NHS Digital

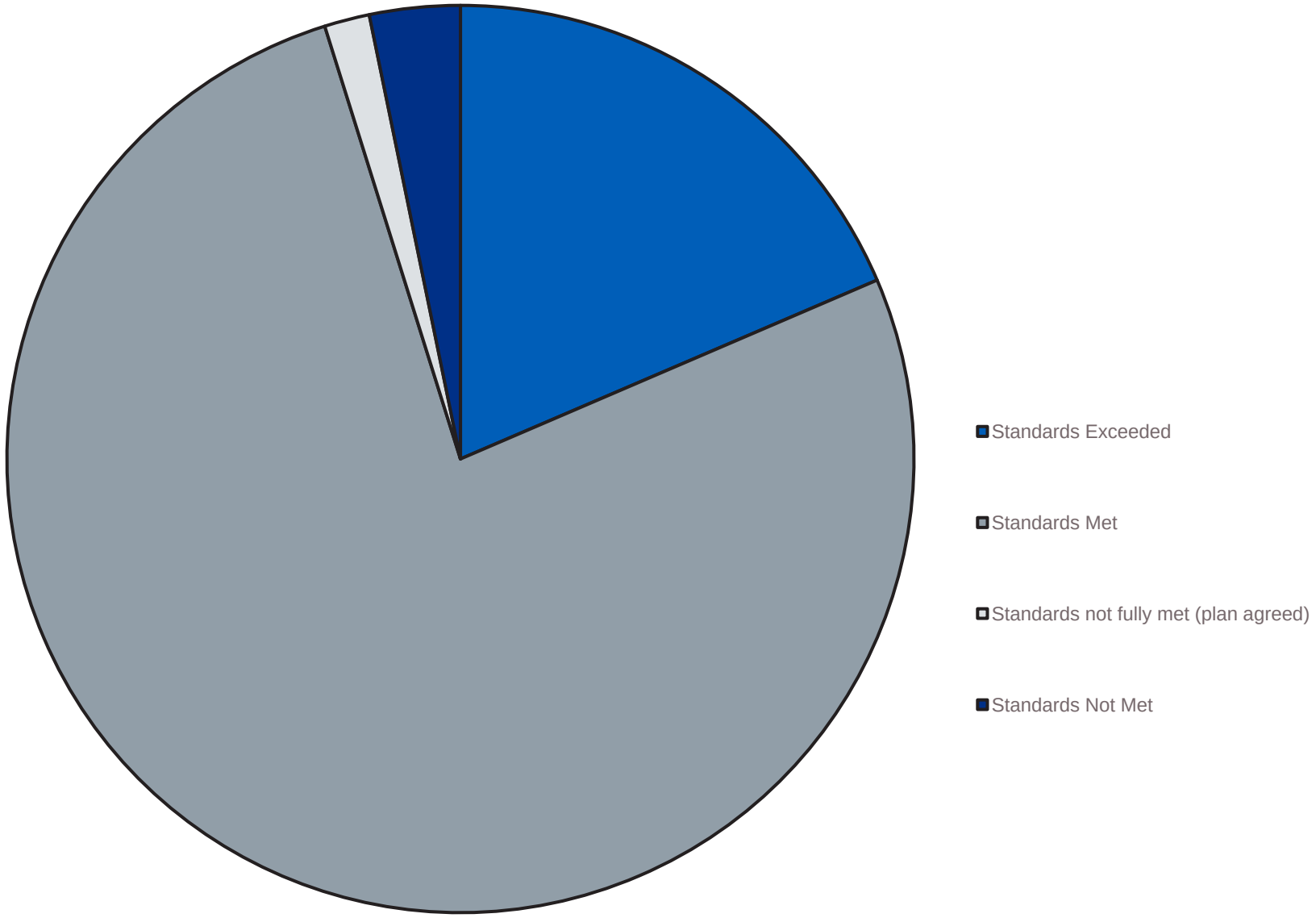
DSP Toolkit - CCGs

What's new for 21-22 and ICBs

October 2021 John Hodson

DSP Toolkit 20-21 Results

DSP Toolkit Status of CCGs 20-21



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

Audit Guide available at:
https://www.dsptoolkit.nhs.uk/News/auditnews

Deadline is 30th June 2022

Baseline 28th February 2022 for Trusts, CCGs(Voluntary), 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

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

Briefing at: https://www.dsptoolkit.nhs.uk/News/CCG-ICB-DSP-Toolkit

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

Scope of the 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 2022 deadline and Improvement plans

There will be flexibility on the acceptance of Improvement plans (and their 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 ICBs

Incidents

Should be reported by the organisation legally responsible and registered with ICO. So pre 1 April CCGs, post April 1 ICB

ICB Toolkit set up

Inherit STP ODS Code and Name	• Existing codes used across NHS Digital Services. • Background at Integrated Care Boards - NHS Digital • Name will change once overall naming convention agreed, i.e. NHS South Yorkshire Integrated Care Board
DSP Toolkit	• STP Organisations set up ready • CCG Toolkits will be closed and name change to agreed naming convention, i.e. NHS Doncaster CCG (Closed)
Administrators	• Email NHS Digital to set up an administrator exeter.helpdesk@nhs.net • They can set up other administrators, members and auditor accounts • Don't delete from CCGs just yet as may be required for Incidents and data transfer
Blank assessment	• Empty assessment produced • Manual data transfer required
Organisation Profile	• Select CCG as your category • You are not required to answer the questions about key roles or Cyber essentials to set up the organisation profile

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.

Completing the ICB Toolkit

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 undertake DQ audits 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.

Evidence Item 1.1.7

Data Quality

Evidence item 1.1.7

- Was the scope of the last data quality audit in line with guidelines.

Tooltip

- The data quality audit should be in the last twelve months and scoped to the [Service User Data Audit guidance.](https://www.dsptoolkit.nhs.uk/help/11)

To meet the DSP Toolkit in an ICB

1.1.7 **Was the scope of the last data quality audit in line with guidelines.**

Step 1 – Complete the Audit/s

- Acceptable to different data audits across merging CCGs and for them to have been completed before the ICB is established
- Must follow the guidance for DQ and be undertaken in the last twelve months

Step 2 – Documentation

- Produce report and action plan following audit
- Can be completed pre-ICB

Step 3 – ICB Reporting

Acceptable to have a summary report of all DQ audits presented to the DQ owner of the ICB or accountable group

Evidence Item 1.1.4

Review of Asset registers and data flows

Evidence item 1.1.4

- When did your organisation last review both the list of all systems/information assets holding or sharing personal information and data flows?

Tooltip

- The list should be reviewed since 1st July 2021 to ensure it is still up to date and correct. It should be approved by the SIRO or equivalent.

To meet the DSP Toolkit in an ICB

1.1.4 **When did your organisation last review both the list of all systems/information assets holding or sharing personal information and data flows?**

Step 1 – Complete the Reviews

- Acceptable to different data Asset registers and data flows systems across merging CCGs and for them to have been reviewed before the ICB is established
- Must follow the relevant guidance for data flows be undertaken since 01 July 2021

Step 2 – Documentation

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

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.

FAQs

Training

What staff training can be included?

Training requirement is designed to be a ’simple’ calculation.

So thew bottom half of the equation is the number of staff in the ICB.

The top half of the equation is the number of staff who have been trained.

This training can be completed training since 01 July 2021-30 June 2022 can be included.

Must the training be counted once staff were ICB employed?

It doesn’t matter if they did when they were employed by the CCG or anyone else.

Do all merging CCs need to meet the 95% target

It doesn’t matter if all the merging CCGs met 95% only that the ICB total is above 95%

Help and Support

Resources to help

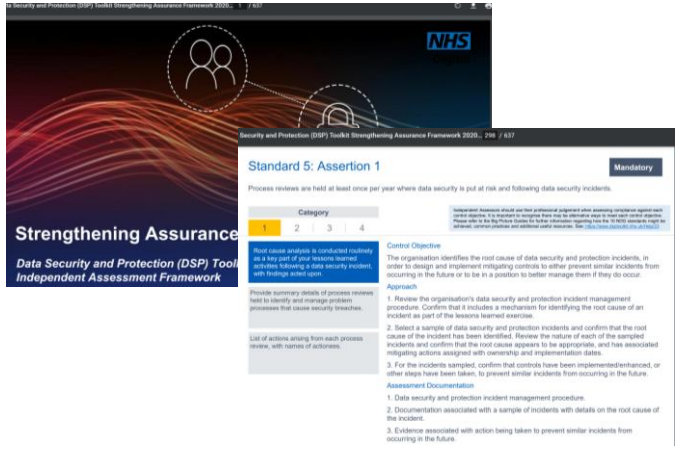
ICCG Briefing: Briefing at: https://www.dsptoolkit.nhs.uk/News/CCG-ICB-DSP-Toolkit *and the exeter.helpdesk@nhs.net.*

Plus Monthly webinars News (dsptoolkit.nhs.uk)

Audit Guides

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

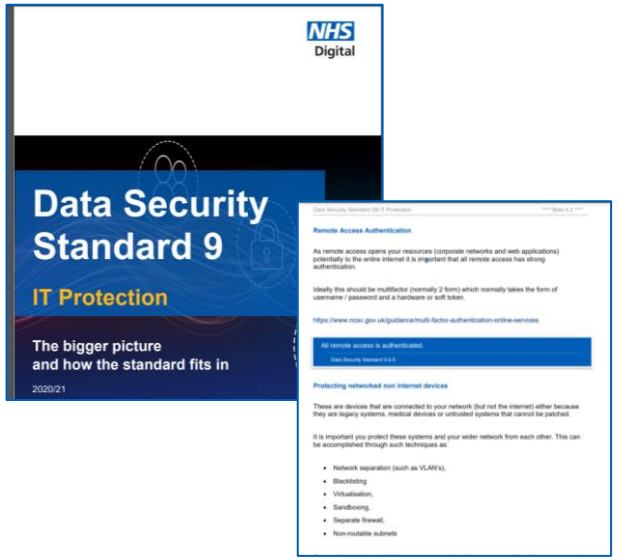
Useful as set out the requirement in a ISO 27001 style with control objective and documentation.



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?

Thank You

@nhsdigital

company/nhs-digital

digital.nhs.uk

NHS Digital