Part of Objective A - Managing risk

Principle: A2 Risk management

← Previous Chapter

Principle: A1 Governance

Current Chapter

Current chapter – Principle: A2 Risk management

View all

Next Chapter →

Principle: A3 Asset management

Page contents

A2.a Risk management process

A2.b Assurance

A2.a Risk management process

"Your organisation has effective internal processes for managing risks to the security and governance of information, systems and networks related to the

operation of your essential function(s), and communicating associated activities. This includes a process for data protection impact assessments (DPIAs)."

Overview

This contributing outcome is about ensuring your organisation has effective processes for managing risk.

Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities which 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).

Risk assessments

You should conduct risk assessments on a scheduled basis, and whenever significant changes occur to your organisational systems or processes.

The DSPT does not mandate a specific approach to risk assessment, however, it's important to consider:

- your organisation's business priorities and objectives
- who or what those things should be protected from
- any legal and regulatory obligations that apply to your organisation
- the cyber security risk red lines your organisation will and won't cross to complete the things it needs to do

For more information on understanding and managing risk from a cyber security perspective, see NCSC guidance on A basic risk assessment and management method. For information on managing privacy risk, see Information Commissioner's Office (ICO) guidance on risks and data protection impact assessments.

Linking risk assessment to controls

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

Under the new framework, you should link your cyber security and information governance (IG) controls to your risk assessments. Ways of clearly demonstrating links between controls and risks may include:

- listing controls against each risk in your risk register
- creating a controls catalogue which cross-references each control against individual risks

This should give you confidence that your controls are sufficient and proportionate, and that time and resources are not being wasted on solutions that do not effectively contribute towards the management of cyber security and IG risk.

Data protection by design and by default

The requirements of data protection by design and by default should be clearly incorporated into your overall approach to cyber security and wider IG risk. Examples of where considerations should be made include:

- developing new IT systems, services and processes that involve processing personal data
- developing organisational policies, processes and strategies that have privacy implications
- embarking on data sharing initiatives
- using personal data for new purposes
- changes to the scope or purpose of current processing activities

See ICO guidance on data protection by design and by default for more information.

Data protection impact assessments

Conducting data protection impact assessments (DPIAs) is an important pillar of data protection by design and by default.

You should demonstrate that your organisation conducts DPIAs before beginning any type of processing which is 'likely to result in a high risk to the rights and freedoms' of individuals. For a detailed list of situations where this applies, see guidance from the ICO.

See NHS England's universal IG templates page for a template DPIA document which you can use, or reference your own processes against, to ensure all appropriate bases are covered.

Threat analysis

For cyber risk assessments, you should incorporate knowledge of threats including:

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

Exceeding the 'standards met' expectation for 2024-25

Threat analysis

To meet the higher bar of performing detailed threat analysis, the analysis underpinning your risk assessments should be:

- detailed and comprehensive
- specific to your organisation
- underpinned by a robust knowledge base of attacker tactics and techniques

Adverse impacts

To meet the highest achievement benchmark, your risk assessments should consider potential adverse impacts beyond immediate ones on people, processes and technology. Adverse impacts include your organisation's long-term objectives, its image and reputation.

Your risk assessments should evidence that you have taken measures to control these adverse impacts, informed by your knowledge of specific techniques which an attacker might use.

You should also consider adverse impacts on other health and care services, and conversely, how their risks could impact you where you have dependencies. Again, you should be able to provide evidence showing the measures you have taken with attacker actions in mind.

The highest assurance benchmark is a broad system-driven approach to risk assessment which shows detailed consideration of how adverse impacts might arise, a system-wide scope for consequences, and pre-emptive implementation of specific measures to mitigate them.

Updating threat assumptions

To meet the higher bar for achievement, you need to have a documented threat assessment where your assumptions cover a wide range of attackers and capabilities.

Your threat assumptions need to be continuously updated in response to changes in the threat landscape. These could include geo-political campaigns, significant data protection and security incidents in health and care, and the discovery of new vulnerabilities.

Your threat assumptions should also be informed by information sharing resources and initiatives. These might include threat intelligence and services provided by NCSC, forums and engagement with professionals in your industry.

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:

- risk registers
- policy, process, procedure or strategy documents (such as risk management)
- risk assessments reports

- risk mitigation plans
- risk acceptance records
- risk review records
- data protection impact assessments
- documents showing follow-up actions taken

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 where appropriate.

Interpreting indicators of good practice

Indicator of good practice	PA#1 Your organisational process ensures that security and wider IG risks to information, systems and networks relevant to essential function(s) are identified, analysed, prioritised, and managed. This includes incorporating data protection by design and default into your process.
Term	'essential function(s)'
Interpretation	Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions. For more information, see guidance on scoping essential functions.

Indicator of good practice	PA#7 Your risk process clearly demonstrates how your organisation's processing complies with data protection principles and relevant legislation, including the right to a private life.
Term	'data protection principles and relevant legislation'
Interpretation	Principles and legislation which should be considered include: data protection principles relevant laws Caldicott Guardian principles

other legislation, including the common law duty of confidentiality and right to a private life where appropriate

Indicator of good practice	A#2 Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your information, systems and networks.
Term	'adverse impact'
Interpretation	This term refers to the wider downstream effects which incidents might have beyond immediate ones on people, processes and technology. For example, your organisation's long-term objectives, its image and reputation.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | A2 Risk management
National Cyber Security Centre | Risk management
National Cyber Security Centre | Risk management - Introducing system and component driven risk management approaches
Information Commissioner's Office | Risk and data protection impact assessments (DPIAs)
Information Commissioner's Office | Data protection by design and by default

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.

A2.b Assurance

"You have gained confidence in the effectiveness of the security and governance of your technology, people, and processes relevant to your essential function(s)."

Overview

To meet this contributing outcome, your organisation needs to show that it assures its cyber security and information governance (IG) controls to test their effectiveness.

Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities which 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).

Assurance

Assurance is about gaining confidence that your cyber security and IG controls are working effectively. To achieve this, you should employ an array of techniques to proactively test your people, processes and technology. Any weak points identified through your assurance activities should be documented and followed up on.

You should undertake your assurance activities on a scheduled basis to ensure that the measures you have in place have not been compromised by changing circumstances or new threats.

See NCSC's guidance on how to gain and maintain assurance for more information.

Understanding and reviewing assurance methods

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

Under the CAF-aligned DSPT framework, you should understand the assurance methods that are available and review the ones you use to ensure they remain effective. This might mean, for example, optimising your vulnerability testing process or focussing your spot checks on specific areas or processes identified as weak points.

As part of your review you may consider whether you're making most effective use of assurance activities such as:

- penetration testing
- behavioural testing (such as simulated phishing exercises)
- spot checks of processes (such as joiner, mover and leaver procedures, checking new assets are being appropriately registered and responses to subject access requests)
- spot checks of the premises (such as physical security of the building, locked cabinets, staff and visitor ID badges, paper waste, computer equipment)

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:

- minutes and terms of reference from relevant meetings or groups
- independent penetration testing and vulnerability assessment reports
- documents showing follow-up actions taken
- DSPT audit reports
- organisation security certifications - CE, CE+, ISO27001
- incident response records

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 where appropriate.

Interpreting indicators of good practice

Indicator of good practice	A#2 You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential function(s).
Term	'essential function(s)'
Interpretation	Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions. For more information, see guidance on scoping essential functions.

Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | A2 Risk management
National Cyber Security Centre | Risk management - How to gain and maintain assurance
National Cyber Security Centre | Penetration testing

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: 11 September 2024 2:02 pm

← **Previous Chapter**

Principle: A1 Governance

Next Chapter →

Principle: A3 Asset management

Chapters

1. Objective A - Managing risk
2. Principle: A1 Governance
3. **Principle: A2 Risk management**
4. Principle: A3 Asset management
5. Principle: A4 Supply chain