

**Human Tissue Authority (HTA)**

## Data Security and Protection Toolkit (DSPT) Final Report

Date of issue: 30 June 2023 Engagement reference: 2324-HTA-106

**Contents**

[Introduction 3](#_bookmark0)

[Executive summary 4](#_bookmark1)

[Key Findings 6](#_bookmark2)

[Annex 1: Management action plan 7](#_bookmark3)

[Annex 2: DSPT Statements Audited 8](#_bookmark4)

[Annex 3 GIAA Assurance Opinion 31](#_bookmark5)

[Annex 4: Our classification systems 32](#_bookmark6)

[Annex 5: Distribution 33](#_bookmark7)

This document has been prepared for the Human Tissue Authority (HTA) and is only for HTA management and staff. HTA must consult with GIAA (pursuant to part 3 of the Secretary of State Code of Practice issued under section 45 of the FOI Act) before disclosing information within the reports to third parties. Any unauthorised disclosure, copying, distribution or other action taken in reliance of the information contained in this document is strictly prohibited. The report is not intended for any other audience or purpose, and we do not accept or assume any direct or indirect liability or duty of care to any other person to whom this report is provided or shown, save where expressly agreed by our prior consent in writing.

# Introduction

### Background

The Data Security Protection Toolkit (DSPT) is an online self-assessment tool that allows organisations to measure their performance against national data security standards. The annual assessment is used to review a range of strategic policy and regulatory requirement objectives. These include:

* Satisfying the Cabinet Office requirement for the Department of Health and Social Care to provide assurance that all parts of the NHS are meeting mandated data security and protection standards, including encryption, staff training and information risk management and governance structures.
* Providing the assessment of information quality legally required under Quality Account Regulations.
* Supporting the accountability and transparency agendas by requiring organisations to assess and publish performance against a standard framework which enables comparisons.

### Objective

The objective of this independent review was to satisfy the annual requirement for an independent assessment of the DSPT submission.

### Approach

Our assessment involved the following steps:

* Obtaining access to HTA’s DSPT self-assessment.
* Defining the evidence texts that will be examined during the assessment.
* The assertion evidence was assessed against both assertion text and the evidence provided against the DSPT Independent Assessment Framework.

### Scope

The review focused on the 13 mandatory assertions and the subsequent evidence references as extracted from the 2022/23 Version 5 DSPT in the scope detailed below:

|  |  |
| --- | --- |
| 1.3 Accountability and governance | 6.3 NHS Digital alerts |
| 2.1 Staff training and tests | 7.2 Continuity and DRP testing |
| 3.4 Leaders’ and board training | 7.3 Incident response plan |
| 4.1 Staff roles | 8.3 Security patches |
| 4.2 Identity and access | 9.3 Known vulnerabilities |
| 4.5 Passwords management | 10.1 Suppliers’ register |
| 5.1 Process reviews |  |

### Limitations of scope

The remaining assertions from the DSPT, if not listed above, were not assessed as part of the fieldwork.

Assertion 9.3.8, “The organisation maintains a register of medical devices connected to its network” is not applicable and was also excluded.

# Executive summary

### DSPT Independent Assessment Report Outputs

Our review followed the DSPT Independent Assessment Framework and Guidance published by NHS Digital (now part of NHS England). We reviewed 9 assertions across the 10 National Data Guardian Standards (NDG) as pre-determined in-scope by NHS Digital, excluding qualified exemptions and not applicable assertions. These are detailed in Annex 2 – DSPT Statements Audited.

Our work has two report outputs: the **Overall Risk Assessment** and the **Confidence Level**, in line with the DSPT guidance and framework methodology.

### GIAA Independent Assessment Outputs

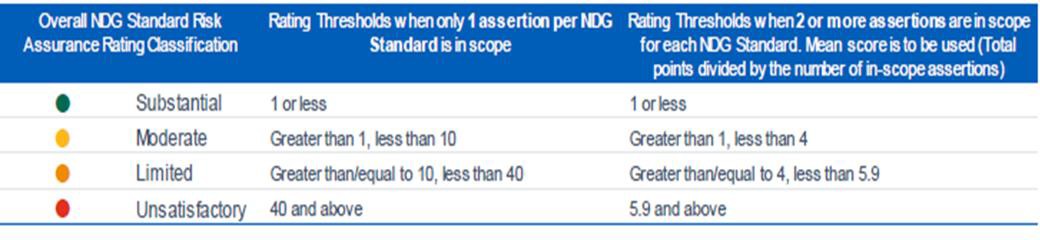
|  |  |
| --- | --- |
| **The Overall Risk Assessment across all 10 NDG Standards for HTA is:** | **The Confidence Level in the veracity of HTA’s self- assessment / DSPT submission is:** |
| Moderate | High |
| There are no standards rated as ‘Unsatisfactory’, and one or none rated as ‘Limited’. However, not all standards are rated as ‘Substantial’. | This means that HTA’s self-assessment against the DSPT matched or deviates only minimally from what has been observed in the Independent Assessment. |

Details of the contributing factors that have informed these report outputs are presented within **Annex 2: DSPT Statements Audited**. A summary is provided in the Overall Risk Assessment table below.

Our separate GIAA governance and risk assurance opinion is at **Annex 3.**

### Scoring

The NDG Standard risk rating is determined by calculating the mean of the total number of assertion level points per NDG Standard. The table below provides the calculations used to determine the NDG Standard risk rating. Low level assertion risk ratings are awarded 1 point, medium 3 points and high 10 points.



### Overall Risk Assessment

The table below shows the ‘Overall NDG Standard Classification’ based upon the ‘Assertion- level Risk Ratings’ as well as the ‘Overall Risk Assessment Across all 10 NDG Standards’. It includes the calculation of each risk rating by detailing the scores obtained at each assertion level with respect to their category, (Low, Medium, and High).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **National Data Guardian (NDG) Standard** | **Assertion-level Risk Ratings.**  Number of Assertions rated: | | | **Overall NDG Standard Classification** | **Overall Risk Assessment across all 10 NDG**  **Standards** |
| **High** | **Medium** | **Low** |
| **1. Personal Confidential Data** |  |  | **9** | **Substantial** | Moderate |
| **2. Staff Responsibilities** |  |  | **1** | **Substantial** |
| **3. Training** |  |  | **2** | **Substantial** |
| **4. Managing Data Access** |  | **2** | **6** | **Moderate** |
| **5. Process Reviews** |  |  | **1** | **Substantial** |
| **6. Responding to Incidents** |  | **1** | **3** | **Moderate** |
| **7. Continuity Planning** |  |  | **7** | **Substantial** |
| **8. Unsupported Systems** |  | **1** | **4** | **Moderate** |
| **9. IT Protection** |  | **1** | **5** | **Moderate** |
| **10. Accountable Suppliers** |  |  | **1** | **Substantial** |
| **TOTAL** | **0** | **5** | **39** |  | |

Due to the nature of the risk rating system used, it is extremely difficult to achieve a ‘substantial’ assessment overall, as any assertion that is not fully met will impact on the scoring for the relevant standard and achieve a maximum ‘moderate’ rating.

Considering the controls and arrangements in place to practice effective data protection and security principles within HTA, a ‘moderate’ opinion provides a good basis on which to build. It should be noted that organisations will determine their requirement to fully meet the DSPT assertions based on their compensating controls, resources, and risk appetite. Any actions taken to implement the recommendation should be proportionate to the data protection and security landscape and implemented in a timely manner.

# Key Findings

### Areas of good practice

During our review we noted areas of good practice for the following assertion references:

* 1.3.1 – HTA has several policies and processes in place to support data protection and data security that have been appropriately reviewed and signed off for use.
* 2.1.1, 3.4.1 and 3.4.2 – Training is undertaken by all employees with bespoke training material provided for the SIRO, the Caldicott Guardian and the Data Protection Officer; this is in addition to the general training schedule.
* 4.2.1 and 4.2.3 – HTA has a good working relationship with third-party IT service provider BCC and the support provided meets the needs of the DSPT requirements.
* 8.3 – Supported systems are kept up to date with the latest critical security patches.

### Areas requiring improvements

There are no areas that require significant improvement to meet DSPT requirements as no assertions have been assessed as ‘not met.’ There are nine assertions that are partially met at the time of the independent assessment.

The actions needed for these assertions to be ‘met’ are noted in **Annex 2** under the heading ‘**Improvements required to meet the DSPT assertion test requirement/s**.’ In addition, we have made several improvement suggestions on the ‘met’ assertions to further enhance the demonstration of controls.

# Annex 1: Management action plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Recommendation(s) | Priority | Action agreed | Implementation date | Owner |
| 1.1 - GIAA comments on potential improvement required to further meet the DSPT assertions as outlined in Annex 2 of the DSPT report for the 22/23 submission, associated with ‘partially met’ assertions, should be addressed to fully meet the relevant DSPT Assertions. | Low | 30 Aug 2023 | 31 Dec 2023 | Information Governance Lead |

# Annex 2: DSPT Statements Audited

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 1.3.1 | There are board-approved data security and protection policies in place that follow relevant guidance. | 1. Relevant data security and data protection policies and procedures. 2. Evidence that policies and procedures have been approved by an appropriate individual / body. | 1. Data security and data protection policies and procedures:    * CW HTA-POL-056 Information Governance and Cyber Risk Policy - published 17 May   CW to address comments, ready for final approval & publication   * + CW HTA-GD-045 Guidance on complying with Subject Access Requests (SAR) - published 15 May   + GA HTA-POL-044 Freedom of Information Policy - published 10 May 23   + LD HTA-POL-088 Records Management & Retention policy - SMT approved Mar 23, published 10 May 23   + UO HTA-POL-083 HTA Data Protection by Design and default Policy - published 17 May   + UO HTA-POL-086 Data Protection Impact Assessment procedure - published 17 May   + UO DRAFT HTA-POL-087 Information Governance Framework - WiP, will be published once other policies published uploaded 07 Jun   UO - Master Information Asset Register uploaded 07 Jun  UO - Master ROPA register uploaded 07 Jun   * + SJ Draft HTA-POL-089 Data Quality Policy &, email for approval from LD, SMT lead uploaded 07 Jun |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 1.3.2 | Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls. | 1. Testing programme or documentation to evidence there is a formal process in place to provide assurance that staff are complying with the relevant guidance and / or policies and procedures. Results of spot checks 2. Copy of action plan that has resulted from any testing having been undertaken. 3. Evidence that the action plan has been reviewed by an appropriate board, committee, meeting or group of the organisation that has representation from senior management. | 1. HTA-POL-110 Data Security Audit Checklist. published 17 May   Approval channels for DP policies:   * + draft version shared with SMT and BDT for review and awareness   + BDT meet fortnightly and SMT meet weekly.   + Relevant SMT lead reviews and approves final version   + Final version published on EDRMs by the Corporate Services Manager.   + HTA staff notified via Wave & HTA newsletters, policies can be uploaded to Astute learning to track if policy read & understood.   Evidence to support policy approval uploaded in 1.3.7   1. LD & CW to agree working from home spot checks process. Home working spot check to be planned following policy and checklist approval. DPO & IT planning random spots checks now, DPO has staff list from HR and has asked Head to Regs to complete the checklist 2. Action Plan to be developed after spot checks - delayed due to staff unavailability.   First set of spot checks undertaken in Q1 and further checks planned for Q3. |  | Yes |
| 1.3.3 | SIRO responsibility for data security has been assigned. | Documented roles and responsibilities for the accountable individual. These should make explicit reference to data security and protection. | 1. SIRO appointed and has completed SIRO training, leaving HTA 16 June. Director of Data, Technology & Development will take over SIRO responsibilities from 16 June for the interim until 15 Sep. SIRO letter uploaded. 2. SIRO is SMT member.   There is no conflict of interest, responsibilities have not been delegated to a junior role in HTA  Roles and responsibilities described in:   * + HTA-POL-056 Information Governance and Cyber Risk Policy   + HTA-POL-088 Records Management and retention policy. |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 1.3.4 | There are clear documented lines of responsibility and accountability to named individuals for data security and data protection. | Formally documented reporting for individuals with responsibility for data security and data protection. | 1. There is a hierarchy of key DSPT roles SIRO, CG & Accountable Officer are SMT members. DPO is part of the Data Technology and Development Directorate Latest org chart to be uploaded as evidence 2. Chief Executive is the HTA Accountable Officer, Director of Resources currently has the SIRO role (leaving 16 Jun), LD will take over SIRO responsibilities until Sep 23 when new Director of Resources is in post (SIRO letter uploaded to 1.3.3) Director of Data Technology and Development has Caldicott Guardian and Board champion responsibilities   Information Governance Lead is also the Data Protection Officer (role transferred from Head of Tech to IGL, Nov 22)  May HTA Org Chart uploaded as evidence Roles and responsibilities described in:   * + HTA-POL-056 Information Governance and Cyber Risk Policy   + HTA-POL-088 Records Management and retention policy   JDs attached as evidence to 1.3.3  3.LD, Director of Data, Technology & Development talked through Data Security and Protection governance structure  Heads of roles responsible for IAR & ROPA (information and processing)  Records Management DRO responsibilities devolved to Heads of HR, Finance, IT, Comms and Policy  All staff are responsible for adhering to policies and reporting breaches |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 1.3.5 | Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility. | 1. Data security and protection risk management framework and risk register. 2. Corporate risk management framework and risk register. 3. Evidence associated with data security and protection risks being reported / escalated. 4. Third party security assessment process and policy. Third party audit reports and template contracts. | 1. IT risks also maintained in Data, Technology and Development directorate operational risk register. Directorate Operational Risk Registers are aligned to the Strategic Risk Register. 2. HTA-POL-025 HTA Risk Management Strategy and Policy approved by ARAC/ Board Mar 23 uploaded   IT Risk Register uploaded 07 Jun.   1. Latest Strategic Risk Workshop held 25 Apr attended by SMT & BDT. DTD Ops Register, Strategic Risk summary and Register updated to evidence. 2. HTA rarely purchase new systems. There are processes in place to manage data security risks including automated MS protection tools RTANCA alerts and security breach logs. |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 1.3.6 | List your organisation’s top three data security and protection risks. | Data security and protection risk management framework. | 1. DSP risk management framework covered by.HTA- POL-025 HTA Risk Management Strategy and Policy. Process in place to escalate critical risks from local risk management to operational and up to a strategic risk depending on severity. Strategic risks are cross cutting; therefore an escalated risk and score will be adjusted to assess the impact on the business.   DSP risks are logged in the IT Risk Register which feeds into the DTP Op risk register.   1. Top 3 IT risks:    * Insufficient IT resources to support delivery and invest in future developments and respond to change    * Investment in system and digital development opportunities    * Shared services and the impact on HTA e.g. HR, IT, Comms, project management, data management, call centres, media and complaints   Top 3 DSP risks:   * + IT service disruption, system investment, and housekeeping   + Cyber threat, although there have been no serious cyber threats in the last 12 months, there have been several near misses that have been contained (international log in attempts)   + Service Delivery failure, safe operation of IT services 3.Strategic risks and issues are reviewed monthly by SMT and reported to ARAC.   ARAC see annual risk report. Operational risks are reviewed at team meetings and Awaydays  IT risks on the DTD risk register are escalated to the Strategic Risk Register where appropriate. Risk can be filtered by category. by directorate, by score etc.  Director of Data, Technology & Development is responsible for DSP risk assessments. |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 1.3.7 | Your organisation has implemented appropriate technical and organisational measures to integrate data protection into your processing activities. | 1. Copy of Data Protection by Design and Default procedure. 2. Evidence, such as minutes or a signed copy of the procedure that demonstrates it has been approved by the organisation's board (or similar). 3. Evidence of any wider practice that the organisation has built in data protection principles into any wider business processes, strategies and organisational vision statements. | 1. Published:    * HTA-POL-083 HTA Data Protection by Design and default Policy (1.3.1) published 17 May    * HTA-POL-084 Record of Processing Activity (ROPA) policy published 15 May    * HTA-POL-085 Information Asset Register policy published 17 May    * HTA-POL-086 Data Protection Impact Assessment procedure (1.3.1) published 17 May 2. GDPR principles built into policies, processes and staff & board member training 3. Documents reviewed by BDT and signed off relevant SMT member 4. Data protection in policies above   Evidence of policies in Astute learning platform (to track staff have read) and published in staff newsletter on Wave https://intranet.hta.gov.uk/news/402?language=en uploaded  Review by BDT & approval chain email uploaded for DPIA & DP by Design policies |  | Yes |
| 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. | 1. Data Protection Impact Assessment Procedure (or similar). 2. Evidence that the procedure has been approved by the SIRO or the individual with responsibility for data security / data protection. 3. Evidence that the procedure has been approved by the organisation's board (or similar) and is scheduled for review at least on a bi-annual basis. | 1. Documents in place    * HTA-POL-086 Data Protection Impact Assessment procedure updated to include Appendix A and B which are the DPIA checklist and the DPIA review and sign off template. Published    * DPIA Log    * DPIA FAQ    * DPIA template 2. SIRO approval for DPIA procedure documents confirmed 05 Jun, email uploaded 3. Policies and documents are aligned to DSPT standards and are reviewed every 12 months. |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 1.3.9 | Data security and protection direction is set at board level and translated into effective organisational practices. | 1. Board agenda and meeting minutes. 2. Example data security and data protection related reports. 3. Documented evidence of delegated authority to another body for the more regular management of Data Security and Protection. 4. Reports from the delegated body to the highest level of Management / Board. | 1. ARAC papers for Jun 22, Oct 22, Jan 23 & Jun 23 uploaded   DSPT Governance Chronology May 2023 (covers Mar 22 - Apr 23) uploaded   1. DSPT papers issued to SMT (included in chronology doc) 2. SMT DSPT papers include RAG status of assertions 3. ARAC ToR details reporting to the HTA Board. ARAC ToR 7 HTA Board approval included in DSPT chronology timeline. Uploaded as evidence |  | Yes |
| 2.1.1 | There is a data protection and security induction in place for all new entrants to the organisation. | 1. Data security and data protection induction training. 2. Data security and data protection training policy / procedure. 3. Evidence that new joiners since last DSPT review completed their data security and data protection induction training shortly after joining the organisation. | 1. Induction training.   New starters have 6 weeks to complete their Induction Plan Starters given system access on day 1 by IT (BCC). HR also meet with new starter on Day 1 to talk through systems and processes. Starters given access to Astute to complete mandatory training. Sample joiner added to in DSPT S2 evidence  TNA plan includes SIRO, Caldicott Guardian & Board training. Approved by RS (SMT member)   1. KS has provided 3 sample new joiners to verify they have completed DSPT training shortly after joining HTA. Names redacted. (In DSPT S2 evidence) 2. Training modules on Astute include:    * using email & internet    * setting a secure password    * introduction to personal data protection Induction list for new starters & staff list added as evidence 25 May |  | Yes |
| 3.4.1 | Have your SIRO and Caldicott Guardian received appropriate data security and protection training? | 1. Training needs analysis. 2. Evidence that the organisation's SIRO and Caldicott Guardian have completed the required training. | 1. Approved TNA paper uploaded as evidence includes DSPT training needs for senior staff 2. SIRO and Caldicott Guardian training uploaded |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 3.4.2 | All board members have completed appropriate data security and protection training. | 1. Data security and protection training procedure. 2. Evidence associated with all Board members having completed their data security and protection training. | 1. The HR learning platform Astute has 15 Data protection courses available. (TNA uploaded 3.4.1) Board members included in DSPT training. DSPT slides issued to Board Members 28 Apr. A board member provided QA of training material before signing off by Board chair & SMT chair approval.   Deadline for completion mid-May 23. Read receipt emails issued to Board members (BMs) to confirm receipt. BMs have 2 weeks to complete and send email to Head of Private Office as proof of completion.   1. All board members have completed DSPT training. Confirmation emails uploaded. |  | Yes |
| 4.1.1 | Your organisation understands who has access to personal and confidential data through your systems, including any systems which do not support individual logins. | 1 Organisation chart / organisation structure.   1. Role / Job descriptions. 2. ESR (Electronic Staff Record) | 1. Org chart updated monthly and available to all staff on HTA Wave: https://intranet.hta.gov.uk/main/ screenshot uploaded as evidence   HR have access to personal data in IRIS and individuals have access to their own data, HR also have password protected access to confidential data in SharePoint.  Regular 6 monthly reviews held to check retention dates and dispose of records accordingly.  key responsibilities for SIRO, CG & DPO included in the Org Chart   1. JDs - HR JDS uploaded:    * Director of Resources (JD owned by HTA)    * IG Lead JD    * Director of DTD JD |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 4.2.1 | When was the last audit of user accounts with access to the organisation's systems held? | Evidence of the previous user access audit e.g., Signed user listing or other confirmation that the user access audit took place. | 1. Last user access audit completed Nov 22 Access management list uploaded as evidence HTA-AdUsersLogon added 05 Jun 2. Evidence of previous audit of HTA users to confirm the accuracy of AD and Azure accounts and access is sync'd.   Email chain of reports for Sep 22 added 05 Jun   1. Disconnect between HR & IT leavers process has been addressed. HR notify CW (Head of IT Ops) and CW notifies BCC.   BCC notifies CW & HR when access list updated. BCC to provide AD user list including deactivated accounts to compare with HR leaver's list.   1. HR advised staff changing roles rarely happens. HR hold a staff list and can adapt this to include change of access. HR change list and leavers flowchart uploaded as evidence |  | Yes |
| 4.2.3 | Logs are retained for a sufficient period, managed securely, reviewed regularly and can be searched to identify malicious activity. | 1. Log retention policy. 2. Documentation associated with automated or manual log review controls. | 1. HTA-POL-088 Records Management and retention policy. published 2. Retention logs can be created in MS Defender in Cloud Apps up to a maximum of 6 months. Retention for 1 month is easier to report on than 6 months as search has to be done by weeks.   MS Sentinel can retain logs more than 6 months if required  Evidence (E): Cloudapplogs2 log activity over 6 months (05 Jun)   1. BCC receives automated messages from MS Defender in Cloud Apps if there is an incident, BCC threat policy also in place   E: Cloudapplogs1 failed login incident   1. SIEM covered by Intune and MS ATP. ARAC report includes score - identity, data & applications   E: Cloud app and policy logs screenshots, copied to Word for GIAA (06 Jun)  Evidence attached of unusual, failed log in incident |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 4.2.4 | Unnecessary user accounts are removed or disabled. | 1. Access management policy or similar. 2. Evidence that 'leavers' access has been removed in line with the policy in the last calendar year. | 1. Leavers’ form for IT & HR. HR share monthly list of Joiners and Leavers with BCC, CW is copied in. Joiners are provided with access to general accounts and requests for access to specialised systems are managed via the Line Manager.   LD has shared the HTA equivalent access management policy, uploaded as evidence. Para 7 of the Password Policy and para 56 of the IG & Assurance Framework or Cyber security   1. There is a process in place for anyone leaving the HTA. This process is led by the Line Manager and includes the return of any equipment, appropriate handover and also the notification to IT of the suspension of account on the last day. There is an additional safety net from IT who correlate requests for suspending accounts with the announcement of leavers / staff changes in the HTA newsletter. Form and flow chart uploaded as evidence.   Leaver process to be tested in mid-June when leaver with general and specialist account access leaves HTA. KS to share evidence on 19 Jun  BCC emails of recent leaver (AM) and upcoming leaver (DS) copied to Word for GIAA, uploaded 05 Jun   1. HR advised staff changing roles rarely happens. HR hold a staff list and can adapt this to include change of access. HR to share blank staff list as evidence. | To enhance existing controls, HTA should draft and implement an access management policy. This should include the requirement to periodically review user access to systems and, for users changing roles, introduce a review and possible revocation of system and data access privileges, or a subset thereof. | Partial |
| 4.5.1 | Your organisation has a password policy giving staff advice on managing their passwords. | Password policy. | 1. HTA-POL-075 Password policy published 15 May. Uploaded 2. Policy includes criteria listed   Criteria met - RS confirmed Patch management policy approval. |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 4.5.2 | Technical controls enforce password policy and mitigate against password- guessing attacks. | 1. Password policy- rules regarding time delay between successive login attempts and / or account lockout. 2. Network password settings. 3. Application password settings. 4. Security Monitoring reports focused on detecting and alerting indicators of malicious or abnormal behaviour, for example: • login attempts that fail the second step of MFA; • brute-forcing of account passwords, including password spraying; • Login attempts from unexpected geographic areas; and • Reports of unexpected account lockouts or other unusual account behaviour from users. 5. Password deny lists. | 1. Throttling built in to MS. allows 5 login attempts before login blocked, also includes MFA. Azure allows 10 attempts before temp block   Word password log in screenshots uploaded for GIAA (O6 Jun)   1. The HTA operates a multi factor authentication to access HTA systems and accounts. This is an automated control to prevents attacks. Managed by BCC.   Covered by:   * + HTA-POL-056 Information Governance and Cyber Risk policy   + HTA-POL-074 IT and Home Working Equipment Policy   + HTA-POL-075 Password policy   + HTA-POL-077 Remote Access policy   Information Asset Register (IAR)uploaded to 1.3.1 to align with the password policy.  BCC to confirm if HTA Email Security Process diagram Dec 21 is the latest version. |  | Yes |
| 4.5.3 | Multifactor authentication is used wherever technically feasible. | Authentication strategy / plan. | 1. Multi Factor Authentication has been considered where appropriate and technically feasible. BCC has conditional access policy which enforces MFA.   BCC provided list of MFA log ins and conditional access policy screen shots added 05 Jun, saved to Word 06 Jun   1. MFA covered by:    * HTA-POL-056 Information Governance and Cyber Risk policy    * HTA-POL-074 IT and Home Working Equipment Policy    * HTA-POL-075 Password policy, uploaded    * HTA-POL-077 Remote Access policy, uploaded SIRO annual information risk management report issued to Audit and Risk Assurance (ARAC) meeting uploaded, next report to be issued Jul 23   3. All sensitive data runs through MFA,  evidence attached of unusual, failed log in incident. |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 4.5.4 | Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength. | System / infrastructure implementation procedure. | 1 BCC generate passwords for new starters, new starters change the password as part of their IT induction.  BCC generate passwords for important / privileged accounts  Password character length for standard and privileged accounts are 8 minimum and expire after 90 days  2. No default for privileged accounts, needs to be set, account is created and password generated  3. Covered in HTA-POL-71 social media policy, para  35. Uploaded as evidence. Covered by:   * HTA-POL-075 Password policy * HTA-POL-056 Information Governance and Cyber Risk policy | HTA’s password policy should be amended to include appropriate password complexity requirements for all relevant systems. | Partial |
| 5.1.1 | Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security or protection incident, with findings acted upon. | 1. Data security and protection incident management procedure. 2. Documentation associated with latest three incidents with details on the root cause of the incident. 3. Evidence associated with action being taken to prevent similar incidents from occurring in the future for latest three incidents. | 1. HTA-POL-056 Information Governance and Cyber Risk policy   SIRO annual information risk management report issued to ARAC, next report to be issued Jun 23 Cyber Security Dashboards & ARAC dashboard uploaded as evidence  RCA template added as evidence   1. As of May 23, no data security and protection incidents have arisen over the last 12 months.   Cyber Security Dashboard for 08 Jun 23 ARAC uploaded to 1.3.9. Evidence includes security incident management flowchart (slide 11) - extract uploaded Criteria met - RS confirmed Patch management policy approval.  There is a policy and procedure where SIRO has oversight of all incidents (Annual report to ARAC). However, since July last year, HTA hasn't had any incidents requiring oversight. |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 6.3.1 | If you have had a data security incident, was it caused by a known vulnerability? | Data security incident reports for the last calendar year. | 1. As of May 23 no data security and protection incidents have arisen over the last 12 months 2. evidence attached of unusual, failed log in incident Cyber Security Dashboard for 08 Jun 23 ARAC uploaded to 1.3.9, evidence. Slides 5 -7 includes identification & protection, detection and response and recovery summaries - extract uploaded |  | Yes |
| 6.3.2 | The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service. | High severity CareCert reports, with response date extracted from NHS Digital website for the following: CC-4306; CC-4291; CC-4282; CC- 4245; CC-4226; CC-4225; CC-4210; CC-4192; CC-4178; CC-4169. | 1. HTA are signed up to the CareCert service. BCC receives reports and must respond within 14 days confirming if applicable or non-applicable.   10 NHS digital cyber alerts added 05 Jun  Linked to RTANCA (NHS Digital Service). BCC, IT service partner, acknowledge alerts and takes action. The IT Operations Manager receives notice & shares with SMT & ARAC.  Email evidence uploaded response to show response to high severity CareCERT alert in Nov 22 and cyber alert in Dec 22.  Cyber Security Dashboard for 08 Jun 23 ARAC uploaded to 1.3.9. evidence. Slides 3, 5, & 7 cover RTANCA alerts - extract uploaded  The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service. |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 6.3.3 | The organisation has a proportionate monitoring solution to detect cyber events on systems and services. | 1. Network diagram showing security monitoring appliances. 2. Security monitoring process / procedure documentation. 3. Alerts / reports evidencing the current security monitoring control environment. 4. Risk acceptances or other documentation outlining the organisation's security monitoring gaps and mitigating controls that have been put in place. 5. Security monitoring strategy / plan (or similar). | 1 MS Active threat protocol and Cloudapp security in place.  The Cyber Security dashboard report presented to ARAC in January 2023 outlined the systems and automated controls the HTA has in place to manage and respond to the cyber security risk. Uploaded as evidence.  Email evidence uploaded response to show response to medium severity CareCERT alert on 02 May.  Cyber Security Dashboard for 08 Jun 23 ARAC uploaded to 1.3.9. evidence   1. BCC advised this assertion is geared up to office working, however 80%+ staff are home workers. IDS managed through home routers, not centrally. ATP Firewall is in place for corporate network at 2RP. BCC to share screenshots 2. Alerts built into Cloud App security, messages issued automatically when alerts occur   BCC shared Cloud app reports, uploaded as Word doc for GIAA review 06 Jun   1. HTA Head of IT Ops and BCC meet every 6 months to review processes and identify improvements to respond to continual emerging cyber risks 2. HTA and BCC have a well-established working relationship which has evolved over the last 15 years through RTANCA. Not all alerts apply to HTA. Dual (duplicate) reporting in place through ALB security network and SIRO reporting | A Security monitoring strategy / plan (or similar) should be documented, implemented and subject to periodic review. | Partial |
| 6.3.4 | All new digital services that are attractive to cyber criminals (such as for fraud) are implementing transactional monitoring techniques from the outset. | 1. Fraud risk assessment associated with each of the organisation's digital services. 2. System / services requirements documentation that includes transaction-level monitoring in any new digital service that could be susceptible to fraud. 3. Evidence that transaction-level monitoring has been implemented for any such service / application in the previous 12 months. | 1. No services purchased in last 12 months. HTA services limited to fees collection and procurement.   All staff are mandated to undertake Fraud Awareness as part of the HTA induction process.  Covered in the HTA-POL-056 Information Governance and Cyber Risk policy in system administrator responsibilities (see 1.3.1) and cyber threat section   1. Transaction-level monitoring dependent on if new digital service has been implemented. 2. Cyber Security Dashboard for 08 Jun 23 ARAC uploaded to 1.3.9. evidence, there is no reference to   new services in the dashboard as no new services have been purchased in the last 12 months | 1. HTA should ensure that any future digital services procured that are susceptible to fraud undergo a fraud risk assessment that considers the nature of the service and the amount and type of data that it processes. 2. Where any new digital system may be susceptible to fraud, there should be a requirement that transaction- level monitoring is included in the specification. | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 7.2.1 | Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan. | Collateral associated with the most recent test of the data security incident response and management plan. | 1.BCP & CIRP Test key milestones:  w/c 24th Apr – Draft BCP circulated to Business Delivery Team (BDT) members (for info) and specific BCP Heads (for comments)  w/c 11th May – Brought to SMT for info  02 Jun - desk top test Rudolph & Invader tests complete  30 Jun produce final report and updated BCP by end of June  30 Jun Complete BC training video ready for Q2 mandatory training cycle  HTA-BCP-004 Business Continuity Plan (BCP) SMT prep email and test agenda email uploaded as evidence   1. BDT & SMT briefed 2. Test recording and hot wash up (lessons learned) outputs uploaded as evidence of live testing 07 Jun Current BCP & previous BP/DR policies uploaded, test data slides, script & recommendations uploaded as evidence   Invader exercise scope to test the HTA’s Business Continuity  Rudolph exercise scope to test if CIRP is fit for purpose   * + Further BCP tests to be rolled into joint CIRP / BCP test with all staff each January |  | Yes |
| 7.2.2 | From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item. | Collateral associated with all BCP tests in the previous 12 months; test plans, test results and recommended remediation actions and improvements. | 1. BCP & CIRP desk top test Rudolph & Invader tests complete 02 Jun  test data slides, script & recommendations uploaded as evidence in 7.2.1  key milestones:  30 Jun produce final report and updated BCP by end of June  30 Jun Complete BC training video ready for Q2 mandatory training cycle  BCP test evidence uploaded in 7.2.1 |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 7.3.1 | On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary. | 1. Data security incident response plan. 2. Forensic / incident response supplier contract   / retainer / insurance policy.   1. Evidence of training / capability of in-house forensic / incident response resource. Any relevant communications with third parties that supported with the investigation / response to the incident. | 1. HTA-BCP-003 critical incident response plan (CIRP) and HTA-BCP-005 critical incident response plan people and contacts issued to all staff Jan 23 includes emergency external points of contact. Updated Feb 23 and reissued to staff on 28 Mar at all staff Awayday. Uploaded   CIRF overview shared on 28 Mar all staff Awayday. New BCP plan was tested 02 Jun, key milestones as per 7.2.1   1. HTA-BCP-005 critical incident response plan people and contacts includes 3rd party contacts 2. HTA-BCP-003 critical incident response plan (CIRP) includes list of associated SOPs   Critical Incident Response Plan (CIRP) intranet page Includes CIRP video: https://intranet.hta.gov.uk/pages/CIRP |  | Yes |
| 7.3.2 | All emergency contacts are kept securely, in hardcopy and are up-to-date. | 1. Hard copy of emergency contacts. 2. Documentation concerning communication and contact arrangements and procedures in the event of system and network availability issues | 1. CIRP, kept secure in IT systems and in hard copy by staff:   HTA-BCP-003 critical incident response plan  HTA-BCP-005 critical incident response plan people and contacts - uploaded as evidence  CIRP tested 02 Jun |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 7.3.4 | Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed. | 1. Backup policy / procedure. 2. RTOs and RPOs for the organisation's key systems, and evidence that these have been agreed with the business. Evidence that tests of the backups are performed on a regular basis to assess their ability to meet the defined RTOs and RPOs. Evidence that these have been completed for the organisation's key systems in the last calendar year. | 1. HTA-POL-094 Patch Management Policy issued to BDT for review 28 Apr. Has been approved by LD & RS. Email chain confirms LD & RS approval 05 Jun. Published policy uploaded 06 Jun   HTA-POL-095 Backup policy & email chain of approval uploaded, has been reviewed by BDT. BBC are responsible for back up management and have provided multi policy screenshots to demonstrate the backup process - 07Jun   1. Back up schedule and back up report for Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) uploaded 2. BCC, IT support providers, monitors scheduled backup jobs on a daily basis and receives daily backup reports - 3VMs & Sharepoint   Monthly reports also available. VEEAM backup software checks for backup consistency. Back up report and configuration uploaded as evidence. BCC provided 05 Jun:  back up info, schedule & testing VEEAM SharePoint screens VEEAM test screen shots  Uploaded to Word doc for GIAA 06 Jun |  | Yes |
| 7.3.5 | Your organisation tests its backups regularly to ensure it can restore from a backup. | Documentation associated with the organisation's previous restore from backup. | HTA runs nightly backups of all servers and cloud data. The IT Operation Manager has tested for backups and test file restoration.  BCC provided 15 png screenshots, copied to Word for GIAA access 05 Jun | . | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 7.3.6 | Your organisation’s backups are kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose. | Backup policy | 1. Copies held within dedicated and secure BCC disaster recovery environment.   BCC provided 10 png screenshots, copied to Word for GIAA access 05 Jun  Backups are incremental. in a chain depending on backup state  BCC provided latest HTA VM layout Diagram reflecting BCC and HTA responsibilities uploaded.  BCC store data in Cloud and moved to NAS drive which is separate from Azure  Part of DR / BCP   1. 3-2-1 approach applied- Azure Cloud, BCC & VEEAM   BCC to provide VEEAM report dashboard to complement the backup schedule  This should be covered in IAR |  | Yes |
| 8.3.1 | How do your systems receive updates and how often? | 1. Patch management procedure and / or strategy / policy. 2. Patch management reporting. 3. Sample of operating system and application patching schedules. 4. Change and installation logs for the last six months to confirm that historic patches have been applied. | 1. HTA-POL-094 Patch Management Policy has been approved by LD & RS. Email chain confirms LD & RS approval 05 Jun. Published policy uploaded 06 Jun Patches received every 30 days and RTANCA notifications from NHSE, action depends on severity 2. patch management scope includes endpoint and production patching controls and response time for severe incidents, 3. Pulseway patch reporting for servers 4. Endpoint os & app patching & portal - covered by Pulseway report   patch control reports from BCC uploaded, copied to Word for GIAA access 05 Jun  SIRO report reviewed at SMT 31 May. LD working on annual report for 08 Jun ARAC meeting. Papers uploaded 06 Jun | HTA’s patch management policy should be updated to include database, infrastructure, and 3rd party patching. | Partial |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 8.3.2 | How often, in days, is automatic patching typically being pushed out to remote endpoints? | 1. Patch management procedure and / or strategy / policy. 2. Patch management technology configurations. | 1. HTA-POL-094 Patch Management Policy has been approved by LD & RS. Email chain confirms LD & RS approval 05 Jun. Published policy uploaded 06 Jun automatic patching pushed out to remote endpoints under 30 days.   Patch control reports from BCC uploaded, copied to Word for GIAA access 05 Jun   1. technical configs align to patch man procedure - covered in policy |  | Yes |
| 8.3.3 | There is a documented approach to applying security updates (patches) agreed by the SIRO. | Patch management procedure and / or strategy  / policy. | 1. HTA-POL-094 Patch Management Policy has been approved by LD & RS. Email chain confirms LD & RS approval 05 Jun. Published policy uploaded 06 Jun Critical and high-risk security patches process included in the policy & severity defs added 2. patches for critical and high-risk vulnerabilities are applied within 14 days - part of RTANCA CareCERT alerts 3. Sample CareCERT alerts - NHS cyber alert email - alerts uploaded in Word as evidence here & in 6.3.3 NHS digital alerts 05 Jun   Pulseway reports for Feb, Mar April, May & Jun uploaded 06 Jun  Criteria met | Retain evidence that the patch management procedure and / or strategy / policy has been the agreed by SIRO or equivalent. | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 8.3.4 | Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted, reviewed regularly and signed off by the SIRO with an auditor agreeing a robust risk management | 1. Example patch status report. 2. Evidence of SIRO risk acceptances where applicable. | 1. ARAC papers including Cyber Security Dashboard and SIRO report for 08 Jun ARAC provided as evidence   HTA-POL-094 Patch Management Policy published 06 Jun  IT shared Pulseway report Jun 23 containing patch events over 30 days.  ATP reports sourced from NHS and NHS tenant Sample ATP compliance report to be provided by BCC IT working with BCC to develop an IT dashboard to include patching summary, end date to be confirmed.   1. critical or high-risk vulnerabilities mitigation covered in HTA-POL-094 Patch Management Policy. BCC receives alerts from NHS.   Alert sign off sheet to be provided by BCC   1. HTA have not had to accept the risk in the last 12 months, has always responded within 14 days as advised. As the worst-case scenario HTA could sandbox and isolate the system affected. External vulnerabilities typically managed at source |  | Yes |
| 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. | 1. Patch status report for the last six months. 2. Patch process treatment procedure or process | 1. Not applicable to HTA has not had any high-risk vulnerabilities where a patch has not been applied for several months   Patching actions be addressed through the monthly reporting from BCC and included in monthly IT SMT reporting.   1. HTA could create a workaround policy id this scenario emerged, could also be added to the IT Risk Register, and escalated to the Ops Register or the Strategic RR depending on severity 2. Technical remediation not relevant currently |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 9.3.1 | All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities. | 1. Software development methodology that includes security requirements in line with industry good practice such as OWASP. 2. Evidence associated with developers in the organisation completing secure design principles training. 3. Evidence associated with the organisation's capability to perform testing on web application code prior to go-live for three latest developments. | 1 MSP ATP used by HTA   1. Not applicable to HTA, s/w dev roles not in place, secure design principle would be outsourced training. no new web applications brought in 2. Not applicable to HTA, roles not in place HTA uses CRM & PowerBI   Uploaded as evidence:   * + Web Application Security Assessment Report Feb 22 (pen test report)   + Appcheck dashboard May 23   + OSWAP security report May 23 |  | Yes |
| 9.3.3 | The organisation has a technology solution or service that prevents users from accessing potentially malicious websites, reducing the risk of the organisation's infrastructure being infected with malware. | Evidence associated with the implementation of the technology solution. This could include reporting from the technology solution outlining the number of attempted connections blocked. | 1. MSP ATP used by HTA. Access limited to 3 users. NHS owns access rights   Covered by ARAC reporting   1. Covered by cyber alerts, reports uploaded 06 Jun |  | Yes |
| 9.3.4 | The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators. | 1. Access management process 2. List of users with access to the organisation's authoritative DNS server. 3. Evidence that individuals had access to the server are approved. 4. Evidence of last three access reviews on the authoritative DNS server. | 1. Managed by BCC, HTA's IT business partner. BCC host Power Domain. 2. Administrator DNS server access - multi-factor authentication 3. Access management list & users list uploaded as evidence   HR & AD list compared   1. Access frequency depends on server or if there is an issue or maintenance required   DN access word doc with screenshots added 07 Jun  Screenshot of group policy to show us who is allowed to make changes. | 1. Evidence should be retained of the contract with the outsourced DNS (BCC) service and 2. Evidence should be retained of AD group policy users that are authorised to make changes to DNS entries. | Partial |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 9.3.5 | The organisation understands and records all IP ranges in use across the organisation. | 1. Consolidated record of IP ranges across the organisation's network. 2. Evidence of IP range reviews (automated or manual). | 1. Email of IP ranges (Azure Live: 10.10.1.0, DR: 10.3.37.0) uploaded as evidence 2. Not done since move from former HO site 3 years ago, therefore no sample review material available. HTA has not required additional IP ranges since Azure was installed several years ago   No changes to DNS requirements needed.  If required, would follow NHS Digital standards. |  | Yes |
| 9.3.6 | The organisation protects its data in transit (including email) using appropriate technical controls, such as encryption. | 1. Encryption policy. 2. Browser and email configurations | 1. Encryption built into MS Exchange server & encryption referenced in IG&CS policy, HTA utilises Intune to set policies and controls in regard to the infrastructure and device settings, email of TLS setting screenshot uploaded 2. Browser and email configurations:   HTA [use.@hta.gov.uk](mailto:use.@hta.gov.uk) email address  IT Ops Manager, Caldicott Guardian and BBC have NHS email addresses to receive NHS related updates BCC confirmed encryption built into 365. | . | Yes |
| 9.3.7 | The organisation has registered and uses the National Cyber Security Centre (NCSC) Web Check service, or equivalent web check service, for its publicly-visible applications. | Evidence associated with website monitoring solution, vulnerability reporting for example. | 1 HTA uses APPCHECK for publicly-visible applications.  2. Cyber Security Dashboard for 08 Jun 23 ARAC uploaded evidence. Slide 4 states that the HTA monitors potential vulnerabilities on its public facing website.  Monthly reporting & Web check reports uploaded  SSL screenshot uploaded & saved in Word for GIAA 06 Jun  IT Ops Manager Cyber Associates Network membership uploaded |  | Yes |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Requirement | DSPT Assessment Documentation Requirement | Evidence viewed / Notes | Improvements required to meet the DSPT assertion test requirement/s | Met? |
| 10.1.1 | The organisation has an up- to-date list of its suppliers, which enables it to identify suppliers that could potentially pose a data security or data protection risk to the organisation. The list includes which suppliers process personal data or provide IT | 1. Supplier management policy / process. 2. Supplier list. | 1. Supplier information is held in CRM   As new suppliers are identified or commissioned, the budget holder is required to complete and submit a "New supplier Form" to Finance. The form includes checks on supplier's credentials.  BCC and Great Plains handle personal info. Frontier handle staff data for payroll purposes. Supplier list uploaded as evidence  Supplier management covered by HTA -POL-027 Procumbent and Tendering Policy. Stored in Wave, https://intranet.hta.gov.uk/pages/policies\_forms (Finance & Governance)   1. HTA suppliers sourced by crown commercial services framework:   government frameworks https:/[/www.crown](http://www.crowncommercial.gov.uk/)c[ommercial.gov.uk/](http://www.crowncommercial.gov.uk/)  Active Supplier details x 3 provided by Finance 07 Jun |  | Yes |

# Annex 3 GIAA Assurance Opinion

|  |  |
| --- | --- |
| Moderate | Moderate  Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control. |

### Rationale

The rating above is based on the work that GIAA has undertaken as part of this year’s DSPT assessment and is based upon our objective and professional view of the governance, risk management and the control framework in place around data security and protection. This work was solely concentrated on the 13 mandatory assertions that formed part of the required DSPT independent assessment process for 2022/23 as mandated by NHS England, formerly NHS Digital.

### Basis of assessment

Based on the work undertaken in support of deriving the DSPT ‘Overall NDG Standard Classification’ based upon the ‘Assertion-level Risk Ratings’ and the ‘Overall Risk Assessment Across all 10 NDG Standards,’ we are of the opinion that a ‘moderate’ assurance opinion is warranted due to the minimal number of enhancements in existing controls required as identified in **Annex 1 – Management Action Plan.**

This ‘moderate’ rating reflects the good arrangements in place to respond to DSPT completion processes, and the fact that our work has not identified any significant issues that require attention. Where we have made recommendations, these are to help HTA enhance the existing control environment for its next DSPT submission.

### Key Findings Summary:

Detailed findings are available in Annex 2. The following key findings summarised here are issues identified around the internal control environment and related processes used by HTA in completing the DSPT submission.

#### Governance Arrangements

Our review has identified that the governance arrangements over the DSPT process have improved from the previous year. Governance arrangements over data security and data protection more generally have become more enhanced and are supported by appropriate structures, policies, and procedures.

#### Cyber and Information Risk Management

Due to the relationship that has been developed with BCC Group, who provide HTA with their IT support services, at the time of our review, IT risks to HTA are well managed and meet the requirements of the DSPT framework. It is vital that BCC continue to provide HTA with high levels of support to ensure IT risks are dealt with effectively and efficiently. We would also recommend that further work in this area is linked to the guidance and improvement plan we have provided as part of our review of **Records Management.**

There are some control enhancements required to improve existing controls, as documented in Annex 2 – DSPT Statements Audited; however, it is important to recognise the journey that HTA has been on in this area. Significant improvements have been seen this year and it is important that HTA maintains traction in this area, as information and cyber threats are constantly evolving.

# Annex 4: Our classification systems

|  |  |
| --- | --- |
| Substantial | Substantial  The framework of governance, risk management and control is adequate and effective. |
| Moderate | Moderate  Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control. |
| Limited | Limited  There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective. |
| Unsatisfactory | Unsatisfactory  There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail. |

### Recommendation

|  |  |  |
| --- | --- | --- |
| Priority | Definition | Action required |
| High | Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk. | Remedial action must be taken urgently and within an agreed timescale. |
| Medium | Weakness in governance, risk management and control that if unresolved exposes the organisation to a high level of residual risk. | Remedial action should be taken at the earliest opportunity and within an agreed timescale. |
| Low | Scope for improvement in governance, risk management and control. | Remedial action should be prioritised and undertaken within an agreed timescale. |

# Annex 5: Distribution

#### Draft and final report

Louise Dineley Director of Data, Technology and Development / SIRO

Sam Mortimer Project Manager in Data, Technology and Development Directorate

Jo Charlton Head of Internal Audit, GIAA (**final ToR and report only**) Karen Holland Group Chief Internal Auditor, GIAA (**final report only**)