Part of Objective D - Minimising the impact of incidents

Principle: D2 Lessons learned

← Previous Chapter

Principle: D1 Response and recovery planning

Current Chapter

Current chapter – Principle: D2 Lessons learned

View all

Page contents

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.”

Overview

This contributing outcome relates to your organisation conducting thorough root cause analysis in the aftermath of incidents and near misses.

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).

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

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).

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 human error or failure to follow 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's 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.

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. These include, but are not necessarily be limited to:

- determining an overall view of the incident or near miss (what led to it, how it was contained and lessons learned for example)
- 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 such as:

- 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 it's necessary to:

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

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 review logs
- policy, process, procedure or strategy documents (such as business continuity and disaster recovery, or 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'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.

Additional guidance

For additional guidance, see:

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

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.

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.”

Overview

To meet this contributing outcome, you need to demonstrate that your organisation conducts lessons learned exercises after incidents and near misses to reduce the likelihood of recurrence and improve your future response capability.

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).

'Near misses' are events which expose breakdowns in your organisational controls, but where an incident is prevented from occurring by fortunate circumstances (see 'D2.a Incident root cause analysis' 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).

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.

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.

Reporting to senior management

For incidents only (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 senior information risk owner (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.

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:

- lessons learned reports
- training needs analysis
- 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'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.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | D2 Lessons learned

Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks.

New frameworks will be added to this document over the course of the year.

Last edited: 29 August 2024 9:33 am

← **Previous Chapter**

Principle: D1 Response and recovery planning

Chapters