

Cyber Assessment Framework–aligned Data Security and Protection Toolkit

# Strengthening Assurance – Independent Assessment: Summary of Guides

Creating a culture  
of Improvement

Information and Technology  
for better health and care

30/09/2024



## Document control

Version number	Revision date	Summary of changes	Approved by
0.1	12/09/2024	First Draft	DRAFT
0.2	16/09/2024	Revised following initial feedback	DRAFT
0.3	20/09/2024	Review comments addressed and Appendix added	DRAFT
0.4	27/09/2024	Finalised following review comments and section 4 updated	DRAFT
1.0	30/09/2024	Approved version uploaded to DSPT portal	DSPT Team

# Contents

<b>1) Introduction</b>	<b>4</b>
a) Purpose of the document	
b) Who is the Guide intended for?	
<b>2) CAF-aligned DSPT</b>	<b>6</b>
a) Goals of moving to the CAF-aligned DSPT	
b) Changes to the assessment process	
<b>3) Independent Assessment Framework and Guide</b>	<b>8</b>
a) Benefits of the Independent Assessment Guide	
b) Independent Assessment Framework	
<b>4) Next steps – Planning for your review</b>	<b>11</b>
a) Scope of assessment	
b) Glossary of terms	
<b>5) Appendices</b>	<b>13</b>
a) Appendix A – Organisational RACI	
b) Appendix B – CAF-aligned DSPT Gantt chart	

## Section 1. Introduction

### Purpose of the document

This document aims to provide summary guidance for all stakeholders involved in the Cyber Assessment Framework (CAF) - aligned Data Security and Protection Toolkit (DSPT) independent assessments. It outlines the use of the CAF-aligned DSPT Independent Assessment Guide and Framework (to be published in November 2024), and how these resources should be used to support the delivery of a successful CAF-aligned DSPT independent assessment.

This document also provides additional context and information on the changes taking place during the year 2024/2025 as the objectives of the DSPT evolve to align closer to the CAF.

The contents of this document apply to the independent assessment arrangements of NHS Trusts (Acute, Foundation, Ambulance and Mental Health), Integrated Care Boards, Commissioning Support Units and Department of Health and Social Care (DHSC) Arm's Length Bodies.

More information will be made available in the NHS England (NHSE) DSPT Independent Assessment Framework, to be published in November 2024. Further updates will be provided on the DSPT News website: <https://www.dsptoolkit.nhs.uk/News>.

#### **Note for IT Suppliers and Independent providers who have been designated operators of essential service (OES):**

For the year 2024/25, Information and Technology (IT) Suppliers and independent providers who have been designated operators of essential service (OES), will be required to undertake a non-CAF aligned - DSPT assessment as per previous years. More information on the arrangements in place for these organisations can be found at [Help \(dsptoolkit.nhs.uk\)](https://www.dsptoolkit.nhs.uk/Help)

## Who is the Guide intended for?



### **CAF-aligned DSPT independent assessment providers**

We recognise that a variety of organisations will be assessing the effectiveness of Health and Social Care organisations' cyber security and information governance (IG) control environments, including but not limited to providers of audit services. The guide, and associated framework, provide guidance materials to inform these assessments – enabling a consistent approach to be applied across the sector (in line with the requirements of NHSE and DHSC), while enabling each organisation/assessor to exercise their professional judgement and knowledge of the organisation being assessed when establishing whether the outcomes have been met.



### **Health and Social Care Boards**

This guide will help Boards understand the role of independent assessment providers in assessing the organisation's performance against the five objectives of the CAF- aligned DSPT. The guide explains the requirements for arranging an independent assessment, and how this should support local assurance, as well as supporting assurance of legal and regulatory requirements e.g. the UK General Data Protection Regulation (GDPR), the Network and Information Systems Regulations 2018 (NIS Regulations), and national policies issued by NHSE and DHSC. Understanding the independent assessment of the CAF – aligned DSPT supports Boards in providing oversight for the organisation's cyber and information security risk.



### **Senior Information Risk Owners**

It remains the responsibility of the Senior Information Risk Owner (SIRO) in each organisation to approve the CAF-aligned DSPT submission. In the context of the CAF-aligned DSPT, this means the SIRO must give approval for the organisation's scoping of their [essential functions](#) and final toolkit submission. This Guide will provide information to help SIROs understand the differences in the assessment process between DSPT and CAF-aligned DSPT, helping them ensure their scoping of essential functions is appropriate.



### **Cyber Security and Information Governance teams**

To ensure cyber security and information governance teams within the organisation are able to understand the purpose of the CAF-aligned DSPT controls, and are given the guidance required to design and implement effective processes to align to those controls. This guide will also support the teams in understanding the appropriate evidence to be collected and provided to the independent assessors during the assessment.



### **Caldicott Guardians, Non-Executive and Executive Directors**

To inform their understanding and awareness of how the Independent Assessment Guide and Framework can be used to monitor the cyber security and information governance controls included in the CAF-aligned DSPT, and the associated risks across the organisation.

## Section 2. CAF-aligned DSPT

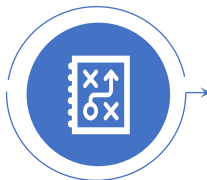
The DSPT changed in September 2024 for NHS Trusts (Acute, Foundation, Ambulance and Mental Health), Integrated Care Boards, Commissioning Support Units and DHSC Arm's Length Bodies to align with the National Cyber Security Centre's (NCSC) CAF. This was a commitment made in the DHSC cyber security strategy for Health and Social Care to 2030 to enhance the cyber security assurance of government organisations, which underpins the five pillars of the Strategy. [A cyber resilient health and adult social care system in England: cyber security strategy to 2030 - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/consultations/a-cyber-resilient-health-and-adult-social-care-system-in-england-cyber-security-strategy-to-2030).

The CAF-aligned DSPT approach is geared towards using principles and expert judgment to guide competent decision-making, with a focus on achieving key outcomes. This new approach will affect the way that people, processes and technology are evaluated and assured in cyber security and information governance (IG). This evaluation will be evidenced through indicators of good practice for each outcome and will be required to meet expected achievement levels. Cyber security plays a critical role in all sectors, but its importance is amplified in the healthcare industry, where sensitive patient data and even lives are at stake. In the NHS, a cyberattack could compromise confidential medical records, disrupt critical medical equipment, or even delay life-saving treatments. Information Governance takes centre stage in the NHS as patients trust their health and care providers with deeply personal and sensitive information. A breach of information governance could lead to added stress for patients and staff alike, disrupting care and leading to a loss of trust.

DHSC, as the competent authority for the health and care sector under the NIS Regulations, may access information from the CAF-aligned DSPT to fulfil its regulatory purpose.

For more information, we recommend that you read the NHSE's [Cyber Assessment Framework \(CAF\)-aligned Data Security and Protection Toolkit \(DSPT\) guidance - NHS England Digital](#).

### Goals of moving to the CAF-aligned DSPT:



#### Enhance risk management

Emphasise good decision-making over compliance, with better understanding and ownership of information risks at the local organisation level where those risks can most effectively be managed.



#### Foster a continuous improvement culture

Support a culture of evaluation and improvement, as organisations will need to understand the effectiveness of their practices at meeting the desired outcomes – and expend effort on what works, not what ticks a compliance box.







#### Improve threat management

Create opportunities for better practice, by prompting and enabling organisations to remain current with new security measures to meet new threats and risks.

## Changes to the assessment process

Several things will be different this year, including the timing and duration of assessments, the introduction of an outcome-based testing methodology, the skills and requirements of both the independent assessors and the relevant departments of the assessed organisation, and the approach to nationally directed technologies and processes, such as Multi Factor Authentication (MFA).

 <b>Assessment duration and planning</b>	<p>We anticipate that assessments this year will need to be conducted between January and June 2025. We expect there will be a minimum of two weeks of fieldwork for the review. Additional time should be planned before and after the field work for pre-review planning and report write up (see Appendix B for an indicative timeline).</p> <p>With the DSPT aligning with CAF, greater reliance on evidence and input from the cyber security and information governance teams should be factored into planning to ensure the CAF-aligned DSPT assessment is completed before the mandatory deadline of 30<sup>th</sup> June 2025. Further information on assessment planning will be available in the independent assessment guide and future communication from NHSE.</p>
 <b>Arranging assessments</b>	<p>NHSE encourages organisations to choose assessors from the <a href="#">NCSC Cyber Resilience Audit Scheme</a> or equivalent. Due to the change in focus and nature of the assessment, it is encouraged that independent assessments are conducted by qualified and skilled assessors who are experienced in and can competently assess against the CAF. (See Appendix A for an indicative RACI for the independent assessments).</p>
 <b>Approach to testing</b>	<p>The CAF-aligned DSPT is less prescriptive in what an organisation presents as evidence for each outcome than the previous DSPT. Indicators of good practice (IGP) give examples of procedures and processes which organisations can refer to when deciding whether they have met the expected achievement levels. There may be some instances where organisations judge that they have met a contributing outcome in a way which does not correspond to, or align with, the suggested IGP's. Assessors will need to work closely with organisations to understand how they can evidence success against the outcomes and expected achievement levels.</p> <p>For a number of outcomes, sample testing will be required by assessors to verify the achievement of one or more IGPs. Where sample testing is required, the organisation will need to provide a list of the entire population, along with evidence that the population is complete and accurate. The assessor will select a sample, the size of which will be a representative proportion of the entire population.</p> <p>Assessors will also now be required to follow up on management actions post-assessment to check that they are aligned to the original assessment findings and to confirm their implementation status. The results of this work should be reported to NHSE.</p>
 <b>Outcomes-based approach, with certain national directive policy requirement</b>	<p>The CAF-aligned DSPT framework primarily adopts an outcome-based approach, emphasising the achievement of best practices without dictating specific methods for their implementation. This flexibility empowers organisations to tailor their practices to their unique circumstances while ensuring adherence to the desired outcomes. However, the framework also has a limited number of national directive policy requirements, deemed essential for achieving the desired outcomes, for example the MFA policy. More information can be found in the NHSE DSPT Independent Assessment Framework, to be published in November 2024.</p>

## Section 3. Independent Assessment Framework and Guide

The 'Independent Assessment: Summary of Guides' (this document) provides the purpose, scope, benefits, and an overview of:

- CAF-aligned DSPT Independent Assessment guide
- CAF-aligned DSPT Independent Assessment framework.

Both of these documents will be published in November 2024.



### Purpose

#### CAF-aligned DSPT Independent Assessment guide

The guide supports organisations and assessors in gaining a deeper understanding of each of the five objectives that make up the CAF-aligned DSPT. It sets out how the independent assessment is scoped, undertaken and reported on. It also details on scoring methodology and provides templates for Terms of Reference and Reports

#### CAF-aligned DSPT Independent Assessment framework

The Independent Assessment Framework will provide specific information about each outcome to the assessors and the cyber security and information governance teams. This will include the approach to be taken when assessing each outcome, as well as identifying the type of evidence to be reviewed to confirm the expected minimum achievement levels have been met.

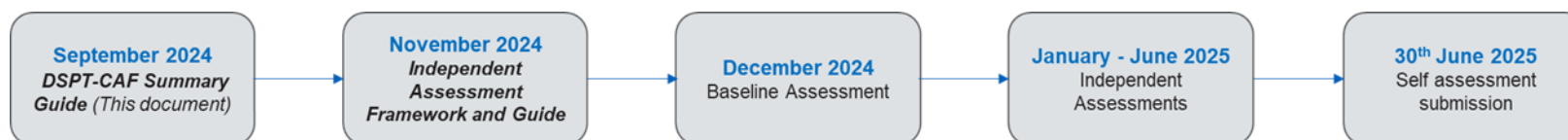


### Scope

The guide details the purpose of each underlying principle and how each supports the design of a robust and resilient organisation. The guide is not exhaustive and will not cover every eventuality. As such, professional judgement will be required when using its contents in preparation for, or during, a CAF-aligned DSPT independent assessment.

The framework covers the four CAF objectives as well as the additional data security objective specific to the healthcare sector. It provides an explanation for each indicator of good practice (IGP), as well as a recommended approach to test the organisation against it, and indication of the type of evidence to be reviewed. The framework also details the necessary thresholds to reach the expected minimum achievement level of each outcome.

### High level CAF aligned DSPT independent assessment programme timeline





## Benefits of the Independent Assessment Framework and Guide

The CAF-aligned DSPT harnesses a less prescriptive approach in the response to each outcome and therefore warrants its own guidance to reflect the changes in the toolkit. This updated guidance is intended to provide the following benefits to Health and Social Care organisations, independent assessment providers, and the Health and Social Care system as a whole:



Health and Social Care organisations: As the focus of DSPT shifts from verifying the implementation of specific controls mandated by evidence items, to assessing adherence to the desired outcomes under the CAF-aligned DSPT independent assessments, organisations will receive an opinion over the effectiveness of their control environments to adhere to the specified outcomes. This would ultimately support them in identifying cyber security and information governance gaps between the organisation's self-assessment and the assessment result, that should be mitigated to improve the posture of the organisation. In addition, the increased insight that national bodies will have into the cyber security and information governance posture of multiple organisations across the sector will enable them to support individual organisations in improving their controls.



Independent assessment providers: In recent times, independent assessment providers have been expected to provide an increased level of assurance, over a wider range of data security and protection controls (including more technical cyber-related controls introduced in the CAF-aligned DSPT). The guidance is not designed to replace the existing expertise, knowledge and professional judgement of independent assessment providers, but should instead support them in identifying how to effectively assess the organisation against the objectives of the CAF-aligned DSPT. It will also help inform the work of cyber security and IG professionals that are new to the health and social care system, helping them to understand assessor's requirements to validate the posture of the organisation during the assessment.



National Bodies/Health and Social Care system: When followed and widely used across the system, the CAF-aligned DSPT framework and guide should provide national bodies with greater insight into the effectiveness of Health and Social Care organisations' cyber security and information governance control environments, as well as their alignment to regulations such as NIS 2018. This will enable new national data security services and guidance to align to known areas of weakness and support shared learnings across the sector from examples of good practice, as well as provide additional support to organisations that may have issues in this area. DHSC, as the competent authority for the health and care sector under the NIS Regulations, may access information from the CAF-aligned DSPT to fulfil its regulatory purpose

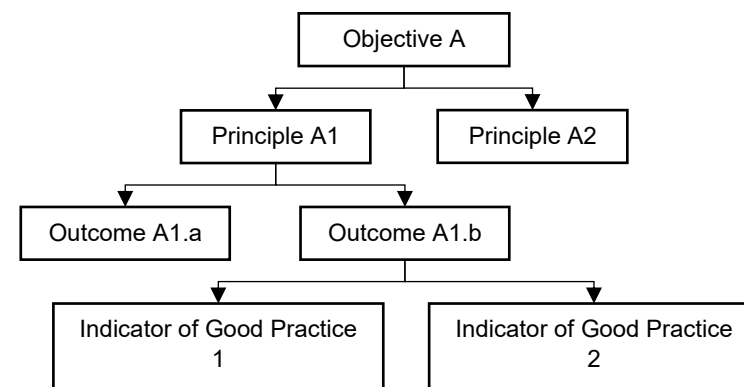
## Overview of the Independent Assessment Framework

The following summary outlines the purpose and scope of the CAF aligned DSPT Independent Assessment Framework.

The NHSE CAF-aligned DSPT Independent Assessment Framework is a resource, created by NHSE, for independent assessors of Health and Care organisations. The framework is the resource that the assessor should use to assess the organisation against the requirements of the CAF-aligned DSPT. It can act as the basis of scoping the terms of reference for each CAF-aligned DSPT assessment, the approach that the assessor could take during their review, and inform the type of evidence that the assessor could request and review as part of their work. Further detail on the framework, and how to navigate it, will be provided in the framework itself.

There are five (A-E) objectives within the CAF-aligned DSPT. The CAF-aligned DSPT independent assessment framework outlines the principles that make up each objective, highlighting the area of scope for each principle. Each principle contains several outcomes, which can be “Achieved”, “Partially Achieved” or “Not Achieved”, depending on the results of their respective indicators of good practice. Each organisation will be assigned a profile, which will be based on the type and size of the organisation. This profile will be used to identify the expected achievement levels for each outcome.

The framework details the control objective of each outcome and IGP, provides guidance as to how to assess the organisation’s control environment against the IGPs, provides indication as to the on-site tests that could be performed and documents that the assessor should typically request and review as part of their work. It also includes details on whether or not the Indicator of Good Practice is required for this year’s assessment for each category of Health and Social Care organisation.



The framework is designed to be used by independent assessment providers. It will enable independent assessment providers to carry out their assessments in an efficient and consistent manner. It is advised that independent assessment providers have experience in reviewing cyber security and information governance control environments, and the assessment approach is not intended to be exhaustive or overly prescriptive, though it does aim to promote consistency of approach. Assessors are expected to use their professional judgement and expertise in further investigating and analysing the specific control environment, and associated risk, of each health and social care organisation.

## Section 4. Next steps - Planning for your review

The below are suggested next steps to conduct ahead of the issuance of the CAF-aligned DSPT Independent Assessment Guide in November 24. These will enable your organisation to plan effectively for the review:

1. **Understand requirements** - Discuss with an independent assessor the timelines and requirements for an independent assessment to be conducted between January and May 2025, including staff requirements and financial resourcing.
2. **Understand CAF profile** - Review the CAF profile as set out for your organisation.
3. **Understand expected achievement levels** - Review the Objectives, Principles, Outcomes, IGPs and expected achievement levels for the assessment of your organisations set out in: [Cyber Assessment Framework \(CAF\)-aligned Data Security and Protection Toolkit \(DSPT\) guidance - NHS England Digital](#)
4. **Update leadership** - Provide an update to the Board and Audit Committee of your organisation, indicating expected timelines, scope of assessment and the results of the self-assessment.

### Scope of assessment

There is a total of 47 outcomes in the CAF-aligned DSPT, which will all be assessed over a multi-year period. Each year, a selection of outcomes from across the five objectives will be tested by independent assessment providers. NHSE will mandate a common core set outcomes to be assessed for all organisations that undertake the CAF-aligned DSPT, while a further number will be selected by individual organisations. These outcomes should be approved by the Board of each organisation, and will reflect areas of concern that warrant additional assurance over the controls in place during that audit period.

More information will be made available in the NHS England (NHSE) DSPT Independent Assessment Framework, to be published in November 2024. Further updates will be provided on the DSPT News website: <https://www.dsptoolkit.nhs.uk/News>

## Glossary of terms

Term / abbreviation	What it stands for
Audit	An independent, objective assurance and consulting activity designed to add value and improve an organisation's operations.
CAF	The Cyber Assessment Framework (CAF) is a systematic and comprehensive approach designed by the National Cyber Security Centre (NCSC) to assess the extent to which cyber risk to essential functions are being managed.
CAF-aligned DSPT Independent Assessment Providers	Organisations who are commissioned directly by Health and Social Care organisations to complete a CAF-aligned DSPT assessment or review.
Control	Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organises, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
Cyber Security	The protection of devices, services and networks - and the information on them - from unauthorised access, theft or damage.
Effectiveness	The degree to which something is successful in producing a desired result.
Evidence	The information, documents or assertions that are analysed by independent assessment providers to assess the posture of an organisation's operations.
DSPT	Data Security and Protection Toolkit.
Fieldwork	The evaluation phase of the assessment.
Information Governance	Information governance (IG) is a strategic framework that involves policies, processes, and controls to manage, protect, and maximise the value of an organisation's information.
Multi-Factor Authentication	Multi-factor authentication (MFA) is an identity verification method in which a user must supply at least 2 pieces of evidence, such as their password and a temporary passcode, to prove their identity.
UK GDPR	UK General Data Protection Regulation, UK GDPR, is a regulation on data protection and privacy. It outlines protected classes of information and expectations for processing and storing protected information.

## Appendix A - Organisational RACI

For each task to be completed during a CAF-aligned DSPT, the indicative RACI table below sets out the people responsible and accountable for the completion, as well as anyone who may be consulted during the task, and who should be informed when the task is being undertaken, and when it has been completed.

Task	Responsible	Accountable	Consulted	Informed
Collect documentation for each principle to be assessed	Information Security Team Information Governance Team	SIRO DPO	Procurement	Wider organisation
Discuss and agree current position of each Outcome (Achieved, Partially Achieved, Not Achieved)	Information Security Team Information Governance Team	SIRO DPO	Procurement	Caldicott Guardians Executive Directors
Agree Terms of Reference and timelines for the assessment	IG/IT Manager	SIRO DPO	Information Security Team Information Governance Team	Caldicott Guardians Executive Directors
Communicate assessment timelines with departments	IG/IT Manager	SIRO DPO		Wider organisation
Kick off call	IG/IT Manager	SIRO DPO		Caldicott Guardians Executive Directors
Arrange fieldwork meetings	IG/IT Manager	SIRO DPO	Caldicott Guardian	
Send documents to assessors	Information Security Team Information Governance Team	SIRO DPO		
Take part in fieldwork meetings and collate additional documents	IG/IT Manager DPO Caldicott Guardian	SIRO	Information Security Team Information Governance Team	
Close out call	IG/IT Manager	SIRO DPO		Caldicott Guardians Executive Directors
Read and discuss draft report	IG/IT Manager SIRO DPO Caldicott Guardian	SIRO		Executive Directors
Agree action owners and timelines	IG/IT Manager SIRO DPO	SIRO	Executive Directors	

	Caldicott Guardian			
Provide management responses	IG/IT Manager	SIRO		DPO Caldicott Guardian Executive Directors
Read and agree final report	IG/IT Manager SIRO DPO Caldicott Guardian	SIRO		Executive Directors
Create action plan for remediation of findings	IG/IT Manager SIRO DPO Caldicott Guardian	SIRO	Executive Directors	
Add assessors to the toolkit	IG Manager	SIRO		DPO Executive Directors
Submit final report to NHSE	SIRO	SIRO		DPO Caldicott Guardian Executive Directors IT/IG Manager
Present final report to audit committee	SIRO			DPO Caldicott Guardian Executive Directors IT/IG Manager
Ongoing reporting of progress to audit committee	SIRO	SIRO		DPO Caldicott Guardian Executive Directors

## Appendix B – CAF-aligned DSPT Gantt Chart

The Gantt chart provides an indicative timeline for the completion of the CAF-aligned DSPT, starting with the preparation of the assessment, and ending with post-assessment activities. Collation of the documents and discussions around the organisation’s position for each outcome should take place year-round and are therefore listed as “Prior to week 1” in the chart. Submitting the final report to NHSE must be done before the 30 June deadline, but this may be farther away than week 9 if the organisation has undertaken their CAF-aligned DSPT early in the year.

### Activities to be undertaken ahead of the assessment

Task	Assigned to		Prior to week 1	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Post week 9
<b>Assessment preparation</b>													
Collate documents for each Outcome in scope	IG team IT team												
Discuss and agree current position of each Outcome (Achieved, Partially Achieved, Not Achieved)	IG Manager IT Manager SIRO												
Draft Terms of Reference and document request list	Assessors												
Agree Terms of Reference with assessors	IG Manager IT Manager SIRO												
Communicate assessment timelines with departments	IG Manager IT Manager												

**Activities to be undertaken during the assessment**

Task	Assigned to		Prior to week 1	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Post week 9
<b>Assessment</b>													
Kick off call	IG Manager IT Manager Assessors												
Arrange fieldwork meetings	IG Manager IT Manager Assessors												
Send documents to assessor	IG Manager IT Manager												
Carry out evidence review	Assessors												
Take part in fieldwork meetings and collate additional documents	IG Manager IT Manager												
Close out call	IG Manager IT Manager Assessors												



### Activities to be undertaken on conclusion of the assessment

Task	Assigned to		Prior to week 1	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Post week 9
<b>Post assessment actions</b>													
Draft report with findings, risks and recommended actions	Assessors												
Read and discuss draft report	IG/IT Manager SIRO DPO Caldicott Guardian												
Agree action owners and timelines	IG/IT Manager SIRO DPO Caldicott Guardian Assessors												
Provide management responses	IG/IT Manager												
Draft final report	Assessors												
Read and agree final report	IG/IT Manager SIRO DPO Caldicott Guardian												
Create action plan for remediation of findings	IG/IT Manager SIRO DPO												
Add assessors to the toolkit	IG Manager												
Submit final report to the Toolkit	Assessors												
Submit final report to NHSE	SIRO												
Present final report to audit committee	SIRO Assessors												
Ongoing reporting of progress to audit committee	SIRO												