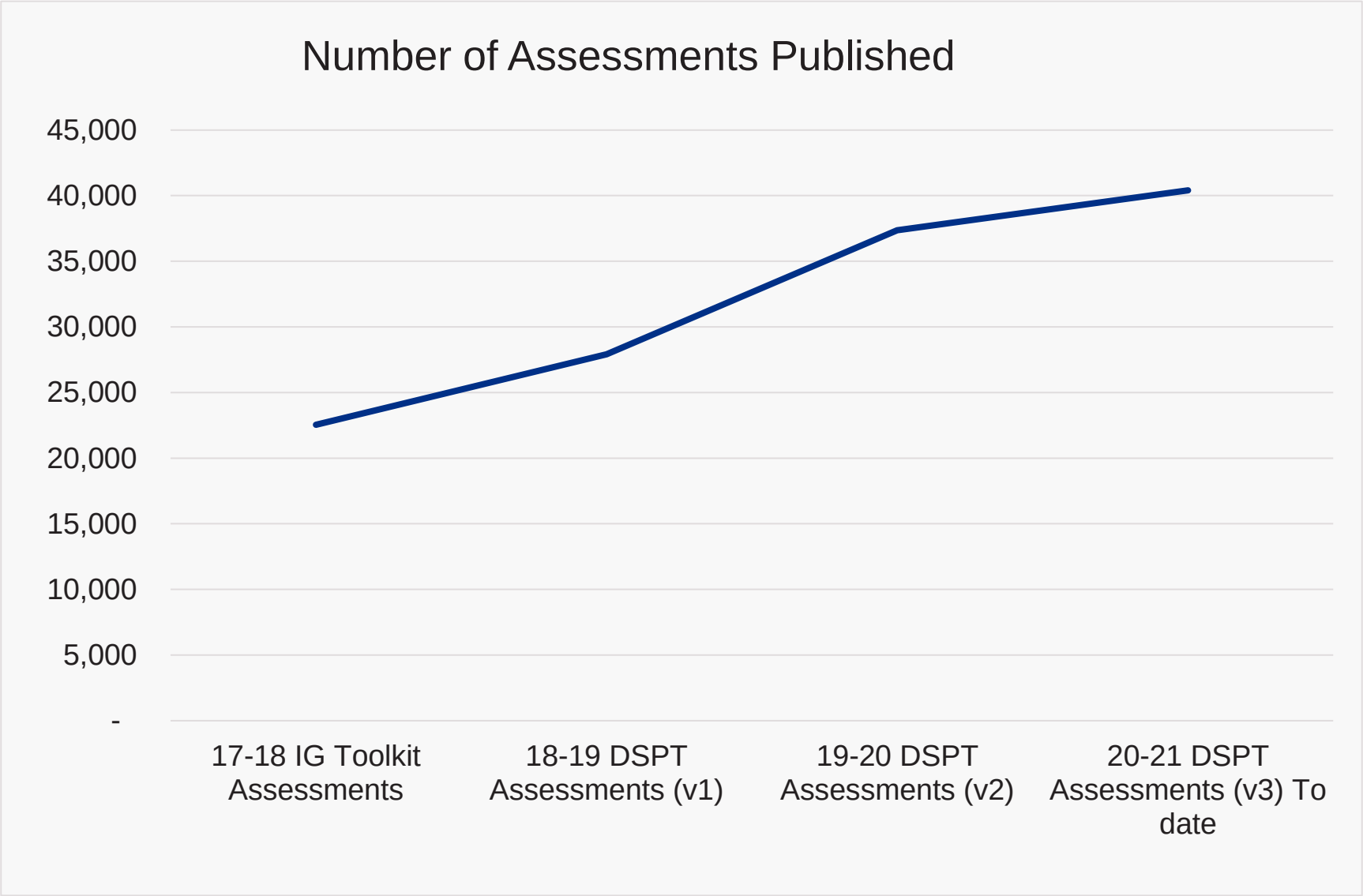
NHS Digital

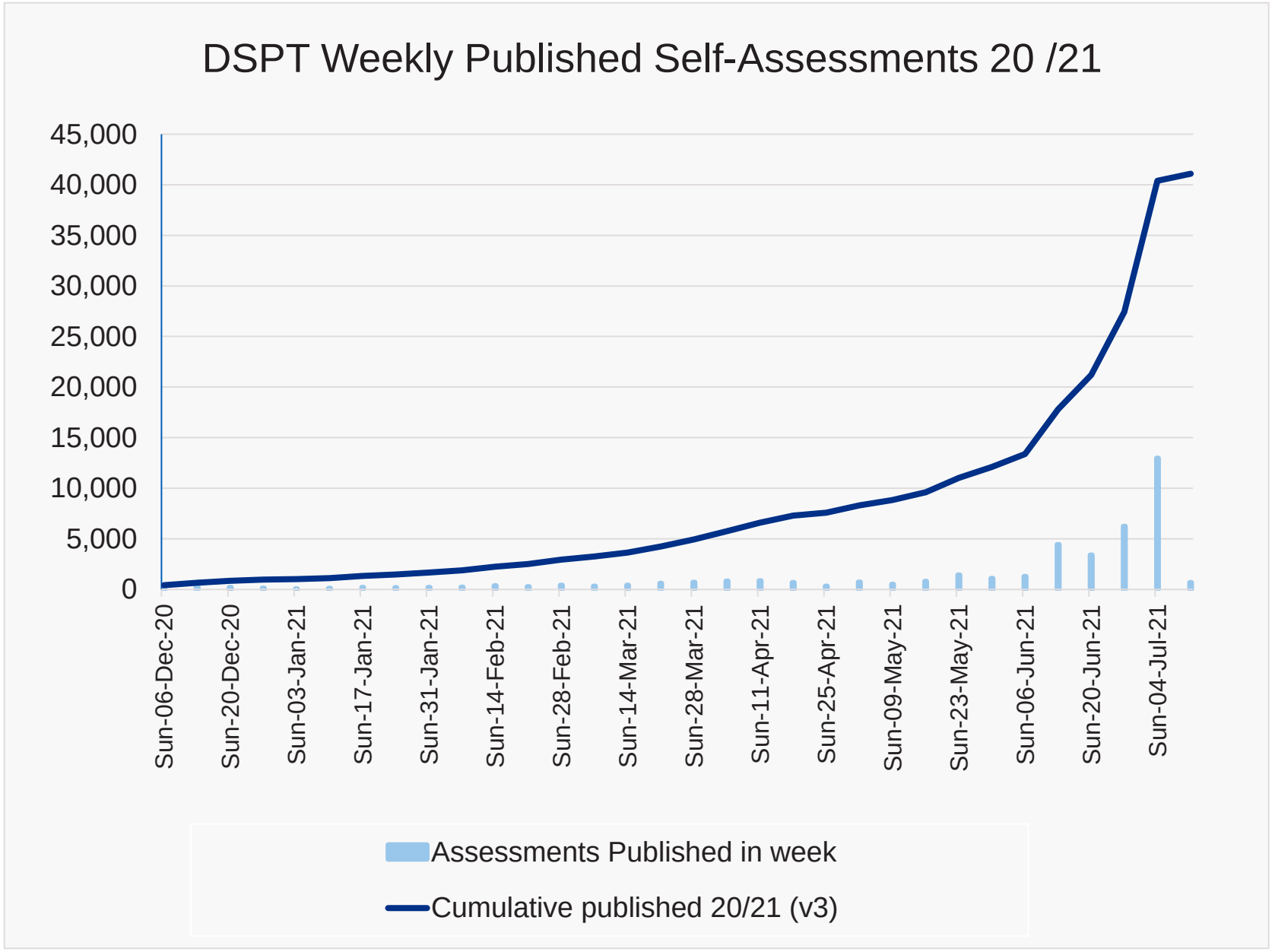
DSP Toolkit

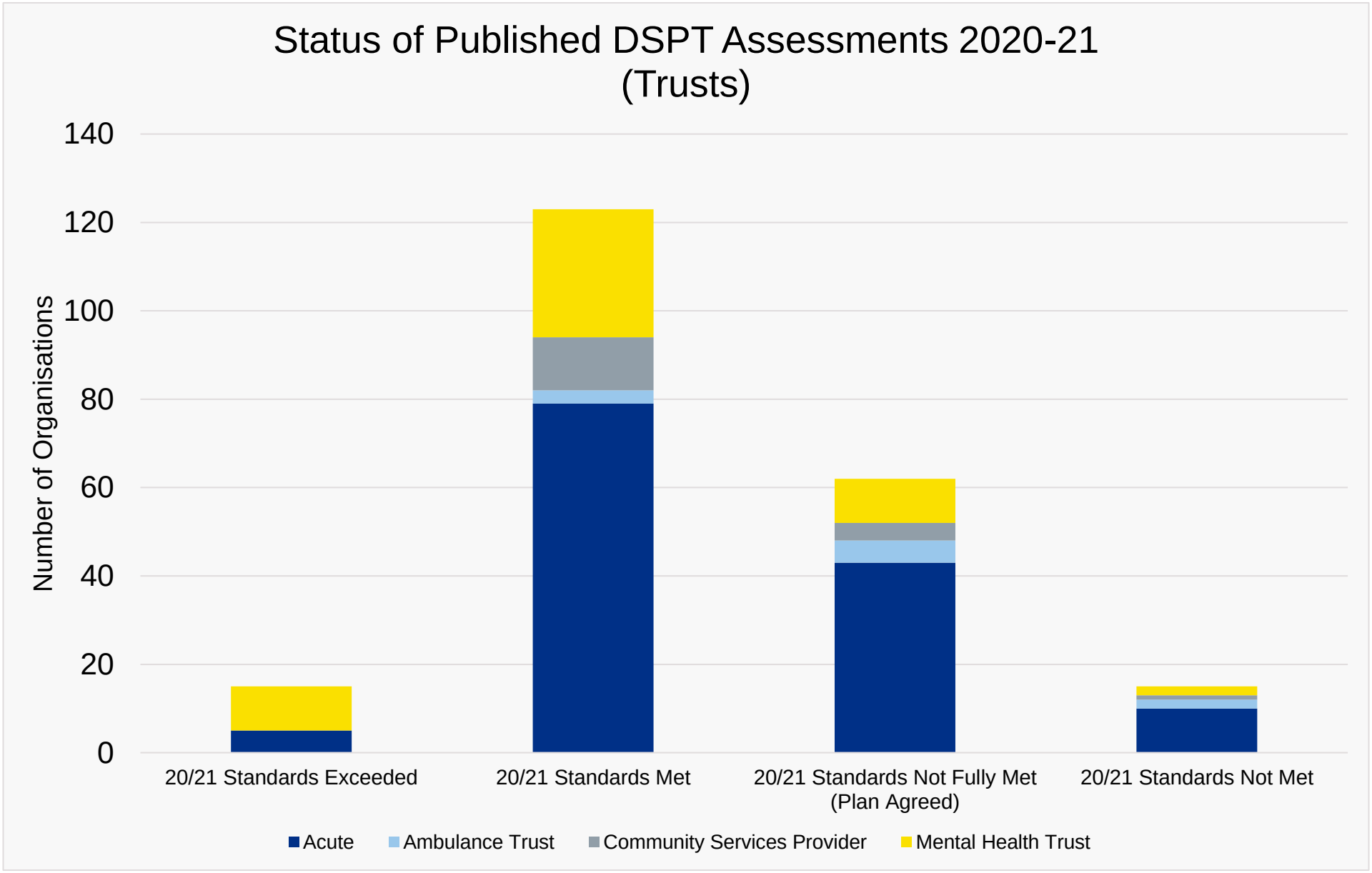
What's new for 21-22

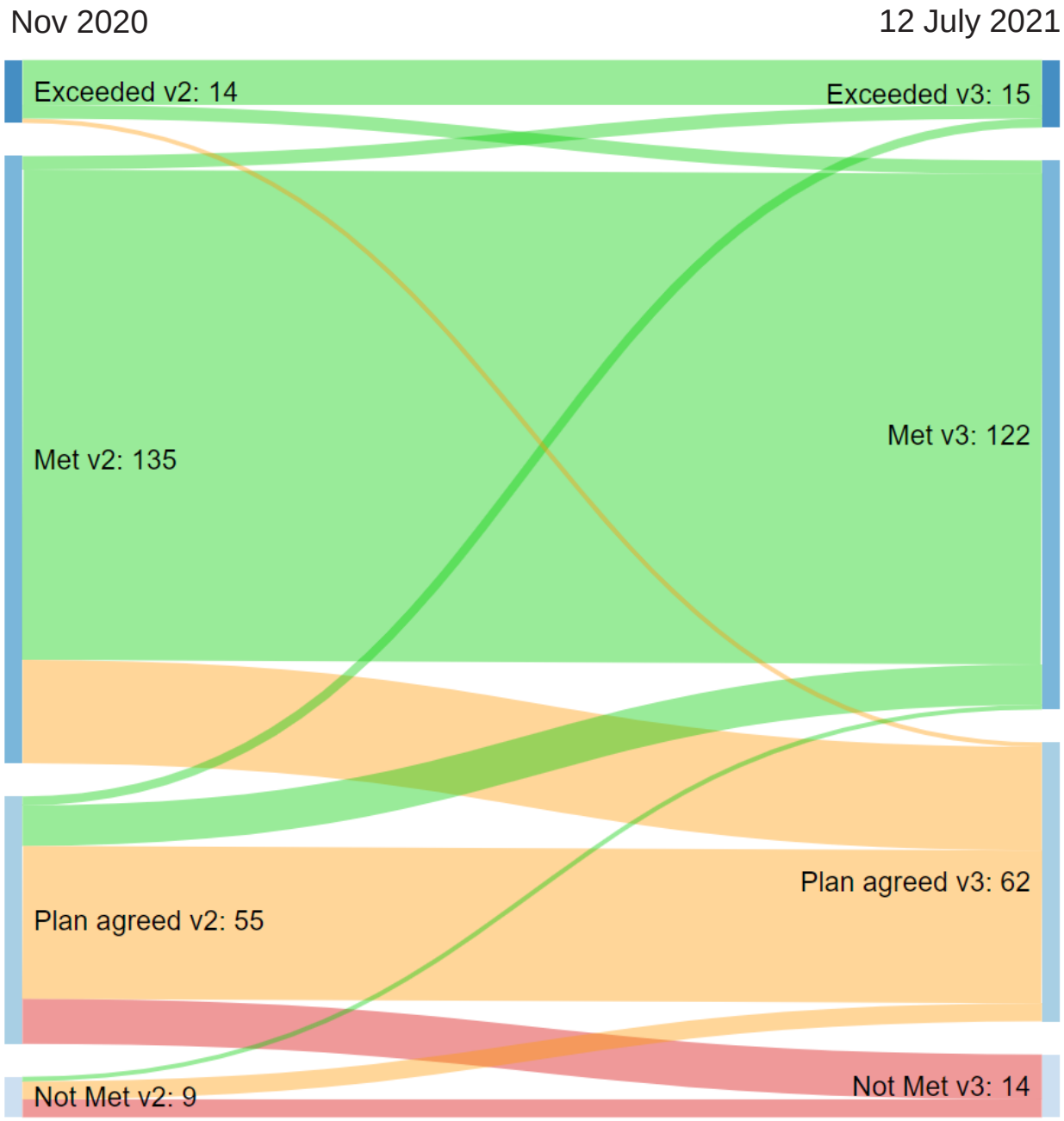
September 2021 John Hodson

DSP Toolkit 20-21 Results


Number of Assessments Published
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) To date


DSPT Weekly Published Self-Assessments 20 /21
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
Sun-06-Dec-20
Sun-20-Dec-20
Sun-03-Jan-21
Sun-17-Jan-21
Sun-31-Jan-21
Sun-14-Feb-21
Sun-28-Feb-21
Sun-14-Mar-21
Sun-28-Mar-21
Sun-11-Apr-21
Sun-25-Apr-21
Sun-09-May-21
Sun-23-May-21
Sun-06-Jun-21
Sun-20-Jun-21
Sun-04-Jul-21
Assessments Published in week
Cumulative published 20/21 (v3)


Status of Published DSPT Assessments 2020-21 (Trusts)
Number of Organisations
140
120
100
80
60
40
20
0
20/21 Standards Exceeded
20/21 Standards Met
20/21 Standards Not Fully Met (Plan Agreed)
20/21 Standards Not Met
Acute
Ambulance Trust
Community Services Provider
Mental Health Trust


Nov 2020
12 July 2021
Exceeded v2: 14
Met v2: 135
Plan agreed v2: 55
Not Met v2: 9
Exceeded v3: 15
Met v3: 122
Plan agreed v3: 62
Not Met v3: 14

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, 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 will be amended to Standards not met.
- All NHS Trusts and Foundation Trusts are classified as Operators of Essential Services under the Network and Information Systems (NIS) Regulations 2018.
- So a Trust may be issued with an Information Notice to require them to provide information or an Enforcement Notice requesting them to take specified steps as required under the regulations.

What are the new Mandatory requirements

NHS Trusts – IT

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.
8.3.5	Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.	Provide details for each patch not applied. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services.
9.3.8	The organisation maintains a register of medical devices connected to its network.	The register should be uploaded and include Vendor, maintenance arrangements, any network segmentation is in place and whether network access is given to supplier/maintainer. See www.****.nhs.uk/CMDs for further information on medical device registers

NHS Trusts – 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
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

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

NHS Trusts

1.1.6	Your organisation has reviewed how you ask for and record consent.	Provide details in the comments. Further details https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/
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.
9.3.9	What is the organisations data security assurance process for medical devices connected to the network.	This should a policy /process document or full explanation covering how the organisation assures data security during the full life cycle of the medical device.

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

NHS Trust

4.2.3	Logs are retained for a sufficient period, **managed securely**, reviewed regularly and can be searched to identify malicious activity	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. **Organisations should consider the ability to trace an incident end to end e.g. network address translation. Please refer to [National Cyber Security Centre guidance.](https://www.ncsc.gov.uk/files/NCSC_SOC_Feeds.pdf)**
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.

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.

Help and Support

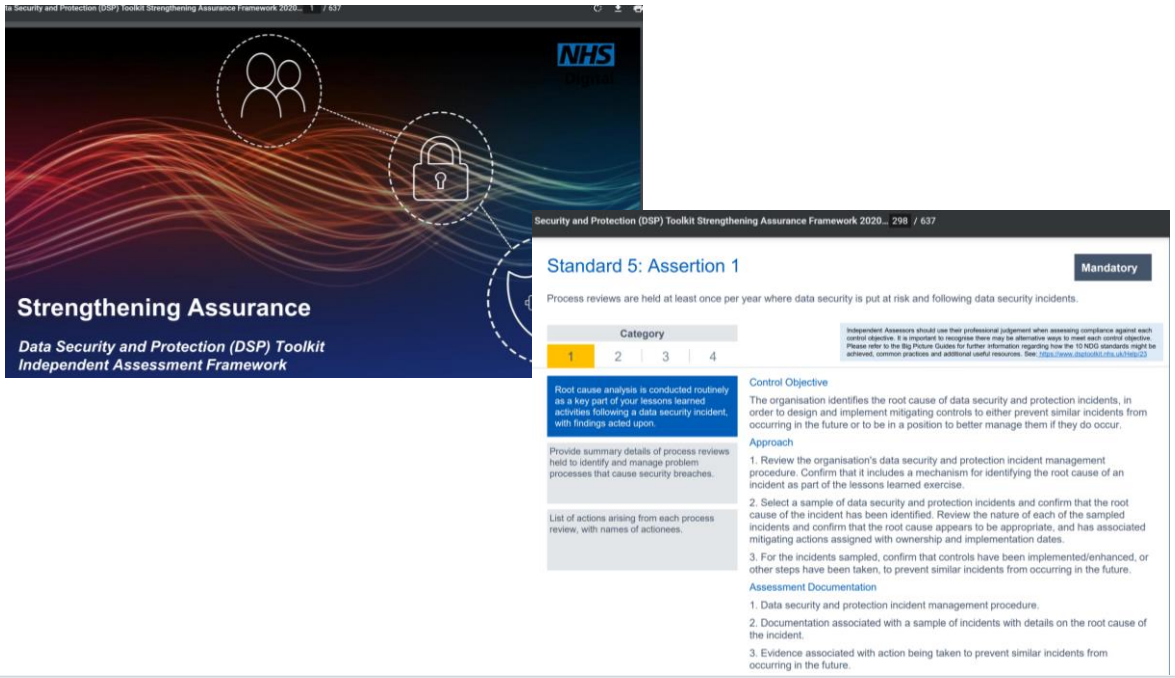
Resources to help

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

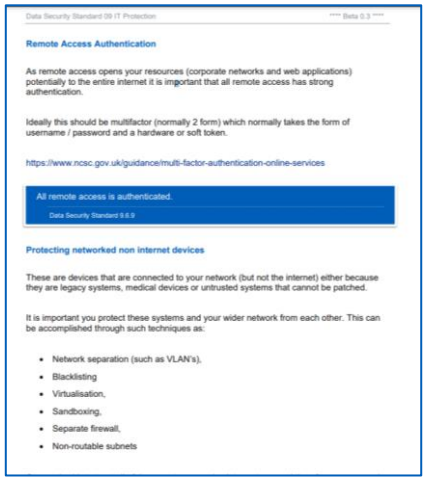
Useful as set out the requirement in a ISO 27001 style with control objective and documentation.



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?

Thank You

@nhsdigital

company/nhs-digital

digital.nhs.uk

NHS Digital