

Meeting Title	Open Board of Directors		
Date	12 May 2022	Agenda item	Bo.5.22.29

Data Security and Protection Toolkit (DSPT) Assessment 2021/22

Presented by	Paul Rice, Chief Digital and Information Officer		
Author	Jenny Pope, Head of Information Governance Graeme Holmes, Information Governance Manager		
Lead Director	Paul Rice, Chief Digital and Information Officer		
Purpose of the paper	This paper sets out the position on the annual Data Security and Protection Toolkit (DSPT) 2021/22 assessment 'rating'		
Key control			
Action required	For approval		
Previously discussed at/ informed by			
Previously approved at:	Committee/Group	Date	
	Digital and Data Transformation Committee	TBC	

Key Options, Issues and Risks

The Data Security & Protection Toolkit (DSPT) is a Department of Health and Social Care (DHSC) policy delivery vehicle that NHS Digital is commissioned to develop and maintain. It is an online self-assessment tool that allows organisations to measure their performance and provide an Assurance of Standards Met against all mandatory Assertions in line with the National Data Guardian's data security standards.

This paper updates the Board on the expected final position. It sets out the recommended Data Security and Protection Toolkit (DSPT) annual assessment 'rating' at this stage. The 2021/22 DSPT Assessment final submission will take place on 30 June 2022.

There are 38 Assertions in total (5 are non-mandatory) comprising of 110 mandatory evidence items. 28 of the Assertions are complete and confirmed at the time of this report. Evidence and supporting statements provided by Assertion Owners are being reviewed. Evidence against all mandatory items will be confirmed complete prior to submission.

Analysis

During the year the Information Governance Service has sought evidence from the business against the mandatory standards set out in the DSPT, receiving assurance from individuals with responsibilities for the area(s) concerned (identified as Assertion Owners) that their evidence complies with the DSPT. A review of all available evidence had been completed at the time of this report. A review of remaining evidence is ongoing.

Audit Yorkshire has begun its review of Assertion items this Assessment year. The review began week commencing 19 April 2022 and is expected to complete during May. The review was incomplete at the time of this report and a report of the outcome by Audit Yorkshire is outstanding.

Recommendation

The Board is asked to note the position outlined. The Digital and Data Transformation Committee is asked to approve the DSPT submission on behalf of the Board of Directors.

Meeting Title	Open Board of Directors		
Date	12 May 2022	Agenda item	Bo.5.22.29

Risk assessment						
Strategic Objective	Appetite (G)					
	Avoid	Minimal	Cautious	Open	Seek	Mature
To provide outstanding care for patients			g			
To deliver our financial plan and key performance targets			g			
To be in the top 20% of NHS employers			g			
To be a continually learning organisation				g		
To collaborate effectively with local and regional partners					g	
The level of risk against each objective should be indicated. Where more than one option is available the level of risk of each option against each element should be indicated by numbering each option and showing numbers in the boxes.	Low		Moderate	High	Significant	
	Risk (*)					
Explanation of variance from Board of Directors Agreed General risk appetite (G)						

Benchmarking implications (see section 4 for details)	Yes	No	N/A
Is there Model Hospital data relevant to the content of this paper?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is there any other national benchmarking data relevant to the content of this paper?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the Trust an outlier (positive or negative) for any benchmarking data relevant to the content of this paper?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Regulation, Legislation and Compliance relevance
NHS Improvement: (please tick those that are relevant) <input type="checkbox"/> Risk Assessment Framework <input type="checkbox"/> Quality Governance Framework <input type="checkbox"/> Code of Governance <input type="checkbox"/> Annual Reporting Manual
Care Quality Commission Domain: Well Led
Care Quality Commission Fundamental Standard: Good Governance
NHS Improvement Effective Use of Resources:
Other (please state): Data Protection Act 2018, General Data Protection Regulation and Data Security and Protection Toolkit (DSPT) standards

Relevance to other Board of Director's Committee: (please select all that apply)					
Workforce	Quality	Finance & Performance	Partnerships	Major Projects	Other (please state)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Meeting Title	Open Board of Directors		
Date	12 May 2022	Agenda item	Bo.5.22.29

1 PURPOSE/ AIM

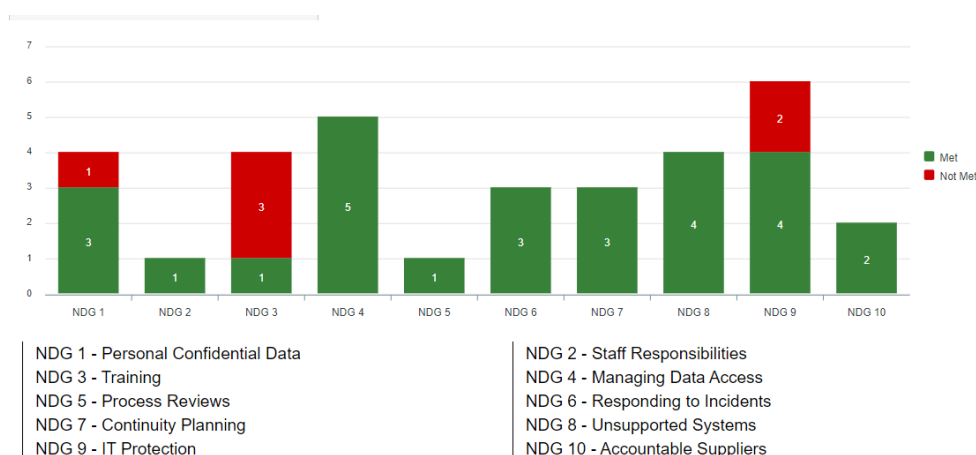
The purpose of this report is to update the Board on the current position of the 2021/22 Data Security and Protection Toolkit (DSPT) Assessment.

2 BACKGROUND/CONTEXT

The Information Governance Service has received updates from Assertion Owners and their assurances on evidence they have provided to comply with the DSPT.

A review of available evidence has been completed and the remainder ongoing.

Progress against individual Assertion Items is monitored via a separate DSPT plan. The graph below summarises the current position.



Audit Yorkshire has reviewed a sample of Assertion items this Assessment year, beginning 19 April and to conclude in May 2022. Its review and report of the outcome of the review was outstanding at the time of this report.

Any recommendations fundamental to, or supplementing existing evidence, will be completed prior to submission. If these are necessary for overall compliance they will be completed by 30 June 2022. A summary position is included within the appendices.

It is to be noted that Audit Yorkshire's review is conducted in accordance with the new national DSPT audit framework, Strengthening Assurance, developed for NHS Digital with a new mandated audit approach and introduced in 2020/21. This means the format and assurance the report provides is again very different to previous years, and the testing beyond what is asked in the DSPT.

3 PROPOSAL

Once all mandatory items for a particular Assertion are complete and have been reviewed they are considered 'met'.

Final submission is 30 June 2022. The usual annual submission deadline of 31 March was changed in 2020/21 for all organisations due to the pandemic.

A separate 'DSPT plan' tracks progress against each Assertion item, mandatory and non-mandatory. The graph above shows a number of Assertion items incomplete at the time of this report. These are related to Standard NDG 1, 3 and 9. They will be complete prior to the final submission.

The SIRO and Digital Data Transformation Committee (DDTC) reviews the final assessment on 15 June 2022 and accepts that the DSPT overall self-assessed rating of 'Standards Met' has been achieved.

Meeting Title	Open Board of Directors		
Date	12 May 2022	Agenda item	Bo.5.22.29

4 BENCHMARKING IMPLICATIONS

N/A

5 RISK ASSESSMENT

Non-compliance with the DSPT could lead to reputational damage to the Trust and scrutiny from external stakeholders.

In the event of an externally reportable serious IG breach, non-compliance with the DSPT may contribute to the Information Commissioner Office (ICO) decision to take any action including potential monetary penalties.

Risks to quality of DSPT Assessments are monitored via the DSPT Plan and via the SIRO.

6 RECOMMENDATIONS

It is recommended that the Board approves the 2020/21 DSPT Assessment, which equates to a position of compliance with all mandatory Assertion items resulting in a 'Standards Met' position. The Digital Data Transformation Committee is asked to approve the DSPT submission on behalf of the Board of Directors on completion of the Assessment, before 30 June 2022. This is subject to final evidence as outlined above.

7 Appendices

Appendix A: Summary Position from DSPT Plan (see separate attachment)

Appendix B: The National Data Guardian 10 data security standards of the DSPT.

Meeting Title	Open Board of Directors		
Date	12 May 2022	Agenda item	Bo.5.22.29

Appendix B

NDG Standard	
1 Personal Confidential Data	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes
2 Staff Responsibilities	All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3 Training	All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.
4 Managing Data Access	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
5 Process Reviews	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6 Responding to Incidents	Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection
7 Continuity Planning	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management
8 Unsupported Systems	No unsupported operating systems, software or internet browsers are used within the IT estate
9 IT Protection	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually
10 Accountable Suppliers	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards