NHS Digital

DSP Toolkit – CAT1

What's new for 22-23

September 2022 John Hodson

Data Security and Protection Toolkit

What is it?

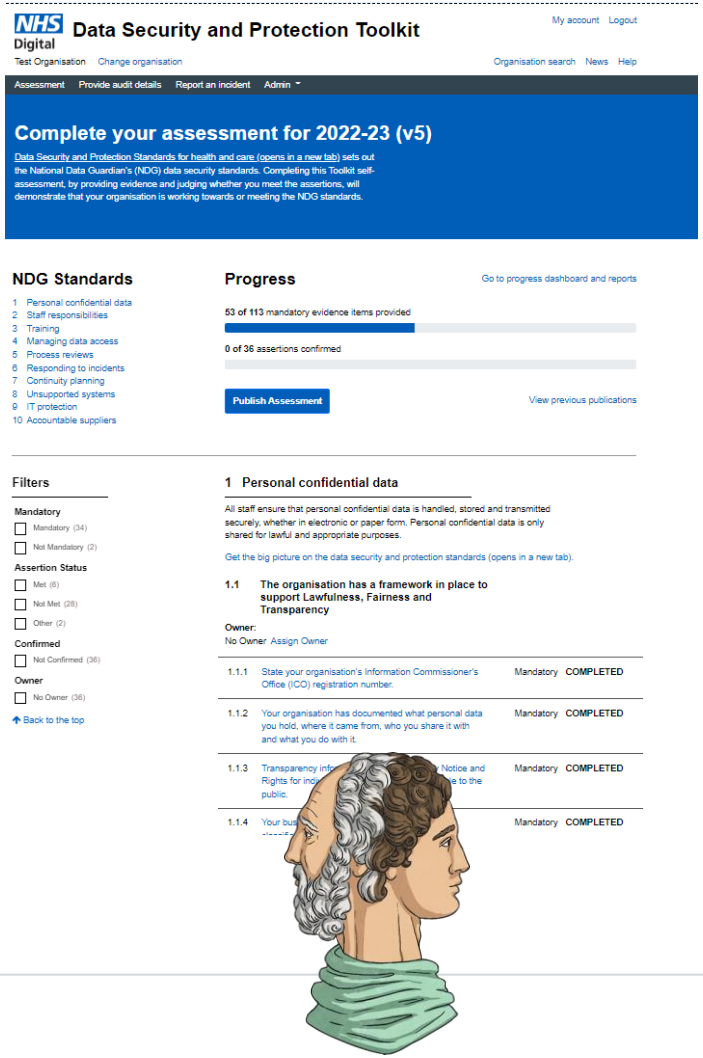
On line Self-Assessment

External assurance

Checklist (DP/Cyber Poverty)

Gateway to systems

Mix of measures (descriptions/outcomes/ checks)



Sector baseline standard

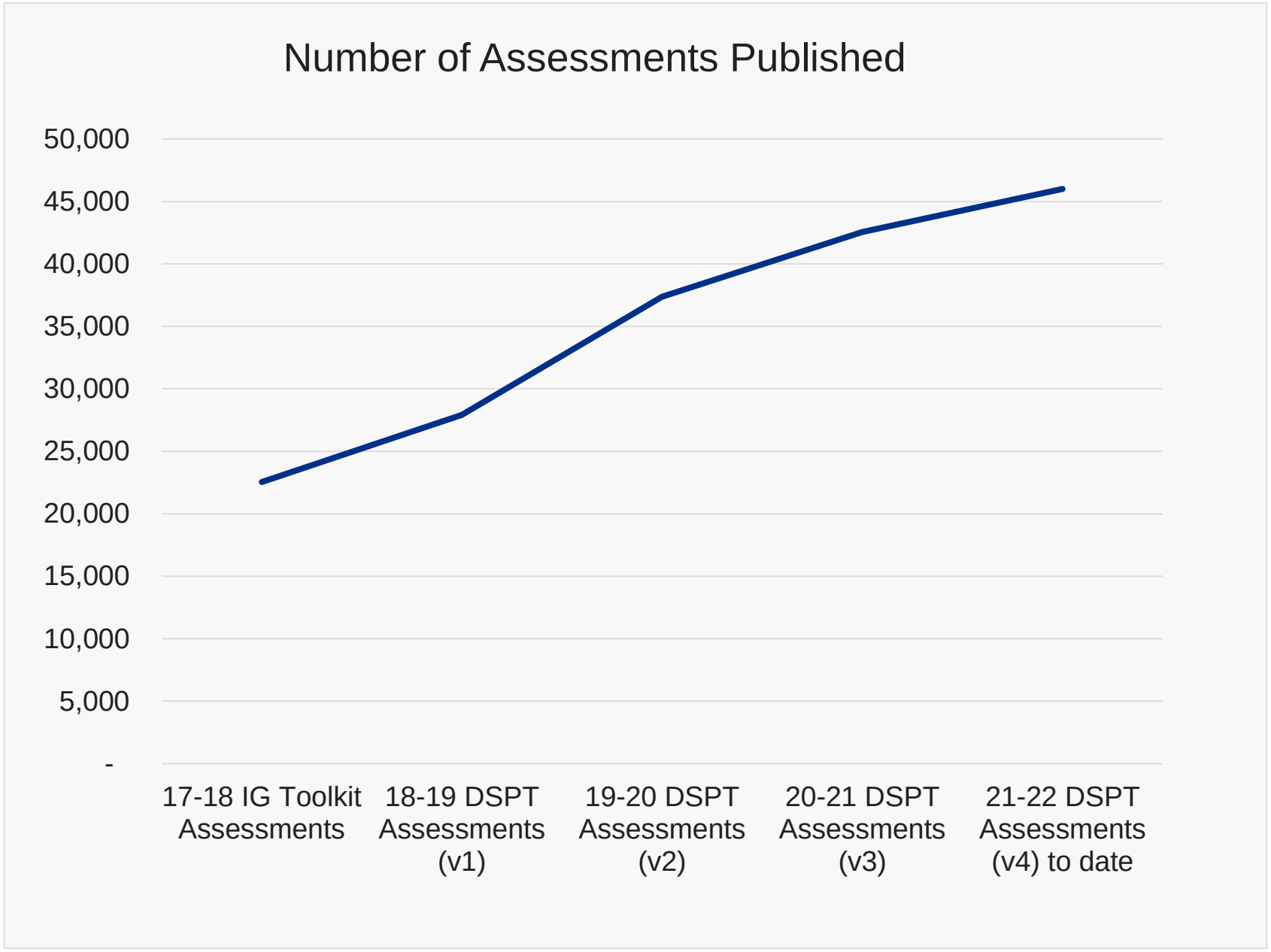
High quality data source

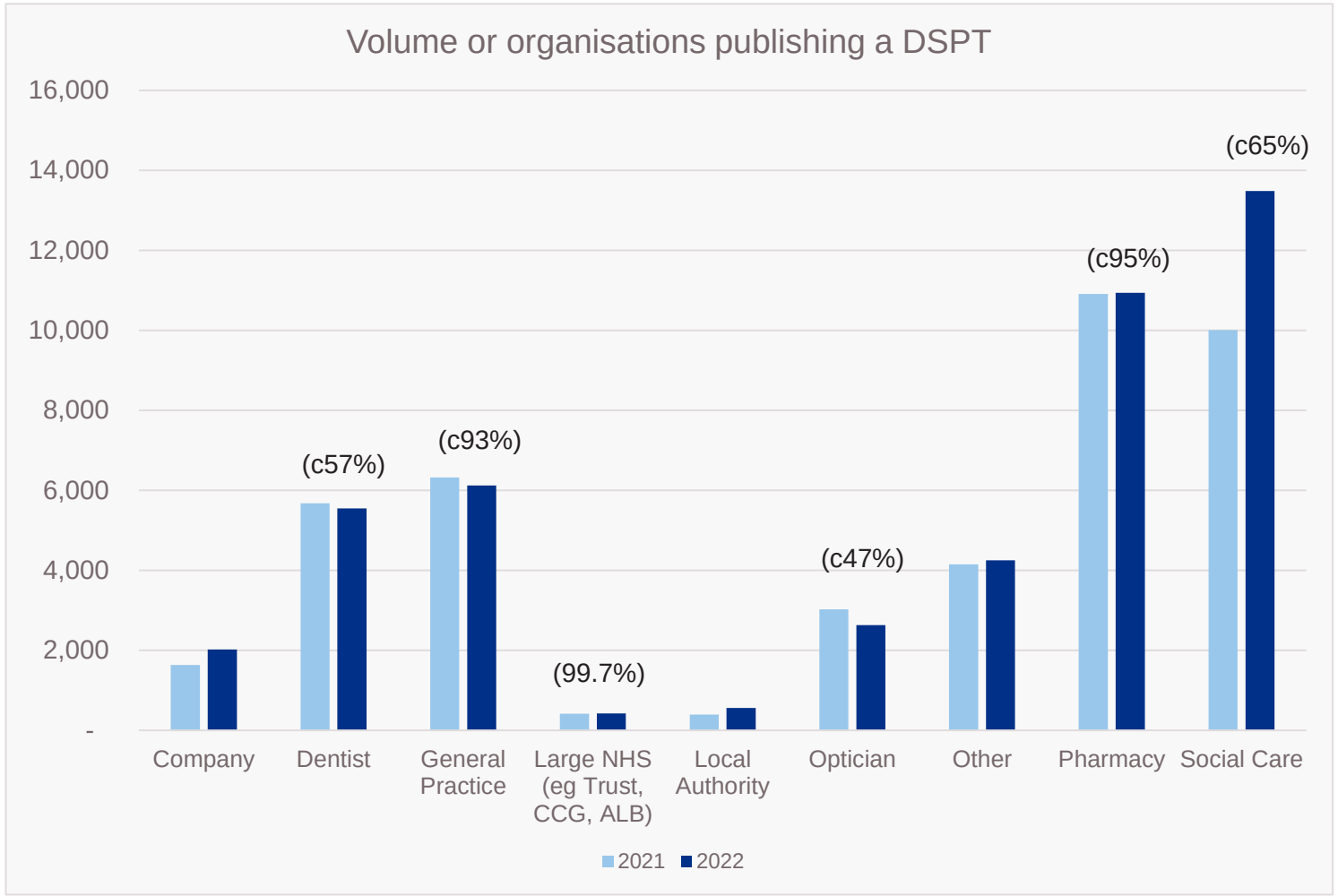
DHSC assurance

Threat horizon scanning

Raising maturity (achievable at a stretch)

DSP Toolkit 21-22 Results

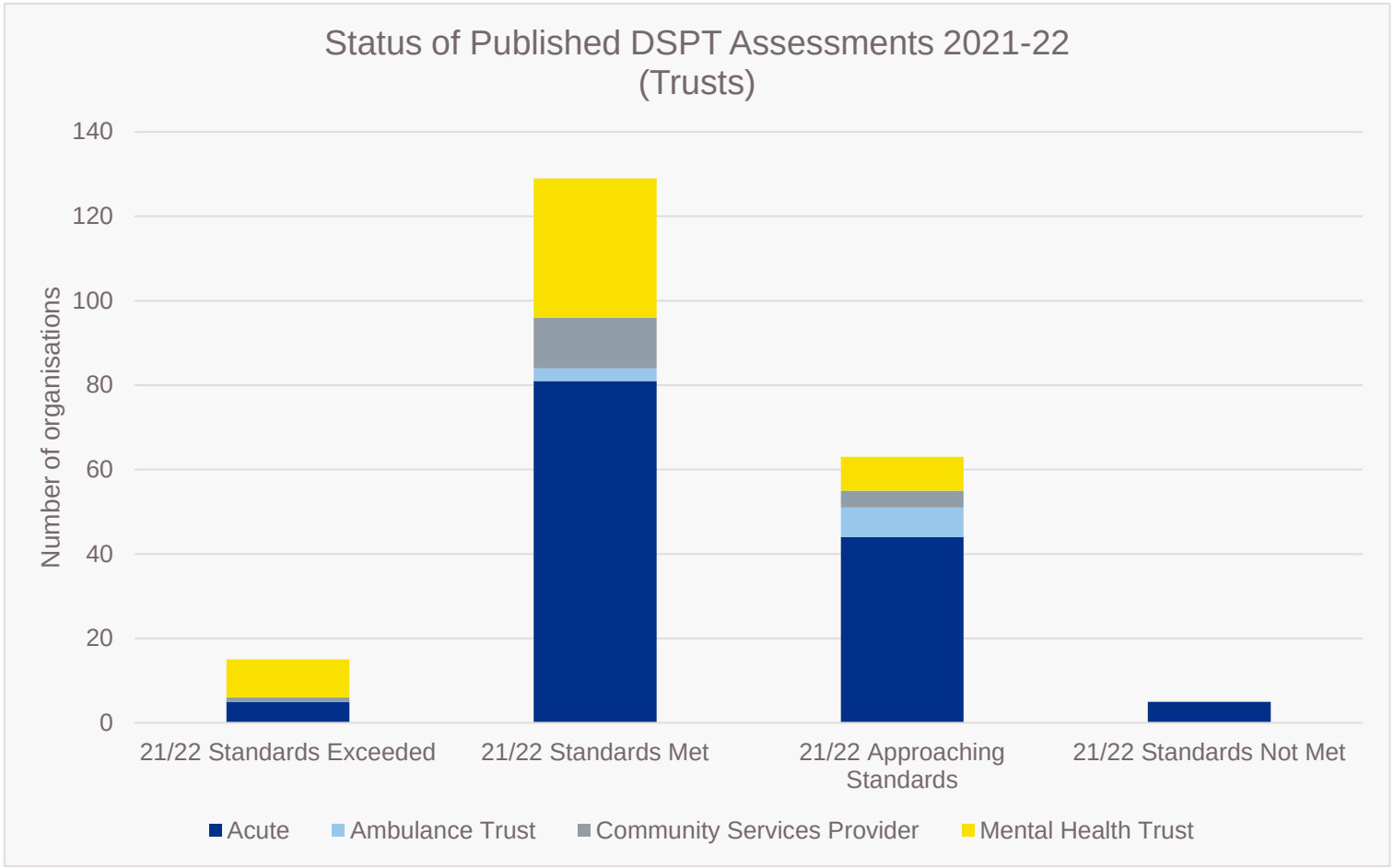

Number of Assessments Published
50,000
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
-
17-18 IG Toolkit Assessments
18-19 DSPT Assessments (v1)
19-20 DSPT Assessments (v2)
20-21 DSPT Assessments (v3)
21-22 DSPT Assessments (v4) to date



The vast majority of organisations that complete the DSPT are smaller organisations.

However, takeup as a proportion of all organisations in their sector remains highest in GP, Pharmacy and Large NHS (Trusts, CCGs etc).

APPROXIMATE proportional takeup is shown in brackets



Status	Number of NHS Trusts
21/22 Standards Exceeded	15
21/22 Standards Met	129
21/22 Approaching Standards	63
21/22 Standards Not Met	5

(Data accurate 5 September)

User feedback

Our **patients and service users can be confident that their personal data is secure** because we complete an annual toolkit.

79%

Agree or strongly agree

The **organisations we deal with can have a level of assurance** because we complete an annual toolkit.

92%

Agree or strongly agree

How satisfied are you with the process of completing the Data Security Protection Toolkit (DSPT)?

79%

Satisfied or strongly satisfied

DSP Toolkit for 22-23

Transition to 22-23 Toolkit

22-23 Standard agreed and available at:
https://www.dsptoolkit.nhs.uk/News/22-23-DSP-Toolkit-evidence-items

Audit and Big Picture guides available in September 2022

Deadline is 30th June 2023

Baseline 28th February 2023 for Trusts, ICBs and ALBS

Assertions and checkboxes are unticked

Responses from 22-23 transferred where evidence item unchanged

Evidence item numbers have been Reordered and gaps removed

Minor changes overall

22-23 DSP Toolkit – Key Changes

Incorporate IG Simplification

NHS E Privacy Team advice on removing duplication, aligning with updated guidance

ICB/ALB move to Category 1

Additional requirements for ALBs and ICBs

Feedback Review

DSPT evidence items reviewed and updated based on feedback, support calls and comments from stakeholders. Evidence items reviewed

Tooltips expanded

More detail drawn from Audit guides

Audit requirements unchanged

The same assertions will be audited in 22-23 as 21-22.

Consent requirement made mandatory

NHS E Privacy Team advice on removing duplication, aligning with updated guidance

Technical requirements strengthened

Specific Improvements to requirements on Medical Devices, ATP, vulnerabilities, unsupported systems, Early Warning Service and network documentation

Training

Change coming from since 1st July to the last 12 months.

Evidence items in the DSP Toolkit

Mandatory evidence items

	Category 1 organisations	Category 2 organisations	Category 3 organisations	Category 4 organisations
Total number of mandatory evidence items 2021-22 v4	110	89	43	29
Total number of mandatory evidence items 2022-23 v5	113	N/A	42	28

Total evidence items

	Category 1 organisations	Category 2 organisations	Category 3 organisations	Category 4 organisations
Total number of evidence items 2021-22 v4	142	137	85	42
Total number of evidence items 2022-23 v5	131	N/A	78	49

Improvement plans what happens next

Improvement plans next steps

- Further information on the news page
- Report produced for NHSE
- A Trust can submit an update to an improvement plan at any time and if all actions complete status will be amended to Standards met for 21-22.
- Trusts will be asked for an update in September 2022 and again in December 2022.
- Organisations not completing their improvement plans can be amended to Standards not met.

What are the new evidence items

CAT1

8.3.8	Your organisation is registered for and actively using the NCSC early warning service.	The [NCSC early warning service](https://www.ncsc.gov.uk/information/early-warning-service) helps organisations investigate cyber attacks on their network by notifying them of malicious activity that has been detected in information feeds.

What are the newly Mandatory requirements

Data protection

1.1.6	Your organisation has reviewed how it asks for and records consent to share personal data.	NHS organisations may require patient consent under data protection legislation for activities such as patient mailing lists. More commonly, patient consent is required under the common law duty of confidentiality. This would apply in situations when a patient's data is used in ways they would not reasonably expect, for example, when used for research purposes. Consent is also required when sharing confidential patient information with a third party, such as a carer or family member. Please provide details of all your organisation's activities in the comments. Consent should be covered in general data protection and confidentiality policies or a separate consent policy in line with [Information Commissioner's Office guidance](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/). You should ensure that you clearly differentiate between consent under data protection legislation and consent under the common law duty of confidentiality.

Cyber

8.3.6	Your organisation is actively using and managing Advanced Threat Protection (ATP) and regularly reviewing alerts from Microsoft defender for endpoint.	Confirm that your organisation has the technology and processes in place to actively manage ATP and Microsoft defender for endpoint. If alternative solution in place provide details in the comments field.
8.4.3	You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.	The organisation has a vulnerability management process that outlines how the organisation identifies and effectively manages vulnerabilities through to remediation. This may include using [NHS Digital's VMS and / or Bitsight service.](https://digital.nhs.uk/cyber)

Technical

8.3.7	95% of your organisation’s server estate and 98% of your desktop estate are on supported versions of operating systems.	Please upload a screenshot/s from Advanced Threat Protection (ATP) demonstrating the percentage of servers and desktops on supported versions of operating systems. If not met, please provide details in the comments on the plan to achieve 95% of your server estate and 98% of your desktop estate on supported versions of operating systems.
9.5.3	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.	Provide details of your organisation's change management process that prevents changes to its IT environment from being implemented without being approved by the appropriate individuals and security implications being considered.

Connected Medical Devices

9.3.9	What is the organisation's data security assurance process for medical devices connected to the network.	This should be a policy / process document or full explanation covering how the organisation assures data security during the full life cycle of the medical device. [Further guidance is available](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-for-procuring-and-deploying-connected-medical-devices)

Where has the wording been tweaked (watch out for date changes)

3.2.1 Training requirement amendment coming…

At least 95% of all staff, have completed their annual Data Security Awareness Training since 1st July 2022.	**Please provide your highest percentage figure for the period 1st July 2022 - 30th June 2023 in the space below with an explanation of how you have calculated the figure.** **This can be calculated from local materials/E Learning system and/or the national Data Security Awareness E-Learning system. If using local training it must cover the areas included in https://portal.e-lfh.org.uk/Component/Details/544182** **All staff, which includes new starters, locums, temporary, students and staff contracted to work in the organisation have completed their annual Data Security Awareness Training (including passing a mandatory test).**

To

At least 95% of all staff, have completed their annual Data Security Awareness Training in the last twelve months.	**Please provide your percentage figure for the last twelve months prior to the date of publication, in the space below with an explanation of how you have calculated the figure.** **This can be calculated from local materials/E Learning system and/or the national Data Security Awareness E-Learning system. If using local training it must cover the areas included in https://portal.e-lfh.org.uk/Component/Details/544182** **All staff, which includes new starters, locums, temporary, students and staff contracted to work in the organisation have completed their annual Data Security Awareness Training (including passing a mandatory test).**

Examples of last twelve months before publication

Publication Date = 30.06.2023

Training included is:

01.07.2022 – 30.06.23

Publication date = 01.06.2023

Training included is:

02.06.2022 – 01.06.2023

Publication date = 01.04.2023

Training included is:

02.04.2022 – 01.04.2023

Publication date = 01.10.2022

Training included is:

02.10.2021 – 01.10.2022

Example Answer for 3.2.1 Training based on 1st June 2023 publication date

96.1% of staff have completed Data Security Awareness training in the last twelve months.

This was calculated as below:

Number of staff (including locums, temporary, students and staff contracted to work in the organisation) in the organisation = 10,000.

Number of staff completing data security awareness training since 2nd June 2022 = 9,610

Broken down into:

Number of staff completing national Data Security Awareness training = 8,140

Number of staff completing face to face IG session with test = 1,500

Number of staff completing data security awareness training with other organisations since 2nd June 2022 = 21

Number of staff figure is taken from email exchange with HR/Payroll team from 20/08/2021 which is available in the 22-23 DSPT Evidence – 3.2.1 Folder on SharePoint.

Number of staff completing face to face IG session with test, is taken from the registers of the session which are available in the 22-23 DSPT Evidence – 3.2.1 Folder on SharePoint.

Number of staff completing data security awareness training with other organisations since 2nd June 2022 is taken from the certificates/emails of the session which are available in the 21-22 DSPT Evidence – 3.2.1 Folder on SharePoint.

Integrated Care Boards

ICBs

The ICB will be responsible for submitting a Data Security and Protection Toolkit (DSPT) for 22-23.

If your ICB is not set up contact the Exeter Helpdesk

Places are not required to complete a separate DSP Toolkit watch out for ODS Code changes in Old CCGs

ICBs are required to complete a DSP Toolkit Audit and complete a baseline

Scope of ICB Toolkit is the legal entity of the Integrated Care board not the patch.

Responses

It is expected that some ICB responses may be made up of a CCG level responses so you can start work now.

For example you may in place ROPAs at a CCG level now and pull them together in a summary paper to an ICB group once established.

The key is to ensure there is a plan to harmonise the work towards an integrated ICB response.

To meet the DSP Toolkit in an ICB

1.1.2 Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Step 1 – Complete the Reviews

- Acceptable to have different information Asset registers and data flows systems across ‘old’ CCGs.
- Must follow the relevant guidance for data flows be undertaken since 01 July 2022

Step 2 – Documentation

- Acceptable for different format of reports to be produced following reviews
- Can be completed in pre-ICB format

Step 3 – ICB Reporting

Acceptable to have a summary report of all reviews presented to the ICB SIRO and the accountable group

ICB SIRO approve overall ICB registers and data flows.

Help and Support

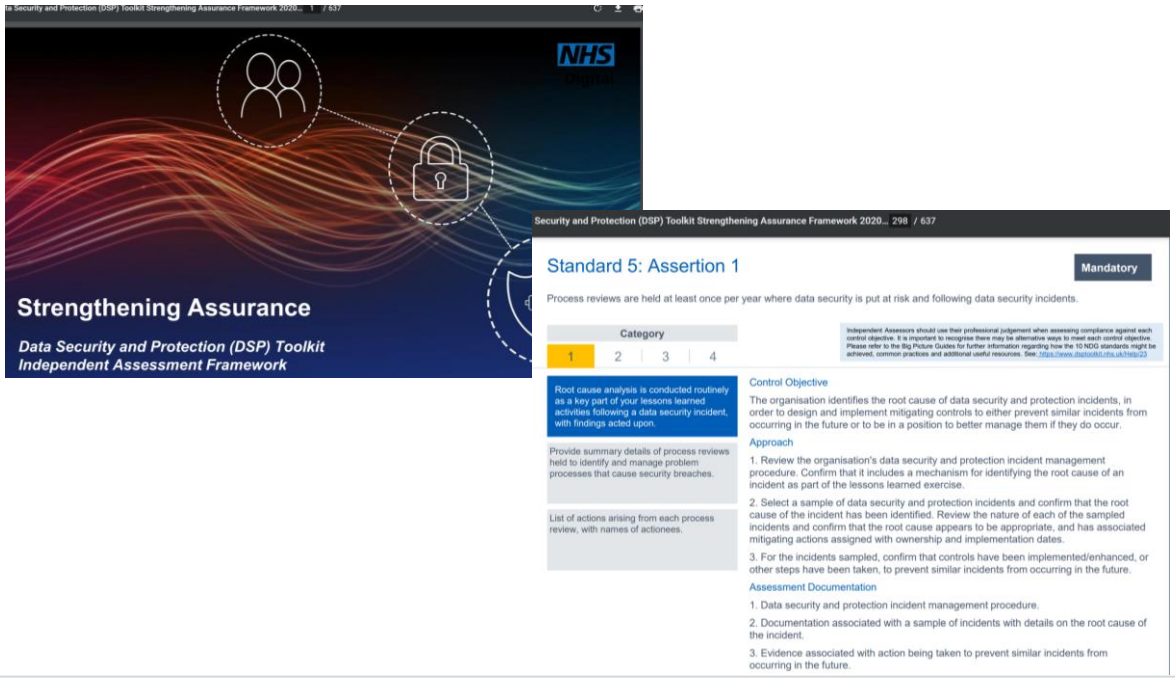
Resources to help

Happy to support regional meetings on briefings. Upcoming CAN Conference and helpdesk exeter.helpdesk@nhs.net.

Audit Guides

https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides

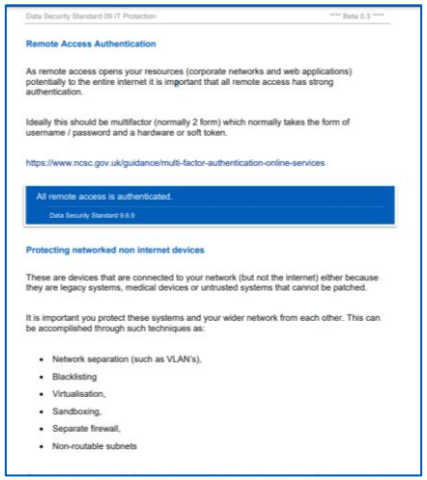
Useful as set out the requirement in a ISO 27001 style with control objective and documentation.



Big Picture Guides

https://www.dsptoolkit.nhs.uk/Help/big-picture-guides

Give background to the requirement and talk more broadly about the subject area with links to wider reading



Any questions?

NHS Digital

Thank You

@nhsdigital

company/nhs-digital

digital.nhs.uk