

DSP Toolkit - CCGs

What's new for 21-22

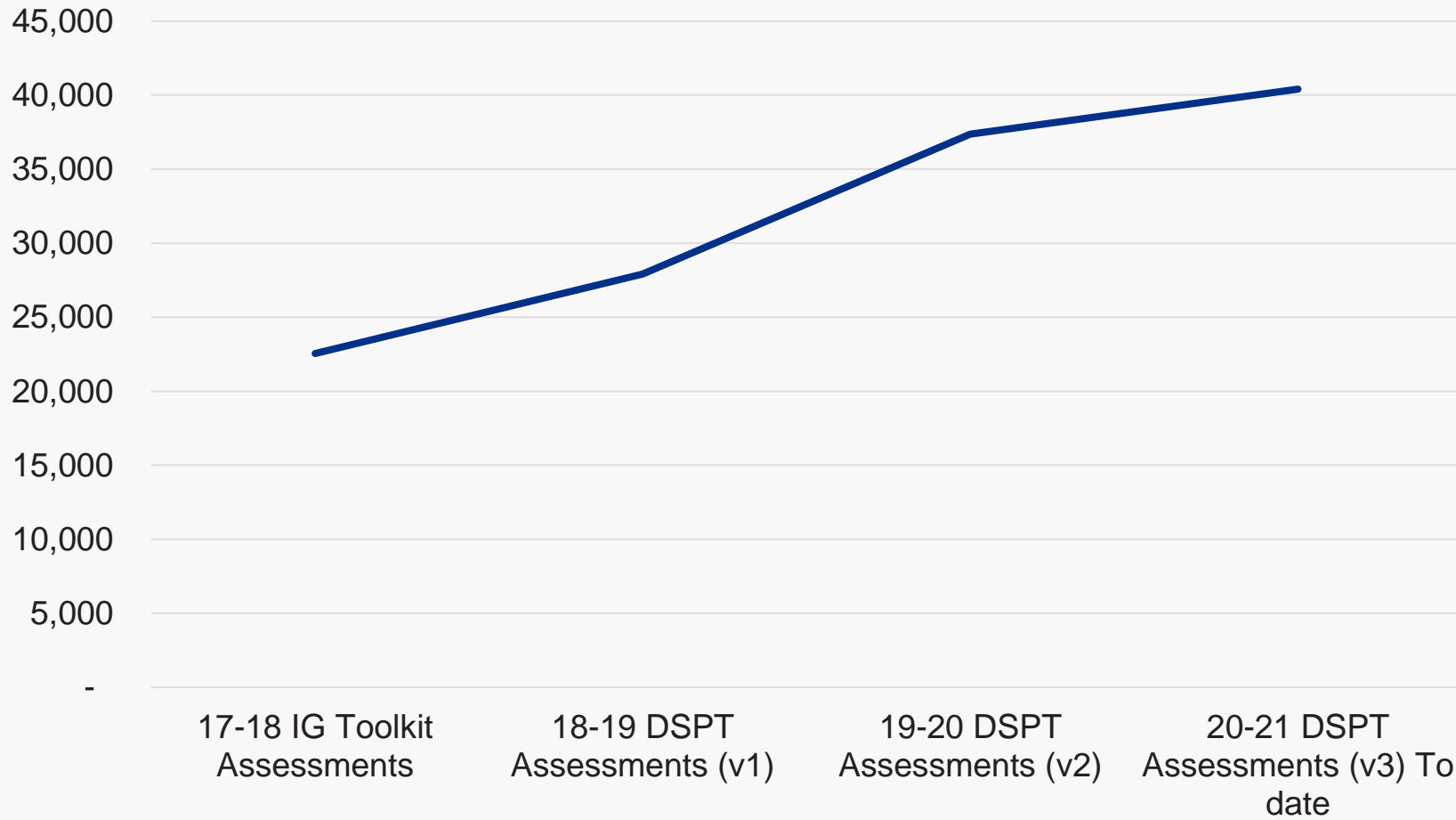
September 2021 John Hodson



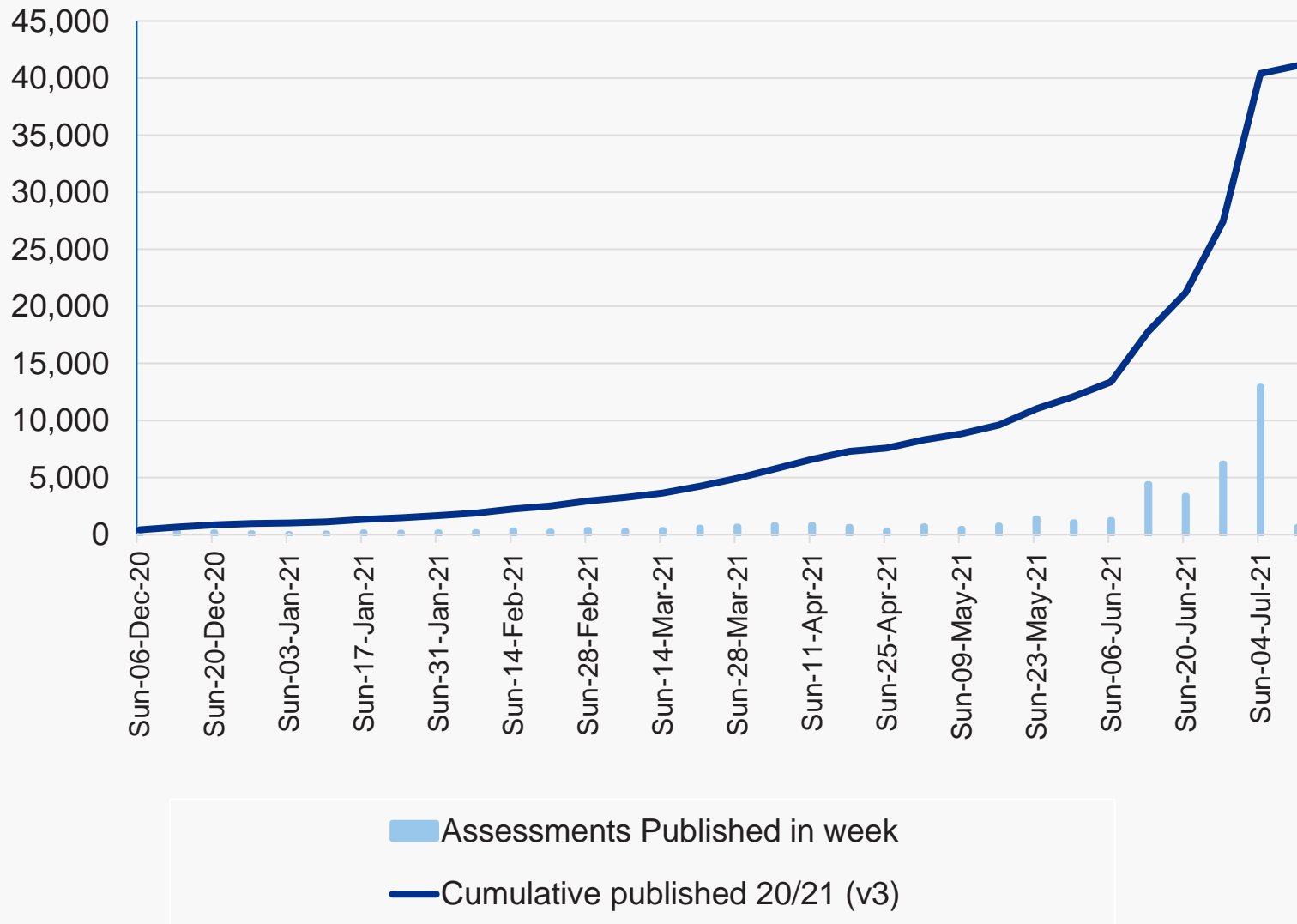
DSP Toolkit 20-21 Results



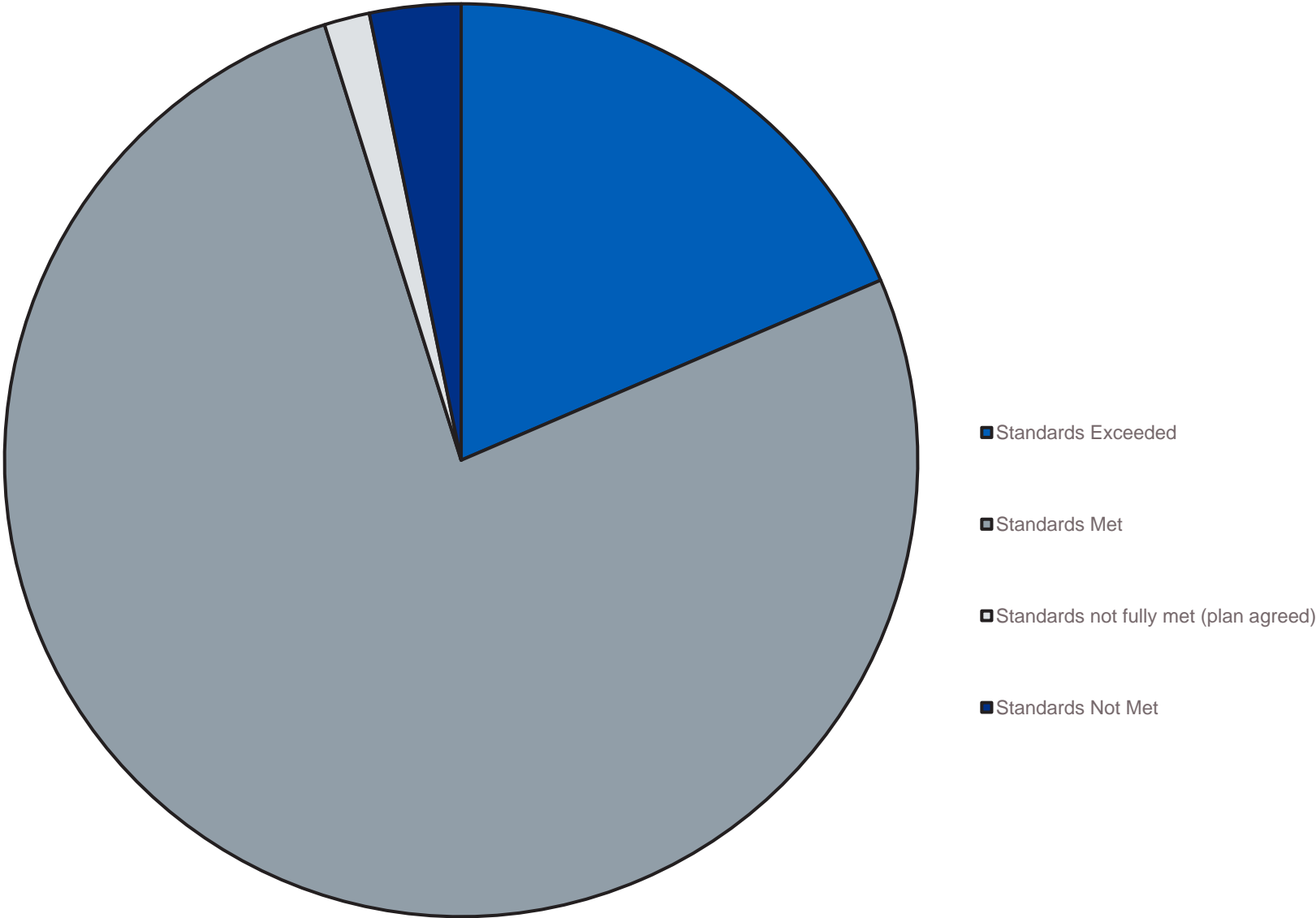
Number of Assessments Published



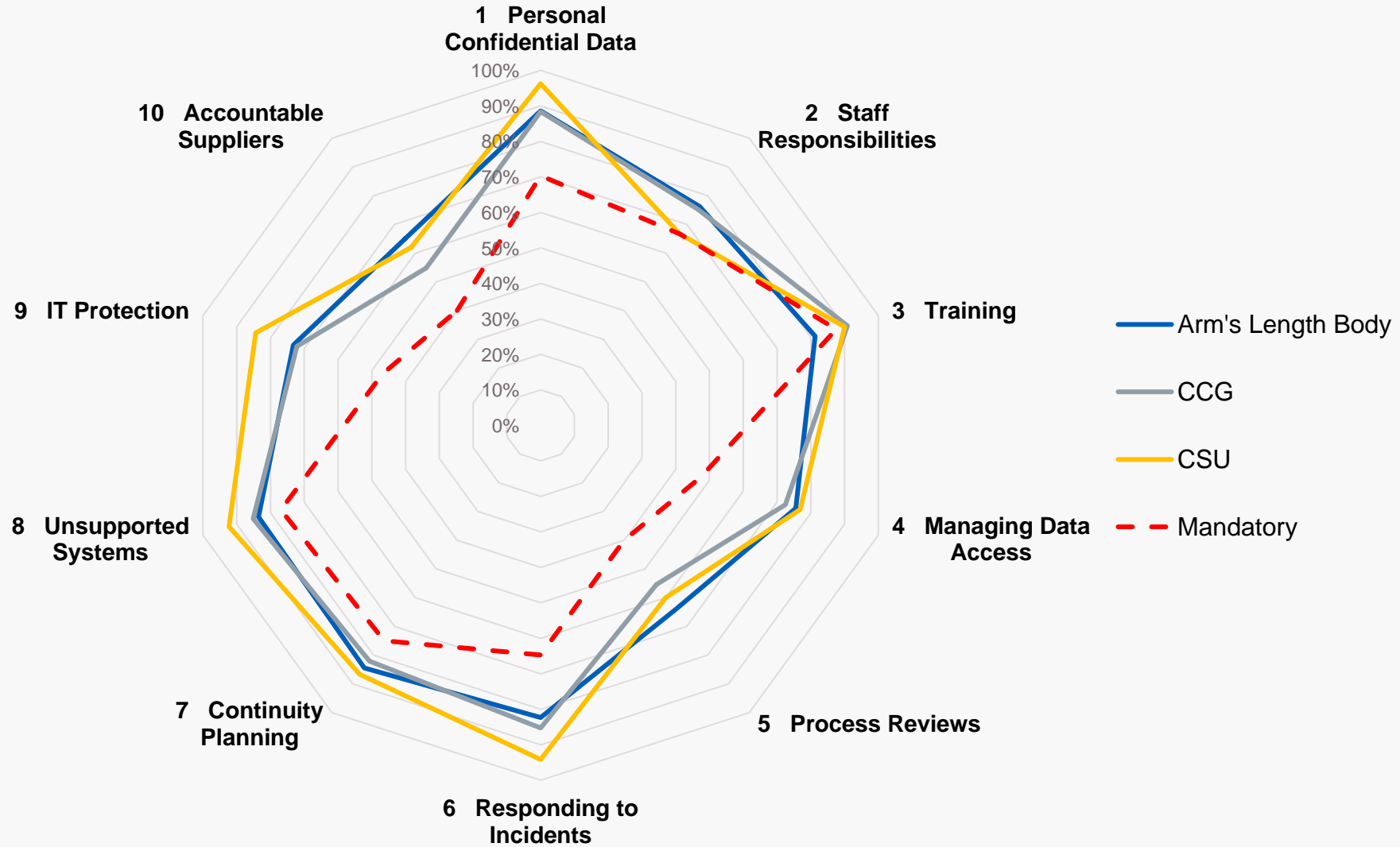
DSPT Weekly Published Self-Assessments 20 /21



DSP Toolkit Status of CCGs 20-21



Percentage of Evidence Items Responded to within NDG standards (Category 2 organisations)



The most responded to Mandatory DSPT requirements CCG, CSU and ALBs

Ref	Question
1.1.1	Has SIRO responsibility for data security been assigned?
1.1.2	List the names and job titles of your key staff with responsibility for data protection and/or security.
1.1.4	Is data security direction set at board level and translated into effective organisational practices?
1.3.1	What is your organisation's Information Commissioner's Office (ICO) registration number?
1.3.2	How is transparency information (e.g. your privacy notice) published and available to the public?
1.6.1	Is there is an approved procedure that sets out the organisation's approach to data protection by design and by default , which includes pseudonymisation requirements?
1.6.2	There are technical controls that prevent information from being inappropriately copied or downloaded .
1.6.3	Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data.
1.6.4	Provide the overall findings of the last data protection by design audit .
1.7.4	Has a records retention schedule been produced?



DSP Toolkit for 21- 22



Transition to 21-22 Toolkit

**21-22 Standard
agreed and
available at:**

[https://www.dsptoolkit.nhs.uk/
News/21-22-DSP-Toolkit-
evidence-items](https://www.dsptoolkit.nhs.uk/News/21-22-DSP-Toolkit-evidence-items)

**Audit Guide
available at:**

[https://www.dsptool
kit.nhs.uk/News/aud
itnews](https://www.dsptoolkit.nhs.uk/News/auditnews)

**Deadline is
30th June
2022**

**Baseline 28th
February
2022 for
Trusts,
CCGs(Volunt
ary), CSUs
and ALBS**

**Responses
from 20-21
transferred
where
evidence
item
unchanged**

**Assertions
are
unconfirmed**

**Evidence
item
numbers
have been
Reordered
and gaps
removed**

**Minor
changes
overall**

21-22 DSP Toolkit – Key Changes

Incorporate IG Simplification

NHS X IG Team advice on removing duplication, aligning with updated guidance

ICO Data Protection

Toolkit has been aligned to the ICO Data Protection Self-Assessment

Feedback Review

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

Connected Medical Devices

Include new requirements for Connected Medical Devices

CSU Technical Requirements

Additional technical requirements reflecting the key role CSU play

Technical requirements strengthened

Specific Improvements to requirements on logging, assets, unsupported systems, patching

Extra non-Mandatory requirements

Connected Medical devices, Support Systems, patching .



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 2020-21 v3.1	111	89	45	31
Total number of mandatory evidence items 2021-22 v4	110	89	43	29

Total evidence items

	Category 1 organisations	Category 2 organisations	Category 3 organisations	Category 4 organisations
Total number of evidence items 2020-21 v3.1	149	146	92	46
Total number of evidence items 2021-22 v4	142	137	85	42



Improvement plans what happens next





Improvement plans next steps

- Further information on the news page
- Report produced for NHSX
- 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 20-21.
- Trusts will be asked for an update in September 2021 and final update in December 2021.
- Organisations not completing their improvement plans can be amended to Standards not met.

What are the new Mandatory requirements



CCG/ICS/ALB

1.1.3	Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.	Please provide documentary evidence.
3.4.2	All board members have completed appropriate data security and protection training.	As defined in your organisations data security and protection training needs analysis. All Board members are current permanent working board members (for example board members who are sick should not be included).



CCG/ICS/ALB Data Protection

1.2.2	Your organisation has a process to recognise and respond to individuals' requests to access their personal data	https://www.nhsx.nhs.uk/information-governance/guidance/subject-access-requests/
1.2.4	Is your organisation compliant with the national data opt-out policy?	Please provide your published [compliance statement](https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out) e.g. within a privacy notice and/or Published Data Release Register in the comments box.
1.3.8	Your organisation understands when you must conduct a Data Protection Impact Assessment and has processes in place, which links to your existing risk management and project management, to action this.	[Information commissioner's office guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) is available

What are the new Non-Mandatory requirements



CCG/ALB

4.4.1	The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.	Organisational policy should set out the rules defining log retention. The average time to detect a cyber attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. Guidance from NCSC on maintaining security of logs is available at https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide Note: you are not expected to purchase a CSOC.
8.3.7	Are 95% of your server estate and 98% of your desktop estate 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.
9.3.8	The organisation maintains a register of medical devices connected to its network.	The register should include Vendor, maintenance arrangements and whether network access is given to supplier/maintainer.



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



CCGs

7.3.5	Do you test your backups regularly to ensure you can restore the service from a backup? Previously [When did you last successfully restore from a backup?]	Backups should be tested frequently. The example provided may relate to a live or test environment.
7.3.6	Are your backups kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose?	Cloud synching services, such as OneDrive, SharePoint or Google Drive, should not be used as your only backup and stored backup should not be permanently connected to your network. Further guidance is available from the [National Cyber Security Centre](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)
8.2.2	The SIRO confirms that the risks of using unsupported systems are being managed and the scale of unsupported software is reported to your board along with the plans to address.	The SIRO has been briefed on the unsupported systems and has made a conscious decision to accept and manage the associated risks. A report has been provided to the board in the last 12 months. If no unsupported systems please tick and state "No unsupported systems" as a comment.
3.1.1 3.2.1	Dates changes to reflect current year	Moved to 01.07.2021 to 30.06.2022



CCG - ICS



ICS

Subject to the passage of legislation, it is expected that Integrated Care Boards (ICBs) will be established on 1st April 2022

The ICB will be responsible for submitting a Data Security and Protection Toolkit (DSPT) for 21-22.

In the event that ICBs are not yet established on the 1 April 2022, the responsibility for submitting the DSPT will remain with existing CCGs.

CCGs or ICBs must publish a DSP Toolkit for 2021-22 by 30th June 2022.

21-22 CCG / ICB Practicalities

DSP Toolkit Category

Both CCGs and ICBs will be Category 2 for 21-22. CCG Category to be renamed CCG/ICB

Baseline

CCGs not required to complete February 2022 Baseline. We are considering options of how to gain an understanding of the starting position of the ICBs.

Setting up ICB Toolkits

As soon as ICBs established ODS will be set up and DSP Toolkit organisations will be created

ICB Toolkit

Covers the legal entity of the ICB not all the organisations in the area

Audit

There is not an expectation that CCGs or ICBs will have a DSP Toolkit audit this year. It will be voluntary.

30th June 2020 and Improvement plans

There will be flexibility on the acceptance of Improvement plans (and there published status) for ICBS in June 2022.

Operator of Essential Service under NIS

It is expected that ICBS will be Operators of Essential Service under NIS, so NIS powers will apply to CCGs

Help and Support



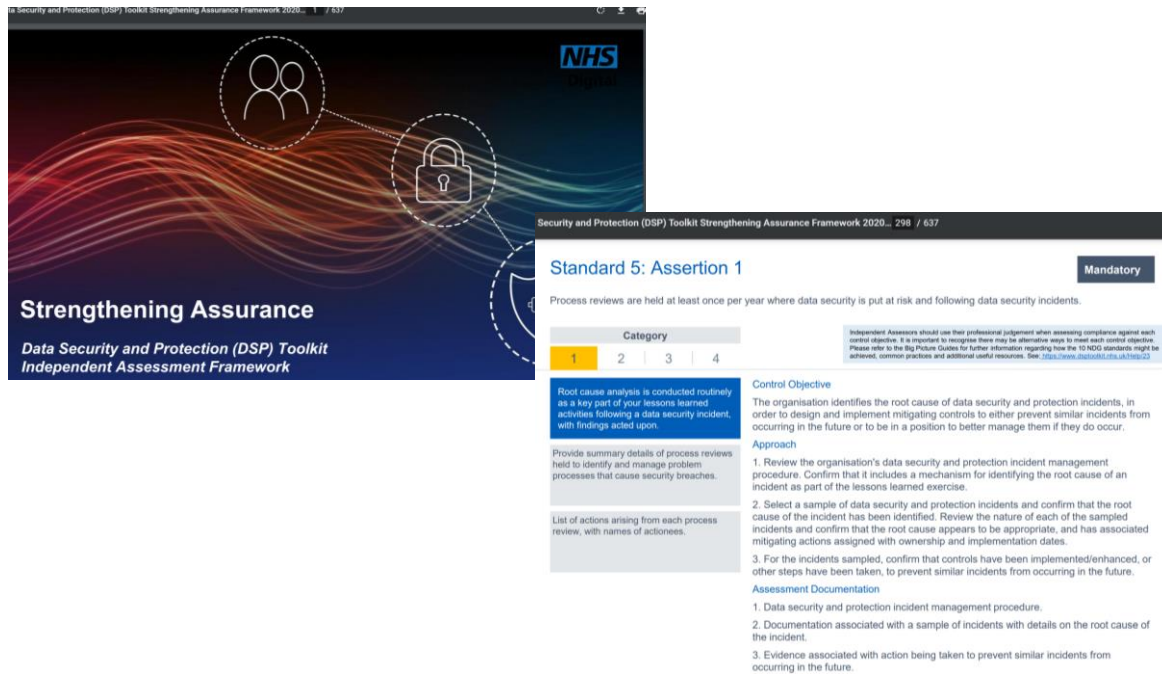
Resources to help

DSP Toolkit website has two main documents to help and the exeter.helpdesk@nhs.net.

Audit Guides

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

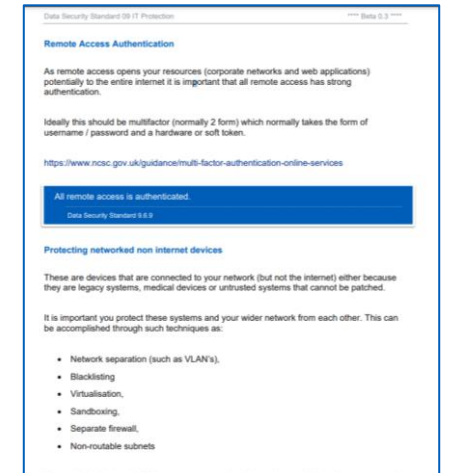
Useful as set out the requirement in a ISO 27001 style with control objective and documentation.



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