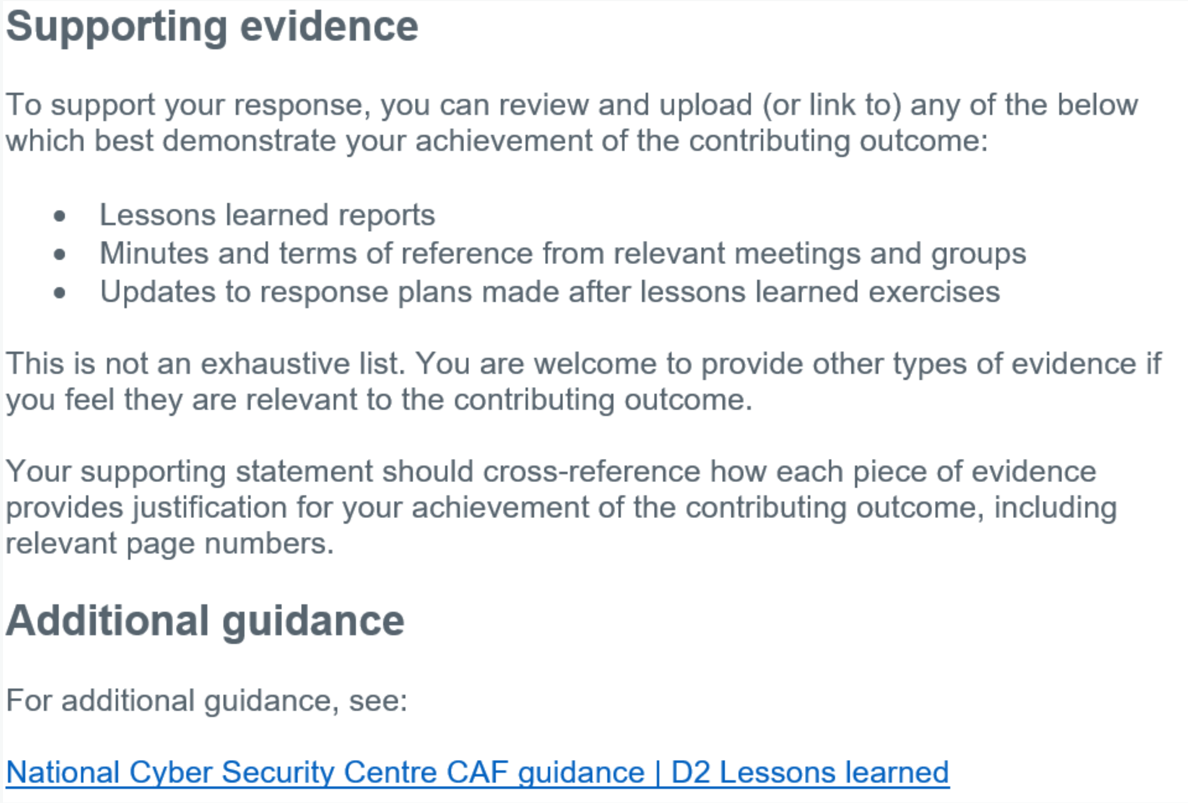
# Principle: D2 Lessons Learned

## Contributing outcome:
## D2.b Using incidents and near misses to drive improvements

## Mapping, Guidance and Evidence to upload



| Contributing outcome | DSPT V6<br>() weak ma |
|---|---|
| **D2.b Using incidents and near misses to drive improvements:** Your organisation uses lessons learned from incidents and near misses to improve your security measures. | 5.1.1<br>5.2.1<br>6.1.2<br>6.3.5 |



## Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Lessons learned reports
- Minutes and terms of reference from relevant meetings and groups
- Updates to response plans made after lessons learned exercises

This is not an exhaustive list. You are 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.

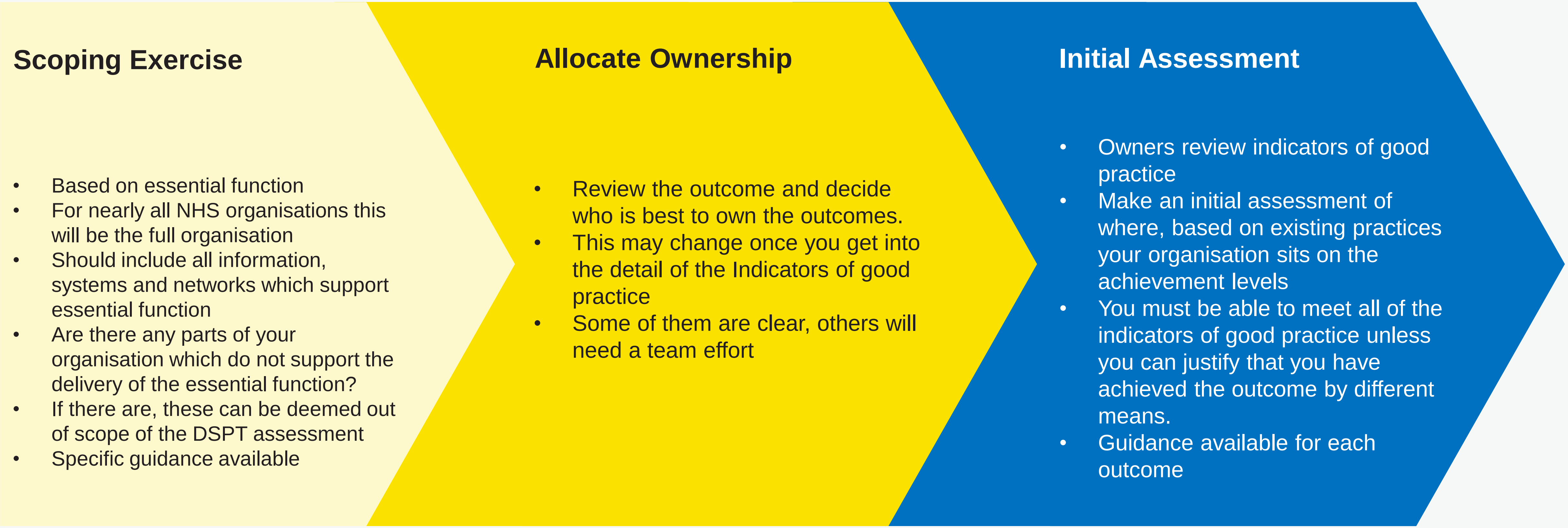
## Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | D2 Lessons learned

# Planning for DSPT in 24-25

# Completing the DSPT 24-25 – Initial Review



## Scoping Exercise

- Based on essential function
- For nearly all NHS organisations this will be the full organisation
- Should include all information, systems and networks which support essential function
- Are there any parts of your organisation which do not support the delivery of the essential function?
- If there are, these can be deemed out of scope of the DSPT assessment
- Specific guidance available

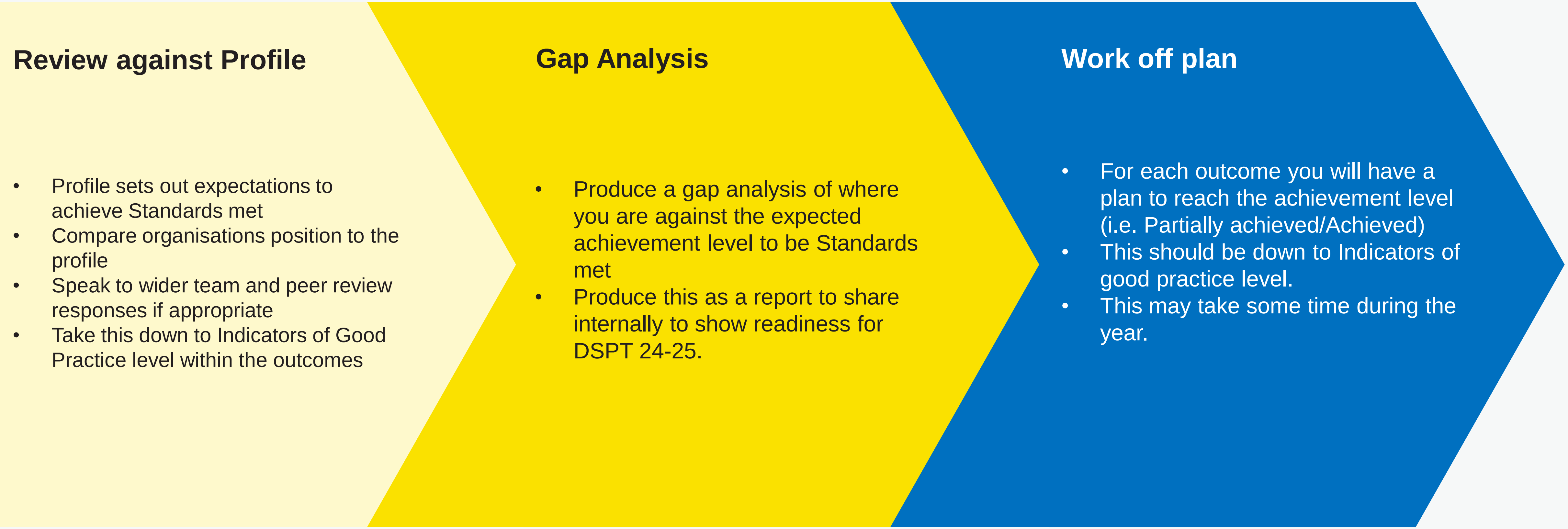
## Allocate Ownership

- Review the outcome and decide who is best to own the outcomes.
- This may change once you get into the detail of the Indicators of good practice
- Some of them are clear, others will need a team effort

## Initial Assessment

- Owners review indicators of good practice
- Make an initial assessment of where, based on existing practices your organisation sits on the achievement levels
- You must be able to meet all of the indicators of good practice unless you can justify that you have achieved the outcome by different means.
- Guidance available for each outcome

# Completing the DSPT 24-25 – Planning to deliver



### Review against Profile

- Profile sets out expectations to achieve Standards met
- Compare organisations position to the profile
- Speak to wider team and peer review responses if appropriate
- Take this down to Indicators of Good Practice level within the outcomes

### Gap Analysis

- Produce a gap analysis of where you are against the expected achievement level to be Standards met
- Produce this as a report to share internally to show readiness for DSPT 24-25.

### Work off plan

- For each outcome you will have a plan to reach the achievement level (i.e. Partially achieved/Achieved)
- This should be down to Indicators of good practice level.
- This may take some time during the year.

# Question and answer session

# Webinars

| Date and time | Topics to be covered |
|---|---|
| Wednesday 14th August 14:00 – 15:30 | Objective C – Detecting cyber security events |

Please use the link below to register for the webinar series:
CAF-aligned DSPT 2024-25 webinar series | NHS England Events
You can ask any questions in advance of the webinar using this form.
If you are interested

NHS
England

# Thank You

@nhsengland

company/nhsengland

england.nhs.uk