Version 5 (10 June 2024)

Audit and Risk Assurance Committee (ARAC) meeting

Agenda

Time and date: 10.00 - 12.00 hours, 12th June 2024
Venue: Wandle 40/41

Time	Item	Subject and paper number	Lead
1. OPENING ADMINISTRATION			
10:00	1.1	Welcome and Apologies	**Chair**
	1.2	Declaration of Interests (AUD14-24)	**Chair**
	1.3	Minutes of the previous meeting (AUD15/24)	**Chair**
	1.4	Matters arising from the previous meeting (AUD16/24)	**Chair**
2. AUDIT /REPORTING			
10:10	2.1	Internal Audit Annex A – Annual Audit Opinion (AUD 17a-24) Annex B – Audit and Risk Assurance Committee report supplement (AUD 17b-24)	**GIAA**
10:35	2.2	Audit Tracker (AUD 18-24) Audit Tracker Update	**Head of Finance and Governance**
10:45	2.3	External Audit Annex A – Annual Audit Opinion (AUD19a-24) Annex B – External Auditors Annual Statement (AUD19b-24)	**NAO/KPMG**
3. UPDATES			
11.05	3.1	Cyber Security Quarterly Update (PowerPoint - slides included) (AUD 20-24A)	**Director of Data, Technology and Development**
11.15	3.2	Information Security (AUD20-24)	**Senior Risk Information Officer (Director of Resources)**

11.25	3.3	Data Security and Protection Toolkit (DSPT) (Powerpoint – slides included) (AUD 20-24B)	**Director of Data, Technology and Development**
4. RISK UPDATE			
11.35	4.1	Risk Update (AUD21-24) Annex A – Strategic Risk Register Summary(AUD21a-24)	**Director of Resources**
5. REGULAR REPORTING: Policies and Procedures			
11.45	5.1 5.2	Gifts and Hospitality Register Annex A – Gifts and Hospitality Register (AUD22-24) Reports on grievances, disputes, fraud, and other information.	**Head of Finance and Governance**
6. CLOSING ADMINISTRATION			
11.50	6.1	Any Other Business	**Chair**
	6.2	Committee Effectiveness (AUD 23-24) Annex A (AUD 23a-24) Annex B (AUD 23b-24) Annex C (AUD 23c-24)	**Chair**
	6.3	Date of next meeting: 17th October 2024	
12:00	**Finish**		
12:00	**Sandwich lunch**		

Link to ARAC (12th June) folder:

Quality Management - 12th June 2024 - All Documents (sharepoint.com)

Minutes of the Audit and Risk Assurance (ARAC) meeting

Date: 7TH February 2024

Time: 10.00 – 12.00

Venue: Virtual

Protective Marking: OFFICIAL

Attendees:

ARAC Members
Professor Gary Crowe (GC), Chair
Helen Dodds (HD)

Observers
Jacky Cooper (JC), Senior Policy Manager, Department of Health and Social Care
Nicholas Doran (ND), National Audit Office
James McGraw (JMcG) National Audit Office
Dean Gibbs (DG), KPMG
Eric Sibisi (ES), KPMG
Joanne Charlton (JC) Government Internal Audit Agency
Rebecca Jones (RJ) Government Internal Audit Agency

In Attendance
Dr Colin Sullivan (CS), CEO
Louise Dineley (LD), Director of Data Technology and Development
Tom Skrinar (TS), Director of Resources
Nicolette Harrison (ANH), Director of Regulation
John McDermott (JMcD), Deputy Director for Performance & Corporate Governance
Morounke Akingbola (MA), Head of Finance and Governance
Aidan McIvor (AMCI), interim Board Secretary (*minute taker*)

HTA observers
James Beyer, Policy Manager
Mark Wrigley, Head of Regulation
Lisa Yeates, Regulation Manager

Item 1 – Welcome and apologies

1. The Chair welcomed Members, the Executive team and colleagues from the Department of Health and Social Care (DHSC), Government Internal Audit

Agency (GIAA), the National Audit Office (NAO), KPMG and HTA staff observers.

2. Apologies were received from Dave Lewis, Member of the Board, whom it was noted had submitted comments to the Committee Chair by email in advance of the meeting.

Item 2 – Declarations of interest

3. The Chair asked Members if there were any declarations of interest to be made; none was declared.

Item 3 – Minutes of 19 October 2023 meeting

4. The Chair and Committee accepted the revised draft minutes as an accurate record of the meeting of 19 October 2023. It was noted, however, that the draft minutes had required significant revision.
5. The minutes were adopted by the Chair and the Committee.

Item 4 – Matters arising from 19 October 2023 meeting

6. The Chair and Committee noted that all actions had been completed, including three from the last meeting (19 October 2023).
7. The Chair noted a suggestion from the Secretariat {Aidan McIvor, (AMCI)}, to revise the format of the Actions Log, to make it more user-friendly. The Chair asked AMCI to provide a revised Action Log ahead of the next ARAC meeting (12 June 2024).

8. **Action:** Secretariat (AMCI) to revise the format of the Actions Log.

Item 5 – Internal Audit 2023/24

9. Jo Charlton (JC) introduced the reports and provided several highlights to the Committee. The Committee noted that 40% of the plan has been delivered and GIAA expects to be able to deliver the remainder of the draft report by 31 March. The Committee noted the Fraud Control Audit has been finalised.
10. The Committee noted there has been a reduction in outstanding recommendations, but it had seen an increase in the number that were

overdue. JC explained GIAA and HTA staff are working closely to track recommendations.

11. JC went on to explain the draft Internal Plan for 2024/25 is a baseline audit plan, which will be subject to a mid-year review of the plan in late summer to ensure audit activity is focussed on the right areas.
12. Five audits will be carried out this year, which, it was noted, will not include FOI and Subject Access Requests; Colin Sullivan (CS) explained these were not a high priority. As regards the licensing audit, Nicky Harrison (NH) outlined what a review would entail, including revocation (termination) of licenses.
13. The Chair went on to welcome the scope of the audit and recognised its scale.
14. As regards Corporate Governance, John McDermott (JMCD) reported that, a Board Effectiveness Review will be carried out, which will address any risks in in the interim.
15. JC advised GIAA apply a standard baseline to every audit and try to make the scope fit. JC went on to advise that GIAA is fully-fee funded, as it no longer receives Grand in Aid. Consequently, GIAA must ensure that the fees charged to its customers cover GIAA audit services.
16. Jo Charlton sought clarification from CS and NH as to the timing and size of the Licensing review. Nicky advised that GIAA would receive a steer on the size and scope of the licensing review by the end of February.

17. The Committee noted the report and agreed the proposed outline Internal Audit Plan for 2024/25, subject to the finalisation that was explained under this item.

Item 6 – Audit Tracker

18. The Committee reviewed the Audit Tracker, which was presented by Morounke Akingbola (MA). The Committee welcomed progress to date, e.g., reducing the number of outstanding audit recommendations (from 24 to 9), when Dr Sullivan, CEO, took up post; the Committee also noted some of the recommendations had been in place for some time, although it was recognised staff resourcing was an issue. The Committee considered how the risk of losing staff with specific skills and experience (‘single point of failure’) is managed.
19. The Committee discussed the processes which had been put in place to ensure greater clarity around ownership of actions and clear timelines for completion.
20. The Committee noted the summaries at Annex A and B and agreed the proposals to close two recommendations.
21. The Chair asked for a ‘checkpoint’ a meeting in late April or early May with Jo Charlton of GIAA, and relevant HTA officials, e.g. Tom Skrinar (TS).

22. **ACTION**: The Secretariat to arrange a 'checkpoint' call in late April between the Chair of ARAC, JC and TS.

Item 7 – External Audit

23. Nicholas Doran of the NAO introduced Dean Gibbs (DG) who presented a summary of the Auditing Planning Report on the 2023/24 financial statements audit. DG highlighted where some revisions have been made to risk assessments, compared to last year, including the implementation of IFRS16, which is no longer an area of focus, as that standard has been successfully implemented.
24. DG outlined the audit plan for 2023/24 and summarised the audit risks which have been identified. They were: 'presumed risk of management override of controls', along with 'accuracy of accruals'. DG advised that the accruals point, which are a legacy of the HTA's relocation from Victoria and related the exit from the lease, is deemed to be an elevated risk.
25. DG reported good progress had been made with the Interim Audit, thanks to the excellent support provided by the HTA management team. DG reported that KPMG's engagement with CQC about the HTA's HR shared services arrangement had been deferred until the final accounts visit.
26. The Committee sought assurance that any lack of engagement from CQC can be overcome so as not to delay the audit work. Tom Skrinar (TS) said he would raise the issue at his meeting with CQC on 9th February.
27. The Committee noted the report.

28. **Action:** Tom Skrinar to raise the engagement issue with CQC on 9th February.

Item 8 – Data Security and Protection Toolkit

29. Louise Dineley (LD) presented an oral update. The Committee noted work on the interim submission will be ready by end of February. The interim submission will be used as the HTA's baseline towards the final submission at the end of June. The GIAA's steer was that as an organisation it is important for the HTA to decide where it wishes to be in terms of levels of compliance and risk appetite. LD reported this is in the forefront of the HTA's mind as to what is the most proportionate, but also realistic for the organisation to achieve.

30. The Committee discussed the progress made to date, including the 'check and challenge' sessions, and the imminent appoint of a new Records Management and Information Governance Officer.
31. The Committee noted the report.

Item 9 – Cyber Security Update

32. Louise Dineley (LD) introduced the report, which it was noted supports HTA's Cyber Security Policy and provides information on the main themes of identify, protect, detect, respond, and recover.
33. The Committee reviewed the Cyber Security dashboard for Quarter 3, 2023/24. The Committee noted progress on the HTA's Microsoft secure score, the volume of Viruses intercepted, Device vulnerability, SPAM activity, staff mandatory training, RTANCA alerts received from NHS X, and the HTA's exposure score. The Committee noted that since the last ARAC meeting, a new Head of IT has been appointed, who joined the HTA in November 2023.
34. LD provided the Committee with several highlights including the fact that 100% of viruses were intercepted and 100% staff had completed the required training.
35. The Committee discussed how this report could be developed to provide additional assurance against related items such as data management, GDPR and reportable incidents.
36. The Committee noted that IT staffing levels were now at establishment for the first time September 2022; this followed a period of staff vacancies and absence due to sickness. The Committee also noted CRM (one of the core systems) updates are being undertaken, the first phase of which will take place in Quarter 4.
37. The Committee noted the Cyber Security report.

Item 10 – Risk Update

38. Tom Skrinar (TS) introduced the paper on the HTA's strategic risks and proposed mitigations. The paper included a revised format of the HTA Strategic Risk Register, which the Committee was asked to agree.
39. The Committee sought updates on the following areas.

    a. *Risk 4* – transitioning to the new outsourced HR. TS updated the Committee on the transition to date, and the discussion which he will

have with CQC on 9th February to consider what the Service Level Agreement will look like.

b. *On Risk 5*, TS updated the Committee on the HTA's budgetary overspend.

c. *Business Continuity* - In answer to Helen Dodds' (HD) questions about Business Continuity and mandatory training, the Committee noted video-enabled training is carried out on a quarterly basis, with nearly 100% attendance rate. Moreover, a full-organisation Business Continuity test will take place on 25th April, which will coincide with an all-staff in-person meeting at 2 Redman Place. John McDermott reported plans are in place to bolster Business Continuity training in 2024/25 through this exercise.

d. *Risk 7 (Failure to optimise the safe use of digital, data & technology)* – In answer to questions from HD, Louise Dineley (LD) advised that the new head of IT is working through a baseline assessment of current systems and opportunities for improvement, including the development of an IT Strategy. LD added that the HTA has strong working relationship with BCC.

e. *Artificial Intelligence (A.I.)* - The Chair asked that A.I. feature in the Strategic Risk Register. LD advised that A.I. is included in the draft Business Plan as part of the HTA's Data Development for the year ahead. Moreover, the HTA is also progressing plans for a separate data collection exercise to understand with evidence the significance of the risk or issues that A.I. pose internally and across regulated activities of licensed establishments.

f. *Horizon-scanning* – The Chair asked that Horizon-scanning feature in the annual audit cycle. LD advised that horizon-scanning will feature in the HTA's work during the new financial year. It was noted that this was not possible previously because of staff shortages, e.g., the Policy team has been under 50% capacity in 2023/24.

g. *Cash flow* - David Lock (DLKC) asked if the non-payment of fees was an issue for the HTA. TS advised this is not an issue for the HTA; if,

however, a smaller organisation has difficulty paying its fees, a payment plan arrangement is in place.

h. *Business Plan* – In answer to a question from the Chair about the risk of delivering the Business Plan, JMCD assured the Committee any such risks are actively managed.

i. *New format* – The Committee welcomed the new format of the Strategic Risk Register, which it agreed. The Chair noted the existing Strategic Risks will need refreshing for the new financial year.

40. The Committee noted the report and agreed the new format of the Strategic Risk Register.

Item 11 – Sector Risk Assessment

41. Nicolette Harrison (ANH) introduced the report on the HTA's assessment of sector-specific risks, which the Committee commended for its comprehensiveness and excellence. During the discussion, the Executive provided updates on: (a) progress on a two-way flow of data sharing – with NHS England, (b) liaison with NHSE on mortuary capacity, and (c) unannounced inspections. The Committee advised that bringing data together and trending it would be helpful, which the Executive will consider for a future meeting.
42. The Committee noted the report.

Item 12 – Summary of Policies

43. Morounke Akingbola (MA) introduced the report.
44. The Committee noted the report.

Item 13 – Whistleblowing Policy and Procedure

45. Morounke Akingbola (MA) introduced the report. The Committee considered and approved the HTA's Whistleblowing Policy & Procedure. The Committee highlighted the need to: (a) reference the ARAC Chair as the Board Champion for Whistleblowing in the actual text of the policy, rather than in an annex, and

(b) how disclosure could be made by staff. The Committee asked that a revised policy be recirculated for approval by 'written procedure' outside the meeting.

46. **Action:** Revised Whistleblowing Policy to be recirculated for approval by 'written procedure' outside the meeting.

Item 13 – ARAC Handbook

47. Morounke Akingbola (MA) introduced the report. The Committee noted a reference to the late Queen at paragraph 29 on page 151 of the pack, which should have read 'The King'. Moreover, the Committee asked that the seasons-themed order of business, e.g., 'winter' or 'autumn', be addressed and revised outside the meeting. Apart from the typographical oversight, which the Executive said would be corrected, and the issue around the season-themed 'order of business', the Committee was content to note the ARAC Handbook.

48. **Action:** The seasons-themed order of business be revised outside the meeting.

Item 15 – ARAC Terms of Reference

49. Morounke Akingbola (MA) introduced the report.
50. The Committee was content to note the ARAC Terms of Reference.

Item 16 – Gifts and Hospitality Register

51. Morounke Akingbola (MA) introduced the register, which was noted by the Committee.

Item 17 – Reports on grievances, disputes fraud and other information

52. No reports of grievances were discussed.
53. There was nothing to report to the Committee under fraud or dispute.

Item 18 – Any other business (AOB)

54. Three items of AOB had been tabled in advance of the meeting: (i) Committee Effectiveness Review, (ii) Government Functional Standards, (iii) Accounting Policies and Judgements.

55. *Committee Effectiveness Review* – The Committee received an oral update from John McDermott (JMCD) on the planned Committee Effectiveness Review, which upon completion, will be analysed. The Chair asked that, if possible, the shorter version of the questionnaire be used. JMCD explained the National Audit Office template for ARAC Effectiveness Review for Board to Members and the Executive came in a standard format.
56. The Committee noted the oral update.

57. *Government Functional Standards* – JMCD presented the update, who advised that the paper that been included in the be pack had included an incomplete annex; the updated version was circulated during the meeting. JMCD reported the paper set out HTA's rationale around the level of compliance aimed for each Government Functional Standard ahead of the 2024/2025 internal audit. The Chair asked that any comments be shared with the Executive 'offline' after the ARAC meeting.

58. *Accounting Policies and Judgements* – The Committee noted that the accounting policies set out in the Annual Report and Accounts have not changed from 2022/23 to 2023/24. The Committee noted there are no critical accounting judgements, and if an important accounting policy changes, the Committee would be notified prior to the next ARAC meeting.

59. No other AOB was raised. The Chair concluded by inviting the Board member observers to remain on the video call after the meeting had ended so that the Chair could seek their reflections on the meeting.

Summary of actions

- **Item 4: Action:** Secretariat (AMCI) to revise the format of the Actions Log.
- **Item 6: Action:** The Secretariat to arrange a 'checkpoint' call in late April between the Chair of ARAC, JC and TS.
- **Item 7: Action:** Tom Skrinar to raise the issue with CQC on 9th February.
- **Item 13: Action:** Revised Whistleblowing Policy to be recirculated for approval by 'written procedure' outside the meeting.

- **Item 14: Action:** The seasons-themed order of business be revised outside the meeting.

Date of next meeting: 12th June 2024 – at 2 Redman Place, London

Audit and Risk Assurance Committee (ARAC)

Date: 12 June 2024

Paper reference: AUD 16/24

Agenda item: 1.4

Author: Aidan McIvor

Matters arising from previous ARAC meeting

Purpose of paper

1. To provide an update to ARAC on the actions arising from previous Meeting. A new format has been prepared, alongside the former Action Log, which has been 'greyed out'.

2. To note there were five actions from the last meeting, all of which have been completed.

Action required

3. ARAC is to note the new format of the Action Log.

Matters Arising / Action Log

R: action not completed by due date
A: action not yet due
G: action complete

ARAC date and agenda item:	Action	Owner	Deadline	Status	Update
07/02/2024 Item 4: Matters Arising	Secretariat to revise the format of the Actions Log	Aidan McIvor, Board Secretary	By next ARAC meeting (12/06/2024)		Action completed in April.
07/02/2024 Item 6: Audit Tracker	Secretariat to arrange a 'checkpoint' call in late April between the Chair of ARAC, Jo Charlton (GIAA), HTA officials.	Aidan McIvor, Board Secretary	By early May 2024.		Action completed; a 'checkpoint' was arranged for 22/04/2024.
07/02/2024 Item 7: External Audit	Tom Skrinar to raise the (engagement) issue with CQC on 09/02/2024.	Tom Skrinar, Director of Resources	By 09/02/2024		Action completed on 9/02/2024.
07/02/2024 Item Whistleblowing Policy	Revised Whistleblowing Policy to be recirculated for approval by 'written procedure' outside the meeting	Morounke Akingbola, Head of Finance and Governance	By next ARAC meeting 12/06/2024		Action completed in April.
07/02/2024	seasons-themed order of business be	Morounke Akingbola, Head of	By next ARAC		Action completed in April.

Item 13: ARAC Handbook	revised outside the meeting	Finance and Governance	meeting 12/06/2024		

Former Action Log

Number	Date Added	Action	Assigned to	Target date	Revised date	Status
ARAC-2022_07	Jan 22	**Change Programme** Executive to investigate Fraud Awareness training opportunities for the Autumn meeting.	Director of Resources and Head of Finance & Governance	Oct 22	Oct 23	**Completed.**
ARAC_2022_28	Jan 23	**Matters arising from 9 June 2022** Executive to amend the matters arising report to include key colour.	Board Support	Feb 23		**Completed**
ARAC_2023_02	Jan 23	**Internal Audit** The Committee agreed the proposed 23/24 Internal Audit Plan and noted the October 2022 GIAA supplementary report	Director of Resources and Head of Finance & Governance	Feb 23		**Completed**
ARAC_2023_03	Jan 23	**Cyber Security Update** Executive to consider the format of the cyber security report.	Director of Data, Technology & Data	May 23		**Completed - presented at 8 June meeting**
ARAC_2023_04	Jan 23	**HTA Summary of Audit Recommendations** The Committee noted the report and accepted the recommendations on page 2 and 3 of the audit tracker report.	Head of Resources	May 23		**Completed.**

Number	Date added	Action	Assigned to	Target date	Revised date	Status
ARAC_2023_05	Jan 23	**External Audit** Director of Resources to provide a timeline note for the Committee regarding the preparation and review of the audited accounts.	Director of Resources	Feb 23	June 23	**Completed**
ARAC_2023_06	Jan 23	**Sector Risk Assessment** Lead of the Private Office to ensure that Sector Risk Assessment is on the Committee's work plan for January 2024.	Lead of the Private Office	May 23		**Completed**
ARAC_2023_07	Jan 23	**Consideration of risk appetite and tolerance within the HTA** The Executive to redraft wording for risks 2, 3 and 7 and circulate to Members for review and approval.	SMT	Feb 23		**Completed**
ARAC_2023_08	Jan 23	**Consideration of risk appetite and tolerance within the HTA** The Executive to include a key to the levels of tolerance within the revised document.	Director of Resources	May 23		**Completed.**
ARAC_2023_09	Jan 23	**Whistleblowing Policy and Procedure** The Committee agreed the amended Whistleblowing Policy	Head of Finance & Governance	April 23		**Completed.**

Number	Date Added	Action	Assigned to	Target date	Revised date	Status
ARAC_2023_10	Jan 23	**ARAC Workplan** Lead of the Private Office and ARAC Chair to develop a more detailed workplan for the Committee	Lead of the Private Office	May 23		**Completed.**
ARAC_2023_11	Jan 23	**ARAC Terms of Reference** The Executive to amend section 18 and 31 as per the Committee's discussion and present to the Board for approval.	Director of Resources and Head of Finance & Governance	March 23		**Completed.** Amendment made 06-02-23 and presented to Board March 2023.
ARAC_2023_12	Jan 23	**Gifts and Hospitality Register** Reminder to be sent to staff that all offers of gifts and hospitality must be reported in a timely manner	Director of Resources and Head of HR	May 23		**Completed.** Item included in February staff newsletter.
ARAC	19th October 2023	**Cyber Security** Joanne Charlton (GIAA) to discuss Cyber Security Essentials with Morounke Akingbola	Director of Resources	December 2023		**Completed.**
ARAC	19th October 2023	**Artificial Intelligence (A.I**.) Helen Dodds asked for more information/thoughts about the risk Artificial Intelligence (AI) poses to be covered at the next Board meeting on 7 December 2023.	Director of Data, Technology and Development	December 2023		**Completed** A.I. was mentioned during the HTA Performance Report at the Board meeting on 7th December 2023**.** A Roadmap to be developed and will come to a future Board event, e.g., a workshop.

ARAC	19th October 2023	**Risk update –** At the request of ARAC, the Remuneration Committee to consider the Risk Update paper at its next meeting.	Director of Resources	January 2024		**Completed.** The Risk Update paper, including how to mitigate the risk around recruitment and retention of staff, was considered by the Remuneration Committee at its meeting on 26th January 2024.

Paper Number AUD 17-24

CONFIDENTIAL

ARAC 12th June 2024

Internal Audit

Paper Number AUD 18-24

CONFIDENTIAL

ARAC 12th June 2024

Audit Tracker

Paper Number AUD 19-24

CONFIDENTIAL

ARAC 12th June 2024

External Audit

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	**RESPOND** ***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 Office), the Information Commissioner's Office (ICO) or law enforcement as applicable (not exhaustive). c) 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.

Paper Number AUD 21-24

CONFIDENTIAL

ARAC 12th June 2024

Strategic Risk Register

Paper Number AUD 23-24

CONFIDENTIAL

ARAC 12th June 2024

Committee Effectiveness