

Audit and Risk Assurance Committee (ARAC)

SIRO Report

**Audit and Risk Assurance (ARAC) meeting**

**Date:** 8 June 2023 **Paper reference:** AUD 23/23 **Agenda item: 9**

**Author:** Richard Sydee Director of Resources

**Protective Marking:** OFFICIAL

# SIRO Report

## Purpose of paper

1. To provide an annual update to the Audit and Risk Assurance Committee (ARAC)

on the annual assessment of the HTA’s information risk management.

## Decision making to date

1. Reviewed by the HTA Senior Management Team (SMT) on 31 May 2023

## Action required

1. To note the Senior Information Risk Officer’s (SIRO) assessment of the management of information across the HTA including compliance with the National Cyber Security Centre (NCSC) Minimum Cyber Security Standards 2018.

## Background

1. The SIRO holds responsibility to manage the strategic information risks that may impinge on our ability to meet corporate objectives, providing oversight and assurance to the Executive and Authority of the HTA. It is a Cabinet Office (CO) requirement that Boards receive regular assurance about information risk

management. This provides for good governance in its own right, ensures that the Board is involved in information assurance and informs the ARAC’s consideration of the Annual Governance Statement (AGS).

1. This report is my annual report to the Accounting Officer and ARAC and supports the assessment contained within the AGS. The SMT has also reviewed this report.
2. As with last year’s report I have assessed the HTA’s cyber security management against outcome-based NCSC *Minimum Cyber Security Standard* – this was agreed by ARAC in February 2020.

## Report

1. The SIRO Report reflects on the HTA’s information governance work undertaken during 2022/2023 and provides assurances that personal data is processed in line with current legislation. This includes:-
   * An overview of key performance indicators relating to the HTA’s processing of information requests within the necessary legal frameworks.
   * An update on the plans the HTA has in place to minimise risk or improve current or future performance
   * Providing assurance of ongoing improvement to manage information risks. information on organisational compliance with, and performance against, the

legislative and regulatory requirements relating to the handling and processing of information in respect of: -

* + - Data Protection Act 2018 including the requirements of UK General Data Protection Regulation and the Freedom of Information Act 2000
    - Environmental Information Regulations 2004
    - NHS Data Protection Toolkit (DSPT)
    - Any Security Incidents requiring notification to the regulator –

Information Commissioners Office (ICO)

1. The HTA routinely assesses the risks to information management across the organisation, through its Information Asset Register and Record of Processing Activities. Understanding what information the HTA holds and how it uses it allows the organisation to assess the risk of data loss, cyber security threats and vulnerabilities and the effective management of information. The HTA has a number of additional controls that support our use of information including detailed policies on Records Management, managing Subject Access Requests

and Freedom of Information Request as well as Standard Operating Procedures (SOPs) on the creation and management of records. These risks are recognised within the HTA’s strategic and operational risk registers which are reviewed monthly by SMT to ensure appropriate resource are in place to mitigate risks.

1. Part of the assurance of the HTA’s arrangements is carried out by our Internal Auditors. In year audit reviews have included audits of our DSPT submission in June 2022 and our approach to Records Management.

## Data Breach Management and Reporting

1. In 2022/23 the HTA reviewed and updated its policy on the management and investigation of data breaches (actual or potential). All incidents are reported to the SIRO and the Data Protection Officer. Details of the incident are logged on the Data Breach log. and promptly investigated and assessed against the ICO guidance. The key assessment includes a review of numbers of people affected, sensitivity, nature of breach and likely impact. Dependent on the assessment, the incident may need escalation to the Caldicott Guardian, and may be self-referred by the HTA to the Information Commissioner’s Office (ICO). The reporting, containment actions, investigation and learning phases of data breach incidents play a key role in the management of risk and improvement of internal controls.
2. During 2022/23 reporting year the HTA recorded 5 potential data breaches, details are contained in the table below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Number of incidents** | **Recorded as personal data breach** | **Reported to ICO** |
| **Data emailed to incorrect recipient** | 4 | 1 | 1 |
| **Loss of physical data** | 1 | 0 | 0 |
| **Other** | 0 | 0 | 0 |

1. As part of the investigation of an incident, learning actions will be captured to identify opportunities to reduce the chances of a similar breach occurring in the future.
2. Learning is shared across the organisation via either specific training or as corporate messages being issued to staff to remind them of good practice in avoiding breaches occurring.

## Freedom of Information and Subject Access Requests

1. During 2022/23 the HTA received 23 requests for information under the Freedom of Information Act. The number of requests is relatively constant and does not vary greatly year on year.

|  |  |  |  |
| --- | --- | --- | --- |
| **Total received** | **Total responded to** | **Refused** | **Rescinded** |
| 23 | 19 | 3 | 1 |

1. During 2022/23 only one of these requests was not provided within the statutory time limit, notification was provided to the requestor ahead of the deadline to advise that the request would exceed the statutory time limit.
2. Under the Data Protection Act 2018, any living person, regardless of their age, can request information about themselves that is held by the HTA. This application process is referred to as a Subject Access Request (SAR). During 2022/23 the HTA received 3 Subject Access Requests.

|  |  |  |  |
| --- | --- | --- | --- |
| **Total received** | **Total responded to** | **Refused** | **Rescinded** |
| **2** | 1 | 1 | 0 |

## HTA Activity during 2022/23

1. During this year we have continued to ensure our systems are secure, complying with advice on security patching in a timely manner, closely monitoring attempts to access HTA systems – both through direct access attempts and other means such as phishing emails.
2. This year we have engaged an Information Governance Manager to strengthen our focus on information risk and governance. This role was initially recruited as a fixed term position but SMT have recently approved a request to make this a permanent post within the HTA’s workforce.

There has also been an extensive review of HTA policies, procedures and thearrangements to manage information, data and records. This programme of work has resulted in over 20 internal policies being reviewed and updated to reflect strengthened controls and assurances on the risks associated with increased remote and mobile working.

1. With the help of ARAC we have continued to develop and refine our cyber dashboard and now believe we have reached a level of maturity where this is relied upon for assurance at all levels of the business. Over the last 12 months the HTA has consistently increased its secure score to a current 93.26%
2. Cyber security risks remain a real threat and mitigating those risks continues to present a challenge to the HTA. During this year we have continued to monitor the threats and attempts to access HTA systems. This information is reported monthly to the SMT portfolio meeting and routinely to ARAC in the cyber security update, We continue to develop future plans that will help maintain and strengthen defences and enhance corporate resilience
3. Our self-assessment against the DSPT for the 2022 submission was one of general compliance with the DSPT mandatory assertions. In terms of the required audit of our evidence, required by the toolkit to be independent of the HTA and undertaken by our Internal Auditors, this led to a limited opinion, with issues acknowledged in relation to the breadth and detail of the evidence provided to support our assessment.
4. Significant resource has been focussed on the 2023 DSPT submission with a number of new policies and procedures developed and implemented and a new approach to gathering and presenting the supporting information required under the independent internal audit review of our submission. We have also focussed specific project management resource on this area to tighten our approach to this return.
5. The ever increasing number of assertions that apply to ALBs leads us to conclude there are some areas where noncompliance poses a low risk to the HTA and the cost of achieving compliance is a significant burden for an organisation our size. Where we make decision to make no further efforts to comply these will be discussed and approved at SMT and drawn to the attention of ARAC.
6. We expect to submit our assessment in line with the 30 June 2023 deadline.
7. Overall, we have a low tolerance of risk for information that falls within the auspices of GDPR and/or is business critical, and the focus of our resource will continue to be the secure and compliant storage of these records.

## Assessment and conclusion

1. As in previous years I have considered the HTA’s compliance with the NCSC Minimum Cyber Security Standard and discussed this with our Chief Information Technology Officer. The requirements have been applied proportionately and matched to the HTA’s organisational risks. Not all the areas apply to the HTA in their entirety. My assessment is contained at Appendix A in this document.
2. It is three years since ARAC approved our move to this assessment criteria, although I feel it remains a robust evaluation of our approach I would recommend that this be considered against other evaluation options ahead of next year’s report to ensure all stakeholders retain confidence in this approach..
3. In line with the Office of the Government SIRO handbook I have also considered a number of the factors that underpin the management of the HTA’s information risks.

* I believe the HTA has an effective Information Governance framework in place and that the HTA complies with all relevant regulatory, statutory and organisation information security policies and standards.
* I am satisfied that the HTA has introduced further processes to ensure staff are aware of the need for information assurance and the risks affecting corporate information.
* The HTA has appropriate and proportionate security controls in place relating to records and will look to further strengthen these by embedding the recommendations for the recent Records Management audit in to our policies and procedures..

1. In conclusion, good progress has been made during 2022/23 with key actions taken to strengthen the HTA’s approach to effectively manage information risks and ensure a robust approach to information governance. In particular, as the potential for cyber risk increases, it is essential the HTA takes action to understand and mitigate risk in this area.



# Appendix A – NCSC - Minimum Cyber Security Standard

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **IDENTIFY**  ***Departments shall put in place appropriate cyber security governance processes.*** | 1. There **shall** be clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services. 2. There **shall** be appropriate management policies and processes in place to direct the Departments overall approach to cyber security. 3. Departments **shall** identify and manage the significant risks to sensitive information and key operational services. 4. Departments **shall** understand and manage security issues that arise because of dependencies on external suppliers or through their supply chain. This includes ensuring that the standards defined in this document are met by the suppliers of third-party services. This could be achieved by having suppliers assure their cyber security against the HMG Cyber Security Standard, or by requiring them to hold a valid [Cyber](https://www.cyberessentials.ncsc.gov.uk/) [Essentials](https://www.cyberessentials.ncsc.gov.uk/)1 certificate as a minimum. Cyber Essentials allows a supplier to demonstrate appropriate diligence with regards to standard number six, but the Department **should**, as part of their risk assessment, determine whether this is sufficient assurance. |  |

1 [Cyber Essentials](https://www.cyberessentials.ncsc.gov.uk/) helps guard against the most common cyber threats and demonstrates a commitment to cyber security. It is based on five technical controls but does not cover the entirety of the HMG Cyber Security Standard.

7

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | e) Departments **shall** ensure that senior accountable individuals receive appropriate training and guidance on cyber security and risk management and **should** promote a culture of awareness and education about cyber security across the Department. |  |
| **2** | **Departments shall identify and catalogue sensitive information they hold.** | 1. Departments **shall** know and record:    1. What sensitive information they hold or process    2. Why they hold or process that information    3. Where the information is held    4. Which computer systems or services process it    5. The impact of its loss, compromise, or disclosure | I believe we do know this and have documentation to  support it in the HTA’s Personal Data Inventory |

|  |  |  |  |
| --- | --- | --- | --- |
| **3** | ***Departments shall identify and catalogue the key operational services they provide.*** | 1. Departments **shall** know and record:    1. What their key operational services are    2. What technologies and services their operational services rely on to remain available and secure    3. What other dependencies the operational services have (power, cooling, data, people etc.) IV. The impact of loss of availability of the service | This is known and given recent upgrades and changes to our systems and infrastructure we now have improved visibility of these services and their dependencies |

|  |  |  |  |
| --- | --- | --- | --- |
| **4** | ***The need for users to access sensitive information or key operational services shall be understood and continually***  ***managed.*** | 1. Users **shall** be given the minimum access to sensitive information or key operational services necessary for their role. 2. Access **shall** be removed when individuals leave their role or the organisation. Periodic reviews **should** also take place to ensure appropriate access is maintained. | I believe we do know this, and this is set out in our policies  The HTA has implemented a checklist process for starters, leavers, and those changing roles. |
| **5** | **PROTECT**  ***Access to sensitive information and key operational services shall only be provided***  ***to identified, authenticated, and authorised users or systems.*** | 1. Access to sensitive information and services **shall** only be provided to authorised, known, and individually referenced users or systems. 2. Users and systems **shall** always be identified and authenticated prior to being provided access to information or services. Depending on the sensitivity of the information or criticality of the service, you may also need to authenticate and authorise the device being used for access. | As above access is provided on a needs basis and set out in policies  We have a number of password protected systems, some with Multi Factor Authentication and complex password requirements. |

|  |  |  |  |
| --- | --- | --- | --- |
| ***6*** | ***Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.*** | This section covers four main areas of technology.   1. **To protect your enterprise technology, you shall:**    1. Track and record all hardware and software assets and their configuration    2. Ensure that any infrastructure is not vulnerable to common cyber-attacks. This **should** be through secure configuration and patching, but where this is not possible, then other mitigations (such as logical separation) **shall** be applied.    3. Validate that through regular testing for the presence of known vulnerabilities or common configuration errors.    4. Use the UK Public Sector DNS Service to resolve internet DNS queries.    5. Ensure that changes to your authoritative DNS entries can only be made by strongly authenticated and authorised administrators.    6. Understand and record the Departmental IP ranges.    7. Where services are outsourced (for example by use of cloud infrastructure or services), you **shall** understand and accurately record which security related responsibilities remain with the Departments and which are the supplier’s responsibility. 2. **To protect your end user devices, you shall:**    1. Identify and account for all end user devices and removable media.    2. Manage devices which have access to sensitive information, or key operational services, such that technical policies can be applied, and controls can be exerted over software that interacts with sensitive information. | We do have such a list  We do this regularly (monthly – reported by material by exception only)  We do this regularly  This is undertaken  I am confident that we do this, and this was reviewed as part of GDPR compliance |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | 1. Be running operating systems and software packages which are patched regularly, and as a minimum in vendor support. 2. Encrypt data at rest where the Department cannot expect physical protection, such as when a mobile device or laptop is taken off-site or on removable media. 3. Have the ability to remotely wipe and/or revoke access from an end user device. | The HTA utilise Bitlocker functionality to ensure data is secure at rest on HTA hardware. Screen out times and locks are controlled centrally. HTA Mobile phone data is also encrypted  When using personal mobile devices, a secure “segment” is created which can be wiped. On all HTA devices this can be done completely. |
|  |  | 1. **To protect email, you shall:**    1. Support Transport Layer Security Version 1.2 (TLS v1.2) for sending and receiving email securely.    2. Have Domain-based Message Authentication Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) records in place for their domains to make email spoofing difficult.    3. Implement spam and malware filtering, and enforce DMARC on inbound email. 2. **To protect digital services, you shall:**    1. Ensure the web application is not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities2.    2. Ensure the underlying infrastructure is secure, including verifying that the hosting environment is maintained securely and that you have appropriately exercised your | The HTA complies with this  Monitor mode – reduces the likelihood of our email domain being spoofed  The HTA complies with this.  Scan for Open Web Application Security Project and Drupal annually |

2 https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | responsibilities for securely configuring the infrastructure and platform.   1. Protect data in transit using well-configured TLS v1.2. 2. Regularly test for the presence of known vulnerabilities and common configuration errors. You **shall** register for and use the NCSC's Web Check service. | We subscribe to NCSC and mailcheck – service ensure our systems are checked multiple times a day. |
| **7** | ***Highly privileged accounts should not***  ***be vulnerable to common cyberattacks.*** | 1. Users with wide ranging or extensive system privilege **shall** not use their highly privileged accounts for high-risk functions, in particular reading email and web browsing. 2. Multi-factor authentication **shall** be used where technically possible, such as where administrative consoles provide access to manage cloud-based infrastructure, platforms, or services. Multi-factor authentication **shall** be used for access to enterprise level social media accounts. 3. Passwords for highly privileged system accounts, social media accounts and infrastructure components **shall** be changed from default values and **shall** not be easy to guess. | All Admin account holder hold a separate normal user account  The HTA does utilise MFA for system access – we are exploring controls on social media accounts |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Passwords which would on their own grant extensive system access, **should** have high complexity. | The HTA complies with this |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **8** | **DETECT**  ***Departments shall take steps to detect common cyberattacks.*** | a)  b) | As a minimum, Departments **shall** capture events that could be combined with common threat intelligence sources e.g. Cyber Security Information Sharing Partnership ([CISP)](https://www.ncsc.gov.uk/cisp) to detect known threats.  Departments **shall** have a clear definition of what must be protected and why (based upon Standard 1), which in turn influences and directs the monitoring solution to detect events which might indicate a situation the Department wishes to avoid. | I am confident we do this, and we provide regular alerts from NHS careCERT which are circulated and incorporated in our practices.  This is established in SOPs and policies |
| c) | Any monitoring solution **should** evolve with the Department’s  business and technology changes, as well as changes in threat. | It will – we will look at this as part of our transformation work. |
| d) | Attackers attempting to use common cyber-attack techniques  **should** not be able to gain access to data or any control of technology services without being detected. | Our supplier - BCC hold analytics and 365 analytics (cloud app security, azure active directory) |
| e) | Digital services that are attractive to cyber criminals for the purposes of fraud **should** implement transactional monitoring techniques from the outset. | We believe this is not relevant to HTA systems |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **9** | **RESPOND**  ***Departments shall have a defined, planned, and tested response to cyber security incidents that impact sensitive information or key operational services.*** | a)  b)  c) | Departments **shall** develop an incident response and management plan, with clearly defined actions, roles, and responsibilities. A copy of all incidents **shall** be recorded regardless of the need to report them.  Departments **shall** have communication plans in the event of an incident which includes notifying (for example) the relevant supervisory body, senior accountable individuals, the Departmental press office, the National Cyber Security Centre (NCSC), Government Security Group (Cabinet Office), the Information Commissioner’s Office (ICO) or law enforcement as applicable (not exhaustive).  In the event of an incident that involves a personal data breach Departments **shall** comply with any legal obligation to report the breach to the Information Commissioner’s  Office. Further information on this can be found [here.](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) | These are set out in our current/proposed policies?  The HTA has a data breach policy  This is set out in our policies. |
|  |  | d) |  |  |
|  | The incident response and management plan **should** be tested at regular intervals to ensure all parties understand their roles and responsibilities as part of the plan. Post testing findings **should** inform the immediate future technical protection of the system or service, to ensure identified issues cannot arise in the same way again.  Systemic vulnerabilities identified **shall** be remediated. | This is not explicit in our policies.  We will consider undertaking annual tabletop exercises – will ensure we consider this as we evolve our systems and include assessments in all change management through change request |
| e) | On discovery of an incident, mitigating measures **shall** be assessed and applied at the earliest opportunity, drawing on expert advice where necessary (e.g., a Cyber Incident  Response (CIR) company or NCSC). |  |
| f) | Post incident lessons **shall** be assessed, and lessons implemented into future iterations of the incident management plan. | This is complied with |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **10** | **RECOVER**  ***Departments shall have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise.*** | a)  b)  c) | Departments **shall** identify and test contingency mechanisms to continue to deliver essential services in the event of any failure, forced shutdown, or compromise of any system or service. This may include the preservation of out of band or manual processes for essential services or CNI.  Restoring the service to normal operation **should** be a well- practised scenario.  Post incident recovery activities **shall** inform the immediate future technical protection of the system or service, to ensure the same issue cannot arise in the same way again. Systemic vulnerabilities identified **shall** be remediated. | We have a number of contingency plans.  Our assets are cloud based and include enhanced protections and recovery functions. |