Audit and Risk Committee (ARAC) meeting
AGENDA

Time and date: 10.00 - 12.00, 14 October 2025
Venue: Virtual Meeting (Microsoft Teams)

Time	Item	Subject and paper number	Lead
09:45	-	*Pre-meeting for Chair and Members only*	*Chair*
1. OPENING ADMINISTRATION			
10:00	1.1	Welcome and Apologies	Chair
	1.2	Declaration of Interests	Chair
	1.3	Minutes of the previous meeting (AUD 28-25)	Chair
	1.4	Matters arising from the previous meeting (AUD 29-25)	Chair
2. AUDIT /REPORTING			
10:05	2.1	Internal Audit – HTA Audit and Risk Committee Progress Report October 2025 (AUD 30-25)	GIAA
10:15	2.2	Internal Audit – Supplementary Pack (AUD 31-25) – Moving to the smaller ALB Audit and associated Fees for 2026/2027 (Oral item)	GIAA
10:30	2.3	Audit Tracker Update (AUD 32-25)	Head of Finance and Governance
10:40	2.4	External Audit Update (Oral Item)	NAO/KPMG
3. UPDATES			
10.50	3.1	Cyber Security Quarterly Update (AUD 33-25 – PowerPoint slides)	Director of Data Technology and Development
11:00	3.2	HTA Health and Safety Update (Oral item)	Director of Finance and Resources
11:10	3.3	Government Functional Standards Update (AUD 34-25)	Deputy Director for Performance and Corporate Governance

Time	Item	Subject and paper number	Lead
4. RISK			
11.20	4.1	Risk Update (including deep dive into “Strategy” Risk (AUD 35-25 - Strategic Risk Register at Annex A)	Director of Finance and Resources (+ Director of Data Technology and Development)
5. REGULAR REPORTING: Policies and Procedures			
11.50	5.1	Interests, Gifts and Hospitality (AUD 36-25)	Head of Finance and Governance.
	5.2	Reports on grievances, disputes, fraud, counter fraud, bribery, corruption and other information (Oral update if required)	Director of Finance and Resources
6. CLOSING ADMINISTRATION AND INFORMATION ITEMS			
11:55	6.1	SIRO Report (AUD 37-25)	Director of Finance and Resources
	6.3	Any Other Business	*As required*
12:00	*Finish (date of next meeting: 10 February 2026*		

DRAFT Minutes of the Audit and Risk Assurance Committee (ARAC) meeting

Date: 10 June 2025

Time: 10.00 – 12.00

Venue: Wandle Rooms, Second Floor, 2RP

Protective Marking: DRAFT

ARAC Members
Gary Crowe, ARAC Chair
Dave Lewis
Jessica Watts

Internal and External Auditors
*Andrew Anjeli, GIAA
*Jo Charlton GIAA
*Dean Gibbs, KPMG *items 2 to 7*
*Nicholas Doran, NAO

Observers
Alina Iljina, HTA Finance Team
Richard Mabbitt, HTA Private Office
Maria Maharaj, HTA Interim Head of Finance and Governance
Steve Stanbury, HTA Board Member
*Helena Youmans, DHSC

HTA Staff
Colin Sullivan, CEO
Nicolette Harrison, Director of Regulation
Katrina Leighton-Hearn, Director of Finance & Resources
John McDermott, Deputy Director for Performance and Corporate Governance
Morounke Akingbola, Head of Finance & Governance
Matt Atkinson, Head of IT
Debra Morgan, EA Private Office (minutes)

Apologies
David Stanton, HTA Board member
Louise Dineley, Director of Data Technology and Development

*Attending remotely

1. Opening Administration

Item 1.1 – Welcome and apologies for absence

1. Gary Crowe welcomed Members, HTA staff, and attendees from the Government Internal Audit Agency, the National Audit Office and KPMG, and the Department of Health and Social Care. Steve Stanbury was observing the meeting as part of his induction as a new HTA Board member, and Board

Chair Lynne Berry, was also observing.

2. Apologies had been received from Louise Dineley: Matt Atkinson was deputising. Board member David Stanton (who would take on the ARAC Chair role in September after Gary Crowe's departure) was also unable to attend.

Item 1.2 – Declarations of interest

3. Gary Crowe noted that the annual check of Board members' interests had been completed in March (as referenced in paper AUD 23-25). The additional interests submitted to DHSC by the four Board members appointed in April were currently being updated, after which the register would be republished.

4. No further new interests were declared by members. None of the interests already declared were identified as posing a conflict for this meeting.

Item 1.3 – Minutes

5. ARAC **AGREED** the minutes of the meeting of 11 February 2024 (AUD 14-25), subject to amendment of Para. 14: Jo Charlton confirmed that it was in fact the DSPT audit rather than the Payroll audit that had been completed.

Item 1.4 – Matters Arising

6. ARAC reviewed the Actions Log (AUD 15-25) and was pleased with progress. The one outstanding action at item 2.1 (on circulating IA Charter model global standards) had been completed in the circulation of papers for the meeting.

2. Audit / Reporting

Items 2.1 – Internal Audit

7. Jo Charlton introduced the suite of internal audit papers provided as AUD 16-25. TGIAA had concluded that an overall 'Moderate' audit opinion for HTA in 2024/25 was appropriate. There were four final reports which GIAA had issued since the last ARAC in February 2025:

    a) Licensing – Moderate
    b) Payroll & Expenses – Moderate
    c) HR Shared Services (Contract Management) – Limited
    d) Government Functional Standards - Moderate

    In response to questions around the 'limited' assurance for HR Shared Services, Katrina Leighton-Hearn reported that that most of the

recommendations around HR were now complete and the SLA with CQC had been reviewed with a view to reducing costs and enhancing service provision. These new arrangements were expected to come online shortly and evidence of work undertaken to meet the recommendations would be shared with GIAA.

8. Jo Charlton summarised the GIAA Draft Annual Opinion 2024-25 and introduced the HTA performance report and annual opinion for 2024-25. She advised ARAC that the new format with the direction of travel was useful context for the reports. She highlighted aged risks around single points of failure related to staffing levels.

9. ARAC members noted that although the HTA was overall at the lower end of the Moderate Assurance rating, this was appropriate for the size of the organisation. Andrew Angeli and Katrina Leighton-Hearn reported an improved frequency of tracking meetings, clearer messaging to key stakeholders and a strong excellent working relationship between the HTA Finance team and GIAA. ARAC endorsed the draft Head of Internal Audit Annual Opinion for 2024-25

10. ARAC noted the Internal Audit Charter 2025-26. The Charter had changed from previous years as a result of the introduction of the Global Internal Audit Standards which came into force on the 1 April 2025. It was important that ARAC and the organisation were familiar with the requirements of the new standards to ensure the essential conditions were met for Internal Audit. **Action: Gary Crowe (as ARAC Chair) and Colin Sullivan (as AO)** to formally approve and sign off the Charter after the meeting.

11. ARAC thanked Jo Charlton for her report and her past support for the Committee, noting that Andrew Anjeli was now the GIAA lead for the HTA.

Item 2.2 – Audit Tracker update

12. Morounke Akingbola summarised progress recorded on the Audit tracker (AUD 17-25).

13. ARAC noted risks associated with payables and receivables linked to delays in the upgrade of the finance system, and that it was proposed this risk be accepted for a further term. ARAC noted

    a) that the upgrade was reliant on other ongoing IT projects and capacity within the Finance function. The replacement of the finance system was on the business plan for 25/26 and the Board would have sight of progress through standing performance reports.

b) External Auditors' feedback that although previous audits had identified controls issues around separation of duties (owing to the workload and size of the Finance Directorate) overall, the system worked well for the organisation's size and scale of operations. Changes in staffing would have an effect on the manual systems currently employed alongside the existing computerised finance system. Katrina Leighton-Hearn noted that an Interim Head of Finance was already in post alongside the outgoing Head, and a recruitment process for a permanent appointee was under way. The hours for the new role had been increased to meet workload demands and create more efficiency in the directorate.
c) Matthew Atkinson also explained that a new finance system would address security concerns: HTA was carrying some vulnerability here which needed to be addressed to meet CAF and cyber security requirements.

ARAC therefore **AGREED** to risk accept the payables and receivables recommendation and the proposed changes to the timelines linked to the Finance System Upgrade

14. ARAC noted outstanding actions associated with Health and Safety. Katrina Leighton-Hearn reported that HTA was in discussion with CQC who had a dedicated team of professional Health and Safety Advisors around options for developing an SLA for CQC to deliver a health and safety service as a longer-term solution. offering greater assurance.

15. ARAC noted outstanding audit action on the audit tracker actions. **Action: Andrew Anjeli** to follow up points of detail after the meeting with Katrina Leighton-Hearn and Louise Dineley.

16. Colin Sullivan thanked ARAC for its feedback and noted that a learning point for the executive was to be more assertive in negotiating recommendations and being better at factoring in optimism bias in agreeing delivery timescales.

Item 2.3 – Annual report and Accounts

17. Katrina Leighton-Hearn and Morounke Akingbola introduced the Annual Report and Accounts (AUD 18-25) which reported on the year end position, additional disclosures and material movements from the previous year.

18. ARAC noted areas of expenditure and income that were materially different to those reported in the 2023-24 Accounts as follows:

a) Revenue from contracts with customers (increased by 18% due to licence fee increases largely to cover the reductions in HTA's grant-in-aid.

b) Other Operating income (a decrease in recharges for seconded staff: 1 secondment compared to 2)
c) Accommodation (a £500k reduction) which related to an reversal of an accrual for rent
d) Movement in the impairment for expected credit losses (£92k reduction) related to a reduction in aged debt that had historically been problematic to collect. The remaining provision was to cover the potential write-off of these debts.)
e) Debtors (reduced by 44% from 23/24 partly due to the write off of bad debts, but also the targeted credit control by the HTAs Finance Manager. HTA had written-off debts for the first time in over seven years, for seven organisations who have gone into liquidation or receivership.

19. ARAC also noted and were content with the two items in the report. One related to the pay ratio disclosure – the inclusion of the interim Finance Director salary which distorts the ratios,(on which advice was being sought by NAO). The other related to a legal issue on which HTA had received a notice of intent, but where the content and legal interpretation was novel, and HTA was not in a position to assess its likelihood of proceeding or potential financial impact

20. ARAC also considered the External Auditor's annual statement (at Annex B), and ISA 260 report (management letter) (at Annex C) and **AGREED** to the Accounting Officer finalising and signing the HTA Annual Report and Accounts 2024/25, subject to any material amendments arising. HTA would delay the Accounting Officer sign off until a final timeline from the NAO had been received to ensure that the accounts would be reviewed in light of any material developments. Any material changes required after the meeting would be discussed with the ARAC Chair, and the committee would be informed prior to sign off.

21. ARAC noted the smooth progression of the Annual Report and Accounts and thanked the finance team and other contributing officers for their efforts and the NAO and KPMG for their support.

22. The Chair requested that a SIRO report be compiled and circulated outside of the meeting as a priority. **ACTION: Katrina Leighton-Hearn.**

Item 2.4 – External Audit

23. Dean Gibbs introduced the audit completion report on the 2024/2025 financial statements (AUD 19-25), which provided an overview of the HTA Annual Report and Accounts for 2024/25 and the anticipated recommendation of an unqualified audit opinion. He noted:

a) (under “Management override and controls”) where manual adjustments were enabled there were instances where the same person had posted and approved journals entries due to tight timelines and a small team. It was important and universally agreed that, going forward, segregation of duty was maintained.
b) his confirmation that the legal claim highlighted as a contingency could not be reliably valued. As there had only been a notice of intentions it was not valid to allocate a value in the accounts;
c) In the summary of adjusted misstatements were entries relating to lease modification due to a rent increase causing an increase in the lease liability at 2 Redman Place. A further lease remeasurement exercise should be undertaken again in 2025/26 as there had been a modification I lease due to a reduction in space occupied;
d) That it was not currently appropriate to write off the original value of CRM,

ACTION: Katrina Leighton Hearn: to include an update on contingent liability at next ARAC meeting.

24. The Committee noted the good co-operation between HTA and NAO in completing the report and thanked NAO and KPMG for their support.

3. Updates

Item 3.1 – Cyber Security dashboard Q4

25. Matt Atkinson (MJA) presented paper AUD 20-25 which summarised another strong quarter across all IT services and the Cyber Security Landscape. No serious outages had been reported and no serious data breaches or incidents had occurred. The Cyber Improvement Programme funding approved by DHSC in December 2024, had provided financial support for the upgrades of two core systems, completed in March 2025.

26 The Committee welcomed this strong performance. It noted that the HTA’s current IT supplier, BCC, had agreed to continue to support the HTA out of contract until a decision had been made on the provider moving forward, giving assurance that the same level of support would be maintained. An update on legacy systems would be provided at the next ARAC meeting **ACTION: Louise Dineley/ Matt Atkinson.**

Item 3.2 – Cyber Assessment Framework update

27. Matt Atkinson introduced paper AUD 21-25. He reported that HTA was in a

strong position. As an ALB, and part of the first tranche of organisations to complete the National Cyber Security Centre's Cyber Assessment Framework, HTA had made an interim submission in December 2024. HTA had completed 12 GIAA recommendations, helping meet or exceed requirements. While HTA was generally in a strong position for submitting its final assessment (including supporting evidence) by the end of June, there was room for improvement in the Records Management and Information Governance area.

28. ARAC noted the report and was pleased at the positive trajectory. It asked for an update on the position of Records Management and Information Governance at its next meeting. **Action Louise Dineley/ Matt Atkinson.**

4. Risk update

Item 4.1 Risk Update and Strategic Risk register

29. Katrina Leighton-Hearn spoke to paper AUD 21-25 and summarized the updated Strategic Risk register; proposed risk appetite statement and the risk management policy. The Strategic Risk Register had been reviewed and refined at BDT and SMT joint workshops. The Risks had been re-brigaded to align with HMT 'Orange Book' risk categories, and present key risks more clearly. Six strategic risks were now included r: Risk 1 - Operational (broadly equating to the previous 'Regulation' risk); Risk 2 - Reputational (previously 'Sector'); Risk 3 - Financial (was previously Risk 5), Risk 4 - Strategy (a new risk); Risk 5 - People (previously Risk 3); and Risk 6 – Security (a new risk).

30. Members supported the reshaping of the SRR and felt the updated presentation was helpful. ARAC felt it would be useful for future Strategic Risk Register Reports to include an indication of when desired tolerance was expected to be met, and some description or narrative around consequences of continued risk where the register showed shortfalls. **ACTION: Katrina Leighton Hearn** to provide additional information in the SRR's next iteration.

31 Morounke Akingbola briefed further on the annexed Risk Management Policy which incorporated tracked changes adopted from the wider HM Treasury Orange Book, for review and approval by ARAC.

32 ARAC **AGREED** the amendments to the Policy and, subject to the feedback above supported the reformulated risk register to be presented to the 26 June Board meeting. Gary Crowe noted that the October ARAC meeting would typically see a deep dive into a specific risk area and that with a change of Committee Members it would be opportune to review the 'Strategy' risk. **Action: Private Office** in discussion with David Stanton provisionally to

schedule a review at the October meeting.

33 Dave Lewis reported that he had recently attended GIAA Risk Training and commended it to fellow Committee members.

5. Regular reporting: policies and procedures

Item 5.1 – Interests and Gifts and Hospitality.

34. ARAC noted the summary of gifts and hospitality received by staff (paper AUD 23-25) with no further comments,

Item 5.2 ARAC Effectiveness Review

35. Gary Crowe summarised the key points of the ARAC Effectiveness Review. He felt that the Committee was fulfilling is role well, and proportionately given the small size of the organisation. A clean audit and unqualified accounts were helpful contextual success indicators. He was particularly mindful of the need to ensure that ARAC was efficiently joined up with RemCo and the Board and adding real value to the work of the executive. He looked forward to discussing the Committee's forward work programme and membership with David Stanton.

36. ARAC members, with Steve Stanbury and Lynne Berry would reflect further on the Committee's role, effectiveness, and membership in an informal post meeting discussion.

Item 5.3 ARAC Terms of Reference

37. Gary Crowe drew members' attention to the proposed updated to the ARAC Terms of Reference (paper AUD 25-25). ARAC welcome the approach being set out to the wider refresh of these and HTA's other governance documents and was content that the changes be submitted to the next Board meeting for formal approval.

Item 5.4 Reports on grievances disputes, Fraud and other information

38. Morounke Akingbola reported that no issues relating to grievances, disputes fraud or other concerns required bringing to the Committee's attention.

Item 5.5 Government functional Standards

39. John McDermott introduced paper AUD 26-25 and highlighted:

a) The new Standard Operating Procedure (SOP) for the annual cycle of compliance activity;
b) That HTA will action the agreed recommendations following the recent internal audit, tracking updates through a monthly action plan;
c) That HTA will maintain a proportionate approach to compliance with the standards and documentation of such, as previously agreed and actioned;
d) That HTA intends to report an interim position to ARAC in October and report the final outcomes to ARAC in February.

40. ARAC acknowledged the update, recommitted to the proportionate approach to this work, and noted that the update had duly picked up Internal Audit recommendations for evidence of implementation, illustrating where the organisation needed to focus additional resource to meet the expectations of the department.

Item 5.6 Anti- Fraud Policy and Fraud Strategy

41. Morounke Akingbola introduced paper AUD 27-25. This was a routine two-yearly update. ARAC noted the importance of strong controls in this area and supported the approach set out in the Policy and Strategy Documents. ARAC therefore **APPROVED** the updates to the Anti-Fraud Policy and the Fraud Strategy

6. Closing Administration

6.1 Any other business

42. Gary Crowe informed the Committee that he and the Private Office were working on the Annual Report for Board which would be circulated for comment prior to presentation at the June 2025 Board meeting.

43. Following comments from the Internal Auditors regarding the 2023-2024 reports ARAC agreed to record that the Internal Audit Charter was approved during the June 2024 meeting.,

44. Attendees thanked Morounke Akingbola for her long and diligent service at the HTA and wished her well in her new role. Her support had been greatly appreciated by the Committee and she would be missed by colleagues.

45. Lynne Berry thanked ARAC for the opportunity to observe the meeting. She felt that it had been a good meeting with constructive participation from all parties. She thanked Gary Crowe, in his final meeting as ARAC chair, and felt that the Committee and HTA staff were well placed to support the new ARAC

chair in what was likely to be a period of considerable change and uncertainty in the wider heath service delivery landscape.

46. ARAC was next scheduled to meet on 14 October 2025.

AUD 29-25

Audit and Risk Committee (ARAC) meeting, 14 October 2025

Agenda item	**1.4 – Matters arising from previous meetings**
For information or decision?	Information
Decision making to date?	Standing item to each Audit and Risk Committee
Recommendation	Audit and Risk Committee is asked to note and comment by exception on the matters arising from previous meetings
Which strategic risks are relevant?	Risk 1: Operational Risk 2: Reputational Risk 3: Financial Risk 4: Strategy Risk 5: People Risk 6: Security
Strategic objective	Efficient and Effective
Core operations / Change activity	Core operations
Business Plan item	Senior Management Team – strategic direction and leadership of operational delivery across the organisation (including risk management and seeking opportunities for ALB collaboration)
Committee oversight?	Audit and Risk Committee
Finance and resource implications	N/A
Timescales	2025/26 (latest position)
Communication(s) (internal/ external stakeholders)	N/A
Identified legislative implications	N/A

Ref	Action	Owner	Deadline	Status	Update
ARAC meeting of 10 June 2025					
Item 2.1	**Internal Audit Charter 2025-26** Chair and AO to formally approve and sign off the Charter after the meeting.	CS, GC	14 October 2025	**G**	**Complete**
Item 2.2	**Audit Tracker** Follow up with GIAA on points of detail after the meeting	AA, KLH, LD	14 October 2025	**G**	**Complete**
Item 2.3	**Annual Report and Accounts** Circulate SIRO report to members	KLH	14 October 2025	**G**	**Complete:** circulated to members and included for reference with papers for meeting of 14 October
Item 2.4	**External Audit** include an update on contingent liability at next ARAC meeting.	KLH	14 October 2025	**A**	**In hand** KLH to update orally at the at the ARAC meeting of 14 October 2025
Item 3.1	**Cyber Security dashboard** Provide an update on legacy systems at the next ARAC meeting	LD, MA	14 October 2025	**A**	**In hand**: Included in Cyber security paper: LD to update further if required
Item 3.2	**CAF update** Provide an update on the position of Records Management and Information Governance at the next ARAC meeting	LD	14 October 2025	**A**	**In hand:** LD to provide an oral update at the ARAC meeting of 14 October 2025
Item 4.1	**Strategic Risk register** Provide additional information around when desired tolerance was expected to be met, and some description or narrative around consequences of continued risk where the register showed shortfalls.	KLH	14 October 2025	**A**	**In Hand** Further updates/discussion under Risk update item at ARAC meeting of 14 October
Item 4.1	**Strategic Risk register** Given changes to Committee membership, consider using the October 'deep dive' into a specific risk area for 'Strategy' Risk.	KLH, DS, PO	14 October 2025	**G**	**Complete:** Scheduled for discussion at ARAC meeting of 14 October 2025
ARAC meeting of 11 February 2025 G					
Item 2.1	**Internal Audit plan for 2025-26** Circulate templates reflecting Internal Audit Charter model global	GIAA representatives	10 June 2025	**G**	**Complete:** covered at ARAC meeting of June 2025 with plan to

	standards for positioning and responsibilities				be presented to members

R	R: action not completed or reported on by due date
A	A: action under way or not yet due
G	G: action complete

- Where no deadline specified in minutes, Action Holders to report on progress at next meeting
- Actions will be removed from the log only when completion has been reported to the Committee, or if the Committee agree that they have been superseded or may otherwise be closed. Copies of past actions logs are available to members on request to Private Office.
- **DS**: David Stanton, ARAC Chair; **KLH**: Katrina Leighton-Hearn Director, Finance and Resources; **CS**: Colin Sullivan, CEO and AO; **LD**: Louise Dineley; Director of Digital Technology and Development; **ZR**: Zuzana Reid, Head of Finance and Governance; **MA**: Matt Atkinson, Head of IT; **PO**: HTA Private Office

HTA
Human Tissue Authority

Audit and Risk Assurance Committee (ARAC)

Internal Audit

Progress Report

Confidential

HTA
Human Tissue Authority

Audit and Risk Assurance Committee (ARAC)

Internal Audit

Supplementary Pack

Confidential

Audit and Risk Assurance Committee (ARAC)

Audit Tracker

Confidential

Audit and Risk Committee (ARAC) meeting, 14 October 2025

Agenda item	**3.1 Cyber Security Update**
For information or decision?	Information
Decision making to date?	Standing item to each Audit and Risk Committee
Recommendation	Audit and Risk Committee is asked to note and comment by exception on the latest updates on cyber security
Which strategic risks are relevant?	Risk 6: Security
Strategic objective	Use of Information
Core operations / Change activity	Core operations
Business Plan item	Information Technology – stable technology operations focusing on user experience and engagement
Committee oversight?	Audit and Risk Committee
Finance and resource implications	N/A
Timescales	2025/26 (latest position)
Communication(s) (internal/external stakeholders)	N/A
Identified legislative implications	N/A

Digital & IT ARAC Report

Quarter 2 Summary

Date: 14th October 2025

Louise Dineley / Matthew Atkinson

HTA
Human Tissue Authority

📋 Executive Summary

The HTA continues to maintain a strong cyber security posture. This represents a point-in-time status. Sustained investment in our IT services is essential to maintain and strengthen this position.

Key Highlights:

- **Operational Resilience:** IT services have performed strongly over the quarter, with no major outages or critical cyber incidents reported.
- **Strategic Investment:** Funding requests have been submitted via the Cyber Improvement Programme to support further cyber capability enhancements.
- **Performance Benchmarking:** Microsoft's cyber security scoring remains stable, with HTA maintaining a positive position relative to other ALBs of similar size.
- **Regulatory Assessment:** The 2024/25 Cyber Assessment Framework submission received a 'Moderate' rating. Recommendations from the independent assessor focused on data and user management, which are being actively addressed.

Cyber Exposure

The recent Cyber risks with NHS (Synnovis), M&S, Co-Op and Jaguar Land Rover could have been prevented before they become a serious issue.

1. **Known System Failings** – Systems were known to have vulnerabilities prior to attacks
2. **Supply Chain Risk** – The NHS attack via Synnovis highlights third-party vulnerabilities
3. **Impact on Service Delivery** – NHS and Jaguar Land Rover experienced direct operational disruption
4. **Financial & Reputational Damage** – M&S and Co-Op suffered major financial losses and data breaches
5. **Data Protection Failures** – Millions of Customer/Member records were exposed
6. **Government Intervention** – Jaguar Land Rover required government Support.

We can use these to learn our own lessons, by ensuring our systems remain in support, assessing our third-party suppliers and maintaining excellent data management and record keeping. Security is a point in time; we need to ensure that we are keeping up with trends and understanding the evolving threats we face.

🔒 Cyber Prevention

Red and Blue Team Engagement (November 2025)

- A simulated cybersecurity exercise where attackers (Red Team) attempt to breach systems while defenders (Blue Team) work to detect and respond, helping to identify vulnerabilities and improve security resilience.
- Open-Source Intelligence, External Penetration Testing, Social Engineering & Object-Based Penetration Test

This test will identify any unforeseen areas of concern and provide clarity around user understanding. This test does not cover system recovery.

Further Improvements

As part of national standards and requirements, technical controls such as data backups and system resilience mechanisms are in place to support IT recovery. Annual business continuity exercises have tested these. A current gap in continuity arrangements is in local arrangements and protocols in the absence of systems , limited access and / or operational recovery. These arrangements are untested. These routines should be regularly reviewed and tested to maintain readiness and minimise disruption during recovery periods.

Cyber Performance & Metrics (July 2025 - September 2025)

The HTA maintains a proactive approach to cyber security by regularly applying system upgrades and security updates to ensure resilience against emerging threats.

User Website Activity

Category	#
Hits / Requests	42,122
Blocked	159

Inbound Email Activity

Category	#
Delivered Safely	82000
Spam	2100 (2.44%)
Blocked	1900 (2.21%)

All RTANCA alerts (5) were acknowledged and confirmed as Not Applicable.

Secure Score - **86.4%** up from 82.1% in previous Quarters our target is still 90% so working towards this.

Exposure Score - **32** which is good compared to ALBs of similar sizes.

Low 0-29 Med 30-69 High 70-100

Compliance Score - **77%** this is higher than previous quarters which was 73% our target is 70%.

📊 Operational Performance & Metrics (July 2025 - September 2025)

We track key cyber performance indicators including website traffic, email spam filtering, and change management activity to monitor system health, detect anomalies, and validate the effectiveness of our controls.

100% of Laptops had their Anti-virus software updated.

100% of laptops (67) were successfully upgraded to Windows 11 during the quarter and are now running the latest security patches.

0 devices were disposed in the quarter.

Administrative Accounts

Category	#
Global Administrators	4
Read-Only Administrators	1

User Accounts

Category	#
Active HTA Users	78
New Starters	9
Leavers	8

Requests for Change

Category	#
Access Changes	3
Software Changes	1
Mailboxes Changes	3
Search Approvals	3

🌐 Threat Landscape (July 2025 - September 2025)

HTA’s cyber threat landscape is shaped by increasingly sophisticated actors, including organised criminal groups and persistent external vectors. We treat cyber threats as organisational risks and adapt our controls and monitoring to reflect this evolving reality recognising this on the Strategic Risk Register (SRR).

No successful external exploits or breaches occurred during the period.

No System Outages due to exploits or vulnerabilities, the main system outage was technical not cyber related.

No reports or notifications of any access to systems from abroad.

⚖️ Risk Management

Reducing our system risks is underpinned by the ambition and delivery of our Digital & IT Strategy. Over the last 2 years the HTA have updated 3 Core IT Systems that were running with operational and security risks.

Two Core Business Systems operate at risk; mitigations remain in place.

The evolving Cyber Threat Landscape driven by sophisticated Cyber Attacks vectors, using advanced Artificial Intelligence modelling.

Ongoing investment to fully realise the ambitions of the Digital & IT Strategy.

Human elements including error, oversight, and inconsistent practices continue to pose a significant risk to the reliability, security, and performance of IT services.

🧠 Culture & Behaviour

HTA recognises that cyber resilience is shaped as much by behaviour and culture as it is by technology. Our approach focuses on embedding awareness, encouraging responsible digital habits, and ensuring leadership models the right behaviours.

No confirmed insider threats or behavioural breaches were recorded.

1 Mass Download Alert which was a false positive.

Specific IT training this quarter with 92% completed.

Courses:

- GDPR in 10 minutes
- Responsibilities under the GDPR
- Using Email and Internet
- Internet, Email & Social Media

🎯 Backup & Recovery

All systems across the HTA are backed up and managed through enterprise technology. The HTA has a dedicated Disaster Recovery site that is independent to the HTA offering segregation between Live and Backup Systems.

Backup recovery tests were 100% successful, confirming data availability.

12 backup restores were completed (4 each month) to assure our recovery.

Backup systems reported 100% completeness.

Over reliance on the successful recovery of IT system is overshadowing the need for practical operational level recovery.

Dedicated Critical Response planning around physical disaster recovery is needed.

🛠️ Infrastructure, Systems & Cyber Improvements

HTA must continue to invest in its infrastructure and systems to reduce technical debt, improve resilience, and align with best practice. These improvements will support our cyber posture and reduce exposure to legacy risks.

All 67 end-user laptops have now been successfully upgraded to Windows 11.

Further legacy system reduction was achieved through the upgrade to the HTA Portal, leaving two core system currently out of support.

App-Based MFA was successfully deployed to 78 users, alongside the distribution of 35 mobile phones to enable secure remote connectivity.

Supply Chain Assurance

HTA recognises that cyber risk extends beyond our internal systems. Our supply chain assurance focuses on ensuring that third-party providers meet our security expectations and that data shared externally is protected through contractual and technical controls.

No Cyber Incidents were reported by our suppliers.

Renewal of the IT Support Contract is being progressed with approvals on procurement routes sought from DHSC.

As part of the Cyber Assessment Framework, our core suppliers provide evidence of their own Framework Compliance with standards such as Cyber Essentials Plus.

Audit and Risk Committee (ARAC) meeting, 14 October 2025

Agenda item	**3.3 Government Functional Standards Update**
Purpose: for information or decision?	Information
Decision making to date?	Standing item to each Audit and Risk Committee
Recommendation	Audit and Risk Committee is asked to note and comment by exception on the latest updates on GFS
Which strategic risks are relevant?	Risk 3: Financial Risk 4: Strategy Risk 5: People Risk 6: Security
Strategic objective	Efficient and Effective
Core operations / Change activity	Core operations
Business Plan item	Corporate Services – coordination of support services including governance quality management, compliance with government standards for operations, critical incident response planning, corporate correspondence, Freedom of Information Act requests, and event management
Committee oversight?	Audit and Risk Committee
Finance and resource implications	N/A
Timescales	2025/26 (latest position)
Communication(s) (internal/external	N/A
Identified legislative implications	N/A

Government Functional Standards Update

Purpose of paper

1. This paper follows on from the previous paper to ARAC in June 2025, setting out the intended proportionate approach to the 2025/26 annual cycle of work for GFS, and provides an update on the progress to date on the work and the intended activities for Q3 and Q4.

Action required

2. ARAC is asked to note progress on the 2025/26 annual cycle of work for GFS and the intended activities for Q3 and Q4.

Background

3. The GFS exist to create and promote consistent and coherent ways of working across government, and provide a stable basis for assurance, risk management and capability improvement.

4. All central government departments and their ALBs should have a plan in place to work to each relevant functional standard in a proportionate way that meets its business plans and priorities.

5. All public bodies are expected to review their position against the standards annually, reporting to their ARAC accordingly.

6. As previously agreed with ARAC, we intend to seek compliance with the GFS in a manner that is proportionate to our size and scale as an organisation.

7. We have a dedicated SOP that sets out the annual cycle of work, provided here in Annex A.

Points to note for this specific annual cycle

8. There are currently 14 published GFS, and relevance to HTA is set out in Annex B. Since the last annual cycle 3 GFS have changed;

    - GFS 3 People
    - GFS 9 Internal Audit
    - GFS 14 Debt

9. As part of the 2025/26 cycle of work, the Corporate Services Team will be ensuring that we complete the 5 audit recommendations agreed with GIAA in our recent internal audit. Progress against these recommendations is provided in Annex C, including moving to the Good / Better / Best self-assessment model.

Progress to date

10. Progress through the various events within our agreement SOP for GFS is on-track at the end of Q2. Work to date has included:

- Setting up dedicated resource folders for each GFS including the current government resources, and our previous assessment / documentation and evidence examples
- Agreeing the outline annual review process and confirming the Functional Leads / Support Leads with SMT
- Providing detailed guidance and meeting with Functional Leads / Support Leads to confirm the resources available and outline the annual review process and requirements
- Starting to record the initial compliance assessments and the approach that the Functional Leads intend to take for documenting their compliance assessments

11. The initial compliance assessment for each GFS and the intended approach that Functional Leads intend to take for documenting their compliance is set out in Annex D.

Intended activities for Q3 and Q4

12. Progress through the various events within our agreed SOP for GFS will continue, including:

- Regular support meetings with Functional Leads / Support Leads to confirm on their compliance assessments, approach to documentation and evidence
- Population of the corporate compliance spreadsheet and dedicated folders with all documentation and evidence examples by Functional Leads / Support Leads
- Objective quality assurance checks of the assessments, documentation and evidence provided by the Functional Leads / Support Leads
- CEO approval for each GFS
- Outcome report to ARAC in February
- GFS statement in Annual Report and Accounts

13. However, it should be noted that staffing developments in the Corporate Services Team may impact on our ability to complete the intended activities to time.

Recommendation

14. ARAC to **note** progress on the 2025/26 annual cycle of work for GFS and the intended activities for Q3 and Q4.

HTA-SOP-160

Government Functional Standards

Purpose

This document sets out the HTA's process for adhering to the Government Functional Standards (GFS), and specifically focuses on the annual assessment cycle.

Related documents

All related documents are published on the Electronic Document Records Management System (EDRMS)

SMT Meeting Documents
ARAC Meeting Documents

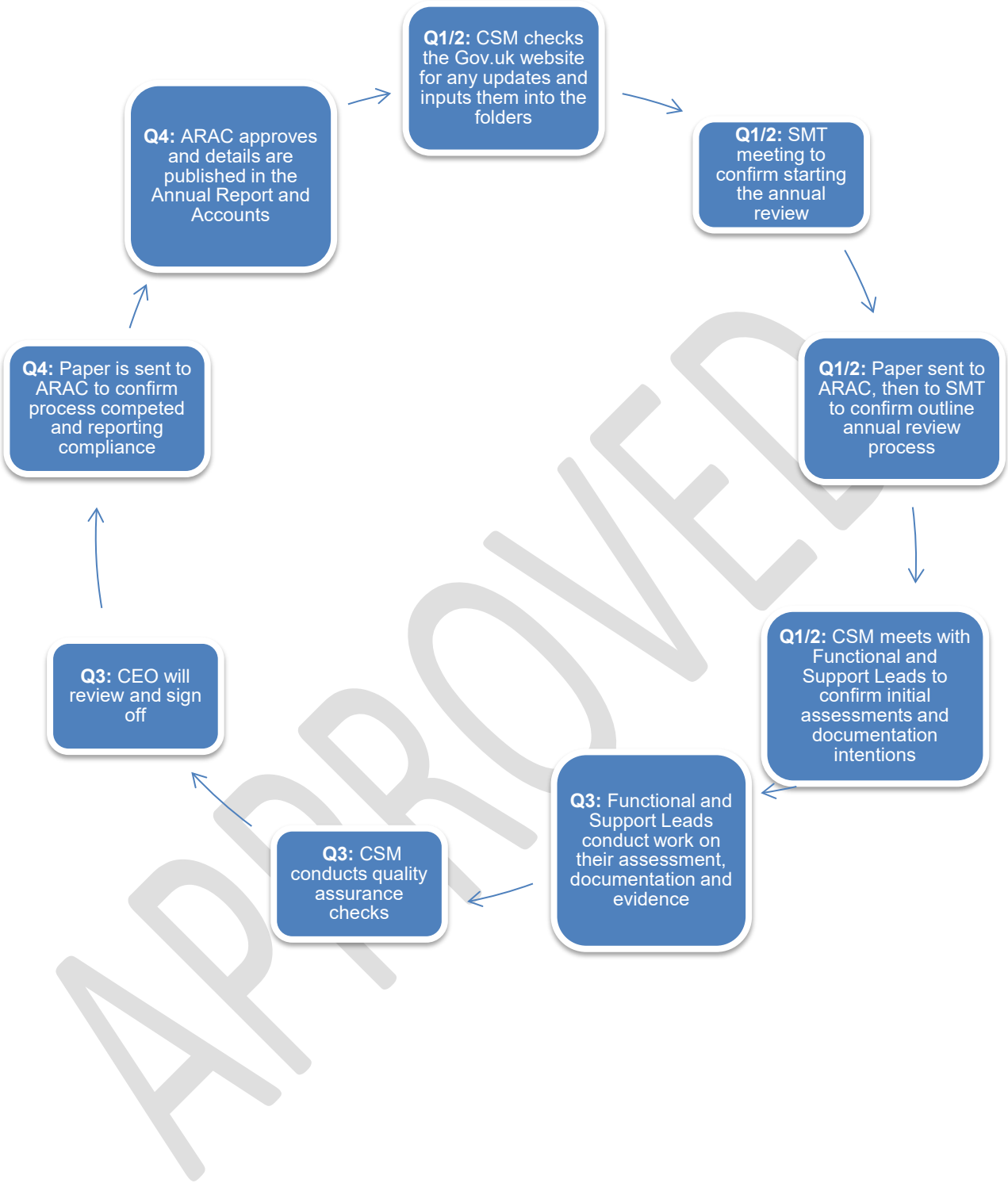
Changes from previous version

This is the first version of this document.

Users

SMT
BDT
Functional Leads (SMT Lead)
Support Leads (Technical Manager)

APPROVED


Q1/2: CSM checks the Gov.uk website for any updates and inputs them into the folders
Q1/2: SMT meeting to confirm starting the annual review
Q1/2: Paper sent to ARAC, then to SMT to confirm outline annual review process
Q1/2: CSM meets with Functional and Support Leads to confirm initial assessments and documentation intentions
Q3: Functional and Support Leads conduct work on their assessment, documentation and evidence
Q3: CSM conducts quality assurance checks
Q3: CEO will review and sign off
Q4: Paper is sent to ARAC to confirm process competed and reporting compliance
Q4: ARAC approves and details are published in the Annual Report and Accounts

APPROVED

Details of procedure

The Government Functional Standards (GFS) are incorporated into the everyday workings of the HTA operations in a proportionate manner. Therefore we maintain year-round awareness to ensure the HTA are adhering to a set of requirements set out by the government. As such the GFS are worked on year round, but we focus our attention on them in Q2 and Q3 of each financial year, performing a targeted review, in preparation for confirmation of our proportionate compliance to Audit and Risk Committee in Q4.

In Q1 the Corporate Services Manager (CSM) checks the government website to that the HTA is working to the current versions of the GFS (Functional Standards - GOV.UK). If there have been any updates since the previous review, the GFS documentation is downloaded and put into the corporate compliance folder for the GFS year required, and the Functional Lead is advised that the GFS has changed. This includes any supporting resources / documentation such as a self-assessment tool.

The corporate compliance EDRMS folders are accessible on the shared drive to all that are required to work on them. Access is limited and controlled by the IT department.

Roles and responsibilities:

Each GFS has a dedicated Functional Lead and Support Lead. This is decided during the Senior Management Team (SMT) meetings, by the CEO and the Senior Management.

Functional Lead: a member of Senior Management. They hold the responsibility for the GFS they are allocated to. They can be the Functional Lead for multiple GFS.

Support Lead: a member of the Business Development Team, or the most appropriate technical manager for the GFS. They support the Functional Lead for the GFS they are allocated to.

The CSM will keep a record on the corporate compliance spreadsheet of the Functional and Support Leads. The CSM is the Operational Lead for the GFS, they hold the responsibility to ensure that the corporate compliance spreadsheet is completed, and all supporting documentation is accessible and available. They will be in contact with the Functional Lead and Support Leads throughout the process. The CSM may hold training sessions with the relevant staff members to inform them of the process and the requirements to complete the corporate compliance spreadsheet.

Staff changes: if a staff member leaves who holds either a Functional Lead role or a Support Lead role, then the replacement will take over the responsibility for the GFS providing the role and requirements stay the same. This will be explained to them by their line manager and/or their Functional Lead. As part of the onboarding process, an introduction meeting occurs for all new starters at the HTA with relevant members of staff and the areas they cover. As such, every member of staff will meet with the CSM, who discuss the responsibilities around GFS, and if applicable, their accountability and role in the annual review process.

Occasionally more staff members will be included in the work for the GFS than is noted as a Functional Lead or a Support Lead. They will be informed of the requirements by the

APPROVED

Functional Lead or Support Lead as background information for what they are working with.

Order of events:

Quarter 1/2:

Step	Action
1	CSM checks the Gov.uk website to see if there are any updates to the GFS.
2	The CSM will put together a resources folder on the shared drive for the year and each of the GFS. A copy of the corporate compliance spreadsheet from the year before is stored here and is worked on throughout the year. Within the specific GFS folders will be a PDF copy of the *current* GFS, and any supporting resources / documentation or tools provided from the GFS website, and our own assessment documentation and evidence examples from the previous year, for guidance.
3	SMT meeting is held at which SMT are reminded that the annual review of the GFS will be taking place and that work will begin to record our proportionate compliance with them.
4	A paper is sent to the June ARAC meeting to outline the annual review process (including this SOP) and our current commitments to the GFS (individual relevance and previous assessment).
5	ARAC agrees or disagrees with our proposed process. If ARAC agrees, then steps continue, if they do not then a discussion at SMT occurs to nuance the intended approach.
6	A paper is provided to a SMT meeting to confirm the outline annual review process (including this SOP) and confirm explicitly who is in place to be Functional Lead for each GFS. This is when the scope of the process and what is expected from all involved is also confirmed with the CEO and SMT.
7	The Functional Lead will decide who is the best person for the role of the Support Lead for their GFS and will inform colleagues of this if this has not already occurred previously.
8	The CSM will contact all the Functional Leads and their Support Leads, confirming the resources available and setting out detailed process guidance, and will hold dedicated meetings to confirm their plans for the weeks ahead, and to set up any further support meetings that may be required.
9	The Functional Leads will look at the previous assessment submissions on the corporate compliance spreadsheet and update these providing an initial compliance assessment, including the position status and ambition against the GFS as required, using the Good / Better / Best self-assessment model.
10	The CSM will record the approach that the Functional Leads* will take for documenting their compliance (from the list below) on the corporate compliance spreadsheet. • Corporate compliance spreadsheet • Completed self-assessment tools

APPROVED

	• Dedicated action plans • Explicit mapping against the "Shall" statements within each GFS (this could be a discrete document or simply embedded comments onto the GFS itself) *The appropriate approach will be determined by the Functional Lead
11	For those that request it, regular meetings will occur with the CSM and the Leads to update as required.
12	A further paper will be sent to October ARAC meeting to confirm process work undertaken to date and the intentions for work in Q3 / 4.
13	Further updates will be given to SMT either in person or by email by the CSM on the process as required.

Quarter 3:

Step	Action
1	The CSM will hold regular support meetings with the Leads to confirm on their compliance assessments, approach to documentation and evidence.
2	The Leads will review and update their initial compliance assessments on the corporate compliance spreadsheet, and will begin to finalise the work needed for documenting compliance, including completion of any tools that have been supplied or any action plans that are required, adding the data / documents to the folders under the corporate compliance EDRMS structure.
3	The Leads will continue to populate the corporate compliance spreadsheet and specific GFS folders, including copying practical evidence examples across to demonstrate compliance as documented.
4	The CSM will begin to feed back to the CEO on the status of each GFS.
5	If required, the CSM will begin to follow up with the Leads to confirm and finalise any work still required.
6	The CSM will conduct objective quality assurance checks throughout to confirm 1) corporate compliance is broadly as expected, 2) that documentation of compliance is clear and understandable, 3) that there is sufficient practical evidence to demonstrate compliance. The Deputy Director for Performance and Corporate Governance will assist with this and act as escalation point for the CSM.
7	The CSM will inform the CEO of the final status for each GFS (compliance assessment, documentation and evidence examples) by the close of November. The CEO will then review and sign off the work by the close of December.

Quarter 4:

Step	Action
1	The CSM will conduct a final assurance check on the corporate compliance spreadsheet and all the specific GFS folders.

APPROVED

2	The CSM then creates a paper for the February ARAC meeting, confirming the completion of the annual cycle work and reporting the HTA's current proportionate compliance with the GFS.
3	ARAC approves the GFS annual cycle of work and current proportionate compliance, or else directs further remedial work in February.
4	ARAC approves the GFS element of the Annual Governance Statement within the Annual Report and Accounts in June.

Review

The SOP will be reviewed every two years or be reviewed and updated as and when required.

Revision history

Reference: HTA-SOP-160

Author(s): Corporate Services Manager

Reviewed by: Deputy Director Performance and Corporate Governance

Approved by: Deputy Director Performance and Corporate Governance

Owner: Deputy Director Performance and Corporate Governance

Distribution: HTA All Staff

Protective Marking: OFFICIAL

- May 2025 / Version: 1.0 / Newly created SOP
- June 2025 / Version: 2.0 Nuances added; 1) use of Good / Better / Best self-assessment model, 2) need for Leads to collate and CSM to review practical evidence examples
- September 2025 / Version: 3.0 Substantial rewrites to clarify process steps
- September 2025 / Version: 4.0 Linguistic clarifications

APPROVED

Relevance of GFS

GFS	Summary	Relevance	Rationale	Changes for 25/26?
Government functional standard GovS 001: government functions	Sets out the role of the Accounting Officer in ensuring functional standards are embedded in Governance and management of functions	Yes	As previously agreed with ARAC and as audited in 24/25	No
Government Functional Standard GovS 002: Project Delivery	Sets expectations for the direction and management of portfolios, programmes, and projects	Yes - limited	As previously agreed with ARAC and as audited in 24/25	No
Government Functional Standard GovS 003: Human Resources	Set expectations for the Leadership and management of human resources across government	No	As previously agreed with ARAC and as audited in 24/25	Yes
Government Functional Standard GovS 004: Property	Sets expectations for the management of government property	No	As previously agreed with ARAC and as audited in 24/25	No
Government Functional Standard GovS 005: Digital	Sets expectations for how all digital, data and technology work and activities should be conducted across government	Yes	As previously agreed with ARAC and as audited in 24/25	No
Government Functional Standard GovS 006: Finance	Sets expectations for the effective management and use of public funds	Yes	As previously agreed with ARAC and as audited in 24/25	No

AUD 34-25 ANNEX B

GFS	Summary	Relevance	Rationale	Changes for 25/26?
Government Functional Standard GovS 007: Security	Set expectations for protecting government's assets (people, property, and information), visitors to government property and citizen data	Yes	As previously agreed with ARAC and as audited in 24/25	No
Government Functional Standard GovS 008: Commercial and Commercial Continuous Improvement Assessment Framework	Sets expectations for expectations and drive consistency in the planning and management of buying goods, works and services	Yes - limited	As previously agreed with ARAC and as audited in 24/25	No
Government Functional Standard GovS 009: Internal Audit	Sets expectations for internal audit activity to enhance the effectiveness and efficiency of governance, risk management and control in government organisations	Yes	As previously agreed with ARAC and as audited in 24/25	Yes
Government Functional Standard GovS 010: Analysis	Sets expectations for the planning and undertaking of analysis to support well informed decision making to deliver better outcomes	Yes - limited	As previously agreed with ARAC and as audited in 24/25	No

AUD 34-25 ANNEX B

GFS	Summary	Relevance	Rationale	Changes for 25/26?
Government Functional Standard GovS 011: Communication	Sets expectations for the management and practice of government communication in order to deliver responsive and informative public service communication that supports the effective delivery of HM Government policy and priorities and assists with the effective operation of public services	Yes	As previously agreed with ARAC and as audited in 24/25	No
Government Functional Standard GovS 013: Counter Fraud	Sets expectations for the management of counter fraud, bribery, and corruption activity in government organisations	Yes	As previously agreed with ARAC and as audited in 24/25	No
Government Functional Standard - GovS 014: Debt	Sets expectations for the management of debt owed to government departments and their arm's length bodies	Yes - limited	As previously agreed with ARAC and as audited in 24/25	Yes
Government Functional Standard GovS 015: Grants	Sets expectations for the management of grant schemes and award	Yes - limited	*Now* considered relevant	No

Progress against recommendations

No.	Theme / Practice area	Recommendation from GIAA	Action plan to address the recommendations all by close of June 2026 (sooner if possible)	Monthly update from CSM on actions to June 2026
1	Accountabilities and responsibilities	**Recommendation 1** Roles and responsibilities for the Chief Executive Officer, the Deputy Director for Performance and Corporate Governance and the Corporate Services Manager should be clearly and explicitly documented within existing guidance such as the draft Standard operating Procedure for Functional Standards.	**Action:** Not agreed – roles are clearly articulated in the SOP, with presentation in line with all our other SOP **Evidence to be provided to GIAA:** N/A **Due date:** N/A	N/A
2	Applicability and ambition	**Recommendation 2** The applicability assessment for the Property functional standard should be revisited and recorded on the spreadsheet.	**Action:** Agreed – applicability of Property Functional Standard to be reviewed by Director of Finance and Resources as part of the next annual review cycle **Evidence to be provided to GIAA:** Evidence to be provided to GIAA: Outputs from the next annual review cycle, including corporate compliance spreadsheet (plus individual compliance documents and practical evidence examples on request) **Due date:** 30th June 2026	<u>April 2025</u> No progress / update provided in April due to prioritisation of other operational work. To be progressed from May as a priority, in accordance with the timelines set out in our SOP <u>May 2025</u> No specific action yet – action related to Property to be picked up as part of the next annual review cycle <u>June 2025</u> No specific action yet – action related to Property to be picked up as part of the next annual review cycle <u>July 2025</u> No specific action yet – action related to Property to be picked up as part of the 25/26 annual review cycle (to be initiated by end of July, all resources prepared: <u>GFS #1 cycle start emails to Leads.msg</u>) <u>August 2025</u> No specific action yet – although 25/26 annual review cycle has started and Leads have been notified of requirements, including for Property: <u>2526 Annual Cycle start - notification for GFS #4.msg</u> <u>September 2025</u> Very limited progress / no update provided in September due to staff absence within Corporate Services Team. Position remains as per August update. Final update from outgoing Corporate Services Manager to be provided in October <u>October 2025</u> *Narrative + link to documentation* <u>November 2025</u> <u>December 2025</u> <u>January 2026</u> <u>February 2026</u> <u>March 2026</u> <u>April 2026</u> <u>May 2026</u> <u>June 2026</u>
3	Applicability and ambition	**Recommendation 3** The compliance ambitions should be determined for each of the functional standards using	**Action:** Agreed – we will move from arbitrary %'s to describing compliance in terms of Good, Better, or Best	<u>April 2025</u> No progress / update provided in April due to prioritisation of other operational work. To be progressed from May as a priority, in accordance with the timelines set out in our SOP

No.	Theme / Practice area	Recommendation from GIAA	Action plan to address the recommendations all by close of June 2026 (sooner if possible)	Monthly update from CSM on actions to June 2026
		consistent criteria and rationale for all standards. Consideration should be given to expressing ambition statements as Good, Better, or Best as intended by the standards and GovS001 and as included in the available Continuous Improvement Assessment Frameworks.	**Evidence to be provided to GIAA:** Evidence to be provided to GIAA: Outputs from the next annual review cycle, including corporate compliance spreadsheet (plus individual compliance documents and practical evidence examples on request) **Due date:** 30th June 2026	<u>May 2025</u> Intention set out in the SOP to provide the June ARAC meeting a paper to outline the annual review process (and specifically of moving to the Good / Better / Best self-assessment model in 25/26) has been missed by the CS team and will need to be created / agreed quickly now to catch up CS team asked to ensure that they work to the letter of the SOP for the remainder of the 25/26 annual cycle. CS team to also prioritise the intended paper / discussion with SMT in June to discuss the annual review that will be taking place and that work will begin to record our proportionate compliance with them, including the requested approach to expressing ambition statements as Good, Better, or Best in the next annual cycle and the other recommendations noted in this action plan. <u>June 2025</u> Intentions for 25/26 annual cycle (including explicit move to use of the Good / Better / Best self-assessment model) have been documented and agreed with ARAC and SMT. SOP updated to clarify the intended use of the Good / Better / Best self-assessment model during the 25/26 cycle: *"The Functional Leads will look at the previous submissions on the corporate compliance spreadsheet and update the position status and ambition against the full standard as required, using the Good / Better / Best self-assessment model."* <u>July 2025</u> Intended use of the Good / Better / Best self-assessment model during the 25/26 cycle explicitly noted in prepared resources to be circulated to Leads initiating the cycle (by end of July): GFS #1 cycle start emails to Leads.msg) Good / Better / Best self-assessment explicitly captured in the 25/26 corporate compliance spreadsheet: HTA Government Functional Standards Review 2025.xlsx <u>August 2025</u> 25/26 annual review cycle has started and Leads have been notified of requirements, including the intended use of the Good / Better / Best self-assessment model: GFS #1 cycle start - confirmation 2.msg 2526 Annual Cycle start - notification for GFS #2.msg 2526 Annual Cycle start - notification for GFS #3.msg 2526 Annual Cycle start - notification for GFS #4.msg 2526 Annual Cycle start - notification for GFS #5.msg 2526 Annual Cycle start - notification for GFS #6.msg 2526 Annual Cycle start - notification for GFS #7.msg 2526 Annual Cycle start - notification for GFS #8.msg

No.	Theme / Practice area	Recommendation from GIAA	Action plan to address the recommendations all by close of June 2026 (sooner if possible)	Monthly update from CSM on actions to June 2026
				2526 Annual Cycle start - notification for GFS #9.msg 2526 Annual Cycle start - notification for GFS #10.msg 2526 Annual Cycle start - notification for GFS #11.msg 2526 Annual Cycle start - notification for GFS #13.msg 2526 Annual Cycle start - notification for GFS #14.msg 2526 Annual Cycle start - notification for GFS #15.msg CS Team have also held dedicated support meetings with Leads, clarifying the requirements for this cycle September 2025 Very limited progress / no update provided in September due to staff absence within Corporate Services Team. Position remains as per August update. Final update from outgoing Corporate Services Manager to be provided in October October 2025 *Narrative + link to documentation* November 2025 December 2025 January 2026 February 2026 March 2026 April 2026 May 2026 June 2026
4	Assurance	**Recommendation 4** The outcomes of formal quality assurance checks of self-assessments should be recorded.	**Action:** Agreed – we will record the formal quality assurance checks of self-assessments by the CSM (and ultimate approval by the CEO) in the corporate compliance spreadsheet as part of the next annual review cycle **Evidence to be provided to GIAA:** Evidence to be provided to GIAA: Outputs from the next annual review cycle, including corporate compliance spreadsheet (plus individual compliance documents and practical evidence examples on request) **Due date:** 30th June 2026	April 2025 No progress / update provided in April due to prioritisation of other operational work. To be progressed from May as a priority, in accordance with the timelines set out in our SOP May 2025 Current GFS documentation has been downloaded and collated into dedicated EDRMS folders for the 25/26 cycle; 2025-26 Next annual cycle to begin shortly, including the recording of formal quality assurance checks by the CSM June 2025 SOP updated to clarify the intended formal quality assurance checks to be conducted during the 25/26 cycle: *"The CSM will conduct quality assurance checks throughout to confirm 1) corporate compliance is broadly as expected, 2) that documentation of compliance is clear and understandable, 3) that there is sufficient practical evidence to demonstrate compliance."* July 2025 Intended implementation of formal quality assurance checks during the 25/26 cycle explicitly

No.	Theme / Practice area	Recommendation from GIAA	Action plan to address the recommendations all by close of June 2026 (sooner if possible)	Monthly update from CSM on actions to June 2026
				noted in prepared resources to be circulated to Leads initiating the cycle (by end of July): GFS #1 cycle start emails to Leads.msg) x3 elements of the quality assurance checks explicitly itemised in the 25/26 corporate compliance spreadsheet: HTA Government Functional Standards Review 2025.xlsx August 2025 25/26 annual review cycle has started and Leads have been notified of requirements, including the intended implementation of formal quality assurance checks: GFS #1 cycle start - confirmation 2.msg 2526 Annual Cycle start - notification for GFS #2.msg 2526 Annual Cycle start - notification for GFS #3.msg 2526 Annual Cycle start - notification for GFS #4.msg 2526 Annual Cycle start - notification for GFS #5.msg 2526 Annual Cycle start - notification for GFS #6.msg 2526 Annual Cycle start - notification for GFS #7.msg 2526 Annual Cycle start - notification for GFS #8.msg 2526 Annual Cycle start - notification for GFS #9.msg 2526 Annual Cycle start - notification for GFS #10.msg 2526 Annual Cycle start - notification for GFS #11.msg 2526 Annual Cycle start - notification for GFS #13.msg 2526 Annual Cycle start - notification for GFS #14.msg 2526 Annual Cycle start - notification for GFS #15.msg CS Team have also held dedicated support meetings with Leads, clarifying the requirements for this cycle September 2025 Very limited progress / no update provided in September due to staff absence within Corporate Services Team. Position remains as per August update. Final update from outgoing Corporate Services Manager to be provided in October October 2025 *Narrative + link to documentation* November 2025 December 2025 January 2026 February 2026 March 2026 April 2026 May 2026 June 2026

No.	Theme / Practice area	Recommendation from GIAA	Action plan to address the recommendations all by close of June 2026 (sooner if possible)	Monthly update from CSM on actions to June 2026
5	Self-assessment	**Recommendation 5** Assessments of compliance for all applicable requirements of the Functional Standards should be: • maintained as per the agreed annual frequency; • based on robust evidence, including where requirements link to other Functional Standards and wider government standards.	**Action:** Agreed – we commit to an ongoing annual review cycle **Evidence to be provided to GIAA:** Evidence to be provided to GIAA: Outputs from the next annual review cycle, including corporate compliance spreadsheet, compliance documents and practical evidence examples related to individual Functional Standards as appropriate (a selection to be provided) and annual report to ARAC **Due date:** 30th June 2026	April 2025 No progress / update provided in April due to prioritisation of other operational work. To be progressed from May as a priority, in accordance with the timelines set out in our SOP May 2025 Current GFS documentation has been downloaded and collated into dedicated EDRMS folders for the 25/26 cycle; 2025-26 Next annual cycle to begin shortly, including the reference to evidence bases and links to other standards June 2025 SOP updated to clarify the intention to collate practical evidence examples in addition to the assessment documentation during the 25/26 cycle: *"The Leads will … to populate the corporate compliance spreadsheet and folders, including copying practical evidence examples across to demonstrate compliance as documented."* July 2025 1. Intended collation of practical evidence examples in addition to the assessment documentation, *and* 2. the requirement to look and link across individual standards during the 25/26 cycle both explicitly noted in prepared resources to be circulated to Leads initiating the cycle (by end of July): GFS #1 cycle start emails to Leads.msg) Links to locations for practical evidence examples explicitly captured in the 25/26 corporate compliance spreadsheet: HTA Government Functional Standards Review 2025.xlsx August 2025 25/26 annual review cycle has started and Leads have been notified of requirements, including 1. the collation of practical evidence examples in addition to the assessment documentation, *and* 2. the requirement to look and link across individual standards: GFS #1 cycle start - confirmation 2.msg 2526 Annual Cycle start - notification for GFS #2.msg 2526 Annual Cycle start - notification for GFS #3.msg 2526 Annual Cycle start - notification for GFS #4.msg 2526 Annual Cycle start - notification for GFS #5.msg 2526 Annual Cycle start - notification for GFS #6.msg 2526 Annual Cycle start - notification for GFS #7.msg 2526 Annual Cycle start - notification for GFS #8.msg 2526 Annual Cycle start - notification for GFS #9.msg 2526 Annual Cycle start - notification for GFS #10.msg 2526 Annual Cycle start - notification for GFS #11.msg

No.	Theme / Practice area	Recommendation from GIAA	Action plan to address the recommendations all by close of June 2026 (sooner if possible)	Monthly update from CSM on actions to June 2026
				2526 Annual Cycle start - notification for GFS #13.msg 2526 Annual Cycle start - notification for GFS #14.msg 2526 Annual Cycle start - notification for GFS #15.msg CS Team have also held dedicated support meetings with Leads, clarifying the requirements for this cycle September 2025 Very limited progress / no update provided in September due to staff absence within Corporate Services Team. Position remains as per August update. Final update from outgoing Corporate Services Manager to be provided in October October 2025 *Narrative + link to documentation* November 2025 December 2025 January 2026 February 2026 March 2026 April 2026 May 2026 June 2026
6	Action plans	**Recommendation 6** A due date should be agreed for action 5 for the GovS013 Counter Fraud functional standard.	**Action:** Agreed – due date for action 5 of Counter Fraud Functional Standard to be added by Director of Finance and Resources as part of the next annual review cycle **Evidence to be provided to GIAA:** Evidence to be provided to GIAA: Updated action plan for Counter Fraud Functional Standard **Due date:** 30th June 2026	April 2025 No progress / update provided in April due to prioritisation of other operational work. To be progressed from May as a priority, in accordance with the timelines set out in our SOP May 2025 No specific action yet – action related to Counter Fraud to be picked up as part of the next annual review cycle June 2025 No specific action yet – action related to Counter Fraud to be picked up as part of the next annual review cycle July 2025 No specific action yet – action related to Counter Fraud to be picked up as part of the 25/26 annual review cycle (to be initiated by end of July, all resources prepared: GFS #1 cycle start emails to Leads.msg) August 2025 No specific action yet – although 25/26 annual review cycle has started and Leads have been notified of requirements, including for Counter Fraud: 2526 Annual Cycle start - notification for GFS #13.msg September 2025 Very limited progress / no update provided in September due to staff absence within Corporate Services Team. Position remains as per August

No.	Theme / Practice area	Recommendation from GIAA	Action plan to address the recommendations all by close of June 2026 (sooner if possible)	Monthly update from CSM on actions to June 2026
				update. Final update from outgoing Corporate Services Manager to be provided in October October 2025 *Narrative + link to documentation* November 2025 December 2025 January 2026 February 2026 March 2026 April 2026 May 2026 June 2026
7	Recruitment and training	**Recommendation 7** Where relevant, new applicants and recruits to HTA functional roles should be made aware of the Functional Standards during recruitment and induction to enable them to understand the requirements to meet standards as part of their day-to-day responsibilities.	**Action:** Not agreed – evidence examples already shared of references to GFS in onboarding plans an annual objectives where relevant to specific staff **Evidence to be provided to GIAA:** N/A **Due date:** N/A	N/A

AUD34-25 ANNEX D

Initial assessment / documentation approach

GFS	Functional Lead	Initial assessment[1]	Documentation approach	Different for 25/26?[2]
Government functional standard GovS 001: government functions	Chief Executive Officer but practically delegated to Deputy Director for Performance and Corporate Governance	Position Status: Better Ambition: Better	**Corporate compliance spreadsheet** Completed self-assessment tool Dedicated action plan **Explicit mapping against the "Shall" statements within the GFS**	No
Government Functional Standard GovS 002: Project Delivery	Deputy Director for Performance and Corporate Governance	Position Status: Better Ambition: Better	**Corporate compliance spreadsheet** **Completed self-assessment tool** Dedicated action plan **Explicit mapping against the "Shall" statements within the GFS**	No

[1] Note – initial compliance assessments are still under discussion with the Corporate Services Team and are indicative only at this point in the cycle
[2] Note – comparisons of compliance assessments to 24/25 are an approximation due to moving from arbitrary %'s to the Good / Better / Best self-assessment model in this cycle

Government Functional Standard GovS 003: Human Resources	Director of Finance and Resources	N/A	N/A	No
Government Functional Standard GovS 004: Property	Director of Finance and Resources	N/A	N/A	No
Government Functional Standard GovS 005: Digital	Director of Data, Technology and Development	Position Status: Better Ambition: Better	**Corporate compliance spreadsheet** **Completed self-assessment tool** Dedicated action plan **Explicit mapping against the "Shall" statements within the GFS**	Assessment upgraded
Government Functional Standard GovS 006: Finance	Director of Finance and Resources	Position Status: Good Ambition: Good	**Corporate compliance spreadsheet** **Completed self-assessment tool** Dedicated action plan Explicit mapping against the "Shall" statements within the GFS	No

Government Functional Standard GovS 007: Security	Director of Finance and Resources	Position Status: Good Ambition: Good	**Corporate compliance spreadsheet** Completed self-assessment tool Dedicated action plan **Explicit mapping against the "Shall" statements within the GFS**	No
Government Functional Standard GovS 008: Commercial and Commercial Continuous Improvement Assessment Framework	Director of Finance and Resources	Position Status: Good Ambition: Good	**Corporate compliance spreadsheet** **Completed self-assessment tool** Dedicated action plan Explicit mapping against the "Shall" statements within the GFS	No
Government Functional Standard GovS 009: Internal Audit	Director of Finance and Resources	Position Status: Good Ambition: Good	**Corporate compliance spreadsheet** **Completed self-assessment tool** Dedicated action plan	No

			Explicit mapping against the "Shall" statements within the GFS	
Government Functional Standard GovS 010: Analysis	Director of Data, Technology and Development	Position Status: Good Ambition: Good	**Corporate compliance spreadsheet** Completed self-assessment tool Dedicated action plan **Explicit mapping against the "Shall" statements within the GFS**	No
Government Functional Standard GovS 011: Communication	Director of Data, Technology and Development	Position Status: Better Ambition: Better	**Corporate compliance spreadsheet** Completed self-assessment tool Dedicated action plan Explicit mapping against the "Shall" statements within the GFS	No
Government Functional Standard GovS 013: Counter Fraud	Director of Finance and Resources	Position Status: Good Ambition: Good	**Corporate compliance spreadsheet** Completed self-assessment tool	No

			Dedicated action plan **Explicit mapping against the "Shall" statements within the GFS**	
Government Functional Standard - GovS 014: Debt	Director of Finance and Resources	Position Status: Good Ambition: Good	**Corporate compliance spreadsheet** **Completed self-assessment tool** Dedicated action plan Explicit mapping against the "Shall" statements within the GFS	Assessment upgraded
Government Functional Standard GovS 015: Grants	Director of Finance and Resources	Position Status: Developing Ambition: Developing	**Corporate compliance spreadsheet** Completed self-assessment tool Dedicated action plan **Explicit mapping against the "Shall" statements within the GFS**	New assessment (now considered relevant)

HTA
Human Tissue Authority

Audit and Risk Assurance Committee (ARAC)

Risk Update

Confidential

HTA
Human Tissue Authority

Audit and Risk Assurance Committee (ARAC)

Interests, Gifts

& Hospitality

Confidential

Audit and Risk Committee (ARAC) meeting, 14 October 2025

Agenda item	**6.1 SIRO Report**
For information or decision?	Information
Decision making to date?	Standing annual item to each Audit and Risk Committee. Circulated to ARAC members 8 September, reviewed by SMT 9 September
Recommendation	Audit and Risk Committee is asked to note and comment by exception on the 2024/25 SIRO report
Which strategic risks are relevant?	Risk 6: Security
Strategic objective	Efficient and Effective
Core operations / Change activity	Core operations
Business Plan item	Audit and Risk – coordination of appropriate organisation controls to facilitate scrutiny and oversight by stakeholders
Committee oversight?	Audit and Risk Committee
Finance and resource implications	N/A
Timescales	2024/25
Communication(s) (internal/external stakeholders)	N/A
Identified legislative implications	N/A

HTA meeting papers are not policy documents. Draft policies may be subject to revision following the HTA Board meeting

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 4th September 2025.

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, the HTA's cyber security management arrangements have been assessed against the standards set by the National Cyber Security Centre and in our annual submission against the Cyber Assessment Framework (CAF).

Report

7. The SIRO Report reflects on the HTA's information governance work undertaken during 2024/25 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) Cyber Assurance Framework (CAF)
     - Any Security Incidents and personal data breaches 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 2024/25.

9. The HTA has a number of additional controls that support our use of information including detailed policies on Records Management, managing Individual Information Right Requests (previously known as Subject Access Requests (SAR) 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 (DPIAs) 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 CAF submission in June 2025 and (has any other audits been done last year). This year we have been assessed around five objectives:

Objective A - Managing risk
Objective B - Protecting against cyber-attack and data breaches
Objective C - Detecting cyber security events
Objective D - Minimising the impact of incidents
Objective E - Using and sharing information appropriately

11. We were audited against 8 mandatory standards and four self-selected standards. The standards that were selected by the HTA represented areas of potential risk and where it was felt that independent validation of the controls and their effectiveness would be beneficial.

12. We received for the a CAF submission a moderate assurance with high confidence and low risk across our actions and controls based on what was reviewed. This was well received by the auditors, and we can take assurance from this work that we are proactive and effective in our cyber security measures.

Policies

13 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 comprises of the following policies:

Policy	Last revision	Next revision
HTA-POL-087- Information Governance Assurance Framework	2025 (published June 2025)	2027
HTA-POL-088 Records Management and Retention Policy	2024 (published July 24)	2026
HTA-GD-010 Records Retention Schedule	2024(published July 24) This retention schedule has been incorporated with policy above.	2026
HTA-POL-056 Information Governance and Cyber Risk	2025 (published April 25)	2027

14 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. This records management programme of work was put on hold due to not having a consistent Records Management and Information Governance (RMIG) Lead in post until February 2025. This programme of work will recommence in 2025 with a Records Management Strategy Paper, which will include retention of records, being presented to the Senior Management Team (SMT).

Data Breach Management and Reporting

15 In 2024/25 the HTA reviewed and updated the Data Breach Policy. The data breach process remains the same as we reported for FY:2023/24; 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.

16. During 2024/25 reporting year there have been no serious security breaches, also known as serious cyber incidents. However, there were two near misses. The incidents were caused by individuals attempting to access their accounts whilst outside of the UK. These do not equate to Cyber Security Incidents as they were not unauthorised access requests, they were breaches of HTA policy and have been dealt with accordingly, but it was pleasing to see that the controls we have in place to identify potential cyber security issues work in practice. As a result to these near misses the HTA took the decision to apply stricter rules on accessing systems abroad.

17. The HTA recorded 3 incidents of data breaches, details are contained in the table below:

Category	Recorded as data breach	Recorded as personal data breach	Reported to ICO	Total
Data emailed to incorrect recipient	2	0	0	2
Loss of physical data	0	0	0	0
Transferring to personal devices	1	0	0	1

18. 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 Individual Information Rights Requests.

19 During 2024/25 the HTA received 27 requests for information under the Freedom of Information Act. The number of requests is relatively constant and does not vary greatly year on year. One FOI was treated as an enquiry and was responded to, but not under the FOI act.

Total received	Total responded to	Refused	Rescinded
27	27	0	0

20 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.

21 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 2024/25 the HTA received 2 Subject Access Requests.

Total received	Total responded to	Refused	Rescinded
2	2	0	0

HTA Activity during 2024/25

22. I took over as Senior Information Risk Owner on joining the HTA in December 2024 and will be undertaking SIRO training for the role by November 2025.

23. This year we appointed 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 2025. We have a permanent Head of IT and the Director of Data, Technology and Development also covers 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. I am comfortable that we have been able to seek expert, in particular legal, advice when required.

24. 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.

25. 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.

26. 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.

27. A further data security risk facing the HTA lies in the reliance on legacy systems, a significant contributory factor is the limited investment in the HTA's IT infrastructure. The reasons for this are multifactorial. I am pleased to confirm that targeted investment over the last 2 years has supported some significant improvements in particular bringing our core systems back into support. This work remains ongoing as identified to GIAA as part of our CAF submission, we need to replace our core and supporting finance systems. I am very pleased that we have developed and are maintaining 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.

28. Our self-assessment against the CAF for the submission in June 2025 demonstrated improvements to our data security and protection practices. It was one of general compliance with the CAF 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'. Furthermore, the GIAA's confidence level in the veracity of HTA's self-assessment was high.

29. 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 Standards and the requirements of the mandated Cyber Assessment Framework and discussed this with the Head of IT and the Director for Data, Technology and Development. 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. I have also considered a number of the factors that underpin the management of the HTA's information risks.

- I am assured that the HTA has in place an effective Information Governance framework. This framework 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 controls in place relating to the management and use of records and continually strengthens these by embedding best practice into our policies and procedures.

- The HTA has a good process in place for the recording and responding to FOI requests, individual information rights requests and all other information enquiries.

- In 2025/26 we will be looking to understand any risks associated with the use of AI as part of our own internal controls and to further strengthen our management of records including retention.

32. In conclusion, good progress has been made during 2024/25 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 continues to take action to understand and mitigate risk in this area.

Katrina Leighton-Hearn, Director of Finance and Resources and SIRO

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[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. 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.	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 will receive SIRO training in 2025/26.

[1] 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.

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 continue to review and update the IAR and ROPA 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 continue to review and update the IAR and ROPA 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.***	Users **shall** be given the minimum access to sensitive information or key operational services necessary for their role. a) 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 continue to strengthen our system access controls as required, updating our Joiners / Movers / Leavers process that includes IT-specific requirements and 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 continue to use 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.	I 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 penetration test in 2024/25 and ongoing vulnerability scans have highlighted good practices and our Cyber Security position. I am informed that any DNS changes that are requested are approved by the Head of IT and actioned only by authorised members. At present this is BCC our third-party supplier. 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.

		b) To protect your end user devices, you <u>shall</u>: VIII. Identify and account for all end user devices and removable media. IX. 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. X. Be running operating systems and software packages which are patched regularly, and as a minimum in vendor support. XI. 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. XII. Have the ability to remotely wipe and/or revoke access from an end user device.	Our software and operating systems are patched and maintained in line with updates.. 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 with risks formally accepted. I confirm that all end user devices within the organisation are encrypted and are managed 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>:** IV. 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[2]. V. Ensure the underlying infrastructure is secure, including verifying that the hosting environment is maintained securely and that you have appropriately exercised your	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.

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

		responsibilities for securely configuring the infrastructure and platform. VI. Protect data in transit using well-configured TLS v1.2. VII. Regularly test for the presence of known vulnerabilities and common configuration errors. You **shall** register for and use the NCSC's Web Check service.	
7	***Highly privileged accounts should not be vulnerable to common cyberattacks.***	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. a) 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. b) 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.	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 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.	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.

		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) 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.	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.

		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.	Our formal reporting to ARAC on Cyber Security reflects on lessons learned from internal and external incidents.
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) 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.