NHS Digital

DSP Toolkit

Update for CCGs, CSUs and ALBs

March 2022 John Hodson

DSP Toolkit for 21-22

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 .

Status Change

Standards not fully met (plan agreed) changed to Approaching Standards.

What are the new Mandatory requirements for CCGs and ALBs

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 for CCGs/CSUs

CCG / CSU /ALBs

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)**
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.**
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.

Improvement plans

Improvement plans

Requirement to submit updated Improvement plan by 31 December 2021 was withdrawn

No new deadline will be set

Due to impact of COVID 19 and Log4J

Updated plans can still be submitted

Where all the outstanding actions are complete we can still amend status for 21-22

Where current status is Approaching Standards this will remain until 21-22 DSP Toolkit submitted

Baseline

Baseline

Required by NHS Trusts, CSUs and DHSC Arm's Length bodies

Not required for CCGs

Deadline 4th March 2022

For CSUs and ALBs
Specific responses required for 6 evidence items to support operational resilience for Cyber security.

CCGs / ICBs

CCG / ICB

Who is completing	CCGs will complete a DSP Toolkit using CCG ODS Code Deadline 30 June 2022
Baseline	CCGs not required to complete a CCG baseline publication CSUs and ALBs were required to complete
Audit	CCGs not required to complete a CCG DSP Toolkit Audit Can complete a Voluntary audit 9.4.5 will be marked exempt for CCGs
22-23 DSP Toolkit	ICB will complete a DSP Toolkit in 22-23 For the legal entity of the ICB not for the whole ICS patch Expected to be Category 1 and may have extra evidence items covering cyber risk management role over ICS patch
Operator of Essential Service under NIS	ICBs will be Operators of Essential Service under Network and Information Systems (NIS) Directive Further detail on NIS https://www.gov.uk/government/publications/network-and-information-systems-regulations-2018-health-sector-guide

Further considerations

ICBs not required to complete a DSP Toolkit for 21-22 or a baseline

ICB ODS Codes will remain the same for 2022-23

Using STP Codes

CCG Improvement plans will require additional information about hand over to ICB

Functionality is available to copy evidence from one DSP Toolkit to another if you are completing multiple CCG Toolkits

News

Further details on News pages of DSP Toolkit

Log4J Evidence item 8.3.4 change Cyber alert CC-3989 should be excluded when determining if the organisation has achieved this evidence item

New Caldicott Guardian guidance and free e-learning available

Organisation Types simplified

Status label changed to Approaching Standards from Standards not fully met (plan agreed)

Social Care support available through Better Security, Better Care programme

What is coming…

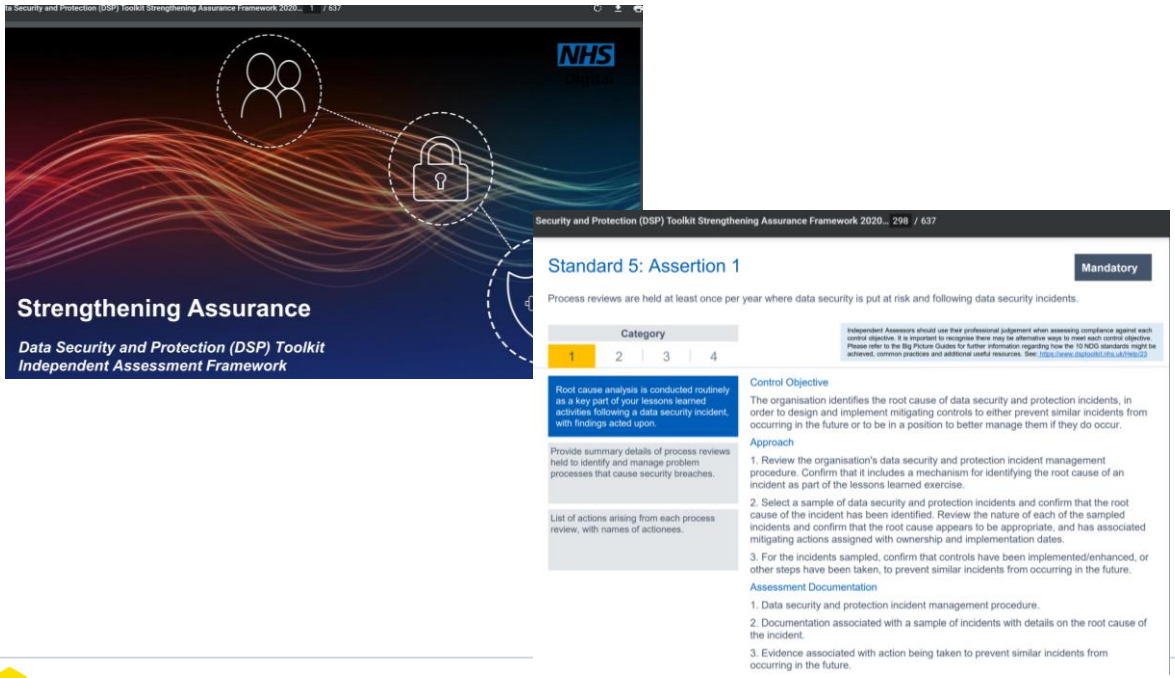
Resources to help

DSP Toolkit website has two main documents to help and our Webinars (https://www.dsptoolkit.nhs.uk/News/webinars) and the exeter.helpdesk@nhs.net.

Audit Guides

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

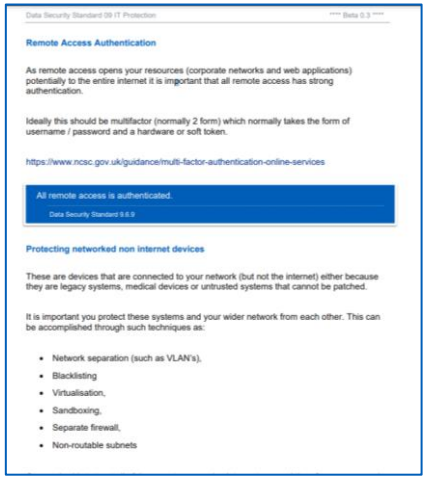
Useful as set out the requirement in a ISO 27001 style with control objective and documentation.



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?

Future Webinar details

https://www.dsptoolkit.nhs.uk/News/webinars

NHS Digital

Thank You

@nhsdigital

company/nhs-digital

digital.nhs.uk