Audit and Risk Assurance (ARAC) meeting

Date: 12 June 2024

Paper reference: AUD 20-24

Agenda item: 3.2

Author: Tom Skrinar
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

2. Reviewed by the HTA Senior Management Team (SMT) on 4 June 2024

Action required

3. 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

4. The SIRO holds responsibility to manage the strategic information risks that may impact 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).

5. This report is my first annual report to the Accounting Officer and ARAC and supports the assessment contained within the AGS. The SMT has also reviewed this report.

6. As with last year's report, I have assessed the HTA's cyber security management against outcome-based NCSC *Minimum Cyber Security Standard* (this approach was agreed by ARAC in February 2020).

Report

7. The SIRO Report reflects on the HTA's information governance work undertaken during 2023/24 and provides assurances to ARAC of the arrangements in place to ensure the proper governance of information within the HTA. 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 the legislative and regulatory requirements relating to the handling and processing of information in respect of:
    - Data Protection Act 2018 (DPA)
    - UK General Data Protection Regulation (GDPR)
    - Freedom of Information Act 2000 (FOIA)
    - Environmental Information Regulations 2004 (EIR)
    - NHS Data Protection Toolkit (DSPT)
    - Any Security Incidents requiring notification to the regulator – Information Commissioners Office (ICO)

8. The HTA routinely assesses the risks to information management across the organisation, through its Information Asset Register (IAR) and Record of Processing Activities (ROPA). Understanding what information the HTA holds and

how it uses it allows the organisation to assess and manage the risks associated with protected information, the risk of data loss, cyber security threats and vulnerabilities and the effective management of information. The HTA completed formal reviews of both the IAR and the ROPA in 2023/24.

9. 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 Requests as well as Standard Operating Procedures (SOPs) on the creation and management of records. We also carry out additional assessments such as Data Protection Impact Assessments to ensure that any changes or additions to current processes are done in a way that minimises data protection risks. Data protection and security risks are recognised within the HTA's operational risk register which is reviewed monthly by BDT to ensure appropriate resource are in place to mitigate risks.

10. 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 2023 and receipt of the final report on the audit of our approach to Records Management completed in Q4 2022/23. This year a sample of 13 Mandatory Assertions across ten Data Security standards (Standard 1 – personal confidential information, Standard 2 – staff responsibilities, Standard 3 – training, Standard 4 – Managing data access, Standard 5 – Process reviews, Standard 6 – responding to incidents, Standard 7 – continuity planning, Standard 8 – unsupported systems, Standard 9 – IT Protection, Standard 10 – Accountable suppliers) was selected covering 45 items of evidence.

11. We will be submitting our DSPT assessment in line with the 30th June 2024 deadline.

Policies

12. The HTA's core data security and information governance policy sit within its Information Governance Framework (IGF), which is under constant review according to changing needs and threats. The IGF now compromises of the following policies:

Policy	Last revision	Next revision
HTA-POL-087-Information Governance Assurance Framework	2023 (published June 2023)	2025

HTA-POL-088 Records Management and Retention Policy	2023	2025
HTA-GD-010 Records Retention Schedule	2024	2025
HTA-POL-056 Information Governance and Cyber Risk	2024	2025

13. The HTA has identified a wider Records Management Programme on its 2024/25 business plan which will include a review of information governance and security policies

Data Breach Management and Reporting

14. In 2023/24 the HTA reviewed and updated its policy on the investigation and management of data breaches (actual or potential). All incidents are reported to the Data Protection Officer for review with high risk incidents additionally reported to the SIRO. Details of incidents are logged in the Data Breach log and promptly investigated by the HTA's Information Governance and Records Manager lead and assessed against the ICO guidance. Dependent on the assessment, the incident may need escalation to the Caldicott Guardian (i.e. if it involves individuals' health and care information), 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 ongoing improvement of internal controls.

15. During 2023/24 reporting year, the HTA recorded 10 incidents of potential breaches, details are contained in the table below:

Category	**Recorded as security breach with no personal data**	**Recorded as personal data breach**	**Reported to ICO**	**Total**
Data emailed to incorrect recipient	3	6	0	9
Loss of physical data				
Other	1 external breach			1

16. As part of the investigation of an incident, learning actions are captured to identify opportunities to reduce the chances of a similar breach occurring in the future. Learning is embedded in policy where appropriate and 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

17. During 2023/24 the HTA received 29 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
29	26[1]	0	0

18. During 2023/24 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.

19. 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 2023/24 the HTA received 1 Subject Access Request.

Total received	Total responded to	Refused	Rescinded
1			

HTA Activity during 2023/24

20. I took over as Senior Information Risk Owner on joining the HTA in late August 2023 and undertook core SIRO training for the role in November. As there had been a gap of nine weeks between my predecessor leaving and me starting, the Director of Data, Technology and Development fulfilled that responsibility in the interim.

21. This year we engaged a Records Management and Information Governance Lead (also acting as Data Protection Officer, DPO) to strengthen our information risk and governance management, although we have only had the benefit of a consistent permanent resource since February 2024. Furthermore, we were

[1] The HTA sought further clarification on the three requests not responded to and closed the cases after no reply within three months.

without a Head of IT for roughly half of the year (commenced in November 2023). As ARAC is aware, through risk reports throughout the year, this has put a large amount of pressure on the Director of Data, Technology and Development to cover a number of complex responsibilities and, as SIRO, I am extremely grateful for the significant effort she has brought to bear in order to manage data and security risks whilst lacking key staff or the required interim support. I am comfortable that we have been able to seek expert, in particular legal, advice when required.

22. During the year and with the support of the HTA's third party supplier for IT support, 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.

23. As part of the ongoing review of policies and procedures to manage information, data and records, two further policies and a standard operating procedure for IT builds have been produced, as well as a draft acceptable usage policy. With the help of ARAC and the opportunity to benchmark our performance across ALBs we have continued to develop and refine our cyber dashboard.

24. 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 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 and we continue to develop plans to maintain and strengthen defences and enhance corporate resilience.

25. A further data security risk facing the HTA lies in the fact that we have not significantly invested in our IT infrastructure for several years. As identified to GIAA as part of our DSPT submission, we have two systems that are no longer supported and will require replacement or significant upgrading. I am very pleased that we are developing a comprehensive, long-term IT investment strategy that will ensure that all of our systems and infrastructure will be brought up to date and made better able to manage modern data security risks. The replacement of unsupported applications will need to be part of that plan and we will follow best practice in managing any heightened security risk in the meantime.

26. Our self-assessment against the DSPT for the submission in June 2023 demonstrated improvements to our data security and protection practices. It 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 moderate opinion. This means that there were no standards rated as 'unsatisfactory' and none rated as 'limited' (of the ten areas assessed, we scored 'substantial' for six and 'moderate' for four). Furthermore, the GIAA's confidence level in the veracity of HTA's self-assessment was high.

27. The increasing detail that supports the DSPT assertions presents a challenge to smaller organisations that have less resource to dedicate to governance arrangements that generate the evidence that GIAA seeks. This pressure is felt by organisations such as the HTA that hold a category 1 status alongside large NHS Trusts. The HTA has previously shared feedback on the disproportionate nature of the assessment and evidence requirements for smaller ALBs, but this has not yet resulted in any change. Similar feedback has been provided as part of the recent engagement on the Cyber Assurance Framework (CAF). We would hope to be able to agree compliance arrangements in future that are more commensurate with our size and scale of activity.

28. 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

29. I have considered the HTA's compliance with the NCSC Minimum Cyber Security Standard and discussed this with the Head of IT. 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.

30. It is four years since ARAC approved our move to this assessment criteria. Although I feel it is 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.

31. In line with the SIRO training I have undertaken this year, 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 continually strengthens these by embedding best practice into our policies and procedures.

32. In conclusion, good progress has been made during 2023/24 with key actions taken to strengthen the HTA's approach to effectively manage information risks and ensure a robust approach to information governance. 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.***	a) There **shall** be clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services. b) There **shall** be appropriate management policies and processes in place to direct the Departments overall approach to cyber security. c) Departments **shall** identify and manage the significant risks to sensitive information and key operational services. d) 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 Essentials[2] 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.	I am comfortable that we have clear lines of responsibility and accountability and that we have appropriate policies and processes in place. I am comfortable that policies exist to ensure that that IAOs are able to identify, understand and manage risks. We will ensure that further training is made available to IAOs to develop their understanding of the role and responsibilities. I have received SIRO training in 2023/24.

[2] Cyber Essentials 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.

		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.**	a) Departments **shall** know and record: I. What sensitive information they hold or process II. Why they hold or process that information III. Where the information is held IV. Which computer systems or services process it V. The impact of its loss, compromise, or disclosure	We will strengthen the IAR and ROPA now that we have an Records Management and Information Governance lead in role to ensure that day to day practices align with the records retention schedule and the Records Management Policy.

3	***Departments shall identify and catalogue the key operational services they provide.***	a) Departments **shall** know and record: I. What their key operational services are II. What technologies and services their operational services rely on to remain available and secure III. What other dependencies the operational services have (power, cooling, data, people etc.) IV. The impact of loss of availability of the service	We will strengthen the IAR and ROPA now that we have an Records Management and Information Governance lead in role to ensure that day to day practices align with the records retention schedule and the Records Management Policy.

4	***The need for users to access sensitive information or key operational services shall be understood and continually managed.***	a) Users **shall** be given the minimum access to sensitive information or key operational services necessary for their role. b) Access **shall** be removed when individuals leave their role or the organisation. Periodic reviews **should** also take place to ensure appropriate access is maintained.	We have strengthened our system access controls 2023/24 through an updated Joiners / Movers / Leavers process that includes IT-specific requirements and implemented a change control process.
5	**<u>PROTECT</u>** ***Access to sensitive information and key operational services shall only be provided to identified, authenticated, and authorised users or systems.***	a) Access to sensitive information and services **shall** only be provided to authorised, known, and individually referenced users or systems. b) 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 we have introduced a strict change manage process and access is provided on a needs basis and set out in policies Where available we have deployed Multi Factor Authentication. This is an ongoing task to review our existing processes.

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. **a) To protect your enterprise technology, you <u>shall</u>:** I. Track and record all hardware and software assets and their configuration II. 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. III. Validate that through regular testing for the presence of known vulnerabilities or common configuration errors. IV. Use the UK Public Sector DNS Service to resolve internet DNS queries. V. Ensure that changes to your authoritative DNS entries can only be made by strongly authenticated and authorised administrators. VI. Understand and record the Departmental IP ranges. VII. 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. **b) To protect your end user devices, you <u>shall</u>:** I. Identify and account for all end user devices and removable media. II. 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.	II am comfortable that our IT assets are recorded within a suitable system, being under a structured programme with automated update processes and patching regime. I am confident that our recent penetration test and ongoing vulnerability scans have highlighted good practices and our strong Cyber Security position. I am informed that all DNS related changes are recorded against our Change Management process and only our third-party support organisation have access to make changes to our DNS settings. As part of the outsourcing of our IT services, the administrative actions and controls are managed on our behalf. This is a delegated support service, in accordance with HTA policies and governance, that is checked through management review meetings. Internally there is restricted access to administrative processes, as to ensure demarcation between internal and external support partners. Within control of the business financially and resourcefully our software and operating systems are patched and maintained. As a small ALB there are occasions when it may not financially viable to replace systems immediately when outside of support, these are managed accordingly. I confirm that all end user devices within the organisation are encrypted and are managed

		III. Be running operating systems and software packages which are patched regularly, and as a minimum in vendor support. IV. 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. V. Have the ability to remotely wipe and/or revoke access from an end user device.	through InTune with Bitlocker functionality to ensure data is secure at rest on HTA hardware. On mobile devices Screen out times and locks are controlled centrally through InTune policies. HTA Mobile phone data is also encrypted.

		c) To protect email, you <u>shall</u>: I. Support Transport Layer Security Version 1.2 (TLS v1.2) for sending and receiving email securely. II. 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. III. Implement spam and malware filtering, and enforce DMARC on inbound email. **d) To protect digital services, you <u>shall</u>:** I. Ensure the web application is not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities[3]. II. Ensure the underlying infrastructure is secure, including verifying that the hosting environment is maintained securely and that you have appropriately exercised your responsibilities for securely configuring the infrastructure and platform. III. Protect data in transit using well-configured TLS v1.2. IV. Regularly test for the presence of known vulnerabilities and common configuration errors. You **shall** register for and use the NCSC's Web Check service.	I confirm that all email security protocols are in place to protect ingress and egress of our data. We have robust email filtering solutions and have these configured with recommended security profiles. As above as an organisation we are committed to ensuring that our data is transmitted in the most secure way, this is achieved by having the correct security principles applied. As an organisation we are registered with the NCSC and use their web check service. We also have AppCheck to vulnerability assess our systems.
7	***Highly privileged accounts should not***	a) 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.	As stated within the Information Governance and Cyber Risk policy, privileged accounts must not be used for standard tasks and operations. I can confirm that this is the case and any Administration

[3] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

	be vulnerable to common cyberattacks.	b) 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. c) 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. Passwords which would on their own grant extensive system access, **should** have high complexity.	Account is identified with access granted to the necessary services it administrates.

8	**DETECT** ***Departments shall take steps to detect common cyberattacks.***	a) As a minimum, Departments **shall** capture events that could be combined with common threat intelligence sources e.g. Cyber Security Information Sharing Partnership (CISP) to detect known threats. b) 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. c) Any monitoring solution **should** evolve with the Department's business and technology changes, as well as changes in threat. 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. e) Digital services that are attractive to cyber criminals for the purposes of fraud **should** implement transactional monitoring techniques from the outset.	HTA systems are configured to alert and identify risks as they are found. Our systems are continuously actively monitoring activities and will stop any attempts at infiltrating our networks. Our defender suites across the servers and workstations is monitored by NHS as part of our working agreement with them and our inbound and outbound mail is monitored by best of breed IT solutions. Phishing and Malware attacks are identified and mitigated as part of the solution. It will – we will look at this as part of our transformation work. Our supplier - BCC hold analytics and 365 analytics (cloud app security, azure active directory) We believe this is not relevant to HTA systems

9	**<u>RESPOND</u>** ***Departments shall have a defined, planned, and tested response to cyber security incidents that impact sensitive information or key operational services.***	a) 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. b) 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 c) 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.	I confirm that the HTA Operational breach log is active to manage all types of breaches across the organisation, there is a strong communication programme to alert staff to a major incident and annual BCP meetings are scheduled with all staff. Our IT systems are cloud hosted, through Microsoft and Microsoft Azure, this limits the risk of a potential major incident from physical factors, should as flooding, power and robbery. A full BCP of IT services is therefore, challenging, with only selected highlighted services being open to event planning.
		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. 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.	As an organisation we take incidents seriously and will endeavour to perform a root cause analysis (RCA) and look at lessons learnt to ensure that a repeat incident is significantly reduced, this is managed through our Operational Risk Registers. This is complied with

10	**<u>RECOVER</u>** ***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) 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. b) Restoring the service to normal operation **should** be a well-practised scenario. c) 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.	Our IT services are backed up and offsite backup copies are created. As our systems are predominantly Microsoft based, these are protected against such failures. Internal services hosted by our Azure infrastructure, are replicated, and following our strict backup regime, individual services are backed up independently.