

Data Security and Protection Toolkit Independent Assessment – Phase 2

**Bradford Teaching Hospital NHS Foundation Trust
BH/25/2021**



Table of contents

Heading	Page
Executive summary	1
Distribution List	6
Detailed advisory report	7
Appendix A – Basis of our classifications	15
Appendix B – Limitations and responsibilities	19
Appendix C – National Data Guardian (NDG) Standards	20

Report Author: Kuljit Singh
Report Version: Final
Report Date: 26 May 2021



Introduction and Background

Department of Health policy requires that all organisations which process NHS patient information, for whatever purpose, should provide assurance via the Data Security and Protection (DSP) Toolkit. The DSP Toolkit is an online tool that enables organisations to measure their performance against national data security and information governance standards, and to evidence this by the publication of annual assessments.

Completion of the DSP Toolkit provides Health and Social Care organisations with insight into the technical and operational data security and protection control environment and relative strengths and weaknesses of those controls.

Trusts and CCGs are subject to mandatory audit of their Toolkit self-assessment. This year, the review was conducted in accordance with the new national DSP audit framework, Strengthening Assurance, developed for NHS Digital by external assessors PWC. The approach to testing *'[goes] beyond what is asked in the DSP Toolkit'* with a view to *'inform and drive measurable improvement of data security ... and not just simply assess compliance with the DSP Toolkit'* (Introduction p5).

In considering whether the organisations meet each evidence requirement, we have exercised our professional judgment and drawn on our prior knowledge of the organisations' data security and protection control environment.

The audit was conducted in accordance with the advised scope for 2020-21.

The audit is taking place in two stages, comprising:

1. a substantive review during March 2021. We recognise that the Toolkit is due for submission at the end of June 2021, and at the point of the review, some assertions and supporting evidence may be incomplete. We will take this opportunity to provide interim auditor feedback through an advisory report, indicating any areas likely to require more focused attention prior to submission, and
2. a follow-up review during May 2021, checking that any areas of risk have been appropriately addressed, and resulting in the formal audit opinion.

Reporting period: 01 April 2020 to 30 April 2021

System Objective

The objective of the Toolkit is to enable organisations to measure their performance against the National Data Guardian's ten data security standards.



Objectives & Scope

The objective of the review is twofold:

- a) to satisfy the annual requirement for an independent assessment of the DSP Toolkit submission
- b) to understand and help address data security and data protection risk and identify opportunities for improvement.

In order to meet this objective, the audit tested the sample of assertions selected by NHS Digital for assessment in the current year, focusing on the mandatory evidence questions. The results of the assessment are summarised below, in accordance with the Strengthening Assurance reporting requirements described at Appendix A. Further detail of the audit findings and recommendations are given in Section 3.



Section 1: Executive Summary

Audit Assessment

Interim Assessment at date of report	Risk Rating across all 10 NDG Standards	Moderate
	Assurance level based on the confidence level of the Independent Assessor in the veracity of the self-assessment	Medium

Whilst the outputs of our assessment denote an 'Overall risk assessment across all 10 NDG Standards' as 'Moderate', and an 'Assurance level based on the confidence level of the Independent Assessor in the veracity of the self-assessment' as 'Medium', it is important to detail the contributing factors that lead to these report outputs. The above ratings should not be viewed in too negative a light as it reflects a number assertion owners not providing relevant supporting evidence to supplement assertion requirements and does not reflect the good practice and effective controls (some of which are outlined on the following page).

Derivation:

National Data Guardian Standard*	Number of assertions assessed	Number rated Critical	Rated High	Rated Medium	Rated Low	Risk Points for Standard (Low = 1)	Standard Level Classification	Overall Risk Assessment	Overall Confidence in Submission
1. Personal Confidential Data	2 of 8 in standard	0	0	0	2	2	Substantial	Moderate	Medium
2. Staff Responsibilities	1 of 1	0	0	0	1	1	Substantial		
3. Training	1 of 4	0	0	0	1	1	Substantial		
4. Managing Data Access	1 of 5	0	0	1	0	2	Moderate		
5. Process Reviews	1 of 3	0	0	1	0	3	Moderate		



Section 1: Executive Summary

National Data Guardian Standard*	Number of assertions assessed	Number rated Critical	Rated High	Rated Medium	Rated Low	Risk Points for Standard (Low = 1)	Standard Level Classification	Overall Risk Assessment	Overall Confidence in Submission
6. Responding to Incidents	1 of 3	0	0	0	1	1	Substantial		
7. Continuity Planning	2 of 3	0	0	1	1	3	Moderate		
8. Unsupported Systems	2 of 4	0	0	1	1	2	Moderate		
9. IT Protection	1 of 6	0	0	0	1	1	Substantial		
10. Accountable Suppliers	1 of 5	0	0	1	0	3	Moderate		
Total	13 of 34	0	0	5	8	19			

*See Appendix C for an expanded description of each Standard

Note: In accordance with NHS Digital guidance, each assertion is risk assessed and a score awarded based on likelihood and impact. Full detail of the assessment and scoring methodology is shown in Appendices A and B.

Summary of Findings

On completion of sample testing as required by the Strengthening Assurance Framework, the review found an overall medium level of risk to the confidentiality, integrity and availability of the Foundation Trust's data assets.

Robust policies and procedures were seen to be in place to deliver compliance with the data security and protection requirements set out in the Toolkit, however the Foundation Trust's assertions could not be fully verified by confirmatory evidence.

This resulted in a Medium confidence rating in the veracity of the Foundation Trust's self-assessment return.

Examples of good practice included:



- Adoption of a comprehensive approach to Data Protection by Design and Default, with a Pseudonymisation policy in place. Data protection has been adopted into wider business, alongside significant technical controls to prevent information being inappropriately downloaded.
- Robust procedures for staff data security and awareness induction and ongoing refresher training were found to be in place, underpinned by an appropriate training needs analysis review. Monitoring arrangements are embedded to ensure staff are compliant with induction training.
- The audit review identified a comprehensive process for the management of alerts received, involving the containing and investigation of these.
- The Foundation Trust has a patch management process in place, which is supported by management reporting on key performance indicator data.
- Regular penetration tests are performed and supported by action plans, to help ensure that risks from unauthorised access to the network are minimised. A penetration test was recently undertaken in March 2021, the Foundation Trust is awaiting the final report findings.

The audit found that the Foundation Trust's active engagement with the Toolkit standards had successfully identified areas where the control environment could be strengthened still further. Action plans were in place and sighted by the SIRO and IG Team, to ensure full compliance with those requirements, these areas are highlighted at Section 3.



Section 2: Distribution List

Name	For action	For information
Draft to		
<ul style="list-style-type: none"> Jenny Pope Head of Information Governance/Data Protection Officer 	✓	
<ul style="list-style-type: none"> Paul Rice, Chief Digital and Information Officer 	✓	
<ul style="list-style-type: none"> Graeme Holmes, Information Governance Manager 	✓	
Final Report to		
<ul style="list-style-type: none"> Matthew Horner, Director of Finance 		✓
<ul style="list-style-type: none"> Jacqui Maurice, Head of Corporate Governance 		✓
<ul style="list-style-type: none"> Sheridan Osborne, Corporate Governance Officer 		✓
<ul style="list-style-type: none"> Laura Parsons, Associate Director of Corporate Governance/Board Secretary 		✓

Audit Assessment

Finding <div>1</div>	Finding: Physical access prevention controls (1.6.3) <p>NHS Digital Big Picture guidance recommends best practice with recommendations and examples of how the standards might be achieved. The guidance for this assertion stipulates "It is important that only the people who are intended to see, access, modify and delete data do so and not others. These can include, but are not limited to":</p> <ul style="list-style-type: none"> • lockable doors, windows and cupboards • clear desk procedures • identification ID key card • access code locks for secure areas. <p>The Assertion Owner has provided insufficient evidence to confirm the undertaking of regular formal audits, to assess unauthorised access controls to locations where Personal data is stored and processed.</p>
	Implication
Finding rating	It important that only the people who are intended to see, access, modify and delete data do so and not others. As technology and IT risks continue to change, there is a risk that controls may become ineffective or outdated. Consequently, this may leave the Foundation Trust more vulnerable to cyber-attack.
Low	
	Recommendation <p>1. A regular formal testing programme of audits should be in place, to assess that physical access prevention controls are being implemented in practice and continue to work effectively.</p> <p>Responsible officer: Ian Scott, Deputy Head of Information Technology</p> <p>Completion date: 30 June 2021</p>



Finding <div>2</div>	Finding: Employment Contracts (2.2.2) <p>Clauses in Foundation Trust employment contracts should reference data security (confidentiality, integrity and availability). The review confirmed that Foundation Trust contracts contain a section on Duty of Confidentiality. It stipulates that 'confidential information should not be disclosed to any other person unless in the pursuit of your duties or with specific permission given but us. You must ensure that the confidentiality and security of all information is maintained in accordance with the requirements of the UK Data Protection legislation'.</p> <p>The contract does not currently mention requirements to adhere to relevant IT security policies and procedures, as required to evidence compliance with the Toolkit.</p>
	Implication
Finding rating	It is important that all staff understand their contractual employment 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.
Moderate	
	Recommendation <p>2. Information Governance Team to liaise with Human Resources to discuss revision of Employment contracts to ensure they make appropriate reference to data security IT policies and procedures.</p> <p>Responsible officer: Jenny Pope, Head of Information Governance/Data Protection Officer</p> <p>Completion date: 30 June 2021</p>



Finding <div>3</div>	Finding: User Access Audit (4.2.1)
	<p>The Foundation Trust should undertake an audit within each reporting year to review staff user accounts in all IT systems, to make sure there are not any inappropriate access permissions. The audit should include findings and provide details of any remedial actions that should occur.</p> <p>The audit review established that the Foundation Trust has not undertaken User Access Audit in the last year, in line with DSPT requirements.</p>
	Implication
Finding rating	There is a risk that users may have inappropriate or incorrect system access rights, leading to a potential data breach.
Moderate	
	Recommendation
	<p>3. An audit of user accounts should be held on an annual basis. The audit should include findings and provide details of any remedial actions for improvement. The report should be presented to the SIRO for their information and approval.</p>
	<p>Responsible officer: James Townend, End User Computing Manager</p> <p>Completion date: 30 June 2021</p>



Finding <div>4</div>	Finding: Process Reviews (5.1.1 & 5.1.2) <p>Best practice guidance issued by NHS Digital in Big Picture Guide 5 states that process reviews should be held at least once per year where data security has been put at risk, and following data security incidents.</p> <p>The review established that a detailed guidance documentation on Information risk incident reporting and investigation, which incorporates Root Cause Analysis.</p> <p>The Assertion Owner has not provided evidence to demonstrate examples of process reviews being undertaken periodically alongside the Root Cause Analysis conducted following a data security incident.</p> <p>No evidence was made available for review on the findings taken from the root cause analysis, or the mitigating actions being incorporated into an action plan, which appropriately assigned ownership and implementation dates.</p>
	Implication
Finding rating	<p>In most cases, breaches or cyber-attacks are unwittingly facilitated by the behaviour of employees who can be classed as 'non-malicious insiders', and are primarily motivated to get their job done, particularly if they are working with ineffective technologies or processes. If the Foundation Trust cannot identify those areas where the controls are not working effectively, it cannot take measures to improve these.</p>
Moderate	
	Action Points
	<p>4. A Root Cause Analysis should be carried out for those categories of data security and prevention incidents where multiple issues have been reported on the Datix system, to understand whether it is possible that these could be commonly attributed to weaknesses in the controls in place. In the event that the processes under review involve clinicians, they should be actively involved in the review process.</p> <p>5. The outcomes from process review should be documented in full and a responsible officer allocated to each action identified. Action Plans should be monitored on a regular basis, and assurance provided to the Board.</p>
	<p>Responsible officer: Ian Scott, Deputy Head of Information Technology</p> <p>Completion date: 30 June 2021</p>



Finding <div>5</div>	Finding: Disaster Recovery Plan (7.2.1 & 7.2.4) <p>The Foundation Trust should have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services. The plan should be subject to testing. This can be through live testing (simulation / active testing) or through desktop-based scenarios.</p> <p>The Foundation Trust has previously undertaken annual 'go dark' exercises.</p> <p>The planning for an exercise this year has been impacted by COVID-19 social distancing rules.</p> <p>No evidence was provided to support alternative exercises already having been undertaken or planned exercises upon the easing of COVID-19 restrictions.</p>
	Implication
Finding rating	<p>During any data security incident planning exercise, there should be a clear focus on enabling senior management to make good decisions about the Foundation Trust's response, and this requires a genuine understanding of the topic. If senior managers do not attend business continuity exercises they may not understand potential issues, the resources needed and their availability, which may prolong the length of time to resolve a real time incident.</p>
Moderate	
	Recommendation <p>6. A data security incident business continuity test should be undertaken annually, attended by representatives of the Board of Directors and Senior Operational teams.</p> <p>7. Following every business continuity test, the issues and actions should be fully documented, with names of actionees listed against each item. Action plans should be monitored to ensure that the necessary improvements identified are carried out as planned.</p> <p>Responsible officer: Ian Scott, Deputy Head of Information Technology</p> <p>Completion date: 30 June 2021</p>



Finding <div>6</div>	Finding: Security Patching (8.3.4) <p>Software should receive the latest security patches to correct any known asset vulnerabilities). Those security updates / patches need to be applied in a timely fashion.</p> <p>The Senior Information Risk Owner (SIRO) should have an active role in the process, and be informed when systems cannot be upgraded and the risks of using unsupported systems, and whether these risks are being treated or tolerated. The SIRO should also be notified where high risk vulnerability patches have not been applied with the reasons for this within 14 days, to allow a detailed review and approval of this.</p> <p>The Assertion Owner did not provide evidence of the documented acceptance of the risk associated with not patching high risk vulnerabilities, supported by comprehensive assessment and risk acceptance by the organisation's SIRO.</p>
	Implication
Finding rating	
Moderate	<p>The organisation does not have effective measures in place to manage vulnerabilities in its network and information systems, increasing the risk of disruption to essential services.</p>
	Recommendation <p>8. The Foundation Trust should maintain a documented record of risk acceptance of not patching a high risk or critical vulnerability; this should incorporate a formal assessment and agreement by the SIRO.</p> <p>Responsible officer: Ian Scott, Deputy Head of Information Technology</p> <p>Completion date: 30 June 2021</p>



Finding <div>7</div>	Finding: Annual Penetration Test (9.2.1) <p>NHS Digital Big Picture guidance states that a penetration test should be undertaken on an annual basis as a minimum. The scope of the test should be agreed between key stakeholders, including the SIRO. The penetration test must include the following elements:</p> <ul style="list-style-type: none"> • all webserver the organisation utilises • vulnerability scans • checking that the default password of network components have been changed. <p>A Penetration test was conducted in March 2021, however the Assertion Owner has not provided evidence of the scoping of the Penetration test. Therefore insufficient evidence is available to confirm adherence to this assertion control.</p>
	Implication
Finding rating	<p>If the Foundation Trust does not scope penetration testing, they may not be able to identify known vulnerabilities in the estate and take the necessary actions to mitigate these.</p>
Moderate	
	Recommendation <p>9. The IT penetration testing should be scoped in negotiation between the SIRO, business and testing team on an annual basis, in line with the minimum standards set out in best practice guidance issued by NHS Digital.</p> <p>Responsible officer: Steve Pearson, Network & Telecoms Manager</p> <p>Completion date: 30 June 2021</p>



Finding <div>8</div>	Finding: Accountable Suppliers (10.2.1, 10.2.2 & 10.2.4) <p>Due diligence should be undertaken to gain assurance of contractor compliance with data protection laws and the National Data Guardian's (NDG) Data Security Standards. The Foundation Trust should ensure that any supplier of critical IT systems that could impact on the delivery of care, or that processes personal identifiable data, has the appropriate certification.</p> <p>Depending on the nature and criticality of the service provided, certification might include:</p> <ul style="list-style-type: none"> • ISO/IEC 27001:2013 certification: supplier holds a current ISO/IEC27001:2013 certificate issued by a United Kingdom Accreditation Service (UKAS) • Cyber Essentials (CE) certification: supplier holds a current CE certificate from an accredited CE certification body. • Cyber Essentials Plus (CE+) certification: supplier holds a current CE+ certificate from an accredited CE+ Certification Body. • Digital Marketplace: supplier services are available through the UK Government Digital Marketplace under a current framework agreement. <p>The Foundation Trust did not provide evidence as part of the audit review that they have sought certification from IT contractors and assessed them for compliance with Data Security Standards. Additionally no supporting evidence was presented of formal contracts with suppliers, which outline security related responsibilities that remain with the organisation and which are the supplier's responsibility as part of the working arrangement.</p>
	Implication
Finding rating	<p>The GDPR gives data processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties. If the Foundation Trust cannot verify that a contractor fully complies with the required legislation and/or industry standards, this will pose a risk to the Foundation Trust.</p>
Moderate	
	Recommendation <p>10.The Foundation Trust ensures that any contractor of IT systems that could impact on the delivery of care, or process personal identifiable data, has appropriate certification in place verifying compliance with data security standards. The certification is subject to an undertaking by the Foundation Trust of a supplier risk assessment to confirm it meets the necessary assurance requirements.</p> <p>11.Where Foundation Trust IT services are outsourced, the organisation has formally and accurately recorded the organisation's security related responsibilities and those of the supplier's responsibility through contracting documentation.</p> <p>Responsible officer: Ian Scott, Deputy Head of Information Technology</p> <p>Completion date: 30 June 2021</p>



Appendix A – Basis of our classifications

Evidence Text Risk Ratings

Evidence Texts are risk assessed on their likelihood and impact based on the assessment rationale in the Impact table below and the Likelihood Table on the following page

Impact rating	Assessment rationale
Critical	<p>A Critical Impact Finding could apply to Health and Social Care organisations that use extremely complex technologies to deliver multiple services or process large volumes of patient data, including processing for other organisations. Many of the services are at the highest level of risk, including those offered to other organisations. New and emerging technologies are utilised across multiple delivery channels. The organisation is responsible for/ maintains nearly all connection types to transfer/store/process personal, patient identifiable and/or business-critical data with customers and third parties. A Critical finding that could have a:</p> <ul style="list-style-type: none">• Critical impact on operational performance or the ability to deliver services / care; or• Critical monetary or financial statement impact; or• Critical breach in laws and regulations that could result in material fines or consequences; or• Critical impact on the reputation or brand of the organisation which could threaten its future viability.
Significant	<p>A Significant Impact Finding could apply to a Health and Social Care organisation that use complex technology in terms of scope and sophistication. The organisation may offer high-risk products and services that may include emerging technologies. The organisation is responsible for/ maintains the largest proportion of connection types to transfer/store/process personal, patient identifiable or business-critical data with customers and third parties; other organisations and/or third-parties are responsible for/maintain a low proportion of connection types. A Significant finding that could have a:</p> <ul style="list-style-type: none">• Significant impact on operational performance; or• Significant monetary or financial statement impact; or• Significant breach in laws and regulations resulting in large fines and consequences; or• Significant impact on the reputation or brand of the organisation.
Moderate	<p>A Moderate Impact Finding could apply to a Health and Social Care organisation that uses technology which may be somewhat complex in terms of volume and sophistication. The organisation is responsible for/maintains a some connection types to transfer/store/process personal, patient identifiable and/or business- critical data with customers and third parties; other organisations and/or third-parties are responsible for/maintain a most of the organisation's connection types. A Moderate finding that could have a:</p> <ul style="list-style-type: none">• Moderate impact on the organisation's operational performance; or• Moderate monetary or financial statement impact; or• Moderate breach in laws and regulations with moderate consequences; or• Moderate impact on the reputation of the organisation.
Minor	<p>A Minor Impact Finding could apply to a Health and Social Care organisation with limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services. The institution primarily uses established technologies. It is responsible for/maintains minimal numbers of connection types to transfer/store/process personal, patient identifiable or business-critical data too customers and third parties; other organisations and/or third-parties are largely responsible for/maintain connection types. A Minor finding that could have a:</p> <ul style="list-style-type: none">• Minor impact on the organisation's operational performance; or• Minor monetary or financial statement impact; or• Minor breach in laws and regulations with limited consequences; or• Minor impact on the reputation of the organisation.
Very Low / Insignificant	<p>A Low Impact Finding could apply to a Health and Social Care organisation that has very limited use of technology. The variety of products and services are limited and the organisation has a small geographic footprint with few employees. It is responsible for/maintains no connection types to transfer/store/process personal, patient identifiable or business-critical data too customers and third parties. A Low finding that could have a:</p> <ul style="list-style-type: none">• Insignificant impact on the organisation's operational performance; or• Insignificant monetary or financial statement impact; or• Insignificant breach in laws and regulations with little consequence; or• Insignificant impact on the reputation of the organisation.



Risk Ratings

Evidence texts are risk assessed on their likelihood and impact based on the assessment rationale in the Likelihood table opposite and the Impact table on the previous page.

Likelihood rating	Assessment rationale
>80%	> 80% likely to happen in the next 12 months
60% - 80%	60% - 80% likely to happen in the next 12 months
40% - 60%	40% - 60% likely to happen in the next 12 months
20% - 40%	20% - 40% likely to happen in the next 12 months
< 20%	Low likelihood to happen in the next 12 months

How to determine the Evidence Text Risk Rating

The DSP Toolkit Independent Assessment Provider must calculate the risk rating for each in-scope DSP Toolkit evidence text assessed as part of their DSP Toolkit review. Once the Independent Assessment Provider has assigned a likelihood and impact rating to each assessed DSP Toolkit evidence text, the following risk matrix can be used to allocate a risk rating. This rating reflects the risk of the organisation being unable to meet the evidence text controls objective as a result of a control failing or the absence or ineffectiveness of a control. For example, if the DSP Toolkit Independent Assessment Provider assigned a Likelihood rating of '40%-60%' and an impact rating of 'Moderate', the risk rating for the individual evidence text would be Low.

The following grid should be used to determine the evidence text risk ratings. Issues with a low impact and low likelihood rating should not be considered as report-worthy. However; if the Independent Assessor deemed relevant, such issues may be discussed in the report or included in Appendix F.

Table 3. Assigning Evidence Text Risk Ratings

Likelihood rating (in next 12 months)	Impact rating				
	Critical	Significant	Moderate	Minor	Very Low / Insignificant
>80%	Critical	High	Medium	Low	Low
60% - 80%	High	Medium	Medium	Low	Low
40% - 60%	Medium	Medium	Low	Low	Low
20% - 40%	Medium	Low	Low	Low	Not reportable
< 20%	Low	Low	Low	Not reportable	Not reportable

How to determine the Assertion Level Risk Rating

The DSP Toolkit Independent Assessment Provider must then exercise professional judgement to assign a risk rating at the assertion level. The Independent Assessor leverages knowledge and subject matter expertise alongside observations made during the assessment to assign each assertion a risk rating of 'Critical', 'High', 'Medium' or 'Low' based on the evidence text ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place. The Independent Assessor then uses [Table 4](#) to assign a score for each assertion to be used in the calculation of NDG Standard level risk.

Table 4. Points corresponding to Assertion risk ratings

Rating	Points for each Assertion
Critical	40
High	10
Medium	3
Low	1



How to determine the National Data Guardian (NDG) Standard Risk Rating

The Independent Assessor will calculate an aggregate score and classification for each NDG Standard - i.e. the overall NDG Standard risk rating that will appear in the Executive Summary of the DSP Toolkit Independent Assessment Provider report. That is, the Executive Summary reporting will be at the NDG standard level; providing 10 'scores'; one for each standard. This guide also outlines how an overall risk rating score can be calculated. It is understood that this will be an expectation of key stakeholders to provide an overall risk rating though it should be noted and understood that abstracting scores to a high level and using aggregate or average scores can be very misleading as they can sometimes mask significant or critical issues at the lower levels; i.e. at the assertion level.

For some NDG standards there may be multiple assertions in the scope of the independent assessment and for some NDG standards there may only be one assertion in scope. The NDG Standard risk rating is determined by calculating the mean of the total number of assertion level points per NDG Standard and then referring to Table 5 to assign a rating. For example, a DSP Toolkit Independent Assessment Provider who assessed 8 DSP Toolkit Assertions aligned to NDG Standard One, may rate 5 assertions as Critical, 2 as High and 1 as a Medium. Using [Table 4](#), this gives the DSP Toolkit Independent Assessment Provider a total of 223 points (200 for Critical findings, 20 for High and 3 for Medium = 223 points). These figures should be divided by the number of assertions reviewed and rounded to the nearest one decimal place. In this instance there are 8 in-scope assertions which will result in a mean points per assertion of 28 ($223 \div 8 = 27.9$ rounded to one decimal place). [Table 5](#) should then be used to determine the overall NDG Standard risk rating. In this example the rating would lead to an 'Unsatisfactory' classification. This will be done for each NDG standard to support an overall risk rating.

Table 5. Calculation and assignment of the NDG Standard risk ratings

Overall NDG Standard Risk Rating Classification		Rating Thresholds when only 1 assertion per NDG Standard is in scope	Rating Thresholds when 2 or more assertions are in scope for each NDG Standard. Mean score (Total points divided by the number of in-scope assertions)
●	Substantial	1 or less	1 or less
●	Moderate	Greater than 1, less than 10	Greater than 1, less than 4
●	Limited	Greater than/equal to 10, less than 40	Greater than/equal to 4, less than 5.9
●	Unsatisfactory	40 and above	5.9 and above

How to determine the Overall Risk Rating

Once the Independent Assessment Provider has calculated the risk rating for each Standard the following table can be used to allocate an overall risk rating. Table 6 below allows the independent assessment provider to determine the overall rating.

Table 6. Determination of Overall Risk Rating

Overall risk rating across all in-scope standards	
Unsatisfactory	1 or more Standards is rated as 'Unsatisfactory'
Limited	No standards are rated as 'Unsatisfactory', but 2 or more are rated as 'Limited'
Moderate	There are no standards rated as 'Unsatisfactory', and 1 or none rated as 'Limited'. However, not all standards are rated as 'Substantial'.
Substantial	All of the standards are rated as 'Substantial'



How to determine the Overall Confidence-level in the veracity of the organisation's self-assessment / DSP Toolkit submission

Once the Independent Assessment Provider has completed the fieldwork and calculated the ratings for assertions, for each of the 10 National Data Guardian Standards and the overall risk rating then the confidence-level in the veracity of the organisation's DSP Toolkit self-assessment submission should be determined by comparing the independent assessment findings against the latest DSP Toolkit submission. The following definitions should be used for aiding the decision of applying a confidence-level.

Table 7. Determination of confidence-level in the veracity of the organisation's self-assessment / DSP Toolkit submission

Level of deviation from the DSP Toolkit submission and assessment findings	Confidence-level	Suggested Assurance level (subject to Independent Assessor judgement / knowledge, Independent Assessor to differentiate between Unsatisfactory and Limited)
High – the organisation's self-assessment against the Toolkit differs significantly from the Independent Assessment For example, the organisation has declared as "Standards Met" or "Standards Exceeded" but the independent assessment has found individual National Data Guardian Standards as 'Unsatisfactory' and the overall rating is 'Unsatisfactory'.	Low	Unsatisfactory OR Limited
Medium - the organisation's self-assessment against the Toolkit differs somewhat from the Independent Assessment For example, the Independent Assessor has exercised professional judgement in comparing the self-assessment to their independent assessment and there is a non-trivial deviation or discord between the two.	Medium	Moderate
Low - the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment	High	Substantial



Appendix B - Limitations and Responsibilities

Limitations inherent to the assessment provider's work		
We have undertaken this DSP Toolkit review subject to the limitations outlined below:		Responsibilities of management and Assessment Providers
Internal control Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.	Future periods Our assessment of controls is for the period specified only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that: <ul style="list-style-type: none">• The design of controls may become inadequate because of changes in operating environment, law, regulation or other changes; or The degree of compliance with policies and procedures may deteriorate.	<p>It is Health and Social Care Management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and possible security threat. DSP Toolkit Assessment reviews should not be seen as a substitute for management's responsibilities for the design and operation of these systems.</p> <p>The DSP Toolkit Independent Assessment Provider endeavor to plan their work to ensure there is a reasonable expectation of detecting significant control weaknesses and, if detected, we carry out additional work directed towards identification of consequent security threat or other irregularities. However, the DSP Toolkit Independent Assessment Provider's procedures alone, even when carried out with due professional care, do not guarantee that security threat will be detected.</p> <p>Accordingly, the DSP Toolkit Independent Assessment Provider's examinations should not be relied upon solely to disclose security threat, defalcations or other irregularities which may exist.</p>



Appendix C - National Data Guardian (NDG) Standards

National Data Guardian Standard	Description
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 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.

