Data Security and Protection Toolkit

Strengthening Assurance- Independent Assessment and Audit: Summary of Guides

Creating a culture of Improvement

Information and technology for better health and care

26/09/2023

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
16/04/2020	Updated for DSPT Summary of Guides 20-21		1.1
17/08/2021	Updated for DSPT 2021-22		1.2
26/09/2022	Updated for DSPT 2022-23 Version 5		1.3
26/09/2023	Updated for DSPT 2023-24 Version 6		1.4

Document Control: The controlled copy of this document is maintained by NHS England's Data Security Centre. 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 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, 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 NHS England DSP Toolkit Summary of Guides consists of three sections that are listed below.

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

1. Introduction

In order to conduct independent assessments against the NHS England DSP Toolkit, assessors must consult both:

- The NHS England DSP Toolkit Independent Assessment Guide; and
- The NHS England DSP Toolkit Independent Assessment Framework.

The purpose of this document is to provide guidance on how these two resources should be used alongside one another during the delivery of a successful DSP Toolkit independent assessment (including internal audit).

2. Summary - Independent Assessment Guide

2. Summary – Independent Assessment Guide

The following summary outlines the purpose and scope of the Independent Assessment Guide. It also provides an overview of the Guide's content.

1. Who is the intended audience for the guide?

The 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. The guide, and associated framework, act as guidance materials to inform these assessments – enabling a consistent approach to be applied across the sector (in line with the requirements of NHS England), while enabling each organisation/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 the updated guidance?

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 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. The 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 could be independently assessed. It will also help inform 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. More professionals will be required to deliver an increased workload and drive improvements in data security.
- **National Bodies/Health and Social Care sector:** When followed and widely used across the sector, the updated guide should provide 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. Summary – Independent Assessment Guide
continued

3. 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. The guide therefore considers both the security of electronic data and related processes and transactions, including paper records.

4. 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.

5. 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.

3. Summary - Independent Assessment Framework

3. Summary – Independent Assessment Framework

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

The NHS England Data Security and Protection Toolkit (DSP Toolkit) Independent Assessment Framework is a resource, created by NHS England, for independent assessors of Health and Social Care organisations.

The resource is the framework that the internal auditor or assessor could use to assess the organisation against the requirements of the DSP Toolkit. It can act as the basis of scoping the terms of reference for each DSP Toolkit audit or assessment, the approach that the auditor or assessor could take during their review, and the evidence that the assessor could request and review as part of their work.

Further detail on the framework, and how to navigate it, is provided in the framework itself. For each of the evidence texts within the DSP Toolkit, the DSP Toolkit Independent Assessment Framework outlines the control objective of the evidence text, provides a step by step guide as to how to audit or assess the organisation's control environment against the objective, an indication as to the on-site tests that could be performed and documents that the 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 intended to be exhaustive or overly prescriptive, though it does aim to promote consistency of approach. Auditors and 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.

3. Summary – Independent Assessment Framework
continued

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 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 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 8.3.3 *("There is a documented approach to applying security updates (patches) agreed by the SIRO.")*, 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.

The content of the framework is intended to act as a guide, outlining how evidence texts could be tested. However, there are other ways of testing some of the evidence texts and independent assessors should be able to do so, based on their professional judgement and knowledge of the organisation being assessed.

Details on how the observations against each evidence text should be risk assessed, and translated into findings in the report, are outlined in the DSP Toolkit Independent Assessment Guide.

3. Summary – Independent Assessment Framework
continued

The DSP Toolkit is designed to be applicable to **three** different categories of Health and Social Care organisation. **The categories reflect the nature of the organisations' data security and protection requirements; the volume and sensitivity of patient data processed; regulatory requirements and the relevant resilience and availability requirements** (e.g. for Operators of Essential Services or Digital Service Providers under the NIS Directive).

More DSP Toolkit assertions and evidence text items are mandatory for category 1 organisations and recommended for categories 3, and 4. The categories and the types of organisation in those categories are shown in the table below. The DSP Toolkit Independent Assessment Framework and associated guidance has been designed to cater for reviews for category one organisations.

Category 1

- Acute Hospital/Trust
- Ambulance Trust
- Community Services Provider
- Mental Health Trust
- Arm's Length Body
- Integrated Care Boards
- Commissioning Support Unit
- IT Supplier