Data Security and Protection Toolkit

Strengthening Assurance- Independent Assessment and Audit Framework

IT Suppliers and independent sector Operators of Essential Service (OES)

2024/25 Version 7 DSPT (NDG)

Creating a culture of Improvement

Information and technology for better health and care

12/09/2024

© NHS England copyright 2024

Document Control

Revision history

Revision Date	Summary of changes	Changes marked	Version Number
04/10/2019	Initial Draft for consultation	00/00/2019	1.0
20/04/2020	Changes to guidance and scoring methodology following initial feedback from Independent Assessment pilot	20/04/2020	1.1
22/05/2020	Update to reporting template to include ‘direction of travel’ observation heading. Clarification of evidence item level risk scoring methodology	26/05/2020	1.4
05/06/2020	Update to Tables 3 and 5 in the risk and confidence evaluation methodology with associated changes in the Appendices	05/06/2020	1.7
25/06/2020	Updates to examples of risk scoring in the Appendices	25/06/2020	1.9
30/06/2020	Include slide referring to Independent Assessors use of professional judgement and Big Picture Guides	30/06/2020	1.10
05/08/2021	Updated in line with 2021-22 DSPT Standard changes	05/08/2021	1.11
16/11/2021	Updated following feedback from DSPT Auditor Workshop	17/11/2021	2.0
26/09/2022	Updated to reflect Version 5 DSPT 2022/23	26/09/2022	2.1
26/09/2023	Updated to reflect Version 6 DSPT 2023/24	26/09/2023	2.2
13/09/2024	Updated to reflect version 7 DSPT 2024/25	13/09/2024	2.3

Document Control: The controlled copy of this document is maintained by NHS England’s Cyber Operations. Updates will be managed in accordance with changes made to the Data Security and Protection (DSP) Toolkit. It is expected that this document will be updated at least annually. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Glossary of Terms

Term / Abbreviation	What it stands for
Audit	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled . • An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines). • An internal audit is conducted by the organisation itself, or by an external party on its behalf.
Audit Scope	Extent and boundaries of an audit.
Control	Measure that is modifying risk. • Controls include any process, policy, device, practice, or other actions which modify risk. • It is possible that controls not always exert the intended or assumed modifying effect.
Documented Evidence	Information required to be controlled and maintained by an organisation and the medium on which it is contained.
DSP Toolkit	Data Security and Protection Toolkit.
DSP Toolkit Independent Assessment Providers	Organisations who are commissioned directly by Health and Social Care organisations to complete a DSP Toolkit assessment or review.
Effectiveness	Extent to which planned activities are realised and planned results achieved.
GDPR	General Data Protection Regulation, GDPR, is an EU regulation on data protection and privacy. It outlines protected classes of information and expectations for processing and storing protected information.
List-X	A commercial site (i.e. non-government) on UK soil that is approved to hold UK government protectively marked information marked as 'Secret' or above, or international partners information classified 'Confidential' or above.
NDG	National Data Guardian.
Personal Data	Protected under Data Protection legislation / GDPR, personal data is data relating to an identified or identifiable natural person.

Glossary of Terms

Term / Abbreviation	What it stands for
PII	Personally identifiable information, PII, is data which could identify a specific individual and is a subset of personal data, which is protected under GDPR.
Special Category Data	Special category data is personal data deemed to be more sensitive under GDPR, and includes an individual's race, ethnic origin, religion, politics, trade union membership, genetics, biometrics, health, sex life, and sexual orientation. There are additional requirements for protecting special category data under GDPR.
Statement of Work (SoW)	A statement of work, SoW, often serves the same purpose as a Terms of Reference.
Terms of Reference	Used to define the scope of an audit, the terms of reference, ToR, should establish the focus and objectives of the audit, the audit timetable (including reporting), and a summary of staff to be engaged in the work, along with the audit tools and techniques that will be used. The terms of reference should be agreed prior to the audit starting.

Contents

The DSP Toolkit Independent Assessment Guide consists of four main sections which are listed below along with an introductory statement summarising the content of each section.

The links below are interactive; please click on the link to be navigated to the content you require.

1. Executive Summary Page 06

An overview of the importance of data security and data protection to Health and Social Care organisations and why the related control environments require attention from Independent Assessment Providers.

2. Introduction Page 08

This section provides answers to key questions regarding the purpose, ambition and structure of the DSP Toolkit Independent Assessment Guide.

3. Guide for DSP Toolkit Independent Assessment Providers Page 13

This section contains a suggested approach, based on industry good practice, that assessment providers should consider throughout their assessment lifecycle.

4. What is the Data Security and Protection (DSP) Toolkit? Page 36

An overview of the DSP Toolkit, including the changes made in the two versions of the toolkit.

Appendices Page 41

This section contains templates for risk and controls matrices, as well as assessment terms of references and reports.

1. Executive Summary

1. Executive Summary

Why data security and data protection issues require attention from Independent Assessors and Auditors.

Data and information is a critical business asset that is fundamental to the continued delivery and operation of health and care services across the UK. The Health and Social Care sector must have confidence in the confidentiality, integrity and availability of their data assets. Any personal data collected, stored and processed by public bodies are also subject to specific legal and regulatory requirements.

Data security and data protection related incidents are increasing in frequency and severity; with hacking, ransomware, cyber-fraud and accidental data losses all having been observed across the Health and Social Care sector. For example, we need look no further than the WannaCry ransomware attack in May 2017 that impacted NHS bodies and many local authorities' IT services. Although Microsoft released patches to address the vulnerability, many organisations including several across the public sector didn't apply the patches, highlighting an inadequate ability to adapt to new and emerging threats.

The need to demonstrate an ability to defend against, block and withstand cyber-attacks has been amplified by the introduction of the EU Directive on security of Network and Information Systems (NIS Directive) and the EU General Data Protection Regulation (GDPR). The NIS Directive focuses on Critical National Infrastructure and 'Operators of Essential Services'. The GDPR focuses on the processing of EU residents' personal data. As such, it is essential that Health and Social Care sector organisations take proactive measures to defend themselves from cyber-attacks and evidence their ability to do so in line with regulatory and legal requirements.

An additional complexity arises when a Health and Social Care organisation needs to share data. Organisations need to have mutual trust in each other's ability to keep data secure and also have a requirement to take assurance from each other's risk management and information assurance arrangements for this to happen successfully. Not getting this right means that either organisations fail to deliver the benefits of joining up services or put information at increased risk by sharing it insecurely across a wider network.

Achieving a realistic understanding of data security and data protection issues is therefore essential to protecting Health and Social Care organisations, personnel, patients and other stakeholders; particularly as the drive to making Health and Social Care services more 'digital' continues.

The DSP Toolkit is one of several mechanisms in place to support Health and Social Care organisations in their ongoing journey to manage data security and data protection risk. The DSP Toolkit allows organisations which access NHS patient data and systems to measure their performance against the National Data Guardian's ten data security standards, as well as supporting compliance with legal and regulatory requirements (e.g. the GDPR and NIS Directive) and Department of Health and Social Care policy through completion of an annual DSP Toolkit online self-assessment.

Completion of the DSP Toolkit therefore provides Health and Social Care organisations with valuable insight into the technical and operational data security and data protection control environment and relative strengths and weaknesses of those controls. However, the completion of the DSP Toolkit itself by the organisation is not the only mechanism in place to provide the level of comfort Health and Social Care organisation Boards need to achieve a reliable understanding of data security and data protection risk. Another mechanism is to independently assess/audit the data security and protection control environments of health and social care organisations.

The role other independent assessment providers play in helping to strengthen the reliance Health and Social Care Organisations Boards, Department of Health and Social Care and NHS England place on the DSP Toolkit submissions is summarised in the National Data Guardian report, 'Review of Data Security, Consent and Opt-Outs and the Care Quality Commission report, Safe data, safe care'. Both reports include the following recommendation: "Arrangements for internal data security audit and external validation should be reviewed and strengthened to a level similar to those assuring financial integrity and accountability" (NDG 6, CQC 6 Table of recommendations).[1] Therefore, it is essential that independent assessment providers, including internal auditors, focus on the assessment of the effectiveness of health and social organisations' data security and protection controls, as opposed to simply focusing on the veracity of their DSP Toolkit submissions.

The DSP Toolkit Independent Assessment Guide must be followed by all organisations required to complete an annual DSPT Audit/Assessment. It provides a basis for the efficient and consistent delivery of DSP Toolkit independent assessments. The guide is applicable to version 2024/25 of the toolkit

[1] p. 9, *Review of Data Security, Consent and Opt-Outs,* June 2016; p. 29, *Safe data, safe care,* July 2016.

2. Introduction

2.1 - Some Key Developments since the introduction of the Data Security and Protection (DSP) Toolkit

The Data Security and Protection (DSP) Toolkit is an online tool that enables organisations to measure their performance against data security and information governance requirements which reflect legal rules and Department of Health and Social Care policy. The Toolkit has been developed in response to The NDG Review (Review of Data Security, Consent and Opt-Outs) published in July 2016 and the government response published in July 2017.

The DSP Toolkit is provided by NHS England. Operation of the toolkit (and where appropriate, regulatory activity) is performed in partnership by the Department of Health and Social Care, NHS England, Information Commissioner's Office, Care Quality Commission and National Cyber Security Centre.

Category 2
Large IT Suppliers and Operators of Essential Services

Category 3
Dentists, Pharmacies, Care Homes, Local Authorities etc

Category 4
GPs

All types of Health and Social Care organisations complete a DSP Toolkit assessment against the 2023-24 v6 standard

Organisations taking part in the DSP Toolkit

23,015

Social care organisations have completed an assessment against the 2023-24 v6 standard

6,188

Increase, compared with 2022-23

Social care take-up

59,559

The number of organisations who have published an assessment against the 2023-24 v6 standard

33,000

Increase since the DSPT was launched in 2018-19

Number of published DSP Toolkit assessments

100%

Percentage of Trusts, Arm's Length Bodies, Commissioning Support Units and Integrated Care Boards who published a DSP Toolkit assessment against the 2023-24 v6 standard.

Completion rate of Large NHS Organisations

Figures taken 23 August 2024

2.2 - Introduction

The following introduction provides answers to seven key questions regarding the purpose, ambition and structure of the DSP Toolkit Independent Assessment Guide.

1. Who is the intended audience for this guide?

This guide is intended for multiple stakeholder groups. The majority will require high level awareness of the guide, however, DSP Toolkit independent assessment providers will need to understand and apply the detail of the guide:

- **DSP Toolkit independent assessment providers:** We recognise that a variety of organisations will be responsible for assessing the effectiveness of Health and Social Care organisations' data security and protection control environments, including but not limited to providers of internal audit services. This guide, and associated framework, act as reference materials to support these assessments – enabling a consistent approach to be applied across the sector (in line with the requirements of NHS England), while enabling each Independent Assessor to exercise their professional judgement and knowledge of the organisation being assessed.
- **Health and Social Care Organisation Boards**: to understand the role independent assessment providers play in assessing their organisation's performance against the National Data Guardian's ten data security standards as well as supporting compliance with legal and regulatory requirements (e.g. the General Data Protection Regulation) and Department of Health and Social Care policy.
- **Accountable Officers (Chief Executives) and Senior Information Risk Owners**: to ensure that the independent assessment addresses key information governance risks and contributes to assurance for their annual report and the annual statement of compliance and statement of internal control.
- **Caldicott Guardians, Non-Executive and Executive Directors:** to inform their understanding, awareness and monitoring of the response to data security and data protection risks across the organisation.
- **Governing health bodies, regulators and assurance providers:** for example External Audit providers and the Care Quality Commission, to help assess if the basis on which they are performance managing the Health and Social Care organisation is sufficient in terms of considering their data security and data protection posture.

2. What are the benefits of this updated guidance?

This guide sets out the methodology and replaces the previous guidance 'A Question of Balance', which was written for audit advice against the DSP Toolkit's predecessor, the IG Toolkit. The DSP Toolkit has superseded the IG Toolkit and warrants its own guidance to reflect the changes in the Toolkit, changes in the national requirements and standards and changes in the external risk and threat environment that have caused cyber security to rise up the risk agenda. Updating this guidance is intended to provide the following benefits to Health and Social Care organisations, independent assessment providers, and the Health and Social Care sector as a whole:

- **Health and Social Care organisations:** As the focus of DSP Toolkit independent assessments shifts from verifying the veracity of submissions, to assessing the effectiveness of controls; organisations will receive more valuable assurance over their control environments, ultimately supporting them in improving data security and protection outcomes. In addition, the increased insight that national bodies will have into the data security and protection posture of multiple organisations across the sector, will enable them to support individual organisations in improving their data security and protection controls.
- **Independent assessment providers:** In recent times, independent assessment providers and auditors have been expected to provide an increased level of assurance, over a wider range of data security and protection controls (including more technical controls introduced in the DSP Toolkit). All whilst there is a cyber security skills shortage in the country as a whole. This guidance, while not designed to replace any existing expertise, knowledge and professional judgement; should support independent assessment providers in providing a baseline for how the controls in the DSP Toolkit should ~~could~~ be independently assessed. It ~~will also~~ informs the work of data security and cyber security professionals that are new to the health and social care sector and perhaps unfamiliar with internal audit and independent assessment. More professionals will be required to deliver an increased workload and drive improvements in data security.
- **National Bodies/Health and Social Care sector:** With being widely used across the sector, the updated approach provides national bodies with greater insight into the effectiveness of Health and Social Care organisations' data security and protection control environments. This will enable new national data security services 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.

2.2 - Introduction *continued*

3. What does this Guide comprise of?

The DSP Toolkit Independent Assessment Guide comprises the following three main documents:

- **DSP Toolkit Independent Assessment Guide:** a step-by-step guide for conducting a DSP Toolkit independent assessment.
- **DSP Toolkit Independent Assessment Framework:** a comprehensive overview of all 150 evidence texts and the 42 assertions to which they relate, including indicative testing methodologies required to assess end user organisation's data security and protection controls, procedures and technologies.
- **Summary Guide:** an overview of the purpose of these documents.

4. How have changes to government policy influenced the Department of Health and Social Care's response to data security and cyber security risk?

In the past, much of the guidance, governance, mandatory standards and compliance regimes for data security were compiled and provided by central government bodies. For example, HMG and the Cabinet Office issued the HMG Security Policy Framework, which remains the primary reference point for central government on the subject of 'information assurance'. However, central government is increasingly less inclined to prescribe how individual departments and bodies should approach cyber security, data security and data protection risk management. Whilst principles and standards may be similar for all organisations; each organisation's operating model and risk appetite is different and should drive its own, tailored approach to developing a control environment that is proportionate to the risks, threats and vulnerabilities it faces. This approach therefore gives individual organisations a degree of freedom to make their own decisions about which standards or frameworks they wish to adopt.

The Department of Health and Social Care released version one of the Information Governance Toolkit (IG Toolkit) in 2004. The IGT was an approved Information Standard developed to support organisations to meet their information governance obligations and to enable organisations to measure their performance against the information governance requirements.

Following the National Data Guardian (NDG) Review (see recommendation 2, 2016) a decision was made to develop a new data security and protection standard. The IGT had been in use for a number of years but increasing internet connectivity and elevated cyber security threat meant that more emphasis was needed on operational resilience, network security and data security. The IGT had historically focused on information governance and data protection. The Data Security and Protection (DSP) Toolkit superseded the Information Governance Toolkit on 1 April 2018.

The DSP Toolkit is a single standard that all organisations with access to NHS patient data and systems must adhere to. It is also the vehicle through which a range of strategic policy and regulatory requirement objectives are met. These include:

- Satisfying the Cabinet Office requirement for the Department of Health and Social Care to provide assurance that all parts of the NHS are meeting mandated data security and protection standards, including encryption, staff training and information risk management and governance structures.
- Providing the assessment of information quality legally required under Quality Account Regulations.
- Supporting the accountability and transparency agendas by requiring organisations to assess and publish performance against a standard framework which enables comparisons.
- Providing organisations that process NHS patient data with a clearly presented and peer reviewed roadmap to effective information governance.

2.2 - Introduction *continued*

5. What do we mean by data security and protection and are we looking at both electronic and physical data and information assets?

What we mean by data security and protection is the activity required to protect an organisation's computers, networks, software, data and information from unintended or unauthorised access, change or destruction via physical access, the internet or other communications systems or technologies.

Data security and protection is therefore part of a wide information security agenda. Information security encompasses electronic, physical and behavioural threats to an organisation's systems and data, covering people and processes. Data can, of course, be stored both electronically and physically (e.g. on paper). Paper-based information and physical media used for data processing and storage are therefore in scope. This guide therefore considers both the security of electronic data and related processes and transactions, including paper records.

6. Why should Health and Social Care Boards monitor data security and data protection risks?

As government's guidance to audit committees makes clear, data security and protection is now an area of Management activity that Health and Social Care Boards should scrutinise. Together with the rapidly changing nature of the risk, this means that there is an important role for Boards to perform in understanding whether Management is adopting a clear approach, if they are complying with their own rules and standards and whether they are adequately resourced to carry out these activities. The National Cyber Security Centre (NCSC, the UK's national technical authority on information assurance and cyber security) agree that this is a Board issue. The NCSC launched a Board Toolkit for cyber security in May 2019 - a resource designed to encourage essential cyber security discussions between the Board and their technical experts. Using this NCSC toolkit alongside an annual cycle of continuous engagement with, and use of, the DSP Toolkit will enable informed and useful discussions at Board level across the health and social care landscape.

7. Why do National Bodies monitor data security and protection risks?

The nature of data security and protection attacks and breaches are rapidly changing and increasing in frequency, severity and impact. As such, NHS England's Data Security Centre (DSC) role as a specialist service provider to Health and Social Care organisations offering services to help manage data security and protection risk and recover in the event of an incident is growing in importance. The application of this updated guide should increase NHS England's capability to monitor data security and protection risks, by having greater visibility of, and insight into; individual organisations' control environments, as well as having a 'helicopter view' of the posture of data security across the sector as a whole.

2.3 2024-25v7 Independent Assessment and Audit Mandatory Scope

DSPT independent assessments and audits must follow the scope set out below, as a minimum. Organisations may cover items of their choice in addition to this. However, it should be noted this could potentially have a detrimental effect on the overall scoring. The scope applies to mandatory evidence items only and with the highlighted evidence items out of scope. Evidence items which are covered by an exemption for CE+ and/or ISO27001 will not require further auditing, once it is confirmed that the scope of the certification covers all the health and care data being processed.

Scope	Detail
Org Profile	Check sector, key roles (Mail system & CE+ if used)
13 Mandatory Assertions	1.1 The organisation has a framework in place to support Lawfulness, Fairness and Transparency (Auditors are not required to include 1.1.7 and 1.1.8 in the audit scope) 2.2 Staff contracts set out responsibilities for data security 3.1 Staff have appropriate understanding of information governance and cyber security, with an effective range of approaches taken to training and awareness 3.2 Your organisation engages proactively and widely to improve data security, and has an open and just culture for data security incidents 4.5 You ensure your passwords are suitable for the information you are protecting 5.1 Process reviews are held at least once per year where data security is put at risk and following DS incidents 6.2 All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway 7.1 Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services 8.2 Unsupported software and hardware is categorised and documented, and data security risks are identified and managed 9.2 A penetration test has been scoped and undertaken 9.5 You securely configure the network and information systems that support the delivery of essential services 9.6 The organisation is protected by a well-managed firewall 10.2 Basic due diligence has been undertaken against each supplier that handles personal information

3. Guide for DSP Toolkit Independent Assessment Providers

3.1.1 - Guide for DSP Toolkit Independent Assessment Providers

As discussed in Sections 2 and 3 (the Executive Summary and Introduction, respectively), one of the key outcomes of this updated guidance documentation is to align the methodologies used by DSP Toolkit independent assessment providers across the sector; chiefly internal auditors. We recognise that each independent assessment provider, including internal audit providers, will have their own internal audit methodology and risk assessment/reporting process. However, in this document we have outlined a suggested approach, based on industry good practice, that assessment providers should consider throughout their assessment lifecycle. Similarly to the independent assessment framework, this is not designed to replace existing methodologies and knowledge or experience, particularly where an organisation's Audit and Risk Committee require audits to be performed and reported in a standard format. However, it acts as a reference point for providers, to facilitate and inform alignment across the sector and the bolstering of any gaps in existing methodologies.

There should **be two outputs of each independent assessment**:

1. An assessment of the **overall risk** associated with the organisation's data security and data protection control environment. i.e. the level of risk associated with controls failing and data security and protection objectives not being achieved;
2. An assessment as to the veracity of the organisation's self-assessment / DSP Toolkit submission and the Independent Assessor's level of **confidence** that the submission aligns to their assessment of the risk and controls (output 1).

In essence the first output will be an indicator, for those assertions and evidence text items assessed, as to the level of risk to the organisation and how good, or otherwise, the data security and protection environment is in terms of helping the organisation achieve the objectives in the DSP Toolkit. The second output will support an internal audit provider in arriving at the assurance level that they are required to provide, and that the organisation is obliged to provide, as per one of the DSP Toolkit requirements.

The overall risk evaluation output is seen as key to driving the conversations and improvements required. That is, **this updated guidance aims to support the following requirements:**

1. Better enable NHS organisations to continually improve the quality and consistency of DSP Toolkit submissions across the NHS landscape;
2. Deliver a framework that is adaptable in response to emerging information security, data and health and social care standards;
3. Allow for a range of bodies to deliver independent assessments in a consistent and easily understood fashion;
4. Help drive measurable improvement of data security across the NHS landscape and support annual and incremental improvements in the DSP Toolkit itself;
5. Deliver a framework that better enables and encourages organisations to publish a more granular, evidenced and accurate picture of their organisation's position in terms of data security;
6. Deliver a framework that allows for data security and protection professionals to spend time on-site coaching organisations on security improvement options at the same time as assessing controls and risks;
7. Deliver a framework that helps ensure consistent delivery of 'independent audit', internal audit;
8. Enable and encourage appropriate feedback and dialogue between NHS England and Independent Assessors to help inform NHS wide communications and initiatives to help address common challenges and systemic or thematic security issues and to help inform the development and consumption of NHS England provided national services around data security;
9. Enable leveraging of other sources of assurance across the NHS to reduce the burden on organisations and reduce total effort, cost and help minimise duplication of information gathering.

The remainder of this Guide covers the process (5 key assessment tasks) and is followed by appendices including a description of what the DSP Toolkit is, templates for Terms of Reference and Reports, a cross-reference for related documents and a risk and controls matrix.

3.1.2 - DSP Toolkit Independent Assessment Process

There are five core tasks and a number of sub-tasks central to the delivery of all DSP Toolkit independent assessments, which are outlined below. The remainder of this section (including sub-sections 3.2.1 to 3.2.5) is structured to provide independent assessment providers with further information relating to the five tasks and sub-tasks. Please see these summarised in the table below:

3.2.1 Task One Pre-Assessment Preparation and Information Gathering	**3.2.2 Task Two** Scope DSP Toolkit Independent Assessment	**3.2.3 Task Three** Deliver DSP Toolkit Independent Assessment	**3.2.4 Task Four** Post-DSP Toolkit Review Meeting & Reporting	**3.2.5 Task Five** Assessment Finalisation & Quality Management
Task 3.2.1.1 - Pre-assessment preparation and information gathering	**Task 3.2.2.1** - Conduct Detailed Scoping Meeting to Agree Terms of Reference	**Task 3.2.3.1** - Perform the DSP Toolkit assessment	**Task 3.2.4.1** - Draft & Finalise report	**Task 3.2.5.1** - Skills and training
Task 3.2.1.2 - Develop an initial understanding of risk (i.e. Risk Fundamentals)		**Task 3.2.3.2** - Perform Risk and Confidence Evaluations	**Task 3.2.4.2** - Issue tracking & follow-Up Work	

3.1.3 – Using Professional Judgement

The DSPT Independent Assessment Guide (including the DSP Toolkit Strengthening Assurance Framework and associated "Big Picture Guides") are not exhaustive. Collectively these documents will not cover every eventuality and **professional judgement will be required** in how the standard is met and audited.

Both sets of guidance endeavour to be vendor agnostic. A Health and Social Care organisation may have an excellent vendor-supplied system, which are not referred to in the guides. That is not to discount such a system, which should be implemented and audited on its merits.

The required standards have to be achievable by those whose digital maturity is "still developing". As a consequence, some of the measures outlined could be seen as quite manual or basic in nature. This does not mean that more sophisticated measures cannot be implemented.

At times the Big Picture Guides may go further than the Independent Assessment guides and vice versa. Only the most binary of assertions would lead to one answer. The divergence of guides is either following an implementation theme to the end or the next logical audit artefact.

When implementing or auditing please pay regard to the intent of the evidence, assertions, standards and ultimately the whole 10 National Data Guardian Data Security Standards. It is not the intention of the DSP Toolkit Strengthening Assurance Framework to create tick lists of items to be implemented and audited that do not reflect actual practice.

3.2.1 Task One: Pre-Assessment Preparation and Information Gathering

3.2.1.1 - DSP Toolkit Independent Assessment Workflow

The chart below provides DSP Toolkit independent assessment providers with an overview of the key activities and expected outcomes required for each task. The following sections of this document will explore the five tasks in further detail.

	4.2.1 Pre-assessment Preparation and Information Gathering	4.2.2 Scope DSP Toolkit Independent Assessment	4.2.3 Deliver DSP Toolkit Independent Assessment	4.2.4 Post-Assessment Closing Meeting & Reporting	4.2.5 Assessment Finalisation & quality maintenance
Activities	• Make first contact with Health and Social Care Organisation. • Agree a scoping meeting date. • Review DSP Toolkit evidence including previous internal audits/assessments.	• Understand any issues, incidents or changes since last DSP Toolkit independent assessment. • Review the Health & Social Care Organisation Action Plan. • Address any questions the Health and Social Care Organisation may have and ensure follow-up actions are included in the scope of the independent assessment. • Agree with Health and Social Care Organisation the level of access required, possible timings and availability of their staff to assist the independent assessment. • Agree Terms of Reference & receive formal sign off from sponsor of the review.	• Review Health and Social Care organisation's data security and protection documentation. • Conduct remote and onsite DSP Toolkit assessment utilising evidence provided through the DSP Toolkit. • Document observations and issues as they are identified throughout the DSP Toolkit review. • Discuss with Health and Social Care Organisation their responses, practices and controls as well as address outstanding requests.	• Finalise observations, issues and recommendations including the risk rating of issues. • Prepare the final report and associated working papers. • Complete a closing meeting with the Health and Social Care Organisation to discuss issues and recommendations. • Encourage shadowing, training and knowledge transfer to enable your staff to understand the assessment process consistently and effectively.	• Coordinate any further discussion required with Health & Social Care Organisation. • Ensure agreed recommendations and Health and Social Care actions (in response to recommendations) are tracked and monitored.
Outcome	• Engaged Health and Social Care Organisation sponsor and stakeholders. • Engaged DSP Toolkit independent assessment providers	• Draft Terms of Reference and receive comments from sponsor of the review, including all other nominated stakeholders. • Staff knowledge transfer- where a previous independent assessment was completed by another Internal Auditor Assessment Provider. • Finalise and receive formal sign off of the DSP Toolkit independent assessment Terms of Reference.	• Begin drafting DSP Toolkit Working Papers. • Quantified measure of risk and confidence.	• Draft Assessment report including observations, issues and recommendations. • Finalise DSP Toolkit report. • Informed discussion on how to improve data security and protection controls.	• Independent assessment providers to maintain their own audit trail and files. • Updated issues and recommendations.

3.2.1.2 - Understanding Risk (Risk Fundamentals)

This section provides an introduction to evaluating and quantifying risk, as well as serving as a refresher for those with previous experience in this discipline.

Understanding risk

For the purpose of this Guide for DSP Toolkit independent assessment providers, the following definition of Risk should be used:

> "Risk is the effect of uncertainty on objectives."

This definition of risk can be explained using a combination of two key determinants: the likelihood of a certain event occurring (an expression of the 'uncertainty' in the definition above) and the impact such an event would have on the achievement of one or more objectives. Exploring these two key determinants further, the Guide for DSP independent assessment providers defines **likelihood** as follows:

> "The chance that weaknesses in a set of controls, that make up an evidence text, results in a data security and protection incident or breach"

The definition of **impact** is as follows:

> "Impact is the magnitude of harm to an organisation that could result from a successful threat or breach occurring."

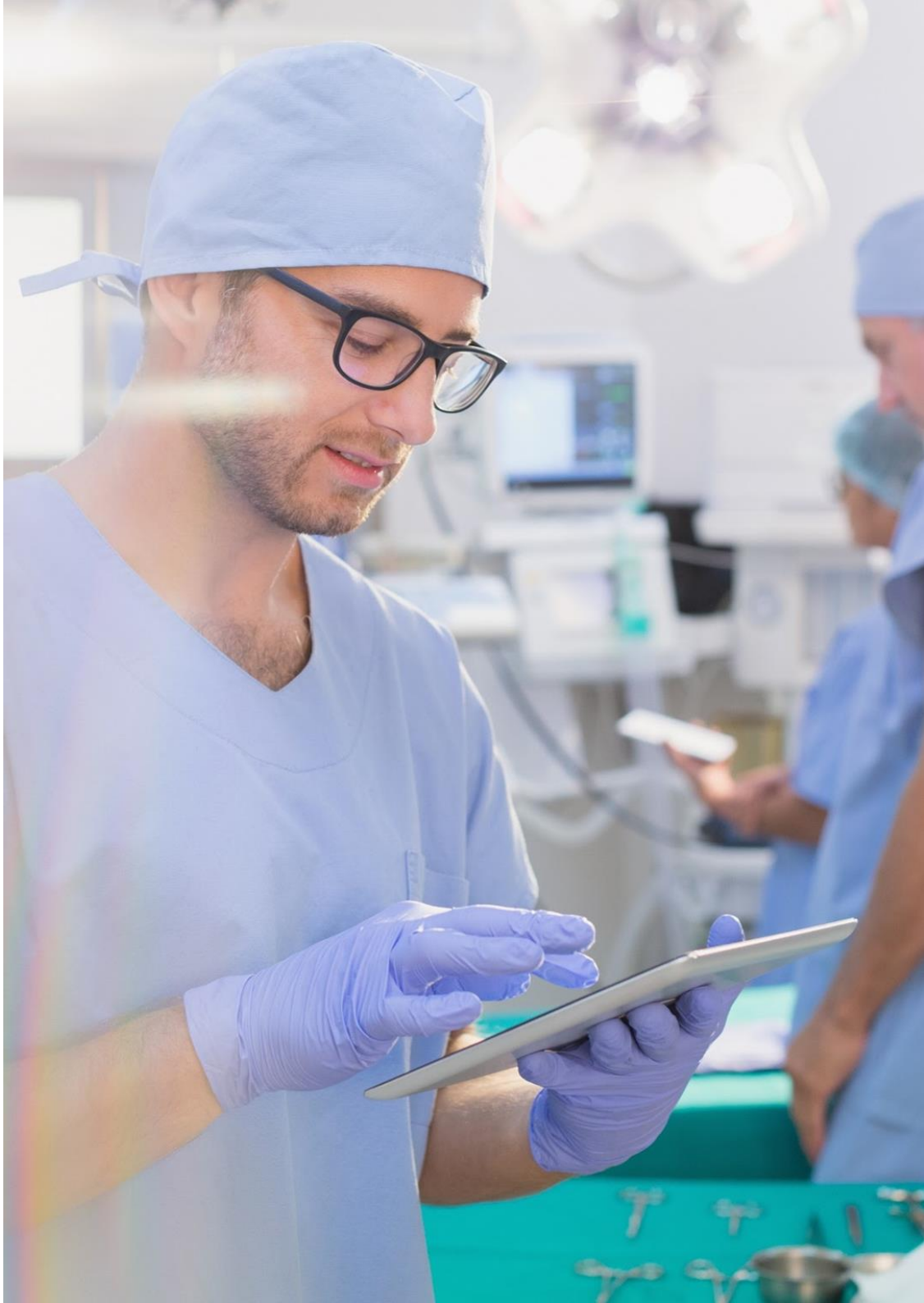
The risk rating is determined at evidence text item level and comprises two elements; likelihood and impact.

The Guide for DSP Toolkit independent assessment providers is designed to assess data security and protection risk, which is defined as:

> "Data security and protection risk is the risk to the organisation's achievement of its objective of preserving confidentiality, integrity and availability of data assets.

To allow the DSP Toolkit independent assessment provider to assess overall data security and protection risk, the risk equation is expanded to cover three important tasks that align to the DSP Toolkit independent assessment Workflow. What this means is that the DSP Toolkit Independent Assessment Methodology has been designed in a task-by-task format to provide Independent Assessors with the guidance they require to assess likelihood, impact and the final risk rating.

3.2.2 Task Two: Scope DSP Toolkit Independent Assessment



3.2.2.1 - Detailed Scoping Meeting to Agree Terms of Reference

Detailed Scoping Meeting

For each DSP Toolkit Independent Assessment, it is essential that the DSP Toolkit Internal Assessment Provider considers the NHS England recommended list of DSP Toolkit Assertions.

For DSP Toolkit Internal Auditors, the Health and Social Care Organisation will be the Audit Sponsor. This means a Health and Social Care Director, responsible for the service area under review, will be responsible for reviewing and signing a draft and final copy of the DSP Toolkit Terms of Reference.

The scoping meeting should be attended by the DSP Toolkit Independent Assessment Provider and the person(s) responsible for signing the draft and final copies of the Terms of Reference. Additional stakeholders may also be invited.

The objective of the DSP Toolkit Scoping meeting will be to cover, as a minimum, the following:

People	Responsibilities and accountabilities for data security and protection controls (i.e. those assertions that the Independent Assessment Provider will assess).
In-scope control Environment	Health and Social Care organisation services or processes in-scope for assessment.
Systems and data	Technology application(s) supporting the organisation service or process in-scope for assessment. Please also discuss the best possible route for accessing systems and data (i.e. onsite or though walkthrough of applications). E.g. How to access in-scope systems.
Laws and Regulations	Applicable laws and regulations relevant to the Data Security and Protection controls the Health and Social Care organisation, including how the organisation ensures ongoing compliance with them.
Efficiency and Effectiveness	Activities, projects or larger programmes of work currently underway that will impact the data security and protection environment in which the Health and Social Care organisation operates.

3.2.2.1 - Detailed Scoping Meeting to Agree Terms of Reference *continued.*

Terms of Reference

Following the DSP Toolkit Scoping meeting, the DSP Toolkit Independent Assessment Provider is responsible for drafting a Terms of Reference (ToR). ToR templates can follow in-house style templates provided by the DSP Toolkit Independent Organisation. However, Independent Organisations may also want to follow NHS England's recommended ToR template, which can be found in the appendix.

The ToR sets out key risks, the focus and objectives of the DSP Toolkit review, the assessment timetable (including reporting) and a summary of staff to be engaged in the work, along with the review tools and techniques that will be used. The ToR should be presented to the nominated contacts for approval prior to any fieldwork being carried out.

Key Activities in the Scoping Process

	Process Activity	Responsibility	Communication and Timing
Planning	Hold planning meeting	• DSP Toolkit Independent Assessment Provider Senior Manager or Data Security and Protection Specialists. • Health and Social Care key stakeholders (where this is a DSP Toolkit Internal Audit, please include Health and Social Care Organisation. sponsor).	Scoping meetings will involve a DSP Toolkit Independent Assessment Provider Senior Manager (or Data Security and Protection Specialists), the Health and Social Care Sponsor/Director and any operational leads nominated by the Health and Social Care Sponsor or Director. This meeting should be arranged for a minimum of five weeks prior to fieldwork commencing.
	Draft Terms of Reference	• DSP Toolkit Independent Assessment Provider	Draft Terms of Reference will be issued to the Health and Social Care Organisation Sponsor/Director at least four weeks before fieldwork.
	Approve Terms of Reference	• DSP Toolkit Independent Assessment Provider and Health and Social Care Organisation Director.	Comments received from Health and Social Care Sponsor/Director will be responded to by Assessment Provider. A final Terms of Reference will be issued by the Assessment Provider at least two weeks in advance of fieldwork.

3.2.3 Task Three: Deliver DSP Toolkit Independent Assessment

3.2.3.1 – Perform the DSP Toolkit Independent Assessment

Undertaking the DSP Toolkit Independent Assessment

DSP Toolkit Independent Assessment Providers must carry out the fieldwork in line with the agreed Terms of Reference. The method used by the Independent Assessment Provider to deliver each DSP Toolkit review will vary depending on the risks in each auditable unit and the effectiveness of controls. Throughout the fieldwork the DSP Toolkit Independent Assessment Provider will keep Health and Social Care management up to date with emerging findings. A closing meeting must be held with the Internal Audit / independent assessment Health and Social Care organisational Sponsor/Director and key staff involved in the review to confirm findings. This helps ensure that the DSP Toolkit Independent Assessor understands and agrees issues identified and that there are no surprises in the draft and final reports.

Activities in the Fieldwork Process

	Audit Process Activity	Responsibility	Communication and Timing
Fieldwork	Opening meeting	• Health and Social Care Organisation Assessment Sponsor/Director • DSP Toolkit Independent Assessment Provider • Key contacts	An opening meeting will typically involve the DSP Toolkit Independent Assessment Provider, the Health and Social Care Organisation Assessment Sponsor/Director and any operational leads nominated by the Health and Social Care Organisation Assessment Sponsor/Director.
	Identify Controls	• DSP Toolkit Independent Assessment Provider • Key contacts	Fieldwork typically will take place over a 1-2 week period. Ongoing feedback will be provided throughout the assessment in terms of progress including any issues arising.
	Test Controls	• DSP Toolkit Independent Assessment Provider	
	Ongoing communication	• DSP Toolkit Independent Assessment Provider	
	Closing meeting	• DSP Toolkit Independent Assessment Provider • Health and Social Care Organisation Assessment Sponsor/Director	A closing meeting will be held within one week of the completion of fieldwork. The closing meeting will include the DSP Toolkit Independent Assessment Provider Manager, the Internal Auditor / Assessment Provider who carried out the work, the Health and Social Care Organisation Assessment Sponsor/Director and operational leads nominated by the Health and Social Care organisation assessment Sponsor or Director.

3.2.3.1 - Perform the DSP Toolkit Independent Assessment
continued.

The DSP Toolkit Independent Assessment Framework

The DSP Toolkit Independent Assessment Framework is a resource for DSP Toolkit Independent Assessment Providers working with Health and Social Care organisations, which acts as the basis of scoping the terms of reference for each DSP Toolkit assessment. It also helps inform the approach that the independent assessment provider should take during their review, and the evidence that they should request and review as part of their work. For each of the evidence texts within the DSP Toolkit, the DSP Toolkit Independent Assessment Framework outlines the control objective of the evidence text, a step by step guide on how to audit or assess the organisation's control environment against the objective, and an indication as to the documents that the Independent Assessor should request and review as part of their work. It also includes details on whether or not the evidence text is mandatory for each category of health and social care organisation.

The framework is designed to be used by individuals with experience in reviewing data security and data protection control environments, and the assessment approach is not exhaustive. Independent 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. The suggested approach and assessment documentation and evidence that might be expected are for guidance only and should not be considered by the independent assessment provider, nor the assessed health and social care organisation as 'the answer.' There may be alternative means and controls adopted to achieve the desired data security and protection outcomes. Assessed health and social care organisations remain accountable for designing and operating their control environments and are not to use this guidance, which, as stated is deliberately not exhaustive, as their 'control design' – they should focus on the most efficacious ways in which data security outcomes can be achieved in their particular operating environment and circumstances.

How to use the DSP Toolkit Independent Assessment Framework

The DSP Toolkit Independent Assessment Framework is provided as an interactive PDF document for ease of navigation. In order to locate a specific assertion, the independent assessment provider should follow the link from the navigation page for the relevant standard. The navigation page for each standard provides links to each assertion within the standard, as well as links to any relevant regulations and guidance. Within each assertion, the independent assessment provider can navigate between the four categories of organisation so that only the relevant evidence texts are considered. A definition of NHS England's DSP Toolkit category types can be found overleaf and also at: https://www.dsptoolkit.nhs.uk/Help/5

The DSP Toolkit independent assessment provider should review the information provided in the DSP Toolkit Independent Assessment Framework for each evidence text they will be auditing or assessing prior to commencing work. This should prevent independent assessment providers requesting information or documentation that has already been provided by the organisation. The team conducting the assessment should identify the individuals responsible for testing each evidence text to ensure that individuals with specialist skills (e.g. data protection, network security) are testing the relevant evidence texts.

From the 'assessment documentation' columns in the relevant evidence texts, a document request list should be compiled prior to conducting the assessment. The evidence requested should provide context around the relevant data security and protection controls, and help identify areas that may require greater attention during the assessment. The testing of a small number of evidence texts may be able to be conducted entirely through document review.

3.2.3.1 - Perform the DSP Toolkit Independent Assessment

continued.

How to use the DSP Toolkit Independent Assessment Framework (continued)

Following the initial review of documentation, the independent assessment provider should examine each evidence text within scope of the review by following the assessment approach outlined in the DSP Toolkit Independent Assessment Framework. Where relevant, the Independent Assessor is expected to use their professional judgement and expertise in tailoring the assessment approach for each evidence text, to the organisation being reviewed. When this is the case, the Independent Assessor should document additional assessment steps performed in their working papers.

During fieldwork, the independent assessment provider should ensure that they review and document sufficient evidence to support their conclusions for each evidence text and assertion, using the assessment documentation outlined in the DSP Toolkit Independent Assessment Framework as a guide. The Independent Assessor should exercise their professional judgement as to whether additional evidence is required.

It is essential that the review considers **whether the Health and Social Care Organisation meets the requirement of each evidence text**, and also considers the broader **maturity of the organisation's data security and protection control environment**.

Details on how the observations against each evidence text and assertion should be risk assessed, and translated into findings in the report, are outlined on the following pages.

3.2.3.2 - Perform Risk and Confidence Evaluations

Risk and Confidence Evaluation Workflow

The diagram / process flow below provides an overview of the steps that should be taken in evaluating the effectiveness of an organisation's data security controls in the scope of the independent assessment (overall risk rating), and the veracity of the organisation's DSP Toolkit response (confidence level). It should be noted that although the confidence level provides an indicator of the organisation's ability to accurately represent their security posture in their DSP Toolkit submission, it is the overall risk assurance rating that is the primary indicator of the strength of the organisation's data security and protection control environment. Both outputs are important as regards the goals of this work – to strengthen assurance (the confidence level helps with this respect) and to foster and create a culture of improvement (the overall risk rating and those evidence text-level, assertion-level and standards-level assessments of risk that make this up help with the culture of improving security and focusing improvement efforts in the right areas). Further detail on the process of evaluating both the overall risk rating and confidence level is provided in subsequent pages, including the tables referred to below. *In order to provide further clarity on how risk ratings for individual evidence text items, assertions and each standard are determined, an example is provided in the Appendix. This example also describes how the overall risk rating is calculated. The flowchart below summarises the key steps to be followed, and key reference materials (Tables 1 - 7) to be used, to calculate risk and confidence level ratings.*

Process for determining Overall Risk and Confidence Ratings

Complete fieldwork observations / assessment of evidence for in-scope evidence texts / controls	The Independent Assessor completes on-site/remote fieldwork to *examine the in-scope evidence texts and the effectiveness of the controls* associated with each in-scope evidence text.
Evidence Text level **Likelihood** evaluation	The Independent Assessor uses **Table 1** to evaluate *the chance that weaknesses in a control or set of controls, that make up an evidence text, results in a data security and protection incident or breach.*
Evidence Text level **Impact** evaluation	The Independent Assessor uses **Table 2** to determine *the magnitude of harm to an organisation that could result from a successful threat occurring.* The impact evaluation is also performed at the evidence text level.
Determine **Evidence Text** Risk rating	The Independent Assessor uses **Table 3** as a 'look-up table' to *assign each evidence text a risk rating of 'Extreme', 'High', 'Medium, or 'Low' (or 'Not Reportable').*
Determine **Assertion** level Risk rating	The Independent Assessor considers the risk ratings for each in-scope evidence text making up an assertion. The Independent Assessor exercises professional judgement *to assign each assertion a risk rating of 'Critical', 'High', 'Medium' or 'Low'* based on the evidence text ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place. The Independent Assessor then uses **Table 4** to *assign a score for each assertion* to be used in the calculation of NDG Standard level risk.
Determine **NDG Standard** level Risk rating	The Independent Assessor calculates *the aggregate (total) score across the number of in-scope assertions for each standard and divides this by the number of in-scope assertions for each standard to get a mean score per standard.* **Table 5** is then used as a look-up table to assign a risk rating to each NDG standard.
Determine **Overall Risk Assurance** rating	The Independent Assessor refers to **Table 6** to determine *the overall risk assurance rating, which is based on the number and severity of standard level risk ratings.*
Confidence-level	
Compare assertion, standard and overall risk rating	The Independent Assessor *conducts a high-level, subjective assessment of the veracity of the organisation's DSP Toolkit submission*, based on the evidence text, assertion, standard and overall risk evaluations in the independent assessment.
Assign confidence level	The Independent Assessor then refers to **Table 7** and exercises professional judgement to assign *a confidence level as to the veracity of the organisation's DSP Toolkit submission.* This can inform an assurance level or assurance rating.

3.2.3.2 - Perform Risk and Confidence Evaluations *continued.*

Once the previous tasks have been completed, the DSP Toolkit Independent Assessment Provider can progress to the Risk Evaluation task. The next three pages provide the detail behind the high-level diagram on the previous page, which suggests how independent assessment providers could calculate the assessment's overall risk rating, as well as the confidence level in the most recent DSP Toolkit submission.

The risk evaluation aims to support the reporting of two outputs; a measure of risk based on how effectively the DSP Toolkit control objectives are achieved; and a measure of confidence in the organisation's DSP Toolkit submission / self-assessment.

How to evaluate the risk and confidence ratings?

As outlined in the previous page, the first step in evaluating the overall risk rating, is to determine the likelihood that the failure to meet the control objectives results in a data security and protection incident. The impact of such an incident on the organisation should then be considered.

Recap: The Risk Equation

Prior to commencing this task, it is worth revisiting how risks are assessed using the Risk equation. The risk equation, as introduced earlier in this document, is comprised of two key elements; likelihood and impact.

This equation is applied at the granular, evidence text level in this suggested methodology and then uses a look-up table to assign a risk rating.

How to derive the likelihood rating?

It is the responsibility of the DSP Toolkit Independent Assessment Provider to complete their DSP Toolkit assessment using the Independent Assessment Framework. Once all DSP Toolkit evidence text items, included in the scope of the DSP Toolkit review, have been assessed, the Independent Assessment Provider can begin assigning a breach or incident likelihood rating. A likelihood rating can be defined as follows:

> "The chance that weaknesses in a control or set of controls, that make up an evidence text, results in a data security or data protection incident or breach."

To derive the likelihood rating for each evidence text, the DSP Toolkit Independent Assessment Provider should select one of the following assessment rationale statements which best describes the conclusion formed following their assessment of the evidence text related controls failing in the next year..

Table 1. Likelihood Assessment (Evidence Text)

<< Return to Risk and Confidence Evaluation workflow

Likelihood rating	Assessment rationale
Almost Certain	Almost certain to happen in the next 12 months (80% or more)
Likely	Likely to happen in the next 12 months (60-80%)
Moderate	Moderately likely to happen in the next 12 months (40-60%)
Unlikely	Unlikely to happen in the next 12 months (20-40%)
Rare	Very low likelihood to happen in the next 12 months (less than 20%)

3.2.3.2 - Perform Risk and Confidence Evaluations *continued.*

<< Return to Risk and Confidence Evaluation workflow

How to derive the Impact Rating?

Once all DSP Toolkit evidence texts included in the scope of the DSP Toolkit review have been assessed (following guidance relating to the control objectives, approach and assessment documentation included in the Independent Assessment Framework) and all findings are recorded in the Assessment Risk and Controls Template), the Independent Assessment Provider can begin assigning an Impact rating. An Impact rating can be defined as follows:

"The magnitude of harm to an organisation that could result from a successful threat occurring."

To derive the impact rating for each evidence text, the DSP Toolkit Independent Assessment Provider should select one of the following impact ratings and assessment rationale statements (see table 2) which best describes the conclusion formed following the assessment of each evidence text. Please also refer to guidance relating to the control objectives, approach and assessment documentation included in the Independent Assessment Framework.

Note to DSP Toolkit Independent Assessment Providers

In assessing the likelihood that controls that make up an evidence text fail and result in a data security and protection incident or breach; and, in also assessing the impact of that breach, the Independent Assessor will need to exercise professional judgement and need to apply an understanding of the organisation and what aspect of the delivery of care the control or evidence text relates to. As regards likelihood, the Independent Assessor will need to understand the plans for the organisation for the next year as regards continued absence of controls, planned implementation of controls or changes that may affect or negate controls that are currently operating. The Independent Assessor will need to deal with a degree of uncertainty and subjectivity in the likelihood measure. Assessing the impact will also involve a degree of judgement and subjectivity but could be less problematic than assessing likelihood.

The Independent Assessor will also need to consider the nature of the control. For example, the Independent Assessor may identify instances of unsupported versions of applications. However, if this application does not support the organisation's key patient-facing services or business operations, or there is another mitigating control such as network segregation, it should not be considered as having a critical or significant likelihood rating. When examining evidence texts to aid in determining assertion ratings, it is imperative that the Independent Assessor exercises their professional judgement and does not rely solely on the toolkit examples provided. For instance, whilst a documented policy may be listed within the toolkit as a requirement but is not evident in the reviewed organisation, the impact of this may not be as significant as the absence of other controls. Poor and missing policy documentation can be a proxy or indicator for sub-standard data security and protection and may make it harder for individuals in the organisation to operate and implement more technical controls appropriately. However, it could be possible that a policy is missing but the technological controls are adequate despite this. One example may be a non-documented password policy that is technically enforced through group policy. Whilst the policy omission may impact general user awareness and cyber security training, the underlying risk mitigation strategy regarding strong access control mechanisms might be satisfied through technical means. In this way, it is expected that Independent Assessors will weigh up the relative importance of different types of controls for delivery of care and cyber threat management when considering impact and likelihood of breaches. Policy and IG controls are important, of course, but Independent Assessors must exercise judgement around impact so as not to over-state risk when using a methodology that aims to 'surface' unacceptable risk and unsatisfactory control environments / critical issues.

Table 2. Impact Assessment (Evidence Text)

Impact rating	Assessment rationale
Catastrophic	A **Catastrophic Impact Finding** could apply to Health and Social Care organisations that use extremely complex technologies to deliver multiple services or process large volumes of patient data, including processing for other organisations. Many of the services are at the highest level of risk, including those offered to other organisations. New and emerging technologies are utilised across multiple delivery channels. The organisation is responsible for/ maintains nearly all connection types to transfer/store/process personal, patient identifiable and/or business-critical data with customers and third parties. A catastrophic finding that could have a: Catastrophic impact on operational performance or the ability to deliver services / care; or Catastrophic monetary or financial statement impact; or Catastrophic breach in laws and regulations that could result in material fines or consequences; or Catastrophic impact on the reputation or brand of the organisation which could threaten its future viability.
Major	A **Major Impact Finding** could apply to a Health and Social Care organisation that uses complex technology in terms of scope and sophistication. The organisation may offer high-risk products and services that may include emerging technologies. The organisation is responsible for/ maintains the largest proportion of connection types to transfer/store/process personal, patient identifiable or business-critical data with customers and third parties; other organisations and/or third-parties are responsible for/maintain a low proportion of connection types. A Significant finding that could have a: • Major impact on operational performance; or • Major monetary or financial statement impact; or • Major breach in laws and regulations resulting in large fines and consequences; or • Major impact on the reputation or brand of the organisation.
Moderate	A **Moderate Impact Finding** could apply to a Health and Social Care organisation that uses technology which may be somewhat complex in terms of volume and sophistication. The organisation is responsible for/maintains a some connection types to transfer/store/process personal, patient identifiable and/or business-critical data with customers and third parties; other organisations and/or third-parties are responsible for/maintain a most of the organisation's connection types. A Moderate finding that could have a: • Moderate impact on the organisation's operational performance; or • Moderate monetary or financial statement impact; or • Moderate breach in laws and regulations with moderate consequences; or • Moderate impact on the reputation of the organisation.
Minor	A **Minor Impact Finding** could apply to a Health and Social Care organisation with limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services. The institution primarily uses established technologies. It is responsible for/maintains minimal numbers of connection types to transfer/store/process personal, patient identifiable or business-critical data too customers and third parties; other organisations and/or third-parties are largely responsible for/maintain connection types. A Minor finding that could have a: • Minor impact on the organisation's operational performance; or • Minor monetary or financial statement impact; or • Minor breach in laws and regulations with limited consequences; or • Minor impact on the reputation of the organisation.
Very Low / Insignificant	A **Low/Insignificant Impact Finding** could apply to a Health and Social Care organisation that has very limited use of technology. The variety of products and services are limited and the organisation has a small geographic footprint with few employees. It is responsible for/maintains no connection types to transfer/store/process personal, patient identifiable or business-critical data too customers and third parties. A Low finding that could have a: • Very low/ insignificant impact on the organisation's operational performance; or • Very low/ insignificant monetary or financial statement impact; or • Very low/ insignificant breach in laws and regulations with little consequence; or • Very low/ insignificant impact on the reputation of the organisation.

3.2.3.2 Perform Risk and Confidence Evaluations *continued.*

How to determine the Evidence Text Risk Rating

The DSP Toolkit Independent Assessment Provider must calculate the risk rating for each in-scope DSP Toolkit evidence text assessed as part of their DSP Toolkit review. Once the Independent Assessment Provider has assigned a likelihood and impact rating to each in-scope and assessed DSP Toolkit evidence text, the following risk rating matrix can be used to allocate a risk rating. This rating reflects the risk of the organisation being unable to meet the control objective as a result of a control failing or the absence or ineffectiveness of a control. For example, if the DSP Toolkit Independent Assessment Provider assigned a Likelihood rating of *'40% - 60%'* and an impact rating of '*Moderate*', the risk rating for the individual evidence text would be 'Low'. The following matrix / 'look-up table' should be used to determine the Evidence Text risk ratings. Issues with a low impact and low likelihood rating should not be reported.

Table 3. Calculation of Evidence Text Risk Rating

<< Return to Risk and Confidence Evaluation workflow

	Impact rating				
Likelihood rating (in next 12 months)	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost Certain	Low	Low	Medium	High	Extreme
Likely	Low	Low	Medium	Medium	High
Moderate	Low	Low	Low	Medium	Medium
Unlikely	Very Low/ Insignificant	Low	Low	Low	**Low**
Rare	Very Low/ Insignificant	Very Low/ Insignificant	Low	**Low**	**Low**

How to determine the Assertion Level Risk Rating

The DSP Toolkit Independent Assessment Provider must then exercise professional judgement to assign a risk rating at the assertion level. The Independent Assessor leverages knowledge and subject matter expertise alongside observations made during the assessment to assign each assertion a risk rating of 'Critical', 'High', 'Medium' or 'Low' based on the evidence text ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating or compensating controls in place. The Independent Assessor then uses **Table 4** to assign a score for each assertion to be used in the calculation of NDG Standard level risk.

How to determine the National Data Guardian (NDG) Standard Risk Rating

The Independent Assessor will calculate an aggregate score and classification for each NDG Standard - i.e. the overall NDG Standard risk rating that will appear in the Executive Summary of the DSP Toolkit Independent Assessment Provider report. That is, the Executive Summary reporting will be at the NDG standard level; providing 10 'scores'; one for each standard. This guide also outlines how an overall risk rating score can be calculated. It is understood that this will be an expectation of key stakeholders to provide an overall risk rating though it should be noted and understood that abstracting scores to a high level and using aggregate or average scores can be very misleading as they can sometimes mask significant or critical issues at the lower levels; i.e. at the assertion level. For some NDG standards there may be multiple assertions in the scope of the independent assessment and for some NDG standards there may only be one assertion in scope. The NDG Standard risk rating is determined by calculating the mean of the total number of assertion level points per NDG Standard. For example, a DSP Toolkit Independent Assessment Provider who assessed 8 DSP Toolkit Assertions aligned to NDG Standard One, may rate 5 assertions as Critical, 2 as High and 1 as a Medium. Using Table 4 below, this gives the DSP Toolkit Independent Assessment Provider a total of 223 points (200 for Critical findings, 20 for High and 3 for Medium = 223 points). These figures should be divided by the number of assertions reviewed and rounded to the nearest one decimal place. In this instance 8 assertions will yield a mean points per assertion of 28 (233 ÷ 8 = 27.9 rounded to one decimal place). Table 5 should then be used to determine the overall NDG Standard Risk Rating, in this instance it would provide an 'Unsatisfactory' classification. This will be done for each NDG standard to support an overall risk rating.

Table 4. Points corresponding to Assertion Risk Ratings

Rating	Points for each Assertion
Critical	40
High	10
Medium	3
Low	1

Table 5. Calculation and Assignment of the NDG Standard Risk Ratings

<< Return to Risk and Confidence Evaluation workflow

Overall NDG Standard Risk Assurance Rating Classification		Rating Thresholds when only **1 assertion per NDG Standard** is in scope	Rating Thresholds when **2 or more assertions** are in scope for each NDG Standard. Mean score is to be used (Total points divided by the number of in-scope assertions)
●	Substantial	1 or less	1 or less
●	Moderate	Greater than 1, less than 10	Greater than 1, less than 4
●	Limited	Greater than/equal to 10, less than 40	Greater than/equal to 4, less than 5.9
●	Unsatisfactory	40 and above	5.9 and above

3.2.3.2 Perform Risk and Confidence Evaluations *continued.*

How to determine the Overall Risk Assurance Rating

Once the Independent Assessment Provider has calculated the risk assurance rating for each Standard the following principle can be used to allocate an overall risk assurance rating.

The DSP Toolkit Independent Assessment Provider should calculate the overall risk rating of the organisation's data security and protection control environment, for the in-scope assessments. Table 6 below allows the independent assessment provider to conduct this calculation.

Table 6. Determination of Overall Risk Assurance Rating

<< Return to Risk and Confidence Evaluation workflow

Overall risk rating across all in-scope standards	
Unsatisfactory	1 or more Standards is rated as 'Unsatisfactory'
Limited	No standards are rated as 'Unsatisfactory', but 2 or more are rated as 'Limited'
Moderate	There are no standards rated as 'Unsatisfactory', and 1 or none rated as 'Limited'. However, not all standards are rated as 'Substantial'.
Substantial	All of the standards are rated as 'Substantial'

How to determine the Overall Confidence-level in the veracity of the organisation's self-assessment / DSP Toolkit submission

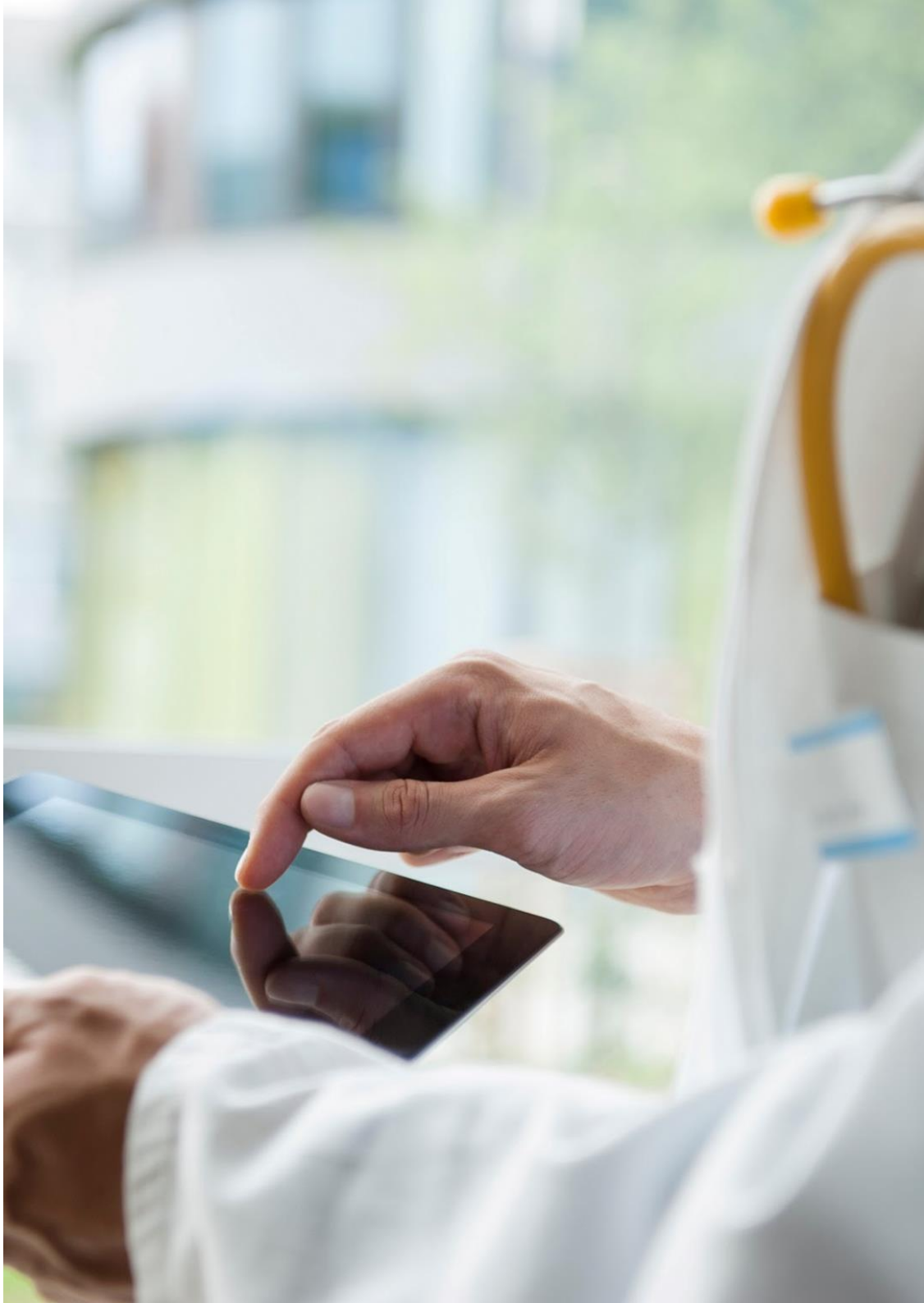
Once the Independent Assessment Provider has completed the fieldwork and calculated the ratings for assertions, for each of the 10 NDG standards and the overall risk, the confidence-level in the veracity of the organisation's DSP Toolkit self-assessment submission should be determined by comparing the independent assessment findings against the latest DSP Toolkit submission. The following definitions should be used for aiding the decision of applying a confidence-level. It is noted that the evidence available to the Independent Assessor at the time of the assessment may differ or may have changed from the evidence in place at the time of the self-assessment. Furthermore, the self-assessment may not have much in the way of evidence. As such the Independent Assessor will need to take that into consideration when determining the confidence level and when writing the report and putting it into context. i.e. a like for like comparison may not be possible so the self-assessment and independent assessment may differ but not necessarily due to a lack of veracity or honesty in the self-assessment.

Table 7. Determination of confidence-level in the veracity of the organisation's self-assessment / DSP Toolkit submission

<< Return to Risk and Confidence Evaluation workflow

Level of deviation from the DSP Toolkit submission and assessment findings	Confidence-level
High level of deviation - the organisation's self-assessment against the Toolkit differs significantly from the Independent Assessment For example, the organisation has declared as "Standards Met" or "Standards Exceeded" but the independent assessment has found individual NDG standards as 'Unsatisfactory' and the overall rating is 'Unsatisfactory'.	Low
Medium level of deviation - the organisation's self-assessment against the Toolkit differs somewhat from the Independent Assessment For example, the Independent Assessor has exercised professional judgement in comparing the self-assessment to their independent assessment and there is a non-trivial deviation or discord between the two.	Medium
Low level of deviation- the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment	High

3.2.4 Task Four: Post-DSP Toolkit Review Meeting & Reporting



3.2.4.1 Draft & Finalise report

Preparing a Draft Report

Reporting is a crucial part of the DSP Toolkit Independent Assessment Provider process and involves both verbal and written communication. Underpinning all of the DSP Toolkit reporting and broader communications are the following principles:

- **'No surprises' –** The DSP Toolkit Independent Assessment Provider will always ensure that findings are discussed with management prior to issuing draft reports. The DSP Toolkit Independent Assessment Provider will always seek to obtain full 'buy in' of management to recommendations to support successful implementation;
- **Clarity and consistency –** The DSP Toolkit Independent Assessment Provider will avoid unnecessary jargon and will not shy away from setting out the key issues or themes arising from the work in clear, unambiguous terms;
- **Objectivity –** The DSP Toolkit Independent Assessment Provider will use a standard scoring mechanism for all findings and for determining the overall rating of a report. This objective approach will be transparent and consistent across all reports;
- **Pragmatic and informed actions –** The DSP Toolkit Independent Assessment Provider will not provide recommendations that run the risk of not being implemented. Rather, in the closing meeting of the audit the DSP Toolkit Independent Assessment Provider will agree pragmatic, proportionate and realistic actions with the sponsor and include those in the DSP Toolkit Independent Assessment Provider report as the responses to each finding that is identified, along with responsible people and target dates for those actions;
- **Prioritisation –** the format of reporting needs to provide a clear steer as to the relative importance of the issues being reported.
- **Coaching towards improvement** – discussion of the emerging findings, draft report and draft recommendations will afford the opportunity for the independent assessment provider to coach the organisation as regards good practice observed elsewhere and potential options for addressing controls weaknesses and generally helping improve data security and data protection. This is a critical feature of the assessments as they should move the organisation towards achievement of improved data security and protection outcomes; and the objective of safeguarding the confidentiality, integrity and availability of data assets.

The basic process for reporting after each assessment is shown below:

	Audit Process Activity	Responsibility	Communication and Timing
Reporting	Draft report.	• The DSP Toolkit Independent Assessment Provider.	Draft report to be issued to Health and Social Care Sponsor/Director two weeks after closing meeting.
	Review report.	• Health and Social Care Sponsor/Director of review.	Health and Social Care Sponsor/Director to provide feedback including relevant actions, responsible officers and target implementation dates. Feedback to be provided within two weeks of the draft report being issued.
	Issue final report.	• The DSP Toolkit Independent Assessment Provider.	The DSP Toolkit Independent Assessment Provider to issue final report within one week of receiving management responses.
	Present final report to Audit and Risk Committee.	• The DSP Toolkit Independent Assessment Provider. • Health and Social Care Sponsor (if required).	Full report circulated and presented at the next scheduled quarterly Audit and Risk Committee meeting.

3.2.4.2 - Issue Tracking & Follow-Up Work

Follow Up

All agreed recommendations arising from the DSP Toolkit Independent Assessment Provider work should be tracked to ensure their successful implementation. This is a critical element of the DSP Toolkit Independent Assessment Provider's work and one which in some organisations is not afforded the attention required.

There are a number of ways that the DSP Toolkit Independent Assessment Provider can work with the Health and Social Care organisation to ensure a slick and effective follow-up process. Typically, this might involve continued work with the Health and Social Care organisation sponsor/director and/or the Head of Risk, Regulation and Performance to ensure the implementation of agreed actions resulting from DSP Toolkit Independent Assessment Provider reviews.

Typically, on an annual, bi-annual, or even quarterly basis, the DSP Toolkit Independent Assessment Provider should follow up on all due actions to verify management's self-assessment of progress against these. This will involve looking at documentary evidence and re-performing testing. Recommendations will only be closed once we are content that the action has been addressed in full and the risk mitigated.

The DSP Toolkit Independent Assessment Provider should use the Health and Social Cares internal follow up process (where necessary). However, where this is not the case, the DSP Toolkit Independent Assessment Provider may provide bespoke tools to support this process.

In some cases, where there have been areas of specific concern raised or an identified need to re-assess the robustness of processes and controls the DSP Toolkit, the Independent Assessment Provider should also conduct specific follow-up reviews. In any such case, the DSP Toolkit Independent Assessment Provider would seek to engage with NHS England Service management Team and the Health and Social Care sponsor/director to ensure that this is the best use of the Independent Assessment Providers time.

N.B. It is expected that much of the follow-up activity will be facilitated or performed by the organisation's internal auditor, though NHS England will share findings, reports and generally enable the follow-up by the internal auditor.

3.2.5 Task Five: Assessment Finalisation and Quality Management

3.2.5.1 - Skills and Training

It is expected that during the reporting phase that knowledge gaps and learning and development needs are likely to be identified for the assessed organisation. The Independent Assessor is also expected to identify anything of interest to other Independent Assessors to help them improve the way they deliver assessments, consistent with the culture of improvement desired in data security and protection.

Independent Organisations and Assessment Provider skills development

DSP Toolkit Independent Assessment Providers, whatever their status or background, will have personnel with training and development needs.

DSP Toolkit Independent Assessment Providers with new joiners or existing personnel who have never completed a NHS England DSP Toolkit Independent Assessment will need induction training, to help them understand their role and the auditee organisation(s). All induction training is the responsibility of the employing organisation; be they a DSP Toolkit Independent organisation or an Assessment Service Provider.

In particular, Independent Organisations and Assessment Providers with no prior experience of government and Health and Social Care DSP Toolkit Independent Assessments will need training to help them understand the Health and Social Care sector accountability framework, especially those elements relating to governance and accountability. It is recognised such organisations may have data security and data protection assessment and improvement capabilities and insights to share from other industries but it is imperative that they understand the health and social care sector. The task to understand the organisational profile and their operating environment is considered critical but even before this task is complete there is a baseline of sector knowledge that is needed before the data security and protection knowledge of the Independent Assessor can be exploited to add value for the organisations assessed and the wider sector.

The Independent Organisation and Assessment Provider should ensure continuous learning plans are in place to develop existing personnel skills and ensure the organisation and provider stay current with the changing technology and threat landscape. In addition, the Independent organisation and Assessment Provider should assist in the implementation of appropriate performance measurement systems.

Training Needs Analysis (TNA)

Following release of NHS England's recommended list of DSP Toolkit assertions, it is the responsibility of the Independent organisation and Assessment Provider to consider the blend of skills and experience and seniority required to fulfil assessment against each assertion. This can be achieved by conducting a Training Needs Analysis (TNA) of Independent Assessment Provider personnel.

A TNA can help Independent organisations or Assessment Providers understand whether there is sufficient capability and knowledge across their existing personnel to closely align to NHS England's requirement for skills and competencies to deliver DSP Toolkit Independent Assessment.

The TNA therefore helps the organisation or provider define the gap between the existing and the required skills and knowledge. The output articulates:

- the gap between current and required skills and knowledge.
- the general content of the required training, including learning methods and delivery of training.

4. What is the Data Security and Protection (DSP) Toolkit?

4.1 - What is the Data Security and Protection (DSP) Toolkit?

The DSP Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards which reflect legal rules and Department of Health policy.

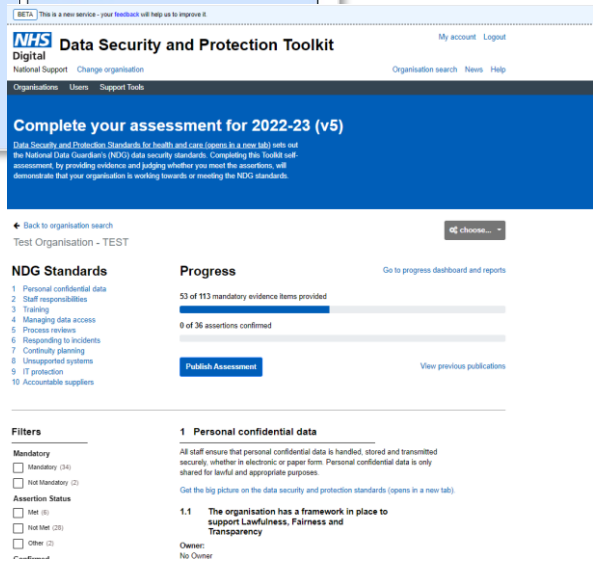
All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled appropriately.

The Toolkit has been developed in response to The National Data Guardian Review (Review of Data Security, Consent and Opt-Outs) published in July 2016 and the government response published in July 2017.

The Data Security and Protection Toolkit is the successor framework to the Information Governance Toolkit ('IGT', IG Toolkit').

Currently in its fifth iteration, the DSP Toolkit has been updated to reflect the key trends within information security and data protection. As such, assurance against an organisation's submission will be retrospective, yet provide insight to the forthcoming version of the DSP Toolkit to address the emerging trends identified within the Health and Social Care environment.

With approximately 48,000 submissions annually from a range of organisation types the assurance across the self-assessments needs to be obtained to advise future information security programmes.



The IG Toolkit (above) has been replaced with the DSP Toolkit (right).

Appendices

Note The examples are for illustrative purposes and may not reflect the current assertion wording and fixed scope

Information and technology
for better health and care

Appendix i. DSP Toolkit Independent Assessment Provider Risk and Control Template & Matrix

DSP Toolkit Independent Assessment Risk and Controls Matrix

Note This is for illustrative purposes and may not reflect the current assertion wording and fixed scope

DSP Toolkit Independent Assessment Framework Guidance						Assessment Results: to be completed by Independent Assessment Provider			
Assertion	Evidence Ref.	Evidence Text (CAT 1)	Control Objective	Approach	Assessment Documentation	Service or processes in-scope for assessment.	Technology application (s) supporting the service or process in-scope for assessment.		Control effectiveness conclusion (results of assessment).
Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS England guidance.	10.2.1	Organisations ensure that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.	The organisation confirms that the supplier has the appropriate information security accreditations/ certifications, prior to signing the contract. The NHS Improvement 2017/18 Data Security Protection Requirements: guidance, states that these could include; ISO 27001:2013, Cyber Essentials, Cyber Essentials Plus, or the Digital Marketplace.	1. Determine if the organisation has formally documented the accreditations/certifications it requires suppliers that provide health and social care services, or have access to the organisation's data, to have obtained prior to signing the contract. Review this document and assess whether the requirements are appropriate. For example, Cyber Essentials may not be sufficient for a supplier with whom a large volume of sensitive patient data is shared. 2. For a sample of in-scope suppliers, review evidence that the accreditations/certifications were sought prior to onboarding, and are requested on at least an annual basis.	1. Supplier requirements document 2. Sample of supplier accreditations/certifications, including detail on their scope.	Finance	ERP Application		Link to working conclusion
						HR	Active Directory		Link to working conclusion

Appendix ii. Example DSP Toolkit Independent Assessment Terms of Reference and Report Templates

DSP Toolkit Independent Assessment Terms of Reference Template

Example

[Health and Social Care Organisation Name]

[DATE]

Information and technology
for better health and care

Independent assessment objectives

Updated guidance was published by NHS Digital in draft form in Autumn 2019. This guidance and any subsequent published updates are to be used by DSP Toolkit independent assessment providers, including internal auditors, when assessing DSP Toolkit submissions.

It is considered essential that the reviews using this updated guidance consider whether the health and social care organisation in question meets the requirement of each evidence text for each in scope assertion and also considers the broader maturity of the organisation's data security and protection control environment.

Independent assessment outputs

The independent assessment will produce the following outputs:

1. An assessment of the overall risk associated with [the organisation]'s data security and data protection control environment. i.e. the level of risk associated with controls failing and data security and protection objectives not being achieved;
2. An assessment as to the veracity of [the organisation]'s self-assessment / DSP Toolkit submission and the Independent Assessor's level of confidence that the submission aligns to their assessment of the risk and controls.

In essence the first output will be an indicator, for those assertions and evidence items assessed, as to the level of risk to the organisation and how good, or otherwise, the data security and protection environment is in terms of helping the organisation achieve the objectives in the DSP Toolkit. The second output will support an internal audit provider in arriving at the assurance level that they are required to provide, and that the organisation is obliged to provide, as per one of the DSP Toolkit requirements.

It should be noted that although the confidence level provides an indicator of the organisation's ability to accurately represent their security posture in their DSP Toolkit submission, it is the overall risk assurancerating that is the primary indicator of the strength of the organisation's data security and protection control environment. Both outputs are important as regards the goals of this work – to strengthen assurance (the confidence level helps with this respect) and to foster and create a culture of improvement - the overall risk assurance rating and those evidence text-level, assertion-level and standards-level assessments of risk that make this up help with the culture of improving security and focusing improvement efforts in the right areas.

Independent assessment objectives

The risk evaluation output is seen as key to driving the conversations and improvements required. That is, this updated guidance aims to support the following requirements:

1. Better enable NHS organisations to continually improve the quality and consistency of DSP Toolkit submissions across the NHS landscape;
2. Deliver a framework that is adaptable in response to emerging information security, data and health and social care standards;
3. Allow for a range of bodies to deliver independent assessments in a consistent and easily understood fashion;
4. Help drive measurable improvement of data security across the NHS landscape and support annual and incremental improvements in the DSP Toolkit itself;
5. Deliver a framework that better enables and encourages organisations to publish a more granular, evidenced and accurate picture of their organisation's position in terms of data security;
6. Deliver a framework that allows for data security and protection professionals to spend time on-site coaching organisations on security improvement options at the same time as assessing controls and risks;
7. Deliver a framework that helps ensure consistent delivery of 'independent audit', internal audit;
8. Enable and encourage appropriate feedback and dialogue between NHS England and Independent Assessors to help inform NHS wide communications and initiatives to help address common challenges and systemic or thematic security issues and to help inform the development and consumption of NHS England provided national services around data security;
9. Enable leveraging of other sources of assurance across the NHS to reduce the burden on organisations and reduce total effort, cost and help minimise duplication of information gathering.

The objective of this independent assessment from [the organisation]'s perspective is to understand and help address data security and data protection risk and identify opportunities for improvement; whilst also satisfying the annual requirement for an independent assessment of the DSP Toolkit submission.

Assessment Scope

Each assessment delivery with consist of five core tasks and a number of subtasks, shown below.

Full details can be obtained in the overarching framework documentation available at https://www.dsptoolkit.nhs.uk/Help/64

Activities to be carried out during [review timeframe]			[timeframe]	
Task One Pre-assessment Preparation and Information	**Task Two** Scope DSP Toolkit Independent Assessment	**Task Three** Deliver DSP Toolkit Independent Assessment	**Task Four** Post-DSP Toolkit Review Meeting & Reporting	**Task Five** Assessment Finalisation & Quality Management
Obtain Trust details and establish points of contact	Conduct Detailed Scoping Meeting to Agree Terms of Reference & discuss self-assessment	Perform the DSP Toolkit Assessment	Draft & Finalise report	Workshop to present and discuss final report
Request a copy of the self-assessment and identify omissions / areas of weakness	Devise the logistics for the assessment and share document and stakeholder list for the assessment	Perform Risk and Confidence Evaluations (See Appendix [Ref])	Issue tracking & follow up work	Proposing suggested changes to the DSP Toolkit

Detailed assessment approach

Our assessment involves the following steps:

- Obtain access to your organisation's DSP Toolkit self-assessment.
- Discuss the mandatory [X] assertions that will be assessed with your organisation and define the evidence texts that will be examined during the assessment.
- Request and review the documentation provided in relation to evidence texts that are in scope of this assessment prior to the onsite visit.
- Interviewing the relevant stakeholders who are responsible for each of the assertions and evidence texts, the self-assessment responses or people, processes and technology.
- Review the operation of key technical controls on-site using the DSP Toolkit Independent Assessment Framework as well as exercising professional judgement and knowledge of the organisation being assessed

Reporting Approach

Our report will incorporate our on-site observations and the analysis of key evidence provided to us. We will structure the report as follows:

- Use the reporting template as per the 'DSP Toolkit Strengthening Assurance Guide'.
- Where relevant and Independent Assessors challenge the self-assessment; present the level of deviation from the DSP Toolkit submission and assessment findings.
- Explicitly reference facts and observations from our on-site assessment to support our confidence and assurance levels.
- Detail recommendations that management can consider to address weaknesses identified.

Ratings

Our reports will include the following ratings:

- Our **confidence level** in the veracity of your self-assessment / DSP Toolkit submission.
- Our **overall risk assurance rating** as regards your organisation's data security and data protection control environment.

Limitations of scope

The scope of this review will be limited to the [X] assertions defined during the scoping exercise. The assessment will consider whether [the organisation] meets the requirement of each evidence text, and also considers the broader maturity of the organisation's data security and protection control environment. Results will be based on interviews with key stakeholders as well as a review of key documents where necessary to attest controls/processes. As we are assessing the operational effectiveness of a sub-set of assertions, our assessment should not be expected to include all possible internal control weaknesses that an end-to-end comprehensive compliance assessment might identify. We are reliant on the accuracy of what we are told in interviews and what we review in documents. Efforts will be made to validate accuracy only on a subset of evidence texts and therefore there is a dependency on [the organisation] to provide accurate information. Furthermore, onsite verbal recommendations by the Independent Assessor staff do not constitute formal professional advice and should be considered in line with broader observations. Our report will contain recommendations for management consideration to address the weaknesses found.

Key Contacts

Independent assessment team

Name	Title	Role	Contact email	Contact number

Key contacts – [the organisation]

Name	Role	Contact email	Contact number

Timetable and information request

Timetable

Document Request	[date]
Agree timescales and workshops	
Fieldwork start	
Fieldwork completed	
Draft report to client	
Response from client	
Final report to client	

Agreed timescales are subject to the following assumptions:

- All relevant documentation, including source data, reports and procedures, will be made available to us promptly on request.
- Staff and management will make reasonable time available for interviews and will respond promptly to follow-up questions or requests for documentation.

Information request

Prior to the onsite assessment commencing, please share the requested documents that are listed in Appendix [X], or the closest equivalent documents / evidence that you have (we note that terminology and document names / policy titles may differ).

Secure data transmission

We request supporting evidence to be sent to us ahead of the fieldwork start date in order for us to begin our review before any on-site work. To ensure that your information remains secure, we use a [secure end-to-end encryption (AES-256)…]

No patient data should be uploaded / sent … during the assessment. We will not request, nor do we require any patient data in order to deliver the independent assessment.

Onsite interviews

You hold ultimate responsibility for scheduling meetings between the Independent Assessors and the identified [organisational] stakeholders. A typical list of roles and likely assertions for each is listed in Appendix [X] and Appendix [Y].

Please provide use of a secure / confidential room large enough for 2 Independent Assessors plus your identified stakeholders that also has conference calling facilities to host our interviews and include colleagues who are supporting the interviews remotely.

DSP Toolkit Independent Assessment Report Template

Example

[Health and Social Care Organisation Name]

[DATE]

Information and technology
for better health and care

Example Report Template

Contents

1. Introduction	
2. Executive Summary	
3. Key Findings	
4. Appendix A: Independent Assessment Results and Ratings	
5. Appendix B: Overall Risk Assurance Rating and Confidence Level - Worked Example	
6. Appendix C: Copy of Final Terms of Reference	
7. Appendix D: Stakeholders and Meetings Held	
8. Appendix E: Documents Received and Reviewed	
9. Appendix F: Non-reportable items – observations on out of scope matters	

Introduction

Why data security and data protection issues require attention from Independent Assessors

Data and information is a critical business asset that is fundamental to the continued delivery and operation of health and care services across the UK. The Health and Social Care sector must have confidence in the confidentiality, integrity and availability of their data assets. Any personal data collected, stored and processed by public bodies are also subject to specific legal and regulatory requirements. Data security and data protection related incidents are increasing in frequency and severity; with hacking, ransomware, cyber-fraud and accidental data losses all having been observed across the Health and Social Care sector. For example, we need look no further than the WannaCry ransomware attack in May 2017 that impacted NHS bodies and many local authorities' IT services. Although Microsoft released patches to address the vulnerability, many organisations including several across the public sector didn't apply the patches, highlighting an inadequate ability to adapt to new and emerging threats.

The need to demonstrate an ability to defend against, block and withstand cyber-attacks has been amplified by the introduction of the EU Directive on security of Network and Information Systems (NIS Directive) and the EU General Data Protection Regulation (GDPR). The NIS Directive focuses on Critical National Infrastructure and 'Operators of Essential Services'. The GDPR focuses on the processing of EU residents' personal data. As such, it is essential that Health and Social Care sector organisations take proactive measures to defend themselves from cyber-attacks and evidence their ability to do so in line with regulatory and legal requirements.

An additional complexity arises when a Health and Social Care organisation needs to share data. Organisations need to have mutual trust in each other's ability to keep data secure and also have a requirement to take assurance from each other's risk management and information assurance arrangements for this to happen successfully. Not getting this right means that either organisations fail to deliver the benefits of joining up services or put information at increased risk by sharing it insecurely across a wider network. Achieving a realistic understanding of data security and data protection issues is therefore essential to protecting Health and Social Care organisations, personnel, patients and other stakeholders; particularly as the drive to making Health and Social Care services more 'digital' continues.

The DSP Toolkit is one of several mechanisms in place to support Health and Social Care organisations in their ongoing journey to manage data security and data protection risk. The DSP Toolkit allows organisations to measure their performance against the National Data Guardian's ten data security standards, as well as supporting compliance with legal and regulatory requirements (e.g. the GDPR and NIS Directive) and Department of Health and Social Care policy through completion of an annual DSP Toolkit online self-assessment.

Completion of the DSP Toolkit therefore provides Health and Social Care organisations with valuable insight into the technical and operational data security and data protection control environment and relative strengths and weaknesses of those controls. However, the completion of the DSP Toolkit itself by the organisation is not the only mechanism in place to provide the level of comfort Health and Social Care organisation Boards need to achieve a reliable understanding of data security and data protection risk. Another mechanism is to independently assess the data security and protection control environments of health and social care organisations. The role other independent assessment providers play in helping to strengthen the reliance Health and Social Care Organisations Boards, Department of Health and Social Care and NHS England place on the DSP Toolkit submissions is summarised in the National Data Guardian report, 'Review of Data Security, Consent and Opt-Outs and the Care Quality Commission report, Safe data, safe care'. Both reports include the following recommendation: "Arrangements for internal data security audit and external validation should be reviewed and strengthened to a level similar to those assuring financial integrity and accountability" (NDG 6, CQC 6 Table of recommendations). Therefore, it is essential that independent assessment providers, including internal auditors, focus on the assessment of the effectiveness of health and social organisations' data security and protection controls, as opposed to simply focusing on the veracity of their DSP Toolkit submissions.

Data Security and Protection (DSP) Toolkit Independent Assessment Framework (https://www.dsptoolkit.nhs.uk/Help/64)

The framework is designed to be used by individuals with experience in reviewing data security and data protection control environments, and the assessment approach is not intended to be exhaustive or overly prescriptive, though it does aim to promote consistency of approach. Independent 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. It is essential that the review considers whether the Health and Social Care organisation meets the requirement of each evidence text, and also considers the broader maturity of the organisation's data security and protection control environment. It should be noted that some of the framework approach steps go beyond what is asked in the DSP Toolkit. This is intentional and is designed to help inform the Independent Assessor's view of the organisation's broader data security and protection control environment. The intention is to inform and drive measurable improvement of data security across the NHS and not just simply assess compliance with the DSP Toolkit. It is important, particularly for technical controls, that the Independent Assessor does not rely solely on the existence of policies and/or procedures, but reviews the operation of the technical control while on-site. For example, in Evidence Text 8.3.1 ("the organisation has a patch management procedure that enables security patches to be applied at the operating system, database, application and infrastructure levels"), the assessment approach step does not only include a desktop review of the organisation's vulnerability management process, but a review of patching schedules for a sample of endpoints, including servers *(Please note 8.3.1 was out of scope for the assessment relating to this report).* The following page describes the scope and approach of the assessment that this report relates to.

Introduction

Background

Objectives

The independent assessment aimed to produce the following outputs:

1. An assessment of the overall risk associated with the [organisation] data security and data protection control environment. i.e. the level of risk associated with weak or failing controls and data security and protection objectives not being achieved;
2. An assessment as to the veracity of the [organisation] self-assessment / DSP Toolkit submission and the Independent Assessor's level of confidence that the submission aligns to their assessment of the risk and controls.

The objective of this independent assessment from the [organisation] perspective is to understand and help address data security and data protection risk and identify opportunities for improvement; whilst also satisfying the annual requirement for an independent assessment of the DSP Toolkit submission.

Assessment approach

Our assessment comprised of the following high-level steps:

- Prior to our on site assessment, we undertook a review of the [organisation] DSP Toolkit self-assessment.
- A preliminary call was held to cover: the purpose of the assessment; the in-scope / mandatory assertions; and, to agree access to artefacts supporting evidence texts to be examined during the assessment.
- We then reviewed the artefacts provided in relation to our evidence text request, initially focusing on those that are in scope of the mandatory assertions but also taking the time to review additional documentation to aid our understanding of the organisation and enable us to better satisfy the assessment objectives.
- Before visiting the [organisation] , the Data Protection Officer / IG Lead / Cyber Security Lead arranged meetings with key stakeholders listed in Appendix [X].
- Onsite interviews were conducted with the relevant stakeholders responsible for each of the assertions and evidence texts or for self-assessment responses or people, processes and technology involved in the in-scope control environment.
- We then reviewed the operation of a subset of evidence texts relating to each in-scope assertion and key technical controls on-site using the DSP Toolkit Independent Assessment Framework.
- We discussed other security frameworks and standards such as Cyber Essentials, ISO 27001 and CIS, to help identify weaknesses and aid potential remediation efforts.

Executive Summary

DSP Toolkit Independent Assessment Report Outputs

Our review followed the draft Data Security and Protection (DSP) Toolkit Independent Assessment Framework and Guidance published by NHS England [*insert date*]. We have reviewed [number] assertions across the 10 National Data Guardian Standards in the DSP Toolkit. [number] these assertions were pre-determined as in-scope by NHS England. [number] assertions were selected following discussions between [organisation's] information governance stakeholders and the Independent Assessor. We have produced a number of observations and recommendations for each of the in-scope assertions. These are detailed in Appendix [letter] - Independent assessment results and ratings. ***The Executive Summary outlines the two report outputs in line with the guidance and framework methodology and [x] key findings.***

Understanding your report ratings - Overall Risk Assurance Rating

The table below shows the ***'Overall Risk Assessment Across all 10 NDG Standards'*** as well as the ***'Overall NDG Standard Classification'*** based upon the **'Assertion-level Risk Assurance Ratings'**. It includes the calculation of each risk assurance rating by detailing the scores obtained at each assertion level with respect to their category, (Low, Medium, High and Critical). To better understand the 'scoring methodology' please see the worked example in Appendix B.

The overall Risk Assurance Rating for [organisation] is 'Unsatisfactory'. As per the published guidance, the overall rating is 'Unsatisfactory' if one or more of the NDG Standards are rated as 'Unsatisfactory'' (***noted in NDG Standard 2***) (https://www.dsptoolkit.nhs.uk/Help/64). This may seem harsh but is intended to highlight the risk of a data breach and help focus efforts in remediation. The rating is based on a mean risk assurance rating score at the National Data Guardian (NDG) standard level. Scores have been calculated using tables 4 & 5 (see section 4.2.3.2 of the independent assessment Guidance document – [**Please** pay attention to the different rating thresholds when using table 5 to calculate and assign NDG Standard Risk Assurance Rating])

National Data Guardian (NDG) Standard	Number of DSP Toolkit Assertions Assessed by Independent Assessor	Assertion level Risk Assessments				NDG standard level Risk Ratings		Overall DSP Toolkit level Ratings
		Number of Assertions rated **Critical** and (Weighted Risk Score)	Number of Assertions rated **High** and (Weighted Risk Score)	Number of Assertions rated **Medium** and (Weighted Risk Score)	Number of Assertions rated **Low** And (Weighted Risk Score)	Risk Rating Scores [total points/ no. assertions assessed- see table 4.]	Overall Risk Rating at the National Data Guardian Standard level [see table 5.]	**Overall risk assurance across all 10 NDG Standards**
1. Personal Confidential Data	**4 assertions assessed out of 8 in this standard**			4		3	Moderate	Unsatisfactory
2. Staff Responsibilities	**1 of 2**	1				40	Unsatisfactory	
3. Training	**3 of 4**				3	1	Substantial	
4. Managing Data Access	**1 of 5**			1		3	Moderate	
5. Process Reviews	**1 of 3**				1	1	Substantial	
6. Responding to Incidents	**2 of 3**				2	1	Substantial	
7. Continuity Planning	**3 of 3**				3	1	Substantial	
8. Unsupported Systems	**1 of 4**			1		3	Moderate	
9. IT Protection	**3 of 7**				3	1	Substantial	
10. Accountable Suppliers	**1 of 5**			1		3	Moderate	
TOTAL	**20 of 44**	1	-	7	12	-	-	

Executive Summary (continued…)

Understanding your report ratings – Assurance Level

The assurance level for [organisation] (based on the confidence level of the Independent Assessor in the veracity of the self-assessment) is 'Moderate'. This means that the organisation's self-assessment against the Toolkit differs somewhat from what has been observed in the Independent Assessment. For example, the Independent Assessor has exercised professional judgement in comparing the self-assessment to their independent assessment and there is a non-trivial deviation or discord between the two. This may be because there is a difference between the timings of the self-assessment and the independent assessment and also a difference between the evidence available to the Independent Assessor at the time of the assessment and the evidence that supported the self-assessment.

Assessing the veracity of your DSP toolkit self-assessment

Assessment Outputs

	Overall risk assurance across all 10 NDG Standards	Confidence level of the Independent Assessor in the veracity of the self-assessment
Independent Assessment Outputs	**Unsatisfactory**	**Moderate**

Whilst the outputs of our assessment denote an 'Overall risk assurance across all 10 NDG Standards' as 'Unsatisfactory', and an 'Confidence level of the Independent Assessor in the veracity of the self-assessment' as 'Moderate', it is important to detail the contributing factors that lead to these report outputs. The above ratings should not be viewed in too negative a light as it reflects the risk of a data breach as a result of [*one particularly weak but important assertion*] ([*report specific content here*]) and does not reflect the good practice and effective controls (some of which are outlined on the following page). In security, the 'weakest link' principle applies and features in the root cause of incidents.

Direction of Travel

[It is expected that the Independent Assessor will outline under this 'direction of travel' heading the improvements that have been observed or that have changed assertion or NDG standard level compliance ratings since the last self-assessment. This can be important to contextualise the overall rating which could be Limited or Unsatisfactory based on a small number of absent or failing controls that are considered important or high value controls for data security, resilience and data protection. This paragraph can help balance the perceived negative rating by recognising that the organisation is doing a number of things right on the data security and cyber security / resilience agendas and, where appropriate, this paragraph can recognise that the organisation is going in the right direction and that it is common for there to be many requirements to improve].

On the following pages, the Executive Summary also **outlines [X] key findings** and provides further context for the ratings above.

Executive Summary (continued…)

Good Practice:

During our review we noted the following areas of good practice:

[please include text here.]

Key Findings Summary:

The following [X] findings are described in more detail in the following section, but are summarised here as being amongst the most important issues to address in order to improve the data security and data protection control environment at [name of health and social care organisation here.]

The following section expands on the implications of the findings and recommendations for management to consider in order to address these key findings.

Key Findings (1 of 5)

Unsupported Operating System and unapproved applications in use across the network 1

Finding rating

Overall Rating for Finding One	Medium

Related assertions:

Findings
Implications
Recommendations

Appendix A - Independent assessment results and ratings

National Data Guardian Standard 1: Personal Confidential Data – Results (partially completed example)

Evidence Text Ref.	Evidence Text for Category	Health & Social Care org. DSPT Self- Assessment Rating	**Independent Assessor– Evidence Text Risk Assurance Rating** [use look-up table 3]	**Independent Assessor- Assertion Rating** *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Assurance Rating.*
1.2.1	Are there Board approved data security and protection policies in place that follow relevant guidance?	Not Met	Medium	Medium
1.2.2	When were each of the data security and protection policies last updated?	Met	Low	
1.4.1	Provide details of the record or register that details each use or sharing of personal information.	Met	Medium	
1.4.2	When were information flows approved by the Board or equivalent?	Met	Medium	
1.4.3	Provide a list of all systems/information assets holding or sharing personal information.	Met	High	
1.4.4	Is your organisation compliant with the national data opt-out policy?	Met	High	
1.6.1	There is an approved procedure that sets out the organisation's approach to data protection	Not Met	High	
1.6.2	There are technical controls that prevent information from being inappropriately copied or downloaded.	Not Met	Medium	
1.6.3	There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.	Not Met with Plan Agreed	Medium	
1.6.4	Provide the overall findings of the last data protection by design audit.	Not Met	High	
1.6.6	Is a Data Protection Impact Assessment carried out before high risk processing commences?	Not Met with Plan Agreed	Medium	
1.8.1	Does your organisation operate and maintain a risk register that follows an acceptable Information Security risk framework which links to the corporate risk framework?	Not Met with Plan Agreed	Medium	
1.8.2	Senior management have visibility of key risk decisions made throughout the organisation.	Not Met with Plan Agreed	Medium	
1.8.3	What are your top three data security and protection risks?	Met		

National Data Guardian Standard 2: Staff Responsibilities – Results (partially completed example)

Evidence Text Ref.	Evidence Text for Category	Health & Social Care org. DSPT Self-Assessment Rating	**Independent Assessor– Evidence Text Risk Assurance Rating** [use look-up table 3]	**Independent Assessor- Assertion Rating** *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Assurance Rating.*
2.1.1	The organisation has identified and catalogued personal and sensitive information it holds.	Not Met with Plan Agreed	Medium	Medium
2.1.2	When did your organisation last review the list of all systems/information assets holding or sharing personal information?	Not Met with Plan Agreed	Medium	

Appendix B - Overall risk assurance rating and confidence level - worked example

Note The examples are for illustrative purposes and may not reflect the current assertion wording and fixed scope

Evidence Text Risk Assurance Ratings

Evidence Texts are risk assessed on their likelihood and impact based on the assessment rationale in the Impact table below and the Likelihood Table on the following page

Impact rating	Assessment rationale
Catastrophic	A **Catastrophic Impact Finding** could apply to Health and Social Care organisations that use extremely complex technologies to deliver multiple services or process large volumes of patient data, including processing for other organisations. Many of the services are at the highest level of risk, including those offered to other organisations. New and emerging technologies are utilised across multiple delivery channels. The organisation is responsible for/ maintains nearly all connection types to transfer/store/process personal, patient identifiable and/or business-critical data with customers and third parties. A Critical finding that could have a: Catastrophic impact on operational performance or the ability to deliver services / care; or Catastrophic monetary or financial statement impact; or Catastrophic breach in laws and regulations that could result in material fines or consequences; or Catastrophic impact on the reputation or brand of the organisation which could threaten its future viability.
Major	A **Major Impact Finding** could apply to a Health and Social Care organisation that uses complex technology in terms of scope and sophistication. The organisation may offer high-risk products and services that may include emerging technologies. The organisation is responsible for/ maintains the largest proportion of connection types to transfer/store/process personal, patient identifiable or business-critical data with customers and third parties; other organisations and/or third-parties are responsible for/maintain a low proportion of connection types. A Significant finding that could have a: • Major impact on operational performance*;* or • Major monetary or financial statement impact; or • Major breach in laws and regulations resulting in large fines and consequences*;* or • Major impact on the reputation or brand of the organisation.
Moderate	A **Moderate Impact Finding** could apply to a Health and Social Care organisation that uses technology which may be somewhat complex in terms of volume and sophistication. The organisation is responsible for/maintains a some connection types to transfer/store/process personal, patient identifiable and/or business-critical data with customers and third parties; other organisations and/or third-parties are responsible for/maintain a most of the organisation's connection types. A Moderate finding that could have a: • Moderate impact on the organisation's operational performance; or • Moderate monetary or financial statement impact; or • Moderate breach in laws and regulations with moderate consequences; or • Moderate impact on the reputation of the organisation.
Minor	A **Minor Impact Finding** could apply to a Health and Social Care organisation with limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services. The institution primarily uses established technologies. It is responsible for/maintains minimal numbers of connection types to transfer/store/process personal, patient identifiable or business-critical data too customers and third parties; other organisations and/or third-parties are largely responsible for/maintain connection types. A Minor finding that could have a: • Minor impact on the organisation's operational performance; or • Minor monetary or financial statement impact; or • Minor breach in laws and regulations with limited consequences; or • Minor impact on the reputation of the organisation.
Very Low / Insignificant	A **Low/Insignificant Impact Finding** could apply to a Health and Social Care organisation that has very limited use of technology. The variety of products and services are limited and the organisation has a small geographic footprint with few employees. It is responsible for/maintains no connection types to transfer/store/process personal, patient identifiable or business-critical data too customers and third parties. A Low finding that could have a: • Very low/ insignificant impact on the organisation's operational performance; or • Very low/ insignificant monetary or financial statement impact; or • Very low/ insignificant breach in laws and regulations with little consequence; or • Very low/ insignificant impact on the reputation of the organisation.

Risk Assurance Ratings

Evidence texts are risk assessed on their likelihood and impact based on the assessment rationale in the Likelihood table opposite and the Impact table on the previous page.

Likelihood rating	Assessment rationale
Almost Certain	Almost certain to happen in the next 12 months (80% or more)
Likely	Likely to happen in the next 12 months (60-80%)
Moderate	Moderately likely to happen in the next 12 months (40-60%)
Unlikely	Unlikely to happen in the next 12 months (20-40%)
Rare	Very low likelihood to happen in the next 12 months (less than 20%)

How to determine the Evidence Text Risk Assurance Rating

The DSP Toolkit Independent Assessment Provider must calculate the risk assurance rating for each in-scope DSP Toolkit evidence text assessed as part of their DSP Toolkit review. Once the Independent Assessment Provider has assigned a likelihood and impact rating to each assessed DSP Toolkit evidence text, the following risk matrix can be used to allocate a risk assurance rating. This rating reflects the risk of the organisation being unable to meet the evidence text controls objective as a result of a control failing or the absence or ineffectiveness of a control. For example, if the DSP Toolkit Independent Assessment Provider assigned a Likelihood rating of '*40%-60%*' and an impact rating of '*Moderate*', the risk assurance rating for the individual evidence text would be Low.

The following grid should be used to determine the evidence text risk assurance ratings. Issues with a low impact and low likelihood rating should not be considered as report-worthy. However; if the Independent Assessor deemed relevant, such issues may be discussed in the report or included in Appendix F.

Table 3. Assigning Evidence Text Risk Assurance Ratings

	Impact rating				
Likelihood rating (in next 12 months)	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost Certain	Low	Low	Medium	High	Extreme
Likely	Low	Low	Medium	Medium	High
Moderate	Low	Low	Low	Medium	Medium
Unlikely	Very Low/ Insignificant	Low	Low	Low	**Low**
Rare	Very Low/ Insignificant	Very Low/ Insignificant	Low	**Low**	**Low**

How to determine the Assertion Level Risk Assurance Rating

The DSP Toolkit Independent Assessment Provider must then exercise professional judgement to assign a risk assurance rating at the assertion level. The Independent Assessor leverages knowledge and subject matter expertise alongside observations made during the assessment to assign each assertion a risk assurance rating of 'Catastrophic', 'High', 'Medium' or 'Low' based on the evidence text ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place. The Independent Assessor then uses **Table 4** to assign a score for each assertion to be used in the calculation of NDG Standard level risk assurance.

Table 4. Points corresponding to Assertion risk assurance ratings

Rating	Points for each Assertion
Critical	40
High	10
Medium	3
Low	1

How to determine the National Data Guardian (NDG) Standard Risk Assurance Rating

The Independent Assessor will calculate an aggregate score and classification for each NDG Standard - i.e. the overall NDG Standard risk assurance rating that will appear in the Executive Summary of the DSP Toolkit Independent Assessment Provider report. That is, the Executive Summary reporting will be at the NDG standard level; providing 10 'scores'; one for each standard. This guide also outlines how an overall risk assurance rating score can be calculated. It is understood that this will be an expectation of key stakeholders to provide an overall risk assurance rating though it should be noted and understood that abstracting scores to a high level and using aggregate or average scores can be very misleading as they can sometimes mask significant or critical issues at the lower levels; i.e. at the assertion level.

For some NDG standards there may be multiple assertions in the scope of the independent assessment and for some NDG standards there may only be one assertion in scope. The NDG Standard risk assurance rating is determined by calculating the mean of the total number of assertion level points per NDG Standard and then referring to Table 5 to assign a rating. For example, a DSP Toolkit Independent Assessment Provider who assessed 8 DSP Toolkit Assertions aligned to NDG Standard One, may rate 5 assertions as Critical, 2 as High and 1 as a Medium. Using **Table 4**, this gives the DSP Toolkit Independent Assessment Provider a total of 223 points (200 for Extreme findings, 20 for High and 3 for Medium = 223 points). These figures should be divided by the number of assertions reviewed and rounded to the nearest one decimal place. In this instance there are 8 in-scope assertions which will result in a mean points per assertion of 28 (233 ÷ 8 = 27.9 rounded to one decimal place). **Table 5** should then be used to determine the overall NDG Standard risk assurance rating. In this example the rating would lead to an 'Unsatisfactory' classification. This will be done for each NDG standard to support an overall risk assurance rating.

Table 5. Calculation and assignment of the NDG Standard risk ratings

Overall NDG Standard Risk Rating Classification		Rating Thresholds when only 1 assertion per NDG Standard is in scope	Rating Thresholds when 2 or more assertions are in scope for each NDG Standard. Mean score (Total points divided by the number of in-scope assertions)
●	Substantial	1 or less	1 or less
●	Moderate	Greater than 1, less than 10	Greater than 1, less than 4
●	Limited	Greater than/equal to 10, less than 40	Greater than/equal to 4, less than 5.9
●	Unsatisfactory	40 and above	5.9 and above

How to determine the Overall Risk Assurance Rating

Once the Independent Assessment Provider has calculated the risk assurance rating for each Standard the following table can be used to allocate an overall risk assurance rating. Table 6 below allows the independent assessment provider to determine the overall rating.

Table 6. Determination of Overall Risk Assurance Rating

Overall risk rating across all in-scope standards	
Unsatisfactory	1 or more Standards is rated as 'Unsatisfactory'
Limited	No standards are rated as 'Unsatisfactory', but 2 or more are rated as 'Limited'
Moderate	There are no standards rated as 'Unsatisfactory', and 1 or none rated as 'Limited'. However, not all standards are rated as 'Substantial'.
Substantial	All of the standards are rated as 'Substantial'

How to determine the Overall Confidence-level in the veracity of the organisation's self-assessment / DSP Toolkit submission

Once the Independent Assessment Provider has completed the fieldwork and calculated the ratings for assertions, for each of the 10 National Data Guardian Standards and the overall risk assurance rating then the confidence-level in the veracity of the organisation's DSP Toolkit self-assessment submission should be determined by comparing the independent assessment findings against the latest DSP Toolkit submission. The following definitions should be used for aiding the decision of applying a confidence-level.

Table 7. Determination of confidence-level in the veracity of the organisation's self-assessment / DSP Toolkit submission

Level of deviation from the DSP Toolkit submission and assessment findings	Confidence-level
High – the organisation's self-assessment against the Toolkit differs significantly from the Independent Assessment For example, the organisation has declared as "Standards Met" or "Standards Exceeded" but the independent assessment has found individual National Data Guardian Standards as 'Unsatisfactory' and the overall rating is 'Unsatisfactory'.	Low
Medium - the organisation's self-assessment against the Toolkit differs somewhat from the Independent Assessment For example, the Independent Assessor has exercised professional judgement in comparing the self-assessment to their independent assessment and there is a non-trivial deviation or discord between the two.	Medium
Low - the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment	High

Example walkthrough - the calculation of Evidence Text, Assertion, Standard and Overall Risk Assurance Ratings

Section 4.2.3.2 provides detailed guidance on how assertion, National Data Guardian Standards risk ratings and overall risk assurance ratings are calculated. In order to provide further clarity and guidance as to how to arrive at the calculations and use the reference tables, an example is provided below. Full size Tables referenced in this section can be found in Section 4.2.3.2.

1. Determination of Evidence Text Risk Rating

An Independent Assessor finishes on-site fieldwork and assigns likelihood and impact values to each in-scope evidence text, using **Table 1** and **Table 2** respectively. It is important that this calculation is completed after all of the in-scope evidence texts have been evaluated / assessed, as the likelihood of a breach occurring in relation to one failed control can be influenced by mitigating or compensating controls relating to a separate evidence text.

Table 3 is then used to determine the risk rating for each in-scope evidence text. Please see an example below.

National Data Guardian Standard 1 [example taken from pg. 63.]	Likelihood Rating	Impact Rating	Evidence TextRisk Assurance Rating
1.2.1	Likely (40 - 60%)	Sig.	Medium
1.2.2	Rare (< 20%)	Mod.	Low
1.4.1	Unlikely (20 - 40%)	Extreme	Medium
1.4.2	Moderate (40 - 60%)	Sig.	Medium
1.4.3	Likely (60 - 80%)	Critical	High
1.4.4	Almost Certain (>80%)	Sig.	High

Images of the Tables or extracts / partial tables are shown here for illustrative purposes:

Table 1. Likelihood Assessment (Evidence Text)

Likelihood rating	Assessment rationale
Almost Certain	Almost certain to happen in the next 12 months (80% or more)
Likely	Likely to happen in the next 12 months (60-80%)
Moderate	Moderately likely to happen in the next 12 months (40-60%)
Unlikely	Unlikely to happen in the next 12 months (20-40%)
Rare	Very low likelihood to happen in the next 12 months (less than 20%)

Table 2 – Impact Assessment (Evidence Text) Excerpt (1 rating shown, for Full Table: Table 2)

Impact rating	Assessment rationale
Catastrophic	A **Catastrophic Impact Finding** could apply to Health and Social Care organisations that use extremely complex technologies to deliver multiple services or process large volumes of patient data, including processing for other organisations. Many of the services are at the highest level of risk, including those offered to other organisations. New and emerging technologies are utilised across multiple delivery channels. The organisation is responsible for/ maintains nearly all connection types to transfer/store/process personal, patient identifiable and/or business-critical data with customers and third parties. A Critical finding that could have a: • Catastrophic impact on operational performance or the ability to deliver services / care; or • Catastrophic monetary or financial statement impact; or • Catastrophic breach in laws and regulations that could result in material fines or consequences; or • Catastrophic impact on the reputation or brand of the organisation which could threaten its future viability.

Table 3 - Assigning Evidence Text Risk Assurance Ratings

	Impact rating				
Likelihood rating (in next 12 months)	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost Certain	Low	Low	Medium	High	Extreme
Likely	Low	Low	Medium	Medium	High
Moderate	Low	Low	Low	Medium	Medium
Unlikely	Not reportable	Low	Low	Low	**Low**
Rare	Not reportable	Not reportable	Low	**Low**	**Low**

2. Determination of the Assertion Level Risk Rating

The DSP Toolkit Independent Assessment Provider must then exercise professional judgement to assign a risk rating at the assertion level. The Independent Assessor leverages knowledge and subject matter expertise alongside observations made during the assessment to assign each assertion a risk rating of 'Extreme', 'High', 'Medium' or 'Low' based on the evidence text ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place. The Independent Assessor then uses Table 4 to assign a score for each assertion to be used in the calculation of NDG Standard level risk.

Table 4. Points corresponding to Assertion Risk Ratings

Rating	Points for each Assertion
Critical	40
High	10
Medium	3
Low	1

Table 5. Calculation and assignment of the NDG Standard risk ratings

Overall NDG Standard Risk Rating Classification		Rating Thresholds when only 1 assertion per NDG Standard is in scope	Rating Thresholds when 2 or more assertions are in scope for each NDG Standard. Mean score (Total points divided by the number of in-scope assertions)
●	Substantial	1 or less	1 or less
●	Moderate	Greater than 1, less than 10	Greater than 1, less than 4
●	Limited	Greater than/equal to 10, less than 40	Greater than/equal to 4, less than 5.9
●	Unsatisfactory	40 and above	5.9 and above

3. Determination of National Data Guardian Standards 'Standard Risk Rating'

In order to determine a risk rating for one of the National Data Guardian Standards; points are assigned to each in-scope assertion in a given Standard using **Table 4.** The total number of points is then divided by the number of in-scope assertions in the Standard. Consider an example where there are 8 assertions in scope for Standard 1 with the following ratings: 1 High, 3 Medium and 4 Low risk assertions. This gives a points total of (1 x 10) + (3 x 3) + (4 x 1) = 23. 23 divided by the total number of assertions (8), gives a mean points total of 2.9 rounded to the nearest one decimal place. **Table 5** is then used to determine the overall National Data Guardian Standards risk rating. In this example, a mean points total of 2.9 results in a '**Moderate**' Risk Rating for the National Data Guardian Standards.

4. Determination of Overall Risk Rating

If the in-scope assertions cover all 10 National Data Guardian Standards there will be risk ratings for each of the 10 Standards. Please see a 'completed' example below. Using Table 6, an independent assessment with 1 'Limited', 4 'Moderate' and 5 'Substantial' standard risk ratings, has an overall risk rating of 'Moderate'.

National Data Guardian Standard	National Data Guardian Standard Risk Rating	Independent Assessor's view on the level of deviation from the DSP Toolkit Self-Assessment	Confidence Level in veracity of self-assessment for this Standard
1	**Moderate**	Low	High
2	**Unsatisfactory**	Medium	Medium
3	**Substantial**	Low	High
4	**Moderate**	Low	High
5	**Substantial**	Medium	Medium
6	**Substantial**	Low	High
7	**Substantial**	Low	High
8	**Moderate**	Low	High
9	**Substantial**	Low	High
10	**Moderate**	High	Low
		Low / Medium deviation overall	Independent Assessor likely to arrive at a **'Medium**' Confidence level in the veracity of the self-assessment overall

Table 6. Determination of Overall Risk Assurance Rating

Overall risk rating across all in-scope standards	
Unsatisfactory	1 or more Standards is rated as 'Unsatisfactory'
Limited	No standards are rated as 'Unsatisfactory', but 2 or more are rated as 'Limited'
Moderate	There are no standards rated as 'Unsatisfactory', and 1 or none rated as 'Limited'. However, not all standards are rated as 'Substantial'.
Substantial	All of the standards are rated as 'Substantial'

5. Determination of Confidence level

If required, the Independent Assessor can use **Table 7** to determine the level of confidence in the veracity of the DSP Toolkit self-assessment. Experience and professional judgement will be required. This can then inform a view on the Assurance level expected to be required for Internal Audit reviews.

National Data Guardian Standard	National Data Guardian Standard Risk Rating	Independent Assessor's view on the level of deviation from the DSP Toolkit Self-Assessment	Confidence Level in veracity of self-assessment for this Standard
1	Moderate	Low	High
2	Unsatisfactory	Medium	Medium
3	Substantial	Low	High
4	Moderate	Low	High
5	Substantial	Medium	Medium
6	Substantial	Low	High
7	Substantial	Low	High
8	Moderate	Low	High
9	Substantial	Low	High
10	Moderate	High	Low
		Low / Medium deviation overall	Independent Assessor likely to arrive at a **'Medium'** Confidence level in the veracity of the self-assessment overall

Table 7. Determination of confidence-level in the veracity of the organisation's self-assessment / DSP Toolkit submission

Level of deviation from the DSP Toolkit submission and assessment findings	Confidence level	Suggested Assurance level
High – the organisation's self-assessment against the Toolkit differs significantly from the Independent Assessment For example, the organisation has declared as "Standards Met" or "Standards Exceeded" but the independent assessment has found individual National Data Guardian Standards as 'Unsatisfactory' and the overall rating is 'Unsatisfactory'.	Low	Unsatisfactory OR Limited
Medium - the organisation's self-assessment against the Toolkit differs somewhat from the Independent Assessment For example, the Independent Assessor has exercised professional judgement in comparing the self-assessment to their independent assessment and there is a non-trivial deviation or discord between the two.	Medium	Moderate
Low - the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment	High	Substantial

** Assurance Level - subject to Independent Assessor judgement / knowledge, Independent Assessor to differentiate between Unsatisfactory and Limited.*

Appendix C - Copy of Final Terms of Reference

Independent assessment objectives

Updated guidance was published by NHS Digital in draft form in Autumn 2019. This guidance and any subsequent updates are to be used by DSP Toolkit independent assessment providers, including internal auditors, when assessing DSP Toolkit submissions.

It is considered essential that the reviews using this updated guidance consider whether the health and social care organisation in question meets the requirement of each evidence text for each in scope assertion and also considers the broader maturity of the organisation's data security and protection control environment.

Independent assessment outputs

The independent assessment will produce the following outputs:

1. An assessment of the overall risk associated with [the organisation]'s data security and data protection control environment. i.e. the level of risk associated with controls failing and data security and protection objectives not being achieved;
2. An assessment as to the veracity of [the organisation]'s self-assessment / DSP Toolkit submission and the Independent Assessor's level of confidence that the submission aligns to their assessment of the risk and controls.

In essence the first output will be an indicator, for those assertions and evidence items assessed, as to the level of risk to the organisation and how good, or otherwise, the data security and protection environment is in terms of helping the organisation achieve the objectives in the DSP Toolkit. The second output will support an internal audit provider in arriving at the assurance level that they are required to provide, and that the organisation is obliged to provide, as per one of the DSP Toolkit requirements.

It should be noted that although the confidence level provides an indicator of the organisation's ability to accurately represent their security posture in their DSP Toolkit submission, it is the overall risk assurance rating that is the primary indicator of the strength of the organisation's data security and protection control environment. Both outputs are important as regards the goals of this work – to strengthen assurance (the confidence level helps with this respect) and to foster and create a culture of improvement - the overall risk assurance rating and those assertion-level and standards-level assessments of risk that make this up help with the culture of improving security and focusing improvement efforts in the right areas.

Independent assessment objectives

The risk evaluation output is seen as key to driving the conversations and improvements required. That is, this updated guidance aims to support the following requirements:

1. Better enable NHS organisations to continually improve the quality and consistency of DSP Toolkit submissions across the NHS landscape;
2. Deliver a framework that is adaptable in response to emerging information security, data and health and social care standards;
3. Allow for a range of bodies to deliver independent assessments in a consistent and easily understood fashion;
4. Help drive measurable improvement of data security across the NHS landscape and support annual and incremental improvements in the DSP Toolkit itself;
5. Deliver a framework that better enables and encourages organisations to publish a more granular, evidenced and accurate picture of their organisation's position in terms of data security;
6. Deliver a framework that allows for data security and protection professionals to spend time on-site coaching organisations on security improvement options at the same time as assessing controls and risks;
7. Deliver a framework that helps ensure consistent delivery of 'independent assessments', including internal audits;
8. Enable and encourage appropriate feedback and dialogue between NHS England and Independent Assessors to help inform NHS wide communications and initiatives to help address common challenges and systemic or thematic security issues and to help inform the development and consumption of NHS England provided national services around data security;
9. Enable leveraging of other sources of assurance across the NHS to reduce the burden on organisations and reduce total effort, cost and help minimise duplication of information gathering.

The objective of this independent assessment from [the organisation]'s perspective is to understand and help address data security and data protection risk and identify opportunities for improvement; whilst also satisfying the annual requirement for an independent assessment of the DSP Toolkit submission.

Assessment Scope

Each assessment delivery with consist of five core tasks and a number of subtasks, shown below.

Full details can be obtained in the overarching framework documentation available at https://www.dsptoolkit.nhs.uk/Help/64

Activities to be carried out during [review timeframe]			[timeframe]	
Task One Pre-assessment Preparation and Information	**Task Two** Scope DSP Toolkit Independent Assessment	**Task Three** Deliver DSP Toolkit Independent Assessment	**Task Four** Post-DSP Toolkit Review Meeting & Reporting	**Task Five** Assessment Finalisation & Quality Management
Obtain Trust details and establish points of contact	Conduct Detailed Scoping Meeting to Agree Terms of Reference & discuss self-assessment	Perform the DSP Toolkit Assessment	Draft & Finalise report	Workshop to present and discuss final report
Request a copy of the self-assessment and identify omissions / areas of weakness	Devise the logistics for the assessment and share document and stakeholder list for the assessment	Perform Risk and Confidence Evaluations (See Appendix A)	Issue tracking & follow up work	Proposing suggested changes to the DSP Toolkit

Detailed assessment approach

Our assessment involves the following steps:

- Obtain access to your organisation's DSP Toolkit self-assessment.
- Discuss the mandatory [X] assertions that will be assessed with your organisation and define the evidence texts that will be examined during the assessment.
- Request and review the documentation provided in relation to evidence texts that are in scope of this assessment prior to the onsite visit.
- Interviewing the relevant stakeholders who are responsible for each of the assertion evidence texts/self-assessment responses or people, processes and technology.
- Review the operation of key technical controls on-site using the DSP Toolkit Independent Assessment Framework as well as exercising professional judgement and knowledge of the organisation being assessed

Reporting Approach

Our report will incorporate our on-site observations and the analysis of key evidence provided to us. We will structure the report as follows:

- Use the reporting template as per the 'DSP Toolkit Strengthening Assurance Guide'.
- Where relevant and Independent Assessors challenge the self-assessment; present the level of deviation from the DSP Toolkit submission and assessment findings.
- Explicitly reference facts and observations from our on-site assessment to support our confidence and assurance levels.
- Detail recommendations that management can consider to address weaknesses identified.

Ratings

Our reports will include the following ratings:

- Our **confidence level** in the veracity of your self-assessment / DSP Toolkit submission.
- Our **overall risk assurance rating** as regards your organisation's data security and data protection control environment.

Limitations of scope

The scope of this review will be limited to the [X] assertions defined during the scoping exercise. The assessment will consider whether [the organisation] meets the requirement of each evidence text, and also considers the broader maturity of the organisation's data security and protection control environment. Results will be based on interviews with key stakeholders as well as a review of key documents where necessary to attest controls/processes. As we are assessing the operational effectiveness of a sub-set of assertions, our assessment should not be expected to include all possible internal control weaknesses that an end-to-end comprehensive compliance assessment might identify. We are reliant on the accuracy of what we are told in interviews and what we review in documents. Efforts will be made to validate accuracy only on a subset of evidence texts and therefore there is a dependency on [the organisation] to provide accurate information. Furthermore, onsite verbal recommendations by the Independent Assessor staff do not constitute formal professional advice and should be considered in line with broader observations. Our report will contain recommendations for management consideration to address the weaknesses found.

… … …

Key Contacts

Independent assessment team

Name	Title	Role	Contact email	Contact number

Key contacts – [the organisation]

Name	Role	Contact email	Contact number

Timetable and information request

Timetable

Document Request	[date]
Agree timescales and workshops	
Fieldwork start	
Fieldwork completed	
Draft report to client	
Response from client	
Final report to client	

Agreed timescales are subject to the following assumptions:

- All relevant documentation, including source data, reports and procedures, will be made available to us promptly on request.
- Staff and management will make reasonable time available for interviews and will respond promptly to follow-up questions or requests for documentation.

Information request

Prior to the onsite assessment commencing, please share the requested documents that are listed in Appendix [X], or the closest equivalent documents / evidence that you have (we note that terminology and document names / policy titles may differ).

Secure data transmission

We request supporting evidence to be sent to us ahead of the fieldwork start date in order for us to begin our review before any on-site work. To ensure that your information remains secure, we use a [secure end-to-end encryption (AES-256)…]

No patient data should be uploaded / sent … during the assessment. We will not request, nor do we require any patient data in order to deliver the independent assessment.

Onsite interviews

You hold ultimate responsibility for scheduling meetings between Independent Assessors and the identified [organisational] stakeholders. A typical list of roles and likely assertions for each is listed in Appendix [X] and Appendix [Y].

Please provide use of a secure / confidential room large enough for 2 Independent Assessors plus your identified stakeholders that also has conference calling facilities to host our interviews and include colleagues who are supporting the interviews remotely.

Appendix D: Stakeholders and Meetings Held

Stakeholders and Meetings Held

Name	Role	Interview Date and Time

Appendix E: Documents Received and Reviewed

Documents Received and Reviewed

NHS England Data Security and Protection - Standard	Assertion	Document Name	Evidence Item Code
NHS England Data Security and Protection - Standard 1	Assertion-1.8		DSP Toolkit Evidence item code - 1.8.1
NHS England Data Security and Protection - Standard 1	Assertion-1.8		DSP Toolkit Evidence item code - 1.8.1
NHS England Data Security and Protection - Standard 1	Assertion-1.8		DSP Toolkit Evidence item code - 1.8.1
NHS England Data Security and Protection - Standard 1	Assertion-1.8		DSP Toolkit Evidence item code - 1.8.1
NHS England Data Security and Protection - Standard 1	Assertion-1.6		DSP Toolkit Evidence item code - 1.6.6
NHS England Data Security and Protection - Standard 1	Assertion-1.6		DSP Toolkit Evidence item code - 1.6.6
NHS England Data Security and Protection - Standard 1	Assertion-1.6		DSP Toolkit Evidence item code - 1.6.2
NHS England Data Security and Protection - Standard 1	Assertion-1.6		DSP Toolkit Evidence item code - 1.6.1
NHS England Data Security and Protection - Standard 1	Assertion-1.4		DSP Toolkit Evidence item code - 1.4.2
NHS England Data Security and Protection - Standard 1	Assertion-1.4		DSP Toolkit Evidence item code - 1.4.1
NHS England Data Security and Protection - Standard 1	Assertion-1.4		DSP Toolkit Evidence item code - 1.4.1

Appendix F: Non-reportable items – observations on out of scope matters

Non-reportable items – observations on out of scope matters

The following observations are included for information purposes and relate to items outside the formally agreed scope and beyond the evidence being scrutinised by the Independent Assessor. It is hoped that the inclusion of such observations is helpful to the assessed organisation in contextualising and remediating data security and data protection issues.