Audit and Risk Assurance Committee (ARAC)

Date: 9 June 2022

Time: 10.00 – 12.00 (Main meeting)

12.00 – 12.30 (Private Members session with auditors)

Venue: Zoom

Protective Marking: OFFICIAL

Agenda

1. Welcome and apologies **(10 mins)**

2. Declarations of interest

3. Minutes of 27 January 2022 meeting (AUD 15/22)

4. Matters arising from 27 January 2022 meeting (AUD 16/22)

Risk Update (20 mins)

5. Risk Update (AUD 17/22)

   Annex A – Risk Register Summary (AUD17a/22)

   Annex B- Strategic Risk Register (AUD 17b/22)

   Annex C- Risk Management Policy and Procedure (AUD 17c/22)

Cyber Security (10 mins)

6. Cyber Security Update (AUD 18/22)

7. SIRO Report (AUD 19/22)

Policies and Procedures (10 mins)

8. Policy and Procedure Schedule (AUD 20/22)

   Annex A- Summary Document (AUD 20a/22)

   Annex B- HTA Critical Incident Response Plan (AUD 20b/22)

   Annex C- HTA-BCP-000 Business Continuity Disaster Recovery Plan (AUD 20c/22)

9. Gifts and Hospitality (AUD 21/22)

   Annex A- HTA-POL-051- Declaration of Interests, Gifts and Hospitality Policy (AUD 21a/22)

   Annex B- Gifts and Hospitality Register (AUD21b/22)

Internal Audit (15 mins)

10. Item 10 is confidential and not included

Audit Tracker (15 mins)

11. Item 11 is confidential and not included

External Audit (15 mins)

12. Item 12 is confidential and not included

Regular Reporting (10 mins)

13. Reports on grievances, disputes, fraud and other information (Oral)

14. Topics for future risk discussions (Oral)

Any Other Business (5 mins)

15. ARAC effectiveness review – summary of responses (AUD25/22)

16. Equality, Diversity and Inclusion Report (AUD 26/22)

17. Any Other Business (Oral)

Minutes of the Audit and Risk Assurance (ARAC) meeting

Date: 27 January 2022

Time: 10.00 – 12.00

Venue: Zoom

Protective Marking: OFFICIAL

Attendees:

ARAC Members
Professor Gary Crowe (GC), ARAC Chair
Dr Stuart Dollow (SD)
Dr Charmaine Griffiths (CG)

Mike Surman (MS), National Audit Office
Rebecca Jones (RJ), Government Internal Audit Agency
Joanne Charlton (JC) Government Internal Audit Agency

Apologies
Jan Williams (JW) ARAC Member
Laura Fawcus (LF), National Audit Office

Observers
Jacky Cooper (JC), Health Ethics, Department of Health and Social Care
Dylan Parrin (DP), Senior Policy Manager, Department of Health and Social Care
Amy Parsons (AP), Department of Health and Social Care
Dean Gibbs (DG), (KPMG)

In Attendance

Dr Colin Sullivan (CS), CEO
Louise Dineley (LD), Director of Data Technology and Development
Richard Sydee (RS), Director of Resources
Nicky Harrison (ANH), Director of Regulation
Morounke Akingbola (MA), Head of Finance and Governance
Kelly Sherlock (KS), Head of Regulation
TJ O'Connor (TOC), Executive Assistant
Alison Margrave (AM), Board Support (*minute taker*)

Item 1 – Welcome and apologies

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

2. Apologies were noted from Jan Williams and Laura Fawcus.

Item 2 – Declarations of interest

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

Item 3 – Minutes of 14 October 2021 ARAC meeting [AUD 1/22 and 1a/22]

4. The Chair introduced the report and referred to his email to Committee members with an additional proposed amendment to minute 8.

5. The Committee noted that the proposed amendment currently allocated to minute 15, should be for minute 14. With this clarification the proposed amendments were accepted, and the revised minutes were agreed to be an accurate record of the meeting on 14 October 2021.

Item 4 – Matters arising from previous meeting [AUD 2/22]

6. The Chair introduced the report. Richard Sydee, Director of Resources, spoke to the items which were still marked live.

Action 1: The matters arising items relating to Risk 6 and Cyber Security Dashboard to be closed but the due date for the FOIA guidance document to be recast.

7. The Chair informed the Committee that he had spoken with Clare Wend-Henson, the staff forum representative and there were no issues to report. There was a positive feeling among staff of returning to a post-pandemic hybrid working model.

8. The Chair informed the Committee that the effectiveness review document will be circulated to members for completion. The results of this review will be reported to the Board in due course.

Action 2: Committee's effectiveness review document to be circulated to members.

9. The Chair noted that training needs and cycle of business matters need updating on the report.

Action 3: The Chair and Richard Sydee to update the training needs and cycle of business matters.

Item 5 – Internal Audit [AUD 3/22, AUD 3a/22, AUD 3b/22 and AUD 3c/22]

10. Jo Charlton (JC) from the Government Internal Audit Agency presented the reports to the Committee and provided key highlights.

11. The report on EDI had been presented in draft form and the field work has been completed for the next two audits. The schedule to complete all work by 31 March looks set to be achieved.

12. JC reported that the planning approach for 22/23 had been adjusted to accommodate the appointment of HTA's new Chief Executive. The proposed plan would therefore be brought to ARAC in early March, outside their normal meeting schedule.

13. In response to a question, JC provided further details about how HTA's preparation of the Governance Statement could be improved.

14. In response to a question, JC undertook to provide further information about addressing deterioration in the culture of compliance, as well as the output of the review of rating benchmarks, both of which were contained in the GIAA Opinion Analysis for 2020-21.

Action 4: Jo Charlton to provide further information to the Committee concerning addressing deterioration in the culture of compliance and the output of the review of rating benchmarks.

15. The Committee questioned the process of closing outstanding audit actions and the liaison between GIAA and HTA. The Chief Executive gave the Committee assurance that this would be a key focus for him.

16. The Committee noted the reports.

Item 6 – Audit Trackers [AUD 4/22]

17. Morounke Akingbola (MA) introduced the report and referred the Committee to the corrected table which she had circulated via email.

18. The Committee noted that a number of these actions were outstanding, and priority should be given to closing these off.

19. The Committee noted the report.

Item 7 – External Audit [AUD 5/22]

20. Mike Surman (MS), National Audit Office, introduced the report and explained the process for outsourcing the work to KMPG but that the responsibility for the audit opinion and reporting will still lie with the National Audit Office. MS provided further information on the detailed handover which had taken place between the teams and the modest increase in the fee cost.

21. Dean Gibbs (DG), KPMG, highlighted the main areas of focus, being IFR16 and payroll requirements for the remuneration report, and the timetable for preparation of this report.

22. The Committee noted the report.

Item 8 – Risk Update [AUD 6/22, Annex A Risk Register Summary, Annex B Strategic Risk Register and Annex C Operational Risk Register]

23. Richard Sydee (RS) introduced the reports and drew the Committee's attention to the fact that Risk 2 had been downgraded from 12 to 9 and Risk 4 had been downgraded from 16 to 12. These two risks remain above tolerance all other risks remain as previous.

24. The Committee discussed ways how these risks could be reduced further, and the action taken by the Executive to pause and reframe deliverables as required.

25. The Committee discussed the challenges in recruitment and the work undertaken by the Executive to improve operational resilience.

26. The Committee were provided with further information about how the Executive is preparing for the DPST.

27. Morounke Akingbola (MA) referred to the Operational Risk Register and asked if there were any questions or comments on these. The Committee noted these documents.

Item 9 – Change Programme [AUD 7/22)

28. Louise Dineley (LD) introduced the report and spoke of the challenges in Q3 which meant the Executive had to pause some work and reframe priorities. Additional resources had now been secured which allowed three commissions to be issued which will help with the delivery of data model aspects in Q4.

29. The Committee acknowledged the challenges but spoke of the importance of data modelling and the ability to identify and study any emerging trends.

30. LD informed the Committee that an annual report of the Development Programme would be drafted in Q4. This would not only look back at what had been achieved but also reframe the scope of the roadmap going forward with a clear strategic intent on how to proceed.

31. The Committee noted the report.

Item 10 – Cyber Security [AUD 8/22]

32. Louise Dineley (LD) introduced the report and provided key highlights. LD spoke of the operational issues which are dealt with daily and the ability to utilise NHS systems. LD highlighted that 100% of staff completed cyber security training in Q2. LD spoke about the actions taken to provide additional protection and how this will be rolled out to all HTA devices.

33. The Committee noted the enhanced report which provided the assurances they sought regarding managing this risk and asked that this report now be simplified for future reporting.

34. The Committee thanked the Executive their work on this important matter and offered congratulations for the staff training achievement.

Item 11 – Policies

35. Morounke Akingbola (MA) introduced this item and the various policies brought forward for the Committee's review.

36. **Anti-fraud, bribery, and corruption policy** [AUD 9/22]. MA informed the Committee that the proposal is that the review of this policy is amended to every

2 years, so the next review would be in 2024. The Committee discussed whether the was a need for an annual certification of the policy, the Executive provided assurance that all staff complete annual training on this subject. The Committee agreed the proposed changes and were supportive of this policy.

37. **Whistleblowing Policy and Procedure** [AUD 10/22]. MA informed the Committee that this policy had been updated to include section on malicious whistleblowing and a link to the bribery and corruption policy. The Committee were supportive on these changes in principle but asked the Executive to seek further assurance regarding the wording around malicious whistleblowing. Joanne Charlton offered advice and guidance on what is used within other regulator organisations.

Action 5: Joanne Charlton to provide advice and guidance on malicious whistleblowing and Executive to amend policy if directed by this advice.

38. **ARAC Handbook** [AUD 11/22]. The Committee discussed whether any further references and sources of information should be provided within the handbook as this is a useful tool for Committee members. The Committee were supportive of the ARAC Handbook.

39. **ARAC Terms of Reference** [AUD 12/22]. The Committee were supportive of the proposed changes and noted that the Executive would capture the title of the staff servicing the Committee in an appropriate way.

Action 6: Policies to be amended and distributed.

Item 12 – Gifts and Hospitality Register [AUD 13/22]

40. Morounke Akingbola introduced the report and drew the Committees attention to the two new entries since the last meeting. The Committee noted the report.

Item 13 – Reports on grievances, disputes, fraud, and other information

41. No reports of grievances were discussed.

42. There was nothing to report to the Committee under fraud or dispute.

Item 14 – Topics for future risk discussions

43. The Chair asked Committee members to identify topics for future risk discussions as part of their Committee Effectiveness Review.

44. The Chair asked the Executive to look at the possibility of arranging training on fraud awareness and management for members at the Autumn meeting.

Action 7: Executive to investigate training opportunities for the Autumn meeting.

Item 15 – Any other business [AUD 14/22, AUD 14a/22, AUD 14b/22 and AUD 14c/22]

45. Richard Sydee introduced the report and gave a brief overview of each item.

46. With regard to the PAC enquiry on Contingent Liabilities HTA has one listed Contingent Liability, relating to the Department underwriting any losses due to professional negligence on the part of the HTA, it's employees and other parties working on its behalf. Whilst not strictly a contingent liability from an HTA accounting perspective this risk remains, and as such the HTA responded confirming this to the Department. The Committee noted this report.

47. Regarding the assessment of the Impact of IFRS16 – Leases, the Committee noted how this will impact the HTA. The external auditors confirmed they were comfortable with the contents of this paper. The Committee noted this report.

48. The Committee noted the handover of the Accounting Officer Responsibility and the paperwork lodged with the Department. The Chief Executive gave assurances to the Committee on his responsibilities and the priorities he gives to his role as the Accounting Officer. The Committee noted this report.

49. The Chief Executive informed the Committee that he would be looking at the cycle and frequency of Board and ARAC Meetings.

50. The Chair thanked Dr Stuart Dollow for his active and ~~diligence~~ diligent participation as his term of appointment ends. The Committee and Executive also expressed their thanks and appreciation. The Committee noted that a new member would need to be appointed by the Board to both ARAC and RemCo.

Action 8: New member to be appointed to both ARAC And RemCo.

51. There being no further business the Chair thanked all for their participation and drew the meeting to a close.

Next Meeting 9 June 2022

AUD 16-22

HTA Audit and Risk Assurance Committee

Matters arising and forward plan

Thursday 9 June 2022

Meeting	Action	Responsibility	Due date	Progress to date	Status
1 February 2018	Action 1: Kevin Wellard to schedule critical incident exercises within the ARAC forward plan and Corporate Business Plan Tracker to occur at approximately 12-18 month intervals.	Director of Data, Technology and Development	June 2018	The members of ARAC will receive an update on this item under the matters arising item and item 12 of the agenda for the 19 June 2018 ARAC meeting. **To be discussed with revised policies on the agenda**	
27 January 2022	Action 6: Policies to be amended and distributed.	Head of Finance and Governance	June 2022	Advice re malicious whistle-blowing yet to be received. Policy amended to remove reference to malicious whistleblowing until advice received. Anti-Fraud policy updated and shared with staff	
27 January 2022	Action 7**:** Executive to investigate training opportunities for the Autumn meeting.	Director of Resources and Head of Finance and Governance	October 2022		Ongoing

Other work

Meeting	Work in Progress	Responsibility	Due date	Progress to date	Status

Risk exploration topics

Topic	Meeting date	Progress
Topics covered		
Outstanding Topics		
HTA continuous business planning arrangements for the triaging of business planning activity		
Media handling- Critical incident handling		
Risks posed by sectors and the HTA's approach to protect public confidence. **HA and PM sector already done**		**Sectors to be done** Research Public Display and Anatomy ODT
Executive to decide whether an examination of the data from the Professional Stakeholder Evaluation is an appropriate topic for an ARAC deep dive. **Action from July 2020 Board meeting**		

Future training	

Topic	**Meeting**	**Provider**	**Progress**	**Complete (Yes/No)**
Training complete				
Joint ARAC Member/Management Team training seminar – undertaking risk assurance mapping and interdependency across the wider health group	February 2017	Internal Auditor/Director of Resources	To focus on wider suggested best practice in accordance with the Risk Management Policy and Strategy and consideration of wider interdependence across the health group.	**Yes**
Value for money auditing and the optimal deployment of resources		NAO	NAO have been invited to host a training session on 18 May 2017.	**Yes**
A NAO perspective on the risks emerging within the health sector	February 2018	NAO Catherine Hepburn		**Yes**
Training and/or discussion on risk updates - ensuring Members gain assurance on how risks are recorded and managed.	June 2019	Jeremy Nolan, (GIAA)	At the ARAC meeting on 23 October, Members invited Jeremy Nolan to facilitate discussion on risk management and how Members can assure themselves that risks are being managed and recorded correctly.	**Yes**
IFRS training	January 2020	NAO	Training given at the end of the meeting	**Yes**
Outstanding training				
Observation and feedback from another ARAC Chair. Has been previously discussed. Do we wish to do this still				
Fraud Awareness		KPMG or AN Other	To be discussed Q1 2022/23	

Forward plan

Standing items	**Assurance reports from Internal Audit** **Audit recommendations tracker report** **Risk update includes strategic risk register review and update on UK transition** **Polices/procedures updates** **Cyber security**	**Meeting Specifics to be covered**
Meeting		
January 2022	Assurance reports from Internal Audit Audit recommendations tracker report Strategic risk register review Polices/procedures updates Anti-Fraud Policy (bi-annually) Whistleblowing Policy Schedule of policies	Review and approval of the Internal Audit proposed Audit plan for the financial year Hold confidential joint meeting with both sets of Auditors (agenda item at start or end of meeting)
June 2022 `	Audit recommendations tracker report Strategic risk register review Policies/procedures updates	Receive Internal Audit Annual Report Approval of the Annual Report and Accounts SIRO Report Review of the External Auditors ISA 260 report (management letter) Consider key messages for the Audit & Risk Assurance Committee's report on its activity and performance (to the Authority)
October 2022	Assurance reports from Internal Audit Audit recommendations tracker report Strategic risk register review Policies/procedures update	Approval of External audit's planning report Review of the Audit & Risk Assurance Committee's Governance including Handbook and Terms of Reference Operational Risk Register review (not standing agenda item)

Policy and Procedures reviewed by ARAC		**Frequency of review**
Expenses Policy HTA/POL/032	Policy covers reimbursement of Travel, Subsistence and other expenses	Annual
Reserves Policy HTA/POL/049	Policy states the minimum level of cash reserves that the HTA should ideally keep as a contingency	Annual
Antifraud Policy HTA/POL/050	Policy covers definitions of fraud, responsibilities of HTA employees	Annual
Whistle-blowing Policy HTA/POL/017	Policy covers procedure to be followed if they have concerns about improper behaviour	Annual
Declaration of Interest, Gifts and Hospitality Policy	Policy covers the procedure for receiving/declining gifts	Annual

Audit and Risk Assurance (ARAC) meeting

Date:	9 June 2022
Paper reference:	AUD 17/22
Agenda item:	5
Author:	Richard Sydee, Director of Resources

OFFICIAL

Risk Update

Purpose of paper

1. To provide ARAC with an update on HTA's strategic risks, and proposed mitigations as of May 2022.

Decision-making to date

2. This paper was approved by the Director of Resources on 26 May 2022.

Action required

3. ARAC Members are asked to:
   - Comment on the strategic risks and assurances within the HTA Strategic Risk Register attached to this paper at Annex A.
   - Note the Risk management policy at Annex B and the proposal that this be reviewed every 3 years; and,
   - Note the risk appetite statements within the policy and consider a recommendation to the Board for these to be reviewed.

Background

4. The strategic risks are reviewed annually by the SMT to ensure they align to the strategic objectives and deliverables agreed within the annual business plan. The risks are then reviewed monthly at SMT and the register is updated and stored. The strategic risk register that was discussed and updated at the beginning of May 2022 is at Annex A.

5. The executive team have reviewed the risk register for the 2022/23 business year and made a number of changes:

   - Most risk titles have been redrafted to better reflect the strategic impact the risk poses.
   - Risk 4 from the 2021/22 register has been revised and now focuses only on workforce and capability issues – with the IT risks now contained separately at Risk 7.
   - Risk 6 has been refocussed to consider the wider organisation transformation aims we have in relation to IT, Inspections process and ambitions to reshape some other functions

Risk assessment

6. **Risk 1 – Failure to regulate appropriately (8 – Medium, below tolerance).** Activity across most regulatory sectors has returned to normal, with the HTA approach to on site and virtual assessments aiming to achieve 210 inspections in the 2022/23 business year.

7. We continue to manage a small number of regulatory matters with establishments, but overall SMT believe this risk remains below tolerance.

8. **Risk 2 – Failure to manage the impact of an incident (9 – Medium, above tolerance).** The HTA believes that our incident management response plans have been effective and robust through the last business year whilst the HTA has managed a number of concurrent extraordinary operating conditions and activity in our regulated area.

9. SMT notes that our arrangements have stood up well and that current activity levels are still high, with some uncertainty on timing in some areas – we continue score this risk above tolerance as 9 - Medium.

10. **Risk 3 – Failure to manage expectations of regulation (9 – Medium, at tolerance).** SMT noted the number of matters currently impacting on the

organisation, and that these matters are all being actively managed. The HTA continues to have clear dialogue with the FII and is preparing in line with known timelines

11. At their May meeting SMT agreed this risk remains unchanged, at tolerance

12. **Risk 4 - Failure to deliver a diverse, capable workforce (8 - Medium, below tolerance).** This risk has been recast, with a narrower focus on the delivery of a diverse and capable workforce.

13. The risk has been scored as 8 – medium and is below a suggested tolerance level of 9, although the risk tolerance level for this risk has not been agreed with the Board

14. **Risk 5 – Insufficient, or ineffective, management of financial resources (9 – Medium, at tolerance).** The GIA funding from the Department has been confirmed and budgets have been amended to reflect additional funding in relation to FII. Delegation letters have been issued and initial forecast for income are in line with budgeted expectations. There are no immediate concerns regarding affordability for the 2022/23 business year, a number of activities in our portfolio pipeline will remain for consideration should funds be released elsewhere

15. **Risk 6 – Failure to achieve the benefits of the organisational transformation programme (6- Medium, at tolerance).** This risk has been restated to reflect revisions to the HTA's programme work and revised our delivery plans for the 2022/23 business year.

16. Proposals for a revised programme of work will be submitted for Board consideration in July 2022, this risk is therefore scored at tolerance until plans for delivery are agreed and commenced.

17. **Risk 7 – Failure to optimise the safe use of digital, data & technology (8 – Medium, below tolerance.** This risk relates to the IT elements of the previous risk 4 and has been separated and recast to provide more oversight of the increasing dependence on DDT for current and future operational success of the HTA

18. This risk was initially assessed as 8 - Medium and below an indicative tolerance level of 8, although the Board have yet to consider or agree risk tolerance of this area.

Risk Management Policy and risk appetite statements

19. The Committee are requested to note the Risk Management Policy which has not changed since it was last tabled and agree the proposed 3-year review period.

20. The Committee are also requested to note the Risk Appetite Statement(s) at pages 17 – 18 of the policy, changes to these statements require Board approval and it is good practice to review risk appetite annually, or an alternatively greed frequency to ensure consideration of any changes to our operating landscape

21. The Committee are invited to consider the statements as previously agreed by the board and make any recommendations for changes and review by the Board at their next appropriate meeting.

Latest review date – 19/05/22

Strategic risk register 2022/23
Risk summary: residual risks

Risk area	Strategy link*	Residual risk	Risk owner	Status	Trend**
R1: Failure to regulate appropriately	Delivery (a-d & f) and Development (a-d) objectives	**8 – Medium**	Director of Regulation	Below tolerance	⇔⇔⇔⇩
R2: Failure to manage an incident	Delivery, Development and Deployment objectives	**9 - Medium**	Director of Regulation	Above tolerance	⇧⇔⇔⇩
R3: Failure to manage expectations of regulation	Delivery e) and Development c)	**9 - Medium**	Director of Regulation	At tolerance	⇔⇔⇔⇔
R4: Failure to utilise our staff capabilities effectively	Delivery, Development and Deployment (a, c, and d)	**8 - Medium**	Director of Data, Technology and Development	Below tolerance	
R5: Insufficient or ineffective management of financial resources	Deployment (b) objective	**6 - Medium**	Director of Resources	Above tolerance	⇔⇔⇔⇔
R6: Failure to achieve the benefits of organisational transformation	Development (a-d) objectives	**9 - Medium**	Director of Data, Technology and Development	At tolerance	⇔⇔⇔⇔
R7: Failure to optimise the safe use of existing and available digital data and technology	Delivery (a-e), Development (a-d) Deployment (a, c and d)	**8 - Medium**	Director of Data, Technology and Development	Below tolerance	

* Strategic objectives 2021-2024:
** This column tracks the four most recent reviews by SMT (Senior Management Team) (e.g.⇧⇔⇩⇔).

AUD 17a/22

R1: There is a risk that we fail to regulate in a manner that maintains public safety and confidence and is appropriate.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
3	5	15 - High	**2**	**4**	**8 - Medium**
Tolerance threshold:					**10 - Medium**

Commentary

At tolerance.

We have a good regulatory framework, with moderate assurance on a recent internal audit on the Effectiveness of the Inspection Process in Quarter 4 2021/22 (final report issued 11 April 2022) and previously substantial assurance on an internal audit on key regulatory processes in Quarter 4 2018/19 (final report issued 16 April 2019). .

The HTA achieved slightly above its target of 140 inspections for 2021/22, through a combination of Virtual Regulatory Assessments, site visits inspections and hybrid approaches. With the lifting of all Covid restrictions and building on the desire to increase the coverage achieved by inspection, whilst focusing resource to risk,

We continue to use all other regulatory tools and processes, such as managing and responding to incident reports (Serious Adverse Events and Reactions and HTA Reportable Incidents), whistleblowing / informant information and ongoing engagement with our regulated sectors, with investigations and active regulatory action having continued. We continue to actively manage a small number of more unusual regulatory matters with establishments.

SMT believes this risk continues to be below tolerance in May 2022.

R2: There is a risk that we will be unable to manage an incident, event or issue impacting on the delivery of HTA objectives.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	5	20	**3**	**3**	**9 - Medium**
Tolerance threshold:					**6 - Medium**

Commentary
This risk concerns our ability to respond to incidents irrespective of their nature or cause, which could be from matters outside the HTA's remit or control as well as matters for which we are directly responsible. The Executive has therefore set a lower tolerance level on this risk as our ability to respond appropriately is within the HTA's control. The HTA believes that our incident management response plans have been well tested and found to be robust and effective through their deployment in several different circumstances over the past two years. These have included managing the impact of the pandemic and related restrictions and in their adaptation for use in managing the potential impacts of EU Exit following the end of the Transition Period. We also found these arrangements useful and effective in preparing for and managing our response to the public revelation of sexual offending in a mortuary through the trial of Fuller and subsequent actions from Quarter 3 of 2021/22 onwards. Having increased the risk scoring in July 2021, in anticipation of the prospective Fuller trial. we now believe that the likelihood of this risk materialising has reduced but given continuing uncertainties, we believe it is still above the tolerance level and has remained unchanged from the last review..

R3: There is a risk that we will fail to manage public and professional expectations of human tissue regulation in particular stemming from limitations in current legislation or misperception of HTA regulatory reach.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
3	4	12 - High	**3**	**3**	**9 – Medium**
Tolerance threshold:					**9 - Medium**

Commentary
At tolerance. We have no indications of any current specific factors that would contribute to this risk. The HTA continues to communicate our remit and advise where appropriate. The HTA is in ongoing dialogue with DHSC (Department of Health and Social Care) and wider stakeholders regarding Sir Jonathan Michael's Independent Inquiry into offending by Fuller and is currently preparing to submit further evidence to the Inquiry. The HTA is ensuring that clear media lines are prepared and shared with the public and the media when necessary. The HTA has an established Horizon Scanning process and is building its Policy function. The HTA is working with colleagues in the Northern Ireland Executive and NHSBT (NHS Blood and Transplant) to ensure there is effective implementation of the recent passing of the deemed consent for organ and tissue donation in Northern Ireland through changes to the Code of Practice F, Part 2. Whilst the recent amendment to s32 Human Tissue Act 2004 by the Health and Social Care Act 2022, to introduce an offence for 'organ tourism', is not expected to have any direct operational impact, the HTA alongside colleagues in DHSC, NHSBT and the health system, will ensure there is clarity over this for the public and practitioners. All these matters are being actively managed. SMT consider this risk remains unchanged and is, at tolerance.

R4: Failure to adequately deliver the diverse, capable workforce the HTA requires or needs to fulfil its functions and objectives

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	3	12 - High	**2**	**4**	**8 – Medium**
Tolerance threshold:					**9 - Medium**

Commentary
Above tolerance.   A significant amount of work was undertaken in 2021/22 to mitigate the risks associated with workforce. Actions included a partial organisational redesign, recruitment of fixed term contracts to a number of significant and standalone roles and the identification of additional skills required to support agreed activity.   The HTA has reframed this risk for 2022/23 to reflect wider workforce issues that need to be considered beyond numbers of staff and vacancies. As we reflect on the past year and look forward the HTA requires a range and changing set of skills, capabilities and capacity to fulfil its functions and objectives. The diversity of our workforce will be essential to ensure our approach to regulation remains responsive, proportionate and supportive to the sectors we regulate and the wider functions we deliver.

R5: There is a risk that the HTA has insufficient or ineffective management of its financial resources

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	5	20 – High	**3**	**2**	**6- Medium**
Tolerance threshold:					**3 - Low**

Commentary
Above tolerance. Budgets for 2022/23 have been agreed and delegation letters to Directors issued. Our Grant in Aid (GIA) funding from the Department has been confirmed at previous levels and we have been provided with cover for asset purchases (Capital DEL - £80k) and depreciation and amortisation costs (Ring Fenced RDEL). The Department have provided additional GIA funding for support in assisting the FII, for 2022/23 only we have been delegated and addition £195k. Invoicing for licence fees in the HA sector were issued in April 2022, this has increased our overall debtors' figure, but aged debt continues to fall. There are no emerging financial pressures, SMT will be reviewing the financial position monthly with formal quarterly reviews with each Directors feeding on to the portfolio management process to ensure more timely decisions to invest emerging underspends in areas identified in our activity pipeline. Activity is planned later in this business year to review the current assumptions in our fees model and ensure they reflects any changes in our approach regulation activity or focus. SMT have agreed that this risk is unchanged.

R6: Failure to identify opportunities and achieve the benefits of transformation and continual change to support modernisation and improvement of the HTA.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
3	3	9 – Medium	**3**	**3**	**9- Medium**
Tolerance threshold:					**9 - Medium**

Commentary
At tolerance. The Development Programme was adversely impacted in 2021/22 by the availability and commitment of resources (people and financial). In spite of an agile approach and incremental developments the deliverables at year end were not as had been intended. A review has been undertaken in Q1 2022/23 with the aim of reframing the approach to development, change and transformation. This review has included a restating of the case for change, the identification of internal and external drivers and the alignment with the strategic direction of the HTA. A revised programme will be presented to SMT for agreement and reporting to the Board in July. The risk is at tolerance as plans for delivery are implemented.

R7: Failure to optimise the safe use of existing and available digital data and technology

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	3	12 – High	**4**	**2**	**8 - Medium**
Tolerance threshold:					**9 - Medium**

Commentary
Over the last 2 years the HTA has been progressing with the planned development of its digital data and technology (systems and architecture) as part of the Development Programme. The planned development had been incremental based on available resources and aimed to future proof business needs. The planned developments also sought to mitigate areas of potential and actual risk that have been the result of limited financial investment and build resilience into systems through compatible design. The failure to maintain investments into the development systems, architecture and supporting resources is a current risk which if left will increase. Work is underway to explore alternative models for service and resource provision and the capabilities to support the development of HTA IT systems as required. In spite of the risk is currently stable, action is required to reduce the increase in tech debt.

Reviews and revisions

(23/02/22) SMT review March 2022

Risks 1,2 and 4 were discussed in detail. SMT agreed that the impact score of risk 1 should be reduced as the tools in place continue to work; risk 2 likelihood score was also adjusted down; and risk 4 likelihood has been reduced from 3 to 2 reducing overall rating to 8 as key posts have been recruited to.

(19/05/22) SMT review April/May 2022

The SMT reviewed the current register in light of the finalised business plan and agreed the following:

- Risk 2 to be shortened in the summary leaving the detail to remain in the register itself;
- Risk 4 it was agreed to separate this risk into a people risk (risk4) and a digital risk (risk 7) which is more reflective of the current situation;
- Risk 6 it was agreed to re-framed to reflect the fact that it is broader than just the Development programme.

Strategic Aims

Delivery: Deliver a right touch programme of licensing, inspection, and incident reporting, targeting our resources where there is most risk to public confidence and patient safety.
(a) Deliver effective regulation of living donation.
(b) Provide high quality advice and guidance in a timely way to support professionals, Government, and the public in matters within our remit.
(c) Be consistent and transparent in our decision-making and regulatory action, supporting those licence holders who are committed to achieving high quality and dealing firmly and fairly with those who   do not comply with our standards.
(d) Inform and involve people with a professional or personal interest in the areas we regulate in matters that are important to them and influence them in matters that are important to us.

Development: • Use data and information to provide real-time analysis, giving us a more responsive, sharper focus for our regulatory work and allowing us to target resources effectively.
(a) Make continuous improvements to systems and processes to minimise waste or duplicated effort, or address areas of risk.
(b) Provide an agile response to innovation and change in the sectors we regulate, making it clear how to comply with new and existing regulatory requirements.
(c) Begin work on implementing a future operating model, which builds our agility, resilience, and sustainability as an organisation.

Deployment: Manage and develop our people in line with the HTA's People Strategy
(a) Ensure the continued financial viability of the HTA while charging fair and transparent licence fees and providing value for money
• Provide a suitable working environment and effective business technology, with due regard for data protection and information security
• Begin work on implementing a future operating model, which builds our agility, resilience, and sustainability as an organisation

AUD 17a/22

Criteria for inclusion of risks

Whether the risk results in a potentially serious impact on delivery of the HTA's strategy or purpose.

Whether it is possible for the HTA to do anything to control the risk (so external risks such as weather events are not included).

Rank

The risk summary is arranged in risk order.

Risk scoring system

We use the five-point rating system when assigning a rating to the likelihood and impact of individual risks:

Likelihood:	1=Rare	2=Unlikely	3=Possible	4=Likely	5=Almost certain
Impact:	1=Very low	2=Low	3=Medium	4=High	5=Very High

IMPACT	Risk Scoring Matrix					
	5. Very High	5 Medium	10 Medium	15 High	20 Very High	25 Very High
	4. High	4 Low	8 Medium	12 High	16 High	20 Very High
	3. Medium	3 Low	6 Medium	9 Medium	12 High	15 High
	2. Low	2 Very Low	4 Low	6 Medium	8 Medium	10 Medium
	1.Very Low	1 Very Low	2 Very Low	3 Low	4 Low	5 Medium
Likelihood						
Risk score = Impact x Likelihood		**1.Rare (≤3%)**	**2.Unlikely (3%-10%)**	**3.Possible (10%-50%)**	**4.Likely (50%-90%)**	**5.Almost certain (≥90%)**

Risk appetite and tolerance

Risk appetite and tolerance are two different but related terms. We define risk appetite as the willingness of the HTA to take risk. As a regulator, our risk appetite will be naturally conservative and for most of our history this has been low. Risk appetite is a general statement of the organisation's overall attitude to risk and is unlikely to change unless the organisation's role or environment changes dramatically.

Risk tolerances are the boundaries for risk taking. The risk appetite statement informs the development of risk tolerances for the HTA and provides guidance on how the risk appetite statement is to be applied in everyday business activities and decisions.

Assessing inherent risk

Inherent risk is usually defined as ‘the exposure arising from a specific risk before any action has been taken to manage it.’ This can be taken to mean ‘if no controls at all are in place.’ However, in reality the very existence of an organisational infrastructure and associated general functions, systems and processes introduces some element of control, even if no other mitigating action were ever taken, and even with no risks in mind. Therefore, for our estimation of inherent risk to be meaningful, we define inherent risk as:

‘the exposure arising from a specific risk before any additional action has been taken to manage it, over and above pre-existing ongoing organisational systems and processes.’

Contingency actions

When putting mitigations in place to ensure that the risk stays within the established tolerance threshold, the organisation must achieve balance between the costs and resources involved in limiting the risk, compared to the cost of the risk translating into an issue. In some circumstances it may be possible to have contingency plans in case mitigations fail, or, if a risk goes over tolerance, it may be necessary to consider additional controls.

When a risk exceeds its tolerance threshold, or when the risk translates into a live issue, we will discuss and agree further mitigations to be taken in the form of an action plan. This should be done at the relevant managerial level and may be escalated if appropriate.

AUD 17b-22 Annex B ARAC NEW - HTA Strategic Risk Register 2022-23 - May 2022

REF	RISK/RISK OWNER	CAUSE AND EFFECTS	INHERENT		PROXIMITY	EXISTING CONTROLS/MITIGATIONS	RESIDUAL		ACTIONS TO IMPROVE MITIGATION	Risk Tolerance	LINE OF DEFENCE			TYPE OF CONTROL	ASSURANCE OVER CONTROL	ASSURED POSITION
			I	L			I	L			1	2	3			
1	***Failure to regulate in a manner that maintains public safety and confidence and is appropriate*** ***(Risk to Delivery objectives a-d & f Development objectives a-d)*** *Risk Owner:* ***Nicky Harrison***	***Causes*** • *Failure to identify regulatory non-compliance* • *Regulation is not transparent, accountable, proportionate, consistent and targeted* • *Regulation is not sufficiently agile to respond to changes in sectors* • *Insufficient capacity and/or capability, including insufficient expertise, due to staff attrition, inadequate contingency planning, difficulty in recruiting (including Independent Assessors (IAs)).* • *Inadequate adherence to agreed policies and procedures in particular in relation to decision making* • *Poor quality or out of date policies and procedures* • *Failure to identify new and emerging issues within HTA remit* • *Failure to properly account for Better Regulation* • *Insufficient funding in regulated sectors* • *Failure to deal with regulatory consequences of the Transition Period and the period after 31 December 2020.* • *Failure to properly manage the business impact of the coronavirus pandemic.* ***Effects*** • *Loss of public confidence* • *Compromises to patient safety* • *Loss of respect from regulated sectors potentially leading to challenge to decisions and non-compliance* • *Reputational damage*	5	3	*Ongoing*	**Regulatory model**	4	2		10						
						Regulatory model comprising a mixture of proactive regulatory assessment (e.g. through site visit inspections and sector engagement) and reactive tools (such as responding to incidents reported to the HTA, investigations of concerns raised etc). Process for consideration of police referral maintained and used. Annual collection of activity data in HA sector; biennial collection of compliance updates data from other sectors.			Following the suspension of routine site visit inspections at the onset of Covid-19 pandemic restrictions, work was undertaken in 2020/21 to develop a risk assessment and a virtual regulatory assessment tool. VRAs are now incorporated into business alongside a decision making framework to inform decisions about whether to undertake a site visit, VRA or hybrid inspection. Development Programme-led activity from 2020/21 to develop a new Target Operating Model to re-state and clarify the key elements in our approach to regulation. A full inspection timetable has been implemented from quarter 3 of the 21/22 business year.		X			Preventative	Board developed and approved the current HTA Strategy and was aware of the risks and opportunities associated with the suspension of routine site visit inspections during Covid restrictions and how VRAs were being incorporated into BAU. Board were aware of the issue of failing to meet the legal obligation to carry out a site visit of HA establishments at least once every two years because of the suspension of routine site visits during Covid. SMT agreed late May 2021 to resumption of routine site visits in HA sector once restrictions are lifted, alongside continuing use of VRAs. Routine site visit elements are now being included in HA inspections, although some are VRA only, determined on a risk-based approach. Continuing use of all other regulatory tools during the pandemic restrictions, including managing HTARIs and SAEARs, investigations, advice to regulated sectors (such as seminars in Anatomy sector, Professional Newsletters). Development and use of emergency mortuary licensing	In-depth evaluation of pilot programme of 10 x virtual regulatory assessments in the HA sector in quarter three 2020/21 carried out and reported to the HTA Board Meeting February 2021 and a further evaluation of the expansion into remaining sectors in summer 2021. VRAs incorporated into BAU in all sectors, as evidenced in Business Plan and inspection schedule. Internal Audit late Quarter 3 / early Quarter 4 2020/21 on 'Inspection Process during Covid-19' - report agreed late May 2021; Moderate assurance; considered by ARAC; all actions now complete (per ARAC Quarter 3 2021). Renewal of some emergency mortuary licences although most have now been revoked as no longer required. SMT consideration of request by UKHSA to extend the small number of Funeral Director removal licences (for post-mortem public health surveillance for Covid-19) agreed on basis of bringing them into a normal regulatory regime i.e. LAAV, open-ended licences funded by appropriate fees. (Head of Regulation written to UKHSA Project Lead 21 Dec. 2021.) Police referral made late 2019/20 has been investigated by the police, supporting Witness Statements provided by the HTA, decision pending with CPS.
						Regulatory decision making framework			Heads of Regulation using dashboards to track open cases and ensure there is effective follow-up, in accordance with the HTA's decision-making framework.		X			Preventative	Reports summarising numbers of Regulatory Decision Meetings included in monthly performance pack and recorded in CRM. Case Review Meetings all summarised in CRM.	Satisfactory Internal Audit Report (strong assurance) November 2020. Lessons learned from Regulatory Decision Meetings (RDMs) held January 2020 and used to inform update to Regulatory Decision Making SOP. Regulatory Decision Making SOP updated February 2020. Evidence of regulatory decision making framework being used in practice e.g. Case Review Meetings recorded in CRM, numbers of RDMs reported in monthly performance
						Annual scheduled review of Strategy					X	X		Preventative	Outputs from annual strategy review translate into revised annual Strategy	Annual Board Strategy session held 27 April 2021 informed annual strategy refresh. Latest update of HTA Strategy published November 2021.
						The HTA has produced a detailed business plan for the remainder of the year. These plans are approved by SMT and balance core regulatory functions, development priorities and resource deployment considerations.			In the continuing absence of a role with specific responsibility for the business plan, SMT and their respective Heads have ensured there is regular review and updating of the operational business plan and monthly performance pack. Consultancy-led review developed a portfolio management approach that SMT could adopt, including some initial tools.		X	X		Preventative	Operational business plan for 2021/22 (using Excel spreadsheet template developed in 2020/21) in use and reviewed regularly by SMT. Contractors engaged Quarter 1 2021/22 to support development of business planning through adoption of a portfolio management approach. 2020/21 narrative Business Plan for 2021/22 published during Quarter 3 (Covid-related delay).	Progress on the Portfolio Management approach regularly discussed at SMT meetings. SMT receives monthly reports of Management Information for review and action. Interim Portfolio Planning Manager appointed December 2021.
						Well established processes support our core regulatory business.			Development and introduction of new regulatory process (VRA) managed as a project with Director of Regulation as SRO, Head of Regulation (for Research and Anatomy) as Deputy SRO, and a RM as Project Manager. Project now in process of closure with formal closure report to be discussed by SMT in January 2022. Post-closure actions are in hand. (December 2021.) Detailed evaluation carried out on two occasions, prior to adoption in HA sector and expansion into other sectors. Completion of further management actions identified by Internal Audit of effectiveness of the inspection process -				X	Detective	Internal audit conducted on Key Regulatory Processes late 2018/19, receiving substantial assurance and noting good areas of best practice. Internal audit on the Inspection Process during Covid-19 conducted late 2020/21 - see R4. Moderate assurance and management actions complete, as noted by ARAC Quarter 3 2021.	Internal Audit 2019: Final report received April 2019 and showed substantial assurance. The two low priority recommendations were followed-up with management actions completed during 2019/20, namely review of SOPs for key regulatory processes (completed) and training on core legislative framework, HT Act which was delivered in March 2020. Internal Audit 2021: low priority actions all complete by Autumn 2021.
						Quality management systems										
						HTA quality management system contains decision making framework, policies and Standard Operating Procedures to achieve adherence to the regulatory model			The HTA's Quality Manager left in 2019/20 and has not been replaced. This function has not been formally re-allocated. A Regulation Manager with experience in QMS continues to coordinate activities to ensure policies are reviewed and updated, with input and support from the Quality Forum as relevant.		X			Preventative/ Monitoring	Management oversight and reporting trough the monthly performance pack. This work had been expected to transfer to a newly created role during Quarter 2 2021/22 but this has not happened, hence the RM is still coordinating this work.	Limitations in QMS still remain. Scheduled reviews have now been re-instated by the RM who is covering this work following the departure of the quality manager in 2020/21. QMS and monthly performance reporting pack includes evidence of degree to which the documents are current.
						People										
						Adherence to the HTA People Strategy which has been substantially amended and approved by the Board					X			Preventative	Management information and assessment presented to the Board quarterly.	Chief Executive's report to the Board now includes HR report - last presented to November 2021 meeting.
						Training and development of professional competence					X			Preventative	Annual PDPs, which include Development Objectives, Corporate Training Programme (led by Head of HR), Career Investment Scheme proposals to SMT, induction programme for new entrants, with a bespoke programme for RMs.	Evidence of corporate training programme, including quarterly mandatory training. Quarterly Regulation-led Training sessions held virtually in July 2021, September 2021 and scheduled for January 2022. 'Lunch and Learn' programme.
						Specialist expertise identified at recruitment to ensure we maintain a broad range of knowledge across all sectors and in developing areas			As vacancies arise, SMT take the opportunity to review business requirements and target building capability and filling skills gaps. An organisational redesign for aspects of the HTA's work was developed during late 2020/21 to enable key gaps and capability issues to be addressed and a large-scale		X	X		Preventative/ Monitoring	SMT assessment of skills requirements and gaps as vacancies occur. Organisational design. Recruitment policy.	Staffing levels and risks reported quarterly to the Board most recently July 2021. Large recruitment programme for 10 vacancies started May 2021, incorporating the new roles created by the organisational redesign of key support functions and search for key additional capability identified as required in the RM cadre. Recruitment policy reviewed by SMT May 2021 to be completed by autumn 2021.
						EU Exit (End of Transition period and HTA Exit SIs 'grace period')										
						Fortnightly Transition Period oversight meetings from February 2020 with+H4:Q16+H4:Q15 Close liaison with DHSC to ensure communications are in line with government policy and that appropriate arrangements are made to support DHSC and stakeholders during the transition period. HA Guide, ODT Framework and other external guidance being updated in line with new legislation to ensure we can regulate accordingly.			Weekly project meetings from Quarter 3 2020/21. Dedicated project manager (external contractor) and Regulation Directorate and comms team resource. Weekly Project Governance meetings from mid-January 2021 (after daily / thrice weekly stand-ups ceased). Continued close liaison with DHSC policy and communications teams and EU Exit and Trade teams, including participation in DHSC-led meetings with ALBs. Project maintaining active oversight of risks, issues, and resource requirements.		X	X		Preventive / Detective / Monitoring	Weekly reporting by ANH to SMT under standing item on SMT agenda. Internal Audit Quarter 3 of 2020/21 - moderate assurance. SMT lead for project - ANH (Director of Regulation). Formal project re-established from Quarter 3 2020/21. SMT papers for key decisions.	EU Exit - dedicated project manager (contractor) appointed Quarter 3 2020/21 until 31 July 2021. (Project due to be closed and handed over to business as usual by 31 July 2021.) EU Exit / UK Transition Project documentation and records in Teams Channel. Internal Audit on Risk focusing on EU Exit - reported January 2021, moderate assurance, completion of management actions tracked in audit tracker by ARAC. Standing item on SMT weekly minutes - EU Exit update - reported in minutes.
									Regulatory model							
									Development work being undertaken to become a more data-driven risk based regulator as part of the HTA		X			Preventative		
									Other							
									Strengthening horizon scanning arrangements		X			Preventative		

REF	RISK/RISK OWNER	CAUSE AND EFFECTS	INHERENT		PROXIMITY	EXISTING CONTROLS/MITIGATIONS	RESIDUAL		ACTIONS TO IMPROVE MITIGATION	Risk Tolerance	LINE OF DEFENCE			TYPE OF CONTROL	ASSURANCE OVER CONTROL	ASSURED POSITION
			I	L			I	L								
2	19/5/22 amended wording ***Inability to manage an incident, event or issue impacting on the delivery of HTA objectives.*** ***This might be an incident:*** • ***relating to an activity we regulate (such as retention of tissue or serious injury or death to a person resulting from a treatment involving processes regulated by the HTA)*** • ***caused by deficiency in the HTA's regulation or operation*** • ***where we need to regulate, such as with emergency mortuaries*** • ***that causes business continuity issues*** ***(Risk to all Delivery Development and Deployment objectives)*** *Risk owner:* ***Nicky Harrison***	***<u>Cause</u>*** • *Insufficient capacity and/or capability (for instance, staff availability, multiple incidents or ineffective knowledge management)* • *Failure to recognise the potential risk caused by an incident (for instance poor decision making, lack of understanding of sector, poor horizon scanning)* • *Failure to work effectively with partners/other organisations* • *Breach of data security* • *IT failure or attack incident affecting access to HTA office* • *External factors such as terrorist incident, large scale infrastructure failure or pandemic* ***<u>Effect</u>*** • *Loss of public confidence* • *Reputational damage* • *Legal action against the HTA* • *Intervention by sponsor*	***5***	***4***	*Future but increased likelihood over next few months*	Critical incident response plan, SOPs and guidance in place, regularly reviewed, including by annual training, and communicated to staff	**3**	**3**		**6**	X	X		Preventative	Policies etc. reviewed annually, training specification and notes after incident reviews	Subject to internal audit reported to ARAC in February 2020 Version 19 of CIRP published July 2019. CIRP deployed in March 2020 to manage coronavirus pandemic. CIRP used as framework for managing Sandpiper critical incident. Business Continuity and Critical Incident Response Plans updated and approved by SMT on 10 June 2021.
						All specific roles identified in the Critical Incident Response Plan are filled.					1 X	2	3	Preventative	Evidence of regular review and updating of the CIRP and no specific CIRP roles left vacant or, if role is vacant, cover arrangements put in place.	CIRP reviewed and updated to version 19 in July 2019. Further minor changes proposed February 2020 updated roles following staff changes. Business Continuity and Critical Incident Response Plans updated and approved by SMT on 10 June 2021.
						Media handling policy and guidance in place and Critical Incident Response Plan includes requirement to involve Comms team. Comms Team have embedded media handling and development of lines to take into business as usual.			Comms Team maintain close working relationships with colleagues across the business and proactively raise awareness of the need for Comms role in shaping lines and dealing with media. Experience of engaging and managing a contract with Crisis comms consultants to support the HTA on a specific critical incident.		X			Preventative	Policy reviewed as scheduled. Reports on any key media issues and activity in the Chief Executive's Report. Evidence of active Comms Team participation in issues with potential for media or public interest.	Media issues are included in the quarterly Board reporting as they arise and as relevant. Media enquiries successfully managed during critical incident phase of Sandpiper.
						Availability of legal advice					X			Preventative	Lawyers specified in Critical Incident Response Plan, SMT updates	In place
						Fit for purpose Police Referrals Policy			Engagement with other potential investigatory authorities, such as NHS Counter Fraud Authority		X			Preventative	Annual review of policy (minimum), usage recorded in SMT minutes	Police referral process used regularly by SMT and captured in SMT minutes. Police referral process shown to have been effective in 2020/21 with a referral to police for a potential breach of the HT Act being taken forward in an active investigation. Police referral policy being updated - considered by the Board November 2021 and on the agenda for finalisation February 2022.
						Onward delegation scheme and decision making framework agreed by the Board					X	X		Preventative	Standing Orders and Board minutes	Standing Orders published May 2017, updated at Board meeting in November 2021.
						Regulatory decision making framework			Regulatory Decision Making process and SOP regularly reviewed and disseminated to staff.		X			Preventative	Reports to Board of key decisions in Chief Executive's Report to the Board.	Number of Regulatory Decision Meetings detailed in monthly management performance pack, for review by SMT. Regulatory Decision Making SOP reviewed and updated March 2020 with the next review due by March 2022.
						IT security controls and information risk management					X	X		All	SIRO annual review and report Internal audit reports	Cyber security review - standing agenda item at ARAC - last discussed June 2020. Cyber Security has been a standing agenda item in the form of a dashboard report at each ARAC meeting.
						Critical incident response plan regularly reviewed and tested			Actions associated with the internal audit reported in February 2020.		X	X		Preventative	Critical Incident Response Plan and notes of test, reported to SMT Use of CIRP reported to SMT.	CIRP used to manage response to coronavirus pandemic from March 2020. CIRP deployed for a short period in May / June 2021 to deal with confidential matter. CIRP used as basis for Sandpiper response planning in Autumn 2021.
						Evaluate test exercise of incident and feedback to all staff.			Question over whether a test of the Plan is required in light of the recent stress test presented by the coronavirus pandemic and more recently in the HTA's response to Sandpiper, managed as a critical incident.		X			Preventative	SMT content that activation and use of CIRP during first wave and first lockdown superseded the need for a test. SMT note CIRP framework used in managing the HTA's planning for and response to the critical incident arising from the police investigation codenamed 'Sandpiper'.	Noted in ARAC Audit Tracker.
						Ensure DIs (or equivalent in ODT sector) are aware of and follow the incident reporting procedure for incidents reportable to the HTA.			Awareness raised of PM sector reporting requirement (HTARIs) at external training events, e.g. 9 April 2021 - Level 3 Diploma (Anatomical Pathology Technology) trainee APT HTA lecture, 18 September 2020 - Level 3 Diploma (Anatomical Pathology Technology) trainee APT HTA lecture Quarterly meeting with NHSBT to review ODT SAEARs cases over 90 days and any complex cases. Publication of quarterly incident numbers in the professional e-newsletter may remind establishments to report. HTA website COVID-19 guidance emphasises that all licensed research and anatomy establishments should have an internal system for reporting adverse events and asked them to consider how best to handle adverse events during the pandemic.		X			Preventative / Detective / Monitoring	Inspections (and audits for ODT) include assessment of licensed establishments' knowledge and use of the relevant HTA incident reporting process. For example, as part of the current VRAs in the HA sector, we are specifically looking at each establishment's incident logs to check a) that they recoding incidents locally, and b) that incidents that should have been reported as SAEARs, were. Annual SARE (Serious Adverse Reactions and Events) HA SAEARs data reported to European Directorate for the Quality of Medicines (EDQM). Monitoring establishments' reporting of incidents through the HTARI, HA SAEARs and ODT SAEARs groups and advice, guidance and CAPAs regarding those incidents.	Findings at inspection (onsite or VRAs). Minutes of quarterly meeting with NHSBT to review SAEARs cases in ODT sector - latest meeting was December 2021. Most recent SARE report submitted summer 2021. Publication of closed SAEAR and HTARI incident summaries included in the HTA publication scheme - published quarterly - and reporting in the Board's data annex. Publication of incident numbers in the regular (bimonthly) Professional Newsletter.
						Management of any risk of incidents likely to arise from the end of the 6 months post-Transition Period grace period for EEA/GB import / export licensing continues to be managed through the defined UK Transition project. The Director of Regulation is SRO, with a dedicated project manager and project resource and close continuing engagement with DHSC.			Continuing engagement with DHSC on ongoing aspects of the UK Transition Period Project, including the Northern Ireland Protocol (and engagement with NI Executive Department of Health).					Preventative / Detective / Monitoring	Director-level oversight as SRO (Director of Regulation), weekly Project meetings, 'stand-up' over the 6 weeks either side of 31/12/20, regular reporting to SMT through standing agenda item and specific papers for key decisions.	Regular reports to SMT - standing item on SMT agenda from February 2020. Internal Audit 2019/20 (Moderate assurance and management actions completed by Autumn 2021). Project formally closed October 2021 and remaining actions handed over to business. Pending clarification of whether any further changes might arise from any changes to the Northern Ireland Protocol.

REF	RISK/RISK OWNER	CAUSE AND EFFECTS	INHERENT RISK		PROXIMITY	EXISTING CONTROLS/MITIGATIONS	RESIDUAL RISK		ACTIONS TO IMPROVE MITIGATION	Risk Tolerance	LINE OF DEFENCE			TYPE OF CONTROL	ASSURANCE OVER CONTROL	ASSURED POSITION
			I	L			I	L			1	2	3			
3	***Failure to manage public and professional expectations of human tissue regulation in particular stemming from limitations in current legislation or misperception of HTA regulatory reach*** ***(Risk to Delivery objective e, and Development c)*** *Risk Owner:* ***Nicky Harrison***	***Cause*** ***External factors*** • *No scheduled review of Human Tissue Act and associated regulations, or Quality and Safety Regulations (other than for EU Exit)* • *Rapidly advancing life sciences* • *Potential move away from the UK as base for some regulated establishments/sectors due to EU Exit and changes in exchange rates* • *Introduction of deemed consent for Organ donation in England* • *Uncertainty posed by EU Exit, and misperceptions stemming from a 'no-deal' scenario* ***Matters which certain stakeholder groups believe require review*** • *Scope of relevant material e.g. waste products* • *Licensing requirements e.g. transplantation research* • *Regulation relating to child bone marrow donors* • *Issues raised by emergence of social media e.g. non-related donors* • *Strengthening of civil sanctions for non-compliance* ***Matters which stakeholders/public may expect to be inside regulatory scope*** • *Efficacy of clinical treatment from banked tissue and treatments carried out in a single surgical procedure* • *Police holdings* • *Products of conception and fetal remains* • *Data generated from human tissue* • *Funeral directors* • *Forensic research facilities* • *Cryonics* • *Body stores / Taphonomy* • *Imported material* • *Clinical waste* • ***Other*** • *Inadequate stakeholder management* ***Effect*** • *Diminished professional confidence in the adequacy of the legislation* • *Reduced public confidence in regulation of matters relating to human tissue* • *Reputational damage*	*4*	*3*	*Ongoing*	Horizon scanning process in place that creates and maintains an up to date log of issues known to the HTA with respect to the legislation (updates, amendments or emerging issues) to inform DH and manage messages	***3***	***3***		**9**		*X*		*Monitoring*	*Ongoing log*	*Log in place and shared with Board in outline at the Strategic planning session in 2021.*
						Active management of professional stakeholders through a variety of channels including advice about relevant materials in and out of scope			*Comms & Engagement strategy under development to strengthen the HTA's approach and impact of stakeholder engagement. Updated C&E Strategy planned for Q4.*		*X*			*Preventative/ Detective*	*Stakeholder Group meeting minutes* *Authority minutes (including Public Authority Meeting)* *TAG and HWG meetings* *Evidence of engagement with other relevant stakeholder forums, not necessarily organised by HTA.*	*Last Stakeholder and Fees Group meeting in October 2019; Histopathology Working Group February 2020; Transplant Advisory Group October 2019.* *Public Authority Meeting in July 2021 - held virtually.* *Professional newsletters issued regularly - last one September 2021.* *Sector-specific engagement e.g. with anatomy sector webinars and engagement with the post-mortem sector through multi-agency forums (Death Investigation Group, Excess Deaths Working Group).*
						Active management of issues raised by the media – including the development of the HTA position on issues			*Lines currently under review and update*		*X*			*Preventative/ Detective*	*Quarterly reports to Board on communication (including media) activities*	*Last report to November Board meeting (2021).*
						Regular reporting to DHSC sponsorship and policy team on matters which risk public and professional confidence						*X*		*Monitoring*	*Quarterly Accountability meetings with DH superseded during the pandemic by DHSC attendance at Board meetings for assurance plus DHSC sponsor team's engagement with HTA.*	*Most recent confirmation in letter from Marina Pappa of DHSC Sponsorship Team to AMS dated 21 July 2021 re Quarter 1 2021/22. AMS met with Sponsorship team regularly during 2021.*
						Action where we believe it will support public confidence					*X*			*Preventative*	*Updated guidance in response to the coronavirus emergency published on the website further sector specific guidance*	Update to the Board and DHSC at Board meeting July 2021.
						Clear view of use of s.15 duty to report issues directly to Ministers in England, Wales and Northern Ireland as new issues emerge			*Demonstrate ongoing engagement of Devolved Assembly in Wales and N Ireland. Effective engagement and collaboration demonstrated through the revision of Code D.*		*X*			*Preventative*	*Duty and its uses understood by SMT and Chair*	*Advice and guidance continues to be provided, for example on the Private Members Bill - Organ Tourism and Cadavers on Display, first introduced into Parliament in 2020 and reintroduced in 2021.* *Engagement with DHSC over Sandpiper issues - advice submitted to Secretary of State 15 December 2021. Also engagement with Welsh Government officials on this matter.* *Ongoing engagement with NI Executive over NI Deemed Consent and need for HTA to update its Code of Practice (F) in recognition of this.*
						No further changes to HTA's Standards since significant changes launched April 2017. Significant activity to update Codes of Practice for Organ Donation and Transplantation (and consent) to support the introduction of deemed consent (May 2020).			Further work planned in 2021/22 to review and update codes of practice . Focus will be on factual update.		*X*			*Preventative*	*Updated draft guidance produced for revised Code D.* *Updated draft of Codes of Practice D to enhance consent expectations for imported bodies and body parts for public display.*	*Draft revised Code of Practice D (Public Display) to align consent expectations for imported bodies and body parts with those for material originating in England, Wales and Northern Ireland received Parliamentary approval in July 2021.*
						Extensive Professional Evaluation Survey undertaken in Q4 2019/20, reported to Board in July 2020 and used to inform further developments.			Further work planned in Q3 & 4 to pilot new approaches to stakeholder engagement		*X*			*Preventative*	*Evidence from Professional Evaluation used as an evidence and information source to inform and drive improvements*	*Evidence from Professional Evaluation presented to the Board in July 2019.*
						Communications work package set up as part of UK Transition project to ensure we are managing our licensed establishments' expectations of what is required at the end of the transition period. As part of this WP we will also attempt to reach out to unknown end users to make them aware of their new regulatory licensing requirements and timelines.			UK Transition Communications Plan updated several times during the life of the project. RM taking responsibility for leading stakeholder engagement and coordinating activities of RM Stakeholder Managers.					*Preventative*	Weekly UK Transition Project meetings - standard agenda item is discussion of Communications Work Package.	UK Transition project documents (in dedicated Teams channel), weekly meeting agendas and action points plus weekly updates to SMT. UK Transition project closed October 2021.
						Regular meetings with DHSC policy team and attendance at other departmental meetings (ALB delivery partners) to inform planning for key pressures such as ongoing response to Covid-19; winter pressures, Transition Period and the period after 31 December 2020. In the last 6 months the HTA has demonstrated its role in strategic and partnership working as part of the wider Life Sciences & regulatory system and has demonstrated a responsiveness to legislative amendments and updates.			*Ongoing engagement with partner organisations to build opportunities for collaboration and support to the life sciences sector.*		*x*			*Preventative*	*Development programme workstream Strengthening of Horizon scanning has identified 4 areas to progress in 2021/22.*	*Regular reporting to SMT and through formal routes*

REF	RISK/RISK OWNER	CAUSE AND EFFECTS	INHERENT		PROXIMITY	EXISTING CONTROLS/MITIGATIONS	RESIDUAL		ACTIONS TO IMPROVE MITIGATION	Risk Tolerance	LINE OF DEFENCE			TYPE OF CONTROL	ASSURANCE OVER CONTROL	ASSURED POSITION
			I	L			I	L								
4	19/5/22 amend to reflect People only ***Failure to adequately deliver a diverse, capable workforce the HTA requires or needs to fulfil its functions and objectives*** ~~***Failure to utilise people, data and business technology capabilities effectively***~~ ***(Risk to Delivery objectives a-e, Development a-d Deployment a, c and d)*** *Risk Owner:* ***Louise Dineley***	• ***Cause*** *Lack of knowledge about individuals' expertise* • *Poor job and organisational design resulting in skills being under used* • *Poor line management practices* • *Poor project management practices* • *Poor leadership from SMT and Head* • *Loss of productivity as a result of the effects of changes to ways of working* • *Lack of ring-fenced resource for 'no-deal' EU Exit* ***Effect*** • *Poor deployment of staff leading to inefficient working* • *Disaffected staff* • *Increased turnover leading to loss of staff* • *Inadequate balance between serving Delivery and Development objectives*	*3*	*4*		***People capability***	*4*	*2*	*All major projects have project management rigour further enhanced through benefits realisation and plans to assess ROI at year end.*	**9**	***1***	***2***	***3***			
						People Strategy for the period 2019 to 2021 is in effect			Recruitment to identified vacancies and skills gaps ongoing. Succession planning and future skills needs to be developed further as part of a workforce model. Work planned for Q2 & 3.		***X***	***X***		*Preventative/ Monitoring*	*Board approval of the Strategy*	*Board approved the Strategy at its meeting in February 2019 and is provided with regular updates on all facets of its progress in quarterly board reporting. Most recently in July 2021*
						Full suite of people policies and procedures (including performance management)			*Review of processes and procedures required to ensure these are appropriately supporting and enabling adherence to the relevant policies. Development of new policies relating to e.g. Due Diligence and Contracting of Suppliers to be undertaken to ensure alignment with DHSC and UKGOV requirements (Q2). Overarching guidance document to assist Line Managers / Heads of Function in understanding corporate policies / relevance to their teams to be developed (for Q2).*		***X***			*Preventative/ Monitoring*	*Full suite of policies in place and available on Wave*	*https://intranet.hta.gov.uk/pages/policies_forms*
						External assessment of utilisation of capabilities			*Further work may be identified as part of the Cultural Review in Q2 Q 3*				***X***	*Monitoring/ Detective*	*Internal audit 'Utilisation of capability' provided moderate assurance in July 2019*	*ARAC received the audit report and monitors progress against recommendations - most recently June 2021.*
						Adherence to the HTA Workforce Capability Development Framework					***X***			*Preventative*	*SMT approved the Framework in September 2020 - as a response to internal audit recommendations*	*ARAC to receive update on the Framework at its meeting in October 2020*
						Investment in the development of the HTA leadership team			*Further work may be identified as part of the Cultural Review in Q2 Q 3*		***X***			*Preventative*	*External consultants engaged to assess team and individual development needs and design appropriate interventions*	*The current programme of work was completed in June 2021.*
						Handover process is formalised via a checklist to ensure corporate knowledge is retained			*Emssure the procecss identified and published is adhered to. Ensure that docuementation is saved in the appropirate EDRMS folder for wider access as needed.*		***X***			*Preventative/ Monitoring*	*Handover checklist is in place and in operation.*	*Evidence provided to internal audit June 2021.*
									More formal assessment of future capability needs and how these should be met including through better knowledge of internal skills. Work to adopt a portfolio management approach to support more effective resource deployment and identification of skills required.		***X***	***X***		*Preventative/ Monitoring*	*Director and Head of HR assessing capability needs as part of future operating model* *HTA Workforce Capability Development Framework sets out how capability needs will be met* *Head of HR has implemented a register of skills within the HTA*	*SMT will be agreeing its approach to filling specific immediate capability needs in October* *Development Programme is picking up medium to long term capability needs.*
									Establish a formal role within SMT terms of reference to look holistically at people and capability issues across the organisation focussing on short and long term impacts and deliverables.			***X***		*Preventative/ Monitoring*	*SMT terms of reference and SMT minutes*	*SMT ToRs revised and approved.* *HMT ToRs in development* *HTAMG ToRs to be revised subsequently*

REF	RISK/RISK OWNER	CAUSE AND EFFECTS	INHERENT RISK PRIORITY		PROXIMITY	EXISTING CONTROLS/MITIGATIONS	RESIDUAL RISK PRIORITY		ACTIONS TO IMPROVE MITIGATION	Risk Tolerance	LINE OF DEFENCE			TYPE OF CONTROL	ASSURANCE OVER CONTROL	ASSURED POSITION
			I	L			I	L			1	2	3			
5	*Insufficient, or ineffective management of, financial resources* *(Risk to Deployment objective b* *Risk Owner:* *Richard Sydee*	***Cause*** • *Fee payers unable to pay licence fees -* • *The number of licenced establishments changes, leading to reduced fee income* • *Management fail to set licence fees at a level that recover sufficient income to meet resource requirements* • *Failure to estimate resource required to meet our regulatory activity* • *Poor budget and/or cash-flow management* • *Unexpected increases in regulatory responsibilities* • *Unforeseeable price increases / reductions in GIA* • *Fraudulent activity detected too late* ***Effect*** • *Payments to suppliers and/or staff delayed* • *Compensatory reductions in staff and other expenditure budgets* • *Increased licence fees* • *Requests for further public funding* • *Draw on reserves* • *Failure to adhere to Cabinet Office Functional Standards* ***Leading to:*** • *Inability to deliver operations and carry out statutory remit* • *Reputational damage and non payment of fees*	5	4	Ongoing	Budget management framework to control and review spend and take early action	2	3		3	X	X		All	Budgetary control policy reviewed annually and agreed by SMT	Revised version reviewed by SMT in November 2020. AUD 16b/21. Next review March 2022 post audit.
						Financial projections, cash flow forecasting and monitoring					X			Monitoring	Monthly finance reports to SMT and quarterly to Authority. Quarterly reports to DH	Last quarterly report to Board in November 2021
						Licence fee modelling								Preventative	Annual update to fees model	No change to fees agreed by the Board November 2021 meeting
						Rigorous debt recovery procedure					X			Preventative	Monthly finance reports to SMT and quarterly to Authority	Level of outstanding debt is being reduced. Older debt are being collected. Although we maintain a tight grip on our position, the overall environment is more uncertain than normal.
						Reserves policy and levels reserves					X			Monitoring	Reserves policy reviewed annually and agreed by ARAC	Last agreed by ARAC October 2021
						Delegation letters set out responsibilities					X	X		Preventative	Delegation letters issued annually	Issued in April 2021
						Fees model provides cost/income information for planning					X			Preventative	Annual review of fees model, reported to SMT and Authority	Went to the Board November 2021
						Annual external audit							X	Detective	NAO report annually	Unqualified Accounts produced June 2021
									Monitoring of income and expenditure (RS) **Ongoing**				X	Detective	Monthly finance reports to SMT and quarterly to Authority. Quarterly reports to DH	Last quarterly report October 2021
									Horizon scanning for changes to DH Grant-in-aid levels and arrangements (RS) **Ongoing**		X	X		Detective	Quarterly Finance Directors and Accountability meetings	FD from NHS Resolution, HRA, NICE and CQC maintain contact over common issues weekly. Quarterly meetings with DHSC which cover finance and non-finance issues/risks.
									Action plan to move from rudimentary to Basic level of maturity on the GovS 013 Functional Standards		X	X		Preventative	Counter fraud Strategy and Action Plan developed and presented to ARAC Oct-19. Annual training of staff completed n Q4	Cabinet Office - CDR submissions made quarterly last submission April 2021 (Q4 2020/21). Counter-fraud activities now part of BAU.

REF	RISK/RISK OWNER	CAUSE AND EFFECTS	INHERENT		PROXIMITY	EXISTING CONTROLS/MITIGATIONS	RESIDUAL		ACTIONS TO IMPROVE MITIGATION	Risk Tolerance	LINE OF DEFENCE			TYPE OF CONTROL	ASSURANCE OVER CONTROL	ASSURED POSITION
			I	L			I	L			1	2	3			
6	***~~Failure to achieve the full benefits of the HTA Development Programme~~*** **19/5 Suggested change per LD** ***Failure to identify opportunities and achieve the benefits of continual change and improvements to support the modernisation of the HTA*** **Deputy Director**	***Causes*** • *Uncertainty of funding* • *Programme and project benefits poorly defined and understood* • *Inadequate programme and project governance arrangements* • *Poorly specified programme and projects* • *Insufficient programme, project and change management skills* • *Inadequate leadership of change* • *Inability to access the necessary skills required at a affordable cost* • *Lack of staff buy-in to change* • *Management and Head stretch of delivering transformation alongside business as usual and other development activity* • *Insufficient agility in (re)deploying people to change projects* • *Poorly specified procurement and inadequate contract management* • *Realisation of single points of failure for DDAT and People Strategy* ***Effects*** • *Wasted public money* • *Failure to achieve the central strategic intent of the Authority* • *Distracts senior management from operations at a time when demands have increased* • *Reputational damage* • *Unaffordable cost over run* • *Staff demotivation* • *Data remains under-utilised* • *Technology inadequate to meet future needs (cost, functionality)* • *Limited ability to achieve improvements in efficiency and effectiveness* • *Pace of change is inadequate and impacts negatively on other work*	3	3		SMT experience of organisational change, programme and project management.	3	3	*Change Manager appointed in August 2020. Ongoing organisational preparedness remains a key workstream in the 21/22 plan.*	9	X			Preventative	Recruitment of an HTA Programme Director	The Director of Data, Technology and Development appointed in October 2019 will act as Programme Director.
						HTA approach to the management of change projects *(underpinned by project management methodologies)*					X			Preventative	Dedicated permanent project manager appointed	PM in place an operating effectively
						A number of trained project managers among HTA staff			*Project Management skills further strengthened by introduction of a toolkit and induction session by PM*		X			Preventative		
						Experience of procurement and contract management					X			Preventative		
						Existing mechanisms for engaging staff			*Plans developing for strengthening internal communications function*		X			Preventative		
						Well established corporate governance arrangements and financial controls						X		Monitoring	*Internal audit of key controls*	Assurance provided by Internal Audit of adequacy of key financial controls
						Agreement to a phased delivery approach to avoid all or nothing investment and align with available funding			*Further alignment of projects on the business plan to strengthen phasing of actions, resource deployment and consolidation of actions to encourage smarter working.*		X			Preventative	*Programme plan in place*	Update reported to July Board meeting
						Project management rigour including benefits to be realised.			Embed Benefits Realisation Management methodology within programme		X			Preventative		
						Monthly reporting to SRO in place			Introduce a Programme Management function		X			Preventative		*Ongoing focus in 21/22 to embed PMO skills and build wider capability across the business*
									Board approval to proceed at key Gateway decision points			X		Monitoring		
									Training plan to encompass project and change management and HTA approach		X			Preventative		*Change management training activity is now in progress following the appointment of the HTA Change Manager. Mandatory all staff sessions were undertaken in quarter 3. Further osu planned in Q4*
						Strengthened planning supports a single message and focus on an agreed set of priorities			Development of procurement plan to deliver the DDAT Strategy		X			Preventative		*Plan in place, work ongoing in 2020/21.*
									SROs identified for Programme and individual projects		X			Preventative		*High level plan in place for 2021/22*
						Project management includes a monitoring of costs			Schedule a regular programme of staff engagement events		X			Preventative		*Reset and relaunch event planned in Q4 providing focus to developments over the next 15 months. Review of stakeholder engagement also extends to inviting a wider contribution to future development plans.*
						Scope of projects aims to deliver benefits including on a phased and incremental design			Establish an external stakeholder communications and engagement plan		X			Preventative		*Work progressed in Q4 20/21*
									Recruitment of new Board Member(s) with digital and organisational change experience			X		Monitoring		
						Agreed priorities in Business Plan and underpinning foundations for future strategy maintain required pace							X	Monitoring/ Detective		
						Identified success measures and benefits to be realised for the Development Programme and individual projects							X	Preventative		

REF	RISK/RISK OWNER	CAUSE AND EFFECTS	INHERENT		PROXIMITY	EXISTING CONTROLS/MITIGATIONS	RESIDUAL		ACTIONS TO IMPROVE MITIGATION	Risk Tolerance	LINE OF DEFENCE			TYPE OF CONTROL	ASSURANCE OVER CONTROL	ASSURED POSITION
			I	L			I	L								
7	Added 19/5/22 ***Failure to optimise the safe use of existing and available digital data and technology*** ***(Risk to Delivery objectives a-e, Development a-d Deployment a, c and d)*** *Risk Owner:* ***Louise Dineley***	• ***Cause*** • *Data holdings poorly managed and under-exploited* • *Inadequate business technology or training in the technology available* • *Lack of ring-fenced resource for 'no-deal' EU Exit* ***Effect*** • *Knowledge and insight that can be obtained from data holdings results in poor quality regulation or opportunities for improvement being missed* • *Poor use of technology resulting in inefficient ways of working* • *Inadequate balance between serving Delivery and Development objectives*	*3*	*4*		**Data capability**	*4*	*2*		**9**	***1***	***2***	***3***			
						Data relating to establishments securely stored with the Customer Relationship Management System (CRM)			Ongoing development of the electronic management of all information and records. Phase 1 complete. Phase 2 underway.		**X**		**X**	Preventative/ Monitoring	Upgrades to CRM, closely managed changes to CMR development. Internal audit of personal data security.	CRM upgrade completed successfully in March 2019
						Appropriate procedures to manage personal data including GDPR compliance.					**X**		**X**	Preventative/ Monitoring	Internal audit on GDPR compliance provided moderate assurance.	Internal audit report in March 2019. Part of ongoing Cyber and data security and SIRO reporting. Now absorbed in BAU Information Governance and Cyber Security work
						Business technology capability										
						Staff training in key business systems and mandatory training on policies and required controls.			System development needed to enable devolution of responsibility to line managers for verifying and ensuring that all their staff are up to date on their mandatory training. Supportive guidance document to assist Line Managers / Heads of Function in understanding corporate policies / relevance to their teams and risks (to HTA) of non-adherence to training to be developed .		**X**			Preventative	Systems training forms part of the induction process for new starters	Ongoing records of all new starters trained in key business systems. New remote induction programme was launched in Summer 2020.
						IT systems protected and assurances received from 3rd party suppliers that protection is up to date			Reporting to ARAC on Cyber Security and system security in place.		**X**	**X**	**X**	Preventative/ Monitoring	Quarterly assurance reports from suppliers. MontAMSy operational cyber risk assessments. Annual SIRO report	Annual SIRO report agreed SMT June 2021. June 2022 is the next reporting date
									Business technology							
									Identify refresher training and targeted software specific training needs.		**X**			Preventative	Evidence of targeted training in last quarter to support the roll out and adoption of EDRMS. Further strengthening of core training requirements included in updated induction programme.	
						System performance analytics available and reported monthly			Use of data analytics to inform and drive changes in practice.						Analytics provide assurance on system performance and support targeted intervention with members of staff as	

HTA
Human Tissue Authority

HTA Policy

HTA Risk Management Strategy and Policy

Purpose

1. The purpose of this document is to define the Human Tissue Authority's (HTAs) strategic intent for risk management and set out the roles and procedures for risk management at the HTA now and in the future. It will be reviewed and updated formally on an annual basis.

2. The HTA strives to be an organisation that demonstrates good governance practices. The environment that we operate within requires us to have in place a proportionate and strategic approach to the day-to-day management of risk. The objective is to ensure that when risks arise, they will be dealt with in a manner that is consistent with the principles and processes outlined in this document.

3. This document applies to all employees of the HTA and those seconded to work in the HTA. There should be an active lead from managers at all levels to ensure that risk management is a fundamental part of the overall approach to regulation, service delivery and corporate governance.

What is risk management?

4. Her Majesty's Treasury, in The Orange Book Management of Risk – Principles and Concepts describes risk as follows:

   'Risk is defined as the uncertainty of outcome, whether a positive opportunity or a negative threat, of actions and events. The risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact that arises if it does actually happen. Risk management includes identifying and assessing risks (the "inherent risks") and then responding to them.'

5. Risk management is essentially about identifying and managing key obstacles to the achievement of strategic and business objectives. It is a tool that is an integral part of effective and efficient management and planning.

Types of risk	
Strategic	Those current business risks that, if realised, could fundamentally affect the way in which we exist or provide services in the next one to five years. These risks will have a detrimental effect on the achievement of our strategic objectives. The risk realisation will lead to failure, loss, or lost opportunity.
Operational	Those current business risks that, if realised, could affect the way in which we operate or provide services in the new year. These risks will have a detrimental effect on our achievement of our business plan. The risk realisation will lead to failure, loss, or lost opportunity.
Project	Those business risks that, if realised, could affect the way in which we deliver any specific project. The risk realisation will lead to failure, loss, or lost opportunity.

Strategic intent

6. The Board recognises that risk management is an integral part of good governance and management practice and to be most effective should be part of the HTA's culture. The Board is committed to ensuring that risk management forms an integral part of the HTA's philosophy, planning and practice, rather than being viewed or practised as a separate activity, and that responsibility for risk management is accepted at all levels of the organisation.

7. The HTA aims to take all reasonable steps in the management of risk with the overall objective of achieving its strategic and business objectives and protecting staff, stakeholders, the public and assets.

8. The HTA recognises that the outcome of a risk management approach will not eliminate risk totally. Rather it provides the means to identify, prioritise and manage the risks and provide a balance between the cost of managing and treating risks, and the anticipated benefits that will be derived from doing so. Risk management should not be so rigid that it stifles innovation and the imaginative use of limited resources in order to achieve objectives.

Risk appetite and tolerance

9. The HTA recognises that there is a relationship between its risk tolerance and risk appetite.

10. The HTA's risk appetite is the total amount and types of risk it is willing to take in the achievement of its objectives. The HTA's risk appetite is set by the Board, and it will regularly review the amount of risk that it is prepared to accept, depending on the prevailing circumstances at the time. The Board will evaluate factors such as the activity and developments in the sectors we

regulate; our culture and the nature of the strategic objectives we are trying to achieve. the HTA's financial strength and organisational capabilities are also taken into account.

11. The HTA's risk tolerance defines the tolerance to risk for each risk that it is prepared to cope with accept or avoid after control measures have been implemented. The HTA's risk tolerance expresses the specific maximum risk that it is willing to take regarding each relevant risk category.

12. The HTA has a low tolerance for risks that may result in compromising the protection of the public's interests that the removal, storage and use of human tissue and organs are undertaken safely and ethically, and with proper consent. The HTA is not willing to accept risks that may result in financial loss or exposure, major breakdown in information systems or information integrity, significant incidents of regulatory non-compliance, potential risk of injury to staff or contractors or reputation damage.

13. The Board has agreed its risk appetite and tolerance statement which can be found at Annex A

Duties and responsibilities

Role of the Board

14. The Board has ultimate responsibility for the management of the HTA's risks. It monitors the HTA's approach to the management of risk, and its effectiveness in managing risk. Predominantly, it considers the risks facing the HTA at the strategic level. Its role includes:

    - instilling a culture of risk management:
        - determining the HTA's 'risk appetite' across the whole organisation or on any relevant single issue, and reviewing this periodically as part of the strategic planning cycle
        - determining which risks are acceptable and which are not
        - determining the appropriate level of risk exposure.

    - satisfying itself that risks are managed appropriately:
        - considering the external environment and identifying emerging strategic risks
        - approving the overall risk management arrangements
        - approving decisions which have a major impact on the HTA's risk profile or exposure and satisfying itself that the HTA's actual level of risk exposure does not exceed that agreed
        - monitoring the management of significant risks and assuring itself that risks are tolerable

    - satisfying itself that the less significant risks are being actively managed, and that the appropriate controls in place are working effectively
    - reviewing the approach to risk management and approving key changes or improvements to processes and procedures. *Role of the Audit and Risk Assurance Committee*

15. The Audit and Risk Assurance Committee reviews and tests the establishment and maintenance of an effective system of internal control and risk management. This process is underpinned by the internal audit function, which provides an opinion on internal control.

16. It is the Audit and Risk Assurance Committee's role to advise the Board on the effectiveness of the HTA's internal control arrangements. As part of this role, it will advise the Board:

    - annually on the HTA's approach to risk management and overall risk management arrangements, approving the Risk Management Strategy and Policy
    - periodically on the management of significant risks (following discussion with the Senior Management Team on specific risks)
    - on the implications of internal audit reports
    - on the implications of the recommendations made by the external auditors.

Role of the SMT

17. As the SMT is the authoritative decision-making body within the HTA's management structure, it has the management responsibility for risk and implementation of the HTA's risk management strategy and reporting requirements.

18. The SMT takes the lead in ensuring that the strategy and practice remain appropriate and fit for purpose. The SMT ensures that assessment and management of risk are an integral feature when authorising and managing existing and new work. SMT members are risk owners of strategic risks.

19. Specifically, the SMT is responsible for:

    - establishing and maintaining a coherent and practical HTA-wide approach to the management of risk, using the procedures set out in this document
    - maintaining the HTA's Risk Management Strategy and Policy
    - identifying and managing the strategic risks faced by the HTA for consideration by the Board
    - reviewing strategic risks on a monthly basis
    - periodic review of the effectiveness of the HTA's risk management arrangements
    - delegating responsibility to Heads for identifying and managing the operational and project risks faced by the HTA.

Role of HMT

20. Chaired on a rolling basis by a Head of Service, the Heads Management Team (HMT) consists of Heads from across the business. It meets bi-monthly and identifies, assesses, manages and/or escalates key corporate or emerging risks. HMT ensures that operational and project risks are reported, managed, and escalated, as necessary.

21. The HMT will make recommendations and proposals to SMT. Where appropriate, HMT will make decisions on operational matters, reporting to SMT. Decisions requiring specific strategic input will be taken to SMT.

22. Where new proposals are being worked up or recommendations are being made, HMT will ensure that all operational aspects have been considered. This is to ensure that IT, cost, resource, and training needs have been considered prior to the recommendation being made to SMT.

HTA Groups

23. The Stakeholder and Fees Group, Histopathology Working Group, and Transplant Advisory Group were originally created to provide a valuable opportunity to gain stakeholders' views on risks. As a result of the last governance audit, these groups are under review and may therefore change.

Director of Resources

24. The Director of Resources acts as central reference point for all risk management issues within the HTA. The Director facilitates and oversees the risk management processes but does not act as the "risk manager" for all risks, as the HTA recognises that risk management forms an integral part of all functions.

25. The Director is responsible for the maintenance of the Strategic Risk Register.

DHSC Sponsor Unit

26. The Department of Health and Social Care Sponsor Unit has a role to play in providing a means of escalation of strategic risks as well as sharing information and guidance.

HTA in a wider risk context

27. The HTA engages with the Department of Health and Social Care ALB Risk Network, which meets regularly throughout the year. This is a forum for

discussing common risk issues and systemic risks and the approach of the Department towards risk management.

28. HTA have committed to consider system-wide and common, interdependent, risks

Procedures

Approach to risk management

29. The starting point for risk management is a clear understanding of what the organisation is trying to achieve. Risk management is about managing the threats that may hinder delivery of priorities and core functions, and maximising opportunities that will help to deliver them. It should take into account the environment within which the HTA operates.

30. The risk management process should be kept as simple and straightforward as possible. It should:

- start from objectives
- put the primary focus on significant risks and related controls
- record details in risk registers
- regularly monitor progress
- allocate risk management responsibilities to individuals
- link actions to manage risks to personal and business plans
- not be so complicated that it alienates management and staff.

31. Risk management involves a 5-stage process, as shown below:

Stage 1 – Risk identification

32. The first step is to identify the ‘key’ risks that could have a significant adverse effect on us or prevent key strategic or business objectives from being met. It is important that those involved with the process clearly understand the service or organisation’s key business objectives i.e., ‘what it wants to achieve’ in order to be able to identify ‘the barriers to achievement.’

33. Details of any new risks should be raised with the Director, or the Head concerned to be considered for recording on the Strategic or the Operational Risk Register, respectively. Project risks are recorded by the project manager, using the system in place for specific projects, and are escalated to the operational and strategic risk registers through HMT and SMT, as necessary.

34. SMT should consider the current portfolio of risk in coming to a decision whether to accept a new strategic risk and HMT should do the same for operational risks. SMT or HMT will also confirm or make changes to the new risk, assign a risk owner, and agree any further action to be taken to manage the risk.

35. Risk identification also includes identifying opportunities, where the outcome is uncertain, and these may be managed using the process set out here. However, strategic considerations about whether to exploit opportunities are made by the Board.

Risk interdependencies

36. Extended Enterprise is the term used to describe risk interdependencies between organisations. As part of a wider group consisting of the DH and all its ALBs, a review of three types of risk needs to be undertaken as part of the risk identification process. Furthermore, escalation of any such risks needs to be factored into our process.

37. The three types of risk to identify are:

1) **Type 1.** A system-wide risk that affects a number of different ALBs (or in some cases all of them including DHSC, e.g., cyber security)
2) **Type 2.** A risk identified in one ALB or DHSC that will affect another
3) **Type 3.** A risk caused by processes and controls in place at one ALB or DHSC that may lead to a risk in another ALB or DHSC.

38. Whilst the HTA needs to ensure the above is conducted consistently, there must also be a means of communicating or feeding back any risks that have materialised from the above. The process for this will be via an ALB wide forum (see para 44).

Stage 2 – Risk analysis

39. There are four important principles for analysing risk:

- consider the likelihood and impact for each risk
- be clear about the difference between inherent and residual risk
  record the assessment of risk in a way that facilitates monitoring and the prioritisation of risks. Tolerance level (score) which the executive accepts or will tolerate

.

40. Having identified new risks, the following details should be provided to SMT or HMT so that they can be recorded in the relevant risk register. The implications of project risks should be considered, and significant ones included in the appropriate register. The details should include:

- a **description** of the risk, its cause, and the effect on the HTA if the risk materialised
- an assessment of the **inherent[1] impact** of the risk if there were no mitigating strategies in place to manage the risk. This should be measured on a scale of 1 to 5 as detailed in the following table:

[1] The concept of inherent and residual impact and likelihood is taken from the Orange Book.

Impact				
	Finance	**Service Quality/Objective**	**Health & Safety**	**Reputation**
(5) ***Very high***	Above £1m	Complete failure of services.	Fatality (Staff, members, and visitors etc…).	Significant reputation damage is causing government intervention e.g., Inquiry, Management and/or Authority re-structure.
(4) ***High***	£0.5m to £1m	Significant reduction in service quality expected. Not delivering statutory remit.	Serious injury occurring.	Reputation damage occurs with the Key Stakeholders (Opinion Leaders) such that their overall confidence in the HTA is affected.
(3) ***Medium***	£250k to 500k	Service quality impaired leading to the temporary suspension of non-statutory remit.	Very minor injury.	Localised reputational damage e.g., within a sector/geographical area.
(2) ***Low***	£50k to £250k	Marginally impaired, stakeholder expectations are not met (non-statutory).	No injury.	Temporary reputational damage, (e.g., practitioner confidence/local media/individuals).
(1) Almost None ***Very low***	Below £50k	Negligible effects on service quality.		No effects on reputation.

NB. *The above figures are based on the impact on HTA's minimum cash reserve of £1.2m, the levels of impact have been based on the retained level of reserves after the event – with the highest impact (catastrophic) leaving just 2 months of cover in cash terms for essential running costs (Salaries and Facilities). The headings in the above table must be taken into account when judging the severity of a risk and not* *just the financial impact i.e., financial impact could be £50k however it could have reputational damage which is catastrophic.*

- an assessment of the **inherent likelihood** of the risk materialising. This should also be measured on a scale of 1 to 5 as detailed below:

Likelihood	
(5) Almost certain	Above 90% chance of occurring
(4) Likely	50 – 90%
(3) Possible	10 – 50%
(2) Unlikely	3 – 10%
(1) Rare	Less than 3% chance of occurring

- a summary of the controls in place and assurance sources that will confirm whether key controls are operating effectively

- an indication of the residual impact and likelihood using the same scoring system shown above. The residual score indicates the level of the risk once the controls have been put in place and action has been taken

- a suggested **owner** (ideally a named individual or role) for the risk.

41. SMT or HMT will record the details of the new risk in the relevant risk register and calculate an inherent score and residual score by multiplying the scores for impact and likelihood using the risk matrix shown below.

Risk matrix

	Risk Scoring Matrix					
IMPACT	**5. Very High**	5 Medium	10 Medium	15 High	20 Very High	25 Very High
	4. High	4 Low	8 Medium	12 High	16 High	20 Very High
	3. Medium	3 Low	6 Medium	9 Medium	12 High	15 High
	2. Low	2 Very Low	4 Low	6 Medium	8 Medium	10 Medium

	1.Very Low	1 Very Low	2 Very Low	3 Low	4 Low	5 Medium
Likelihood						
Risk score = Impact x Likelihood		1.Rare (≤3%)	2.Unlikely (3%-10%)	3.Possible (10%-50%)	4.Likely (50%-90%)	5.Almost certain (≥90%)

Risk scores are not intended to be precise mathematical measures of risk, but are a useful tool to help in the prioritisation of control measures for the treatment of risk. The scoring system allows the levels of risk to be easily identified and therefore prioritised.

Stage 3 - Risk prioritisation

42. Once risks have been identified and analysed, they require a priority to be applied.

43. In line with the colour coded quadrants of the risk matrix above, once risks have been assigned a score, they will fall into one of the following four groups which will determine the manner in which they will need to be managed:

- **Primary Group (red)** – Where risk management should focus most of its time. Risks that fall into this group will require immediate attention. Both the inherent and residual status of the risk will need to be monitored with regard to any effect on the organisation's activities and the progress of any action taken to ensure its effective completion.

- **Contingency Group (orange/amber)** – Where risk management will ensure that contingency plans are in place. Risks that fall into this group may require immediate action but will need to be monitored for any changes in the risk or control environment, which may result in the risk attracting a higher score.

- **House Keeping Group (yellow)** – Basic mechanisms should be in place, (risk management will confirm). Risks that fall into this group will need to be monitored by management.

- **Negligible Group (Blue and green)** – Where risk is so minimal it does not demand specific attention. Risks that fall into this group will require review only, but no further action.

44. New risks that are classified as primary should be bought to the attention of the SMT immediately to enable the risk to be reviewed and actions to be quickly identified.

Stage 4 - Risk Management

45. Once a risk has been identified, analysed, and prioritised, it will be possible for the organisation to decide whether to take further action to address the risk

and if so what type of action. When deciding how best to manage risks, it is useful to ask the following questions:

- how to prevent it from happening - either by putting some controls/countermeasures in place or putting the project or activity in a position where it would have no impact
- how to reduce the risk - what action is needed to reduce the probability of the risk happening
- how to maximise opportunities
- what to do to if the risk does occur - outline some contingent activities
- what are the implications of accepting the risk - ensuring that all the stakeholders are aware of the possible impact?

46. There are several response options that can be taken to address the risks that have been identified. These are set out in the following table. The final two seek to maximise opportunities.

Response options to risks and opportunities	**Description**
Terminate or avoid	An informed decision not to be involved in, or to withdraw from, an activity, in order not to be exposed to a particular risk. Used if risks are not acceptable or outweigh the benefits.
Treat - reduce or mitigate	Take action to reduce the likelihood of a risk, or its impact if it does arise.
Transfer or share	This option aims to pass at least part of the risk to a third party. Insurance is the classic form of transfer, where the insurer picks up the cost if the risk materialises, but the insured retains the impact on other objectives. Contracting or working in partnership are other means.
Tolerate	Tolerated risks are risks that the organisation lives with and keeps under review. The risks have been managed as far as is considered to be reasonably practicable and have adequate control mechanisms in place.
Accept	Here the organisation “takes the chance” that the risk will occur, with its full impact if it did. There is no change to residual risk, or no actions, with this option, but neither are any costs incurred now to manage the risk, or to prepare to manage the risk in future.
Enhance	The opportunity equivalent of mitigating a risk. Enhancing an opportunity seeks to increase the likelihood of it occurring and/or the impact of the opportunity in order to maximize the benefits.
Exploit	The opportunity equivalent of avoiding a risk. Exploiting an opportunity seeks to make the opportunity definitely happen (i.e., increase likelihood to 100%). Aggressive measures are taken which seek to ensure that the benefits from this opportunity are realised.

47. The risk owner will be responsible for:

- managing the risk and ensuring that any agreed controls and/or actions to manage the risk are planned and carried out
- evaluating the effectiveness of the controls in place, any subsequent actions required and considering whether further action is needed
- updating the Risk Register and informing SMT or HTAMG about any changes made to reflect changes in circumstances.

48. The risk owner is also responsible for periodic action to obtain the assurances specified and to report on their effectiveness.

Contingency planning, managing and mitigating risks

49. Mitigating or control actions should be designed to reduce the risk. A review of these plans should be carried out in conjunction with the review of each risk. Contingencies or contingency planning is effectively a ‘Plan B’ should all else fail.

50. When a risk translates into a live issue due to a failure in mitigation or lack of appropriate management action, the following will be undertaken:
    - a root-cause analysis
    - implement corrective and preventative action where appropriate or
    - a review of system capability and training needs

51. If the materialised risk is of a financial or non-financial nature and significant enough, a referral to DHSC would be made.

52. As part of the risk assessment process, each identified risk will be assessed three times:
    - Inherently, as though there were no controls in place, or that all of the controls are failing;
    - Residually, assuming the controls in place are adequately designed and operating effectively;
    - Target, the risk score that should be achieved through implementing actions, bringing the risk in line with articulated appetite and tolerance.

53. Controls to manage the risk and assurance measures can then be applied to provide a proportionate response with need to revisit should the risk assessment score change over time.

Stage 5 - Monitoring

54. The Risk Registers should be monitored regularly to be able to close risks down when their likelihood has passed or to add new risks in the light of new information. Additionally, levels of inherent and residual risk should be assessed, and controls added or amended as appropriate, separated between those planned and those implemented.

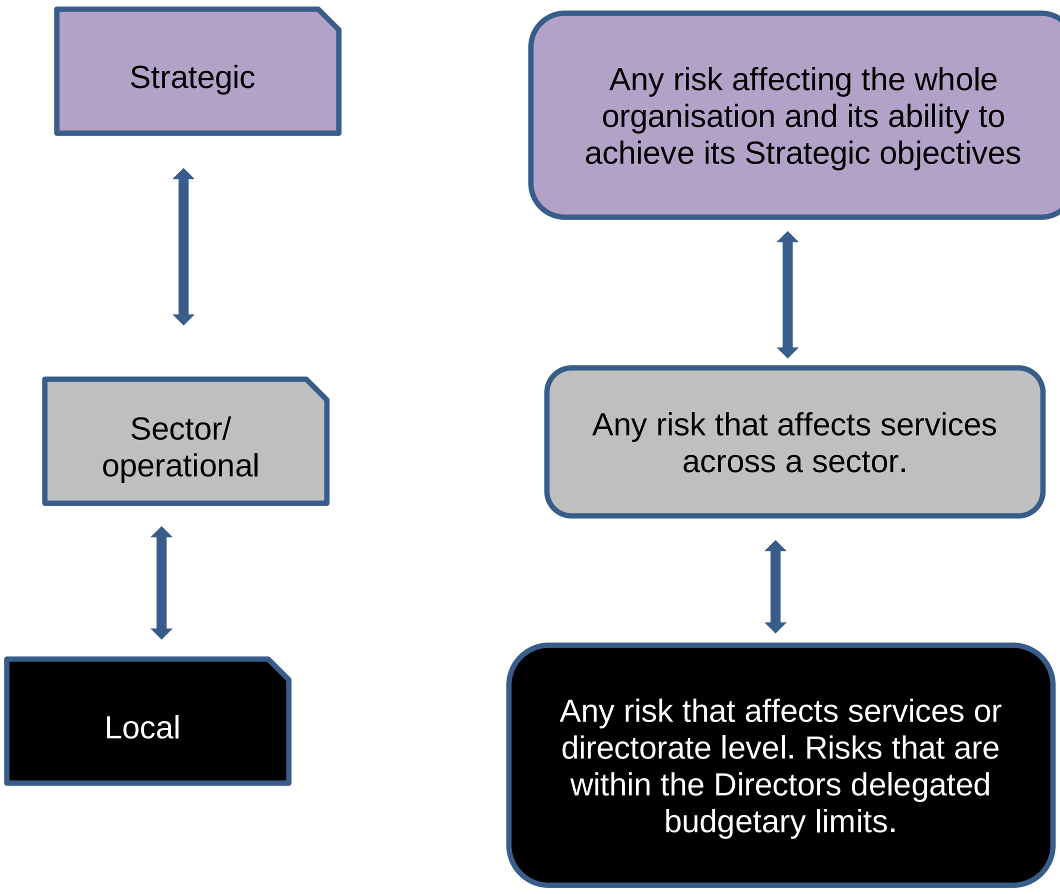
55. The Risk Registers serve as an essential tool for monitoring and reporting on the actions selected to address risks. Some of the actions may have only been to monitor the identified risk for signs of a change in its status. Monitoring risks will also consist of:

- checking that execution of the planned actions is having the desired effect
- watching for the early warning signs that a risk is developing
- modelling trends, predicting potential risks or opportunities
- checking that the overall management of risk is being applied effectively.

56. It should be noted that as risk management is an on-going and iterative process, the status of existing risks will change, and new risks will arise. This means it will be necessary from time to time to return to any one of the five stages of the process as outlined above in relation to a particular risk.

Risk Review and escalation

57. All risks are managed on Strategic and Operational Risk Registers. There are different levels of risk management as identified below:


Strategic
Any risk affecting the whole organisation and its ability to achieve its Strategic objectives
Sector/ operational
Any risk that affects services across a sector.
Local
Any risk that affects services or directorate level. Risks that are within the Directors delegated budgetary limits.

Risk Review

58. The frequency of review of risks, dependent on their risk score, is as follows:
- Red will be reviewed **monthly**
- Orange (Amber) risks will be reviewed monthly if they score 16 or more. Risks scoring below 16 will be reviewed **bi-monthly**
- Yellow risks will be reviewed at least **quarterly**
- Green/Blue risks will be reviewed at least every **six months**

59. Risk review frequency may be increased based on the risk's alignment with the Authorities identified risk appetite.

Risk Escalation

60. Each risk owner, on a regular basis, should review their identified risks and the controls put in place to manage those risks. All levels of risk will be monitored and escalated to the relevant level of Risk Register dependent on:
- The risk score

- The area of effect
- The budgetary requirements to manage/mitigate the risk

Assurance

61. The strategic risk register provides for controls to be categorised into lines of defence and whether they are preventative or detective. In this way, the balance of controls can be identified in order to determine how appropriate and effective controls might be.

62. The three lines of defence are:
1 – embedded in the business operation, such as policies or management checks
2 – corporate oversight, such as review by the Board
3 – external oversight independent of the HTA, such as internal or external audit reviews, or assurance gained by the Department of Health and Social Care.

63. Assurance that controls are operating effectively may be gained from:

    - Internal audit reports
    - External audit reports
    - Feedback from the Department of Health and Social Care
    - Other feedback following review (e.g., external or peer)
    - HTA documents (e.g., minutes, SMT or Board papers reporting performance)
    - Reports from Directors and staff, orally or in writing
    - Checklists.

64. The key sources of assurance used to monitor the effectiveness of controls to manage specific risks are set out in the HTA's risk registers.

65. The strategic risk register includes the assured position - when assurance that the control is working properly was last obtained and in what form. Gaps are highlighted for further action.

Alignment of risks with organisational objectives

66. All risks should be mapped or aligned with the organisational objectives contained in the HTA Strategy and Business Plan. The linkage between objectives and risks should be documented on the risk registers and in the strategic and business plans of the organisation.

67. Failure to align strategic objectives with strategic risks, and business objectives with business (operational/project) risks, will result in a reduced likelihood that all risks relating to organisational objectives have been identified and are subject to appropriate mitigation.

68. Management should also review the relationship between strategic and business objectives and strategic, operational, and project-based risks to ensure that all risks relevant to the objectives have been identified and that all risks currently monitored are genuinely risks.

Managing information Risk

69. The HTA places high importance on minimising information risk and safeguarding the data and records held by the organisation.

70. Information risk is inherent in all organisational activities and everyone working for, or on behalf of the HTA, has a responsibility to continually manage information risk. The aim of information risk management is to provide the means to identify, prioritise and manage the risks to records and data involved in all of the organisation's activities.

71. The HTA will assess information risk in a number of ways, which will include the following;

    - Routine review of flows of records and information in our activities, to ensure any risks identified with these flows are mitigated, including ensuring appropriate controls are in place for personal data and any data transferred outside the HTA.
    - Use the risk assessment methodology (risk matrix) to assess information risks e.g., threats to information.
    - Undertaking Privacy Impact Assessments and System Security Level risk assessments as methods through which information assets can be risk assessed and assured they comply with the required standards.

72. The organisation's risk management procedures provide clear guidance as to the way in which all risks and incidents are identified, assessed, and managed across the organisation, and information risk should be assessed using the same methodology.

Review

73. This policy will be reviewed by the executive every three years or earlier if a change in obligations requires it.

Annex A

Risk Appetite Statement

- Risk appetite is the amount of risk an organisation is willing to accept in pursuit of its strategic goals.

- Following our review of the existing approach to risk we propose that the risk appetite statement considers separately five key areas of risk to which the HTA is exposed and provides an outline of the HTA's appetite for managing these types of risks. The HTA does not have a single risk appetite, but rather appetites across the range of its activities. We recognise that in pursuit of our strategic priorities and outcomes we may choose to accept different degrees of risk in different areas of the business.

- Where we choose to accept an increased level of risk, we will do so, subject always to ensuring that the potential benefits and threats are fully understood before actions are authorised, that there is sufficient capacity, and that sensible and proportionate measures to mitigate risks are established.

- The Executive will manage strategic risks in a manner that is consistent with this statement. The strategic plan and the business plans within the HTA should also be consistent with this statement.

- Below are the risk appetite descriptions established for each key activity identified.

Business Area Risk Appetite Levels

Regulation

Risk 1 – Failure to regulate appropriately
Risk 2 – Failure to manage an incident

- The HTA has **NO** appetite for any activity that disregards the need to obtain consent and any incidents that lead to serious public harm or breach of Data Protection Act.

- There is **LOW** appetite for risks that may result in the HTA providing misleading advice, especially when this advice could lead to an adverse impact on patient safety.

Corporate Governance

- There is a **LOW** appetite for activity that may result in non-compliance with legislation, statutory obligations, and government policies. The HTA has a **ZERO** tolerance for deliberate non-compliance with legal, statutory and policy requirements, except in exceptional circumstances.

Reputational

Risk 3 – Failure to manage expectations of regulation

- The HTA will explore innovative ways of regulating in line with better regulation principles and will have a clear view on its regulatory risk and areas of oversight. It will not tolerate (**ZERO**) any action that could cause reputational damage.

Capabilities

Risk 4 - Failure to utilise our capabilities effectively

- The HTA has a **MODERATE** appetite for change to ensure it has the right resources, capabilities, and organisational structure to optimise performance in the future whilst delivering value for money.

Information security and management

- The HTA has a **LOW** appetite for risk that could lead to information or data security breaches and a **LOW** appetite for system failures that could disrupt normal business. We have **NO** appetite for activities that may increase our exposure to threats on our assets arising from external malicious threats.

- The HTA has **LOW** appetite for activities that may compromise processes governing the use of information, its management and publication. The HTA has **ZERO** tolerance for the deliberate misuse of its information.

Risk 5 – Finance

- The HTA has a **LOW** risk appetite in relation to management of its finance. It will not tolerate annual expenditure in excess of income or any form of spend that contravenes HMT guidance. In addition, The HTA has **ZERO** appetite for any incidence of fraud and fraudulent behaviour.

Annex B

Definitions

1. Governance - the management systems, processes, and behaviours by which the Authority leads, directs, and controls its functions to achieve its organisational objectives, safety, and quality.

2. Board Assurance Framework (BAF) - The BAF enables the Board to: identify and
understand the principal risks to achieving its strategic objectives, and understand the
control and assurance framework in place to manage these risks. Further, identified areas of improvement and action plans are provided.

3. Risk Scoring / Rating - Risk scoring involves the use of the 5x5 risk matrix with impact and likelihood being multiplied to reach the risk score. The scoring system allows individual risks to be prioritised. Risk scores are not intended to be precise mathematical measures of risk, but are a useful tool to help in the prioritisation of action plans for the treatment of risk.

4. Risk Tolerance - The maximum level of risk the organisation is prepared to take in line
with the type of risk and the potential level of harm, recognising the Authority has a low appetite for risks that could affect patient safety.

5. Risk Appetite - The levels and types of risk the Organisation wants to take in pursuance of its objectives. This informs all planning and objective setting, as well as underpinning the threshold used when determining the tolerability of individual risks.

6. Risk Controls – These are the management systems and processes the Authority has in place to manage its risks. Examples include policy, guidance, staff training, appropriate skill mixes and staff numbers, etc.

7. Actions – a specific, measurable, achievable, relevant, and time-specific piece of work that is to be completed, that will address an identified gap in control or assurance.

8. Risk Assurance– evidence that supports the measurement of controls in place, to ensure they are operating effectively, and the desired outcome is being achieved

9. Inadequate Assurance- Where assurance or evidence is limited and cannot provide full assurance that controls are effectively managing the risk. Gaps should be identified and listed with actions to close.

10. Gaps in Assurance – lack of measures or evidence to support the measurement of
controls

11. Internal Assurance - Assurances provided by reviewers, auditors and inspectors who are part of the organisation, or management peer review

12. External Assurance / Independent Assurance –Assurances provided by reviewers,
auditors and inspectors from outside the organisation such as External Audit
Positive and Negative Assurances - Adequate / Positive assurance indicates how
controls are operating to mitigate the risk to the achievement of desired outcome.
Inadequate / Negative assurance is the reverse, where evidence shows that controls are not operating effectively to mitigate the risk to the achievement of the desired outcome.

13. Inherent Risk - This is the score assigned to any risk, which articulates how severe and likely a risk is to occur if the controls in place are found to be ineffective, or absent. It involves the use of the 5x5 risk matrix of impact against likelihood. The scoring matrix and definitions are provided following the glossary.

14. Residual Risk - (This is also known, interchangeably, as the current risk score). It is the score assigned to any risk after the control measures in place are taken into account. It involves the use of the 5x5 risk matrix with impact and likelihood being adjusted following the inherent risk score. The scoring matrix and definitions are provided at para 38 and 39.

15. Target Risk - The keyword here is “target.” This is the future (or prospective) risk score
assigned to any risk after gaps in control measures have been addressed and outstanding actions implemented. It is the level of risk which the Department/Directorate etc feel they can tolerate.

Revision history

Reference: HTA-POL-025

Author(s): Head of Finance

Reviewed by: SMT

Approved by: SMT/ARAC

Owner: Director of Resources
Distribution: All staff/Board (Authority) Members

Protective Marking: OFFICIAL

- (June-21 / Version 14.0: Change Authority to Board, removed Patient death from Impact, sections on: Contingency planning; Risk Review and escalation added; Risk Appetite statement and definitions).
- (May-22 / Version 14.0: No changes; ARAC to recommend the full Board reviews Risk Appetite Statement at its next meeting.

ARAC Cyber Security dashboard

9 June 2022

HTA
Human Tissue Authority

Introduction

The Cyber Security dashboard provides a summary of cyber security systems and protection. The high level summary builds on the detailed report provided to ARAC in January 2022.

HTA
Human Tissue Authority

The Cyber Security Dashboard has been developed using the 6 key outcomes of the HTA's Cyber Security Strategy (2020) This strategy seeks to implement measures to achieve the mandatory protective security outcomes of the Minimum Cyber Security Standard. The HTA's cyber security systems are focused on the following outcomes:

Identify : We have in place appropriate cyber security governance processes. We have identified and catalogued the sensitive information we hold. We have identified and catalogued the key operational services we provide. The need for users to access sensitive information or key operational services is understood and continually managed.

Protect : Access to sensitive information and key operational services is only provided to identified, authenticated and authorised users or systems. Systems that handle sensitive information or key operational services are protected from exploitation of known vulnerabilities. Highly privileged accounts are not vulnerable to common cyber-attacks.

Detect : We take steps to detect common cyber-attacks.

Respond : We have a defined, planned and tested response to cyber security incidents that impact sensitive information or key operational services.

Recover : We have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise.

Cyber security Performance Q4 2021/22 – at a glance

HTA Human Tissue Authority

Microsoft secure score	Viruses intercepted Q4 2021/22	Device exploit availability (no known)	Device vulnerability
84.31%	100%	16 / 52	A total of 9 devices had 15 known vulnerabilities

Alerts received from NHS X	Number of alerts responded to in 48hrs	Staff mandatory training (Completed Q2 2021/22)	Internet use: Identified access to restricted categories
3 (2 relevant to HTA)	100%	100%	3166

ARAC Cyber Security Dashboard – Overview

The dashboard below provides an overview of our systems and the level of risk. This is an automated data generated through our systems, interpreted and accessed through the NHS Threat Protection portal. This presentation provides assurance that HTA ‘s protection systems are performing as intended.

HTA
Human Tissue Authority

Microsoft Secure Score

84.3%
similar NHS entities scored 46.38%
Meaning we have well defined and managed processes in place

Secure score is a defined standard that shows how well we are protected. It also shows how we compare to similar NHS entities. This shows we are significantly better

Antivirus Update Status

100% out of 68 devices MS Defender identifies devices as laptops and servers

Our Antivirus solution is monitored and updated real time ensuring we have the latest known virus threat and unknown breaches kept to a minimum

HTA Exposure Score

24%

Higher the score the more at risk our devices are 24% is in the low bracket. There two software patches which are currently being rolled out.

Phishing & Viruses Detected

41 Viruses over 3 months
Less than 0.12% of mail received
18 Phishing attempts sent to 17 recipients.

With the onset of remote working email viruses and phishing attempts have never been more prevalent. The HTA had 41 viruses included in email with all intercepted by our security systems

Spam Detected

Month	Count
January	1,046
February	1,145
March	1,344
Total	3,535

SPAM accounts for 10% of all inbound email. This figure is what was intercepted by our security systems. User feedback is critical in the event that spam breaches these controls. Incidents are reported to IT for follow up.

Conclusion

- Over the last quarter the HTA’s cyber security threat protection has been maintained via existing monitoring systems and responding to regular alerts via the RTANCA (Response to an NHS Cyber Alert) system.

- All issues identified either through detection, reports or alerts have been actioned without risk to the organisation.

- The information highlights the HTA is in a good position to monitor and protect its systems, devices and users from potential attacks.

- The continual threat and creativity of cyber attacks means that in addition to maintenance of existing systems we need to continue to seek opportunities to improve the security of IT systems and digital data stores.

Audit and Risk Assurance (ARAC) meeting

Date: 9 June 2022

Paper reference: AUD 19/22

Agenda item: 7

Author: Richard Sydee
Director of Resources

OFFICIAL

SIRO Report

Purpose of paper

1. To provide an annual update to the Audit and Risk Assurance Committee (ARAC) on the annual assessment of the HTA's information risk management.

Decision making to date

2. Reviewed by the HTA Senior Management Team (SMT) on 24 May 2022

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 impinge on our ability to meet corporate objectives, providing oversight and assurance to the Executive and Authority of the HTA. It is a Cabinet Office (CO)

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

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

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

Report

7. The HTA routinely assesses the risks to information management across the organisation, through its assessment of the risk of data loss, cyber security, and the inclusion of guidance on creating and managing records throughout its Standard Operating Procedures (SOPs).

8. During this year we have embedded the upgrades to our information systems and processes undertaken during 2020/21, the impact of the COVID-19 pandemic on HTA's established working practices necessitated an acceleration of planned changes to our IT systems and approach to remote information management and security last year and this year has allowed us to:

   - Embed sharing and greater collaboration utilising Microsoft Office 365, and Microsoft Teams, to allow for easier communication and improved workflow through the use of shared documents and drafts.

   - We continue to improve the efficient and effective use of our Electronic Document and Records Management System (EDRMS). This provides a significant improvement to both user experience and our ability to effectively manage our records throughout their lifecycle. We believe there is still further value and improvements that can be driven through this, and this will be part of our ongoing change and upskilling within the information environment of the HTA.

9. With the help of ARAC we have continued to develop and refine our cyber dashboard and now believe we have reached a level of maturity where this can move to standard suite of BAU management and ARAC reports through 2022/23. The move to routine report and SMT scrutiny will further add to the assurance and maturity of HTA's governance of information and cyber security.

10. We have continued to review our approach to assessing and capturing our tolerance of information risk. Given the size of the HTA there is very limited resource to provide continuous oversight of this issue, and this has been a key consideration as we have assessed ourselves against the NHS Data Security Protection Toolkit (DSPT).

11. Our self-assessment against the DSPT for the 2021 submission was one of general compliance with the DSPT mandatory assertions. In terms of the required audit of our evidence, required by the toolkit to be independent of the HTA and undertaken by our Internal Auditors, this led to a limited opinion, with issues acknowledged in relation to the breadth and detail of the evidence provided to support our assessment.

12. I am assured that progress has been made in the HTA's approach to the DSPT for the June 2022 submission. The number of assertions that our IA colleagues are assessing has increased, but we have developed a more robust approach to sourcing and cataloguing evidence for our positively assessed assertions.

13. Our internal assessment is that the HTA will meet the requirements of the 2022/23 mandatory assertions. We are currently working with GIAA colleagues to assess the substance of our evidence for this. We expect to submit our assessment in line with the 30 June 2022 deadline.

14. 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. We acknowledge that we have further work to do in refreshing our records and information management policies and approach and will be subjecting this progress to further Internal Audit review during the 2022/23 business year.

15. As in previous years I have considered the HTA's compliance with the NCSC Minimum Cyber Security Standard and discussed this with our Chief Information Technology Officer. The requirements have been applied proportionately and matched to the HTA's organisational risks. Not all the areas apply to the HTA in their entirety. My assessment is contained at Appendix A in this document.

16. In line with the Office of the Government SIRO handbook I have also considered a number of the factors that underpin the management of the HTA's information risks.

    - I believe the HTA has an effective Information Governance framework in place and that the HTA complies with all relevant regulatory, statutory and organisation information security policies and standards.

    - I am satisfied that the HTA has introduced further processes to ensure staff are aware of the need for information assurance and the risks affecting corporate information.

    - The HTA has appropriate and proportionate security controls in place relating to records and data and that these are regularly assessed.

17. In conclusion, I believe the HTA has progressed in its approach to data, information and records management over the past year and is in a stronger position in terms of its governance in this area as a consequence. As SIRO, I believe the HTA takes issues relating to information risk seriously and has appropriate processes in place to assess and minimise these risks. We will continue to maintain and improve processes over the coming year and ensure we consider how we can maximise the use of our information as a business asset.

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	Yes, the HTA has named individuals: CITO, DPO, Director DTD, SIRO and IAOs The HTA has a strategy and policy (in draft) in place We have identified limited patient data held and documents that contain other personal data. We have considered under our GDPR preparedness activity and have contractual GDPR compliance with our supplier BCC.

[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.

		awareness and education about cyber security across the Department.	The HTA will be rolling out a similar package as part of annual refresher training for staff– this could be beneficial to ARAC. We will explore training options for ARAC over the coming months given the number of new members joining.
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	I believe we do know this and have documentation to support it in the HTA's Personal Data Inventory

3	***Departments shall identify and catalogue the key operational services they provide.***	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	This is known and given recent upgrades and changes to our systems and infrastructure we now have improved visibility of these services and their dependencies

4	***The need for users to access sensitive information or key operational services shall be understood and continually managed.***	a) Users **shall** be given the minimum access to sensitive information or key operational services necessary for their role. b) Access **shall** be removed when individuals leave their role or the organisation. Periodic reviews **should** also take place to ensure appropriate access is maintained.	I believe we do know this, and this is set out in our policies The HTA has implemented a checklist process for starters, leavers, and those changing roles.
5	**<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 access is provided on a needs basis and set out in policies We have a number of password protected systems, some with Multi Factor Authentication and complex password requirements.

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

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

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

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

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

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

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

10	**<u>RECOVER</u>** ***Departments shall have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise.***	a) Departments **shall** identify and test contingency mechanisms to continue to deliver essential services in the event of any failure, forced shutdown, or compromise of any system or service. This may include the preservation of out of band or manual processes for essential services or CNI. b) Restoring the service to normal operation **should** be a well-practised scenario. c) Post incident recovery activities **shall** inform the immediate future technical protection of the system or service, to ensure the same issue cannot arise in the same way again. Systemic vulnerabilities identified **shall** be remediated.	We have a number of contingency plans, some of which we have utilised over the past year in response to COVID 19. During this year we have moved more assets in to the cloud and enhanced and upgraded a number of systems providing increased resilience and more effective remote working.

Audit and Risk Assurance (ARAC) meeting

Date: 9 June 2022

Paper reference: 20/22

Agenda item: 8

Author: Morounke Akingbola, Head of Finance & Governance

OFFICIAL

Policies and Procedures Schedule

Purpose of paper

1. To provide the Committee with a brief overview of items under this agenda item.

Decision making to date

2. None

Action required

3. ARAC Members are asked to comment and note the summary of policies that are tabled at ARAC and to approve the policy documents at Annex B and C.

Policy/Procedure & document reference	Purpose of policy/procedure	Status
Procurement Policy Doc Ref HTA/POL/027	Policy covers the authorisation process for purchases of different values	**Reviewed and approved by SMT Nov-20** Procurement Thresholds updated and NICE added into section on contracts and frameworks
Financial Policies and Procedures Manual HTA/POL/028	This is a compendium of key finance policies in one document. There are links and cross-references to individual policies are made within this document.	**Under review May-22**.
Budgetary Control Policy HTA/POL/031	Policy deals with the budget-setting process of the HTA and includes a draft timetable	**Under review post internal audit review in Q4 2021/22**
Expenses Policy HTA/POL/032	Policy covers reimbursement of Travel, Subsistence, and other expenses	**Reviewed and approved April-22**.
Reserves Policy HTA/POL/049	Policy states the minimum level of cash reserves that the HTA should ideally keep as a contingency	**Reviewed Sept-21** tabled at ARAC Oct-21 meeting
Antifraud Policy HTA/POL/050	Policy covers definitions of fraud, responsibilities of HTA employees	**Reviewed Dec-21 and tabled** at ARAC Jan-22 meeting. Next review date Nov-24
Whistle-blowing Policy HTA/POL/017	Policy covers procedure to be followed if they have concerns about improper behaviour	**Reviewed Dec-21** and tabled at ARAC Jan-22 meeting. Next review date Dec-22

Gifts and Hospitality Policy	Policy covers the procedure for receiving/declining gifts	**Reviewed May-22** tabled at ARAC Jun-22 with the register

HTA Policy

Critical Incident Response Plan (CIRP)

Scope

1. Full access: Human Tissue Authority (HTA) staff and Board Members.

2. Limited access: Key suppliers as defined within the role sheets.

Purpose

3. To respond effectively and appropriately to critical incidents.

4. To maintain public confidence and safety.

5. To maintain transparency and accountability for all decisions made using this response plan.

6. To ensure continuous delivery of the HTA's statutory remit.

7. As far as is practical, to facilitate continuous delivery of the HTA's business plan.

8. To preserve staff safety and wellbeing.

9. Effective communications with the right people at the right time.

Objectives

10. To define a practical working definition of a critical incident.

11. To provide a simple and clear mechanism for escalating, managing, and recovering from critical incidents and to ensure existing SOPs use this mechanism.

12. To identify roles, activities, responses and responsibly for each area of the HTA's business in alignment with the risk register.

13. To support the HTA's risk management strategy and ensure impact assessment undertaken and contingency plans are in place for all inherently major or catastrophic risks.

14. To maintain, review, test and update the critical incident response plan alongside the risk register and business plan.

15. To provide guidance for all HTA governance documents to incorporate at their next review dates.

16. To define, and reflect in their terms of reference, the responsibilities of working groups dealing with any type of day-to-day case which may develop into a critical incident.

17. To provide training and promote awareness of the critical incident response plan to all staff.

Useful links

- Cabinet Office - guidance and links
- How prepared are you? Business continuity management toolkit

Related documents

a) Critical incident log: [Incident Log – Advanced Find for cases flagged as critical incidents]
b) Operational risk register
c) Strategic risk register

Critical Incident Response (CIR) Management

SMT CIR Representative:	Chief Executive
CIR Programme Manager:	Director of Resources
CIR Admin:	Name withheld

Definition of critical incident

18. The HTA defines a critical incident as ***any incident where the effectiveness of the HTA's response is likely to have a major or catastrophic impact on public confidence, finances, quality of service, health and safety of any person or the reputation of the HTA. An incident may be deemed critical if it has a <u>moderate</u> impact on either finance or service quality.***

19. *Major* and *Catastrophic* are clearly defined as levels of impact for each of the contexts above in the HTA's risk management strategy.

20. It is expected that the majority of critical incidents will have been articulated in the HTA's operational risk register as risks with an impact assessment, a risk response and any inherently major or catastrophically graded risks should have a contingency plan outlined.

21. There is a need to flag any cases in CRM, which show signs of developing into critical incidents, for example, more media interest in a case or the HTA's involvement with a case.

22. There is a need to escalate any cases which have developed into critical incidents.

Understanding the risk and critical incident response

23. The HTA's critical incident response plan has strong links to the operational risk register which in turn has strong links with the business plan. The operational risk register records impact and likelihood assessments for identified risks.

The HTA's CIRP strategy

24. The HTA's chosen strategy for responding to critical incidents is to adopt a role-based approach where each role represents the interests of a key area of risk for the HTA.

25. Each role is assigned a role owner and specific responsibilities which cover planning for, responding to and recovering from incidents.

26. Critical Incident role owners are named individuals responsible for maintaining each of the HTA roles and are listed under general contacts.

27. Roles may be delegated by the role owner to ensure continuous cover. It is recognised that these roles are heavily dependent on each other and that communication between them will be essential in responding effectively to incidents. This ensures that there is no ambiguity about who is responsible for which activities, or when those activities should be carried out.

28. Not all scenarios can be predicted, and it is envisaged that the HTA's critical incident response plan will serve to provide a toolkit for individuals assigned to a role, detailing their specific responsibilities and lines of communication.

29. Any role, or staff member, may trigger a response to an incident, at which point the incident is formally managed as a critical incident. While this approach increases the speed, clarity, and flexibility of the HTA's response it is also acknowledged that decisions must be made at the appropriate level. This is reflected in the SMT Role but **for practical purposes the person triggering the response is, by default the incident owner until a new owner is formally identified**.

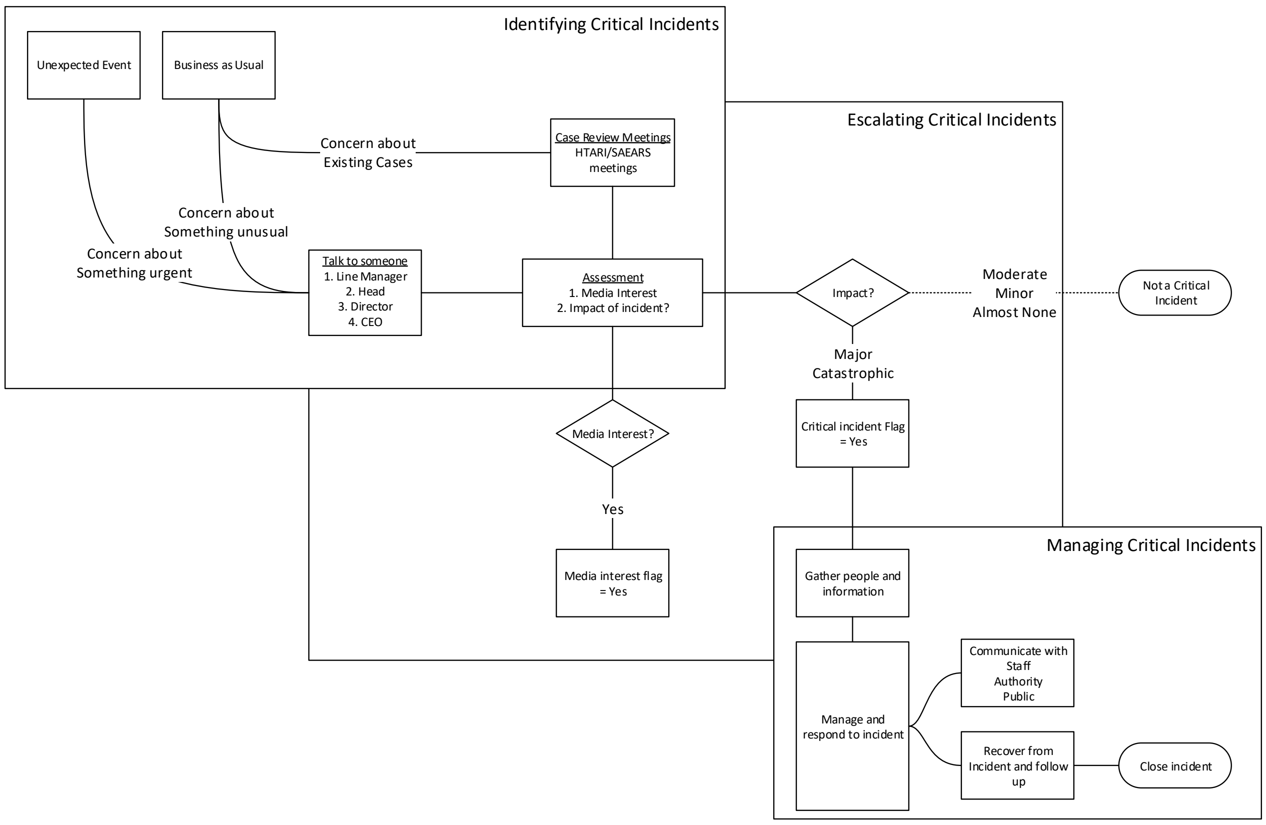
CIRP preparedness and testing

30. The HTA will undertake an annual test of its ability to respond to a Critical Incident. This will be undertaken utilising an unannounced scenario test of a potential incident, the type of incident would change annually and be based on both on rotation and any increased likelihood and potential impact assessed via strategic risk management reviews.

31. Should an event occur then a test would not be undertaken until a period of 12 months has elapsed since the last critical incident response had occurred

Overview of Incident Response

32. The CIRP relies on strong links with day-to-day business processes. It can broadly be broken into three areas: identifying, escalating, and managing critical incidents. Communication between roles throughout is essential.


Identifying Critical Incidents
Unexpected Event
Business as Usual
Concern about Existing Cases
Case Review Meetings
HTARI/SAEARS meetings
Concern about Something unusual
Concern about Something urgent
Talk to someone
1. Line Manager
2. Head
3. Director
4. CEO
Assessment
1. Media Interest
2. Impact of incident?
Escalating Critical Incidents
Impact?
Moderate
Minor
Almost None
Not a Critical Incident
Major
Catastrophic
Critical incident Flag = Yes
Media Interest?
Yes
Media interest flag = Yes
Managing Critical Incidents
Gather people and information
Manage and respond to incident
Communicate with
Staff
Authority
Public
Recover from Incident and follow up
Close incident

Identifying Critical Incidents

33. The HTA routinely deals with cases which potentially involve harm to the public or loss of life. There are clearly defined SOPs for those dealing with these cases.

34. It may not be immediately obvious that the HTA has encountered a critical incident. It is recognised that not all incidents will be the same and not all will be critical. It is important that all staff at the HTA are aware of who they can approach if they suspect a critical incident has occurred or is imminent.

35. It is important that all staff are familiar with the hallmarks of a critical incident and examples of critical incidents in their areas.

36. All role owners, heads and SMT should have a sound understanding of the definition of critical incident.

37. All role owners, heads and SMT should be familiar with the HTA's risk strategy, in particular the impact assessment levels.

38. All role owners, heads and SMT should know how to escalate a critical incident.

Escalating Critical Incidents

39. SOPs which cover with business-as-usual cases should maintain clear escalation links to this response plan.

Managing Critical Incidents

40. The first step in managing a critical incident is to gather as many role owners together as possible. The means to do this may vary depending on the urgency of the situation and the time of the week/day. Various methods are detailed in the role sheets.

41. The initial meeting will determine who should be part of the critical incident response team. This does not need to include all role owners (although there are some which must be part of all response teams) and may include additional members of staff or even external third parties. The role sheet sets out a suggested checklist for the first meeting as well as role membership.

42. Continued management of the critical incident will be largely down to the group to co-ordinate, but it is important that SMT retain oversight and all actions, events and decisions are logged.

43. It may not be possible to create or update a CRM case depending on the circumstances, but notes should be taken, and CRM updated when possible.

Business Continuity

44. Not all critical incidents will have an impact on business continuity, but all business continuity situation may become a critical incident. The HTA has a separate Business Continuity policy to manage business continuity arrangements.

Developing and Implementing Incident Response

45. How roles communicate during a critical incident will depend heavily on the nature of the critical incident and the time of day and week the incident occurs.

46. Where possible, role owners will get together to determine appropriate responses and ideally SMT will be on hand for decisions. Role owners should challenge the situation and assumptions made, agree it is a critical incident, develop a plan of action, decide how that will be resourced and what the media strategy should be, if necessary. This is covered by the first meeting checklist in the role sheets. They must ensure all staff are made aware of the situation. It may also be necessary for the roles to gather somewhere outside of 2 Redman Place (2RP) immediately following an evacuation and/or remain together for decision making purposes after all staff have gone home.

47. It is recognised that this may not always be possible however and it is expected that roles will communicate with each other as needed and that it may not always be necessary or expedient for SMT decisions to be

communicated to all roles prior to action being taken. For example, an updated message for the website may only require dialogue between the Communications role and the SMT role.

Exercising, maintaining, and reviewing CIRP arrangements

48. The CIRP Admin role has responsibility for: making sure that the HTA's critical incident response plan arrangements are reviewed annually and updated; administering the exercise programme; and keeping the CIR plan updated through lessons learned and good practice.

49. The elements of the CIRP will be reviewed alongside the operational risk register and business plans as part of the same cycle. The HTA may, on an ad-hoc basis, request that the Internal Auditors review the HTA's CIRP and the arrangements it outlines. Any review should check that:

    a) all key services and their critical activities and supporting resources have been identified;
    b) arrangements accurately reflect the HTA's objectives;
    c) arrangements are fit for purpose, and appropriate to the level of risk the HTA faces;
    d) CIR maintenance and exercising programmes have been effectively implemented;
    e) CIR arrangements incorporate improvements identified during incidents and exercises and in the maintenance programme;
    f) an effective programme for training and awareness raising is in place;
    g) and change control procedures are in place and working effectively.

50. A full exercise should follow reviews periodically, and after major changes to the HTA's organisational structure or location, to ensure any changes are viable and that key staff are familiar with the plan. Arranging a full exercise of the HTA CIRP is assigned to the CIRP Admin role as a specific responsibility and will include co-ordinating and documenting discussions, table-top exercises, and limited live exercises. Table-top exercises will be based on unseen scenarios and should involve all roles including representatives covering the all-staff role.

51. Individual roles have a responsibility for testing and documenting those elements of the HTA CIRP which fall under their remit. Results of any tests should be notified to the CIRP Admin role.

Embedding Incident Response in the HTA's culture

52. It is important that critical incident response is seen as a natural extension of risk management and next step from existing SOPs and processes. All staff should be encouraged, and should feel able, to talk to someone in the CIRP chain about doubts or concerns. The raising of potential critical incidents should not be discouraged.

53. Similarly, all role owners should be considering constantly whether something is becoming, or has become, a critical incident and know what steps to take.

54. While all roles have a responsibility for promoting awareness of critical incident response within the HTA the CIRP Admin role has specific responsibility for ensuring that new employees are given a copy of the all-staff role sheet when they start and for talking through the HTA critical incident response plan as part of the induction process.

55. The channels for making staff aware of the HTA critical incident response plan include all staff meetings, all staff newsletters, training sessions and exercises.

56. Responsibility for training all staff on CIRP processes and procedures is assigned to the CIRP Admin role, and where appropriate staff may be asked to join in full tabletop exercises or take part in limited live exercises. All roles' owners and delegated role owners will be trained. A log of training should be kept in IRIS HR Portal.

57. Where training is required for third parties (for example Independent and Accredited Assessors), such training and any related guidance is the responsibility of the relevant role.

Identifying Critical Incidents

A critical incident is any incident where the effectiveness of the HTA's response is likely to have a **major** or **catastrophic** impact on public confidence or on the finances, quality of service, health and safety of any person or the reputation of the HTA. An incident may be deemed critical if it has a **moderate** impact on either finance or service quality.

	Finance	**Service Quality/Objective**	**Health & Safety**	**Reputation**
(5) Catastrophic	Above £1m	Complete failure of services. Patient death due to HTA negligence.	Fatality (Staff, members, and visitors etc…).	Significant reputation damage is causing government intervention e.g., inquiry, Management and/or Board re-structure.
(4) Major	£0.5m to £1m	Significant reduction in service quality expected. Not delivering statutory remit.	Serious injury occurring.	Reputation damage occurs with the Key Stakeholders (Opinion Leaders) such that their overall confidence in HTA is affected.
(3) Moderate	£250k to £500k	Service quality impaired leading temporary suspension of non-statutory remit.	Very minor injury.	Localised reputational damage e.g., within a sector/geographical area.
(2) Minor	£50k to £250k	Marginally impaired, stakeholder expectations are not met (non-statutory).	No injury.	Temporary reputational damage, (e.g., practitioner confidence/local media/individuals).
(1) Almost None	Below £50k	Negligible effects on service quality.		No effects on reputation.

Being Prepared for Critical Incidents

- Keep a printed list of key contacts and any other documents you might need access to.
- Be aware of evacuation procedure .
- Know your line manager and direct reportees mobile numbers
- Test remote access and alert line manager/IT of any issues (note that if you are unable to work remotely you may be asked to take annual leave if we can't use the office)

Escalating Critical Incidents

Urgent and immediate

- Talk to a role owner.
- Call any role owner out of hours.

Usual timescale

- Talk to or email a role owner.
- Raise at a regular case review meeting.
- If there is no existing case in CRM create a new 'Incident' case. Include a description, timings, and any actions/decisions so far.
- If there is likely to be media interest set the 'Media Interest' flag to 'yes.
- If a case is deemed a critical incident a role owner should set the 'Critical Incident' flag to yes.
- The role owner is the critical incident lead until a formal owner can be assigned.

What to do during a Critical Incident

- Follow instructions. Check emails, text messages and HTA Portal
- Make a note of key events, actions, and decisions
- Unable to get into office? Consider:
  - Contacting line manager and direct reports
  - Aiming to work remotely using HTA remote desktop.
- Unable to get home? Consider:
  - Walking, staying with a friend/colleague, taking a taxi, staying in a hotel.
  - Contacting Accommodation role for assistance with hotels/taxis.

Recovering from a Critical Incident

- Ensure all electronic files are transferred to HTA and then securely deleted from any alternative storage areas.
- Ensure printed copies outside the office are filed appropriately or securely disposed.

All Staff - General contacts	
HTA switchboard	contact information withheld
HTA Webcurl	contact information withheld
Staff incident information	contact information withheld
Remote access [via RDP Client]	contact information withheld
Out of hours media enquiries	contact information withheld
Body donation enquiries	enquiries@hta.gov.uk or http://www.hta.gov.uk/medical-schools
Licensing enquiries	licensing.enquiries@hta.gov.uk
Finance enquiries	finance@hta.gov.uk
2RP Security	contact information withheld
2RP Reception	contact information withheld

Role Owners and Deputy Owners	
All Staff	information withheld
Accom. /Admin	information withheld
CIRP Admin / H&S	information withheld
Comms	information withheld
Finance	information withheld
Evacuation Officers/FLOs	information withheld
First Aid	information withheld
HR	information withheld
IT	information withheld
Regulation	information withheld
SMT	information withheld
Board & Planning	information withheld
Transplants	information withheld
Licensing	information withheld

Accommodation / HTA Admin	
Critical activities:	• Provide Suitable equipment and facilities • Post • Enquiries • Phones
Example triggers:	• Building evacuation • Major incident affecting Stratford Station
Dependencies:	• 2 Redman Place • Savills (Landlord) • Internet access, MS 365 (EDRMS/Email), CRM
Operational risk register:	No directly related operational risk. **Action: Ensure accommodation risks, impact assessments and mitigating actions have adequate cover in risk register.**

Being Prepared for Critical Incidents

- Aware of SMT contact details for the day.
- Know password for hotel booking system.

What to do during a Critical Incident

Urgent and immediate

- Providing guidance and assistance to stranded staff
- Help book taxis or hotels if possible.

- Consider Health and Safety of staff and Liaise with E&FM team
- Answer redirected phones and direct messages to staff
- Provide Admin support

Usual timescale

- Liaise with E&FM team
- Consider investigating alternative medium-term office space
- Arrange venue space as necessary
- Ensure the enquiries mailbox is checked
- Possible redirection of post, office supplies for staff

Recovering from a Critical Incident

- Move back to 2RP
- Close down alternative site
- Ensure secure moving/filing/destruction of information from alternative site
- Ensure enquiries updated in CRM

Accommodation contacts

DHSC – Emergency Preparedness Resilience & Response Unit	information withheld
CTM hotel booking	information withheld
CTM rail booking	information withheld
CTM Air/Eurostar	information withheld
2RP Reception Security	information withheld
2RP Control Room	information withheld
Royal Mail	information withheld

CIRP Admin

Critical activities:	• CIRP administration
Example triggers:	• None
Dependencies:	• Internet access • EDRMS | Email
Operational risk register:	• None.

Being Prepared for Critical Incidents

- Aware of SMT contact details for the day.
- Ensure HTA CIRP is reviewed and updated annually.
- Promote critical incident response across HTA including running training and induction sessions.
- Administer annual and ad-hoc exercise programme including devising scenarios.
- Ensure onsite HTA battle bags are kept current and their contents tested annually
- Ensure backup legal contacts are up to date.

What to do during a Critical Incident

Urgent and immediate

- Start a log, using any means available of key events and decisions.
- Remind other role owners to keep logs.
- Responsible for onsite battle bag in event of evacuation.
- Be on hand to ensure process is followed and to provide advice guidance.

Usual timescale

- Ensure CRM case has been updated/created correctly to capture details of the incident including a record of key decisions.
- Be on hand to ensure process is followed and to provide advice guidance.

Recovering from a Critical Incident

- Ensure CRM case is updated or created if it was not possible during incident.
- Capture lessons learned within 1 month
- Close incident log.
- Replenish used battle bag supplies.

CIRP Admin contacts

Department of Health and Social Care	information withheld

Communications

Critical activities:	• Co-ordinating HTA's public position and response • Dealing with media enquiries • HTA website (IT – technology; comms – content)
Example triggers:	• Regulatory failure • Web server failure
Dependencies:	• Internet access • HTA Website | EDRMS | Email | Portal • Phone lines
Linked documents:	• Media Lines to take folder
Operational risk register:	Stakeholder management. **Action: There may be risks across the risk register which rely on comms involvement in mitigating actions/contingency plans. Do we have a risk dealing with poor handling of a media crisis?**

Being Prepared for Critical Incidents

- Know passwords for HTA website admin.
- Hot topics / lines to take stored in hard copy.
- Media training pack stored in hard copy.
- Ensure default holding page details kept up to date.

What to do during a Critical Incident

Urgent and immediate

- Ensure Holding page for the external website / portal for external stakeholders/public. This may need to be amended to use mobile numbers if HTA phone switch is not available. Liaise with other roles.
- Co-ordinate all media communications. Review and approve public statements.
- Instruct all staff and all roles to direct all media enquiries to a designated person, email and/or number.
- Monitor news, external sources, and social media.

Usual timescale

- Develop both internal and external communications response. Liaise with other roles.
- Co-ordinate all media communications. Review and approve public statements.
- Monitor news, external sources, and social media.
- Update Incident page and website messages daily including the day's date.
- Update holding page on external website / portal as necessary
- Consider content to go on the portal for external stakeholders/public if necessary
- Consider alternative supplier for the external website.

Recovering from a Critical Incident

- Return incident information line and website messages (for internal staff) to default.
- Consider supplier options – restore external website to normal.

Communications contacts

Big Blue Door (website) support	information withheld
HTA website login	information withheld
Twitter/Facebook login details	information withheld
Portal login	information withheld

Out of hours media number	information withheld

Finance

Critical activities:	• Supplier payments • Staff expenses • Payroll
Example triggers:	• Cashflow shortfall • Inability to collect licence fees
Dependencies:	• Internet access • Access to Great Plains server • CRM • Chris 21 • At least two authorisers for Bank • Remote access
Linked documents:	• None
Operational risk register:	Finance

Being Prepared for Critical Incidents

- Aware of SMT contact details for the day.
- Printed list of supplier details
- Keep record of expenses made in cash/Cc Offsite cheque book
- Arrange and test access to offsite readers
- Ensure secure offsite storage of credit card

What to do during a Critical Incident

Urgent and immediate

- Deal with customer/supplier enquires
- Advise Comms & IT of mobile for website if necessary.
- Liaise with Frontier Payroll Services if incident is close to pay day
- Manage all incident related purchases ensuring short term controls are in place

Usual timescale

- Access to BIB (Bacs).
- Ensure Finance mailbox is checked.
- Consider notifying customers/suppliers and deal with customer/supplier enquires.
- Supplier payments (remotely) Cheque book last resort.
- Tell Payroll alternative notification details.
- Inform Frontier Software regarding continuing payroll if necessary.

Recovering from a Critical Incident

- Assess impact of critical incident on HTA finances and budgets and existing contracts.
- Alert customers to go back to business as usual (email address, telephone) if earlier notification went out.
- Contact Frontier software

Finance contacts

Barclays Corporate	information withheld
BIB Internet Banking Helpdesk	information withheld
Frontier Payroll Software Mailbox-Quedgely PPC	information withheld

HTA Finance Team	information withheld
Contracts and debt recovery	information withheld
FOI/DPA and debt recovery	information withheld

Human Resources (HR)

Critical activities:	• Ensure that staff are safe and well. • Ensure that the HTA can communicate information to all staff who may or may not be in the office. • Supporting other directorates
Example triggers:	• Epidemic
Dependencies:	• Internet access • EDRMS | Email | IRIS HR
Linked documents:	• None
Operational risk register:	People

Being Prepared for Critical Incidents

- Securely maintain an offline or printed list of staff contact details.
- Ensure IT is given updated contact list for SMS broadcast system quarterly.
- Ensure induction material reviewed annually and updated as necessary.
- Quarterly reminder to staff to update personal details in IRIS HR

What to do during a Critical Incident

Urgent and immediate

- Account for staff
- Contact staff as requested by other role owners, line managers or SMT
- Assist emergency services and public authorities in handling casualties (identification of victims, contacting next of kin, etc.)
- Monitor the condition and location of injured.
- Support other directorates for emergency staff cover.
- Provide counselling services as required.

Usual timescale

- Inform agencies
- Agency staff who cannot work would not be paid
- Overview of staff movements.
- Support other directorates for emergency staff cover.

Recovering from a Critical Incident

- Contact recruitment agencies

HR contacts

Health Assured	information withheld
Treasury Solicitors	information withheld

Information Technology (IT)

Critical activities:	• Ensure that key servers and systems are available
Example triggers:	• Power failure • Data failure Server failure • Network failure

Dependencies:	• Internet lines • IT suppliers and supplier data centres (including BCC DR site.) • HTA Server room and network infrastructure.
Linked documents:	• BCC DR schedule
Operational risk register:	Cyber Risk and Information Risk

Being Prepared for Critical Incidents

- Ensure systems and system changes are properly documented and suppliers are aware of key information.
- Know key login account details.
- Ensure servers are backed up and replicated according to 'BCC DR schedule.'
- Ensure DR procedures are tested annually.
- Ensure SMS broadcast system is tested annually and maintain SMS broadcast groups (HTA all staff, Board Members and CIRP role owners).

What to do during a Critical Incident

Urgent and immediate

- Send SMS alerts to broadcast groups as directed by SMT.
- Conduct computer and phone system damage assessment. Investigate root causes and gather evidence.
- Update Portal incident page (http://portal.hta.gov.uk/incidents)
- Redirect phone lines as necessary. (Main switchboard, transplants, media enquiries, emergency mortuaries, enquiries). Update other roles, in particular comms for website holding page).
- Redirect DNS records as necessary.
- Consider invoking DR site. Recovery main site.
- Ensure short term measures are secure.

Usual timescale

- Notify key suppliers
- Monitor DR server performance
- Set up back up office IT at DH or alternative site.
- Consider redirecting portal forms to DR servers by changing database in Portal configuration.
- Arrange DR Portal or Website provision with supplier
- Inform Frontier Payroll Service of DR IP address change.

Recovering from a Critical Incident

- Failback to primary system or site.
- Notify key suppliers
- Restore DNS Records
- Restore main website or portal with supplier. Ensure data migrated and destroyed at DR locations.

IT contacts

BCC - information withheld

BBD: information withheld

2RP Contacts: information withheld

Regulation	
Critical activities:	• Advice and guidance • Licensing and inspections • Regulatory decision making SAEARS/HTARIs • Emergency mortuaries • Living Donation case assessment
Example triggers:	• Poorly managed SAEAR or HTARI • Loss of CRM • Insufficient staff • Severe weather conditions
Dependencies:	• Internet & Remote Access • CRM | EDRMS | HTA Website | Portal • Emergency Mortuary & Enquiries Lines
Linked documents:	• Management of Serious Adverse Events and Reactions • Administration and management of the PM sector HTA Reportable Incidents
Operational risk register:	Policies and Procedures **Action: This is a broad area. Have we covered all of the risks?**

Being Prepared for Critical Incidents

- Print inspection schedule monthly
- Ensure emergency licence packs are stored offsite by designated team members
- Regulation team to keep hard copies of codes and regulations.
- LIPM to keep six licence numbers set aside for emergency mortuaries.

What to do during a Critical Incident

Urgent and immediate

- Cover emergency lines and ensure additional mailboxes are being checked.
- Process emergency mortuary applications
- Scheduled inspections proceed if possible or contact establishments if not
- Notify any meeting/working group attendees
- Maintain list of used emergency mortuary licence numbers.
- Deal with enquiries HTARI/SAEARS using backup systems if possible or by phone if not
- Assess impact on operational activities.

Usual timescale

- Advise SMT and Comms as necessary.
- Consider inspections schedule
- Decide operational priorities and enquiries rota. If necessary, assign dedicated mobile cover and advise Comms of details to update website: Sector specific enquiries & SAEARS & HTARIs
- SAEARS, HTARI, Licensing enquiries, Licensing admin, ODD enquires

Recovering from a Critical Incident

- Ensure CRM and EDRMS are updated.
- Process outstanding applications.
- Replenish used emergency mortuary packs and allocate new emergency mortuary numbers.
- Reschedule postponed inspections

Regulation contacts

information withheld	information withheld

information withheld	information withheld
information withheld	information withheld
information withheld	
information withheld	

Senior Management Team (SMT)

Critical activities:	• Decision making • Leadership • Approvals
Example triggers:	• Any incident
Dependencies:	• Internet access (keep HTA laptops at home) • Barclays card and readers at home • Access to precedent • Access to legal advice
Linked documents:	• Strategic risk register
Operational risk register:	All

Being Prepared for Critical Incidents

- Support and promote business continuity and critical incident response planning and awareness.
- Provide leadership.
- Ensure two Barclays authorisers.
- Ensure SMT Decision maker(s) available.

What to do during a Critical Incident

Urgent and immediate

- SMT Availability.
- Key Decisions.
- Leadership.
- Initiate SMS Broadcast.

Usual timescale

- SMT Availability.
- Key Decisions re business as usual and incident.
- Key stakeholder relationship management including DHSC, Chair and Board.
- Meet to review situation and prioritise work.
- Consider HTA wide staffing levels.
- Authorise payments remotely.
- Consider any wider reporting or notification requirements (e.g., Information Commissioner's Office)

Recovering from a Critical Incident

- Review lessons learned and embedded learning across HTA.

SMT contacts

Colin Sullivan	information withheld
Richard Sydee	information withheld
Nicky Harrison	information withheld
Louise Dineley	information withheld
Blake Morgan (Licensing)	information withheld
Blake Morgan (FOI/DPA)	information withheld

Mills and Reeve (Transplants)	information withheld
Hill Dickinson (Contracts/Debt)	information withheld
Fieldfisher (Licensing)	information withheld

Board and Planning

Critical activities:	• Governance • Project Management
Example triggers:	• Loss of business plan and/or monitoring tools and data • Loss of quality/governance documents • High profile changes poorly implemented and/or stakeholder expectations misjudged.
Dependencies:	• EDRMS
Linked documents:	• HTA business plan • HTAMG programme plan
Operational risk register:	Business planning Development and change

Being Prepared for Critical Incidents

- Ensure governance documents are maintained and reviewed when due.
- Ensure risk owners undertake impact assessments of risks and related activities.
- Ensure offline or printed copies of external groups meeting schedule and membership contacts
- Ensure offline or printed copies of Board meeting schedule and Board member contacts

What to do during a Critical Incident

Urgent and immediate

- Notify members if day of meeting.
- Advise Comms of any upcoming meetings update messages for website.
- Consider any project deadlines and liaise with project managers (Talk to HR role for contact details)
- Consider any FOI deadlines.

Usual timescale

- Consider impact on HTA business plan.
- Consider impact on risk registers.
- Consider impact on project plans.
- Consider HTAMG meetings.
- Board Liaison.
- Alert members of affected groups if there are changes to meeting schedules or arrangements.

Recovering from a Critical Incident

- Re-evaluate HTA business plan
- Review project plans

Board and Planning contacts

Bord Chair	information withheld
FOI/DPA	information withheld

Living Donor Transplants

Critical activities:	• Processing and assessment of applications for organ, PBSC and bone marrow donations from living donors • Potential for reconsideration being ongoing
Example triggers:	• Loss of webforms/portal • Loss of CRM
Dependencies:	• Board members for assessments and panels • IA/AA/LDCs for report submissions / access to HTA decisions • Phone lines • CRM | Portal | EDRMS | Email | Remote Access • Emergency line
Linked documents:	• IA contingency report • Emergency out of hours checklist • Business Continuity and Out of hours assessment process for living donor transplant cases SOP 113 • Emergency Out of Hours Rota – 4 Jan – 1 Aug 2022 • Transplant units list • IA / AA / LDC / SCC contact list
Operational risk register:	No directly related operational risk. **Action: Ensure transplant risks, impact assessments and mitigating actions have adequate cover in risk register.**

Being Prepared for Critical Incidents

- Printed copy of contact lists, as updated.
- Ensure relevant governance documents is reviewed regularly.
- Ensure IA/AA/Board members are trained (including backup procedures.)
- DBS checks

What to do during a Critical Incident

Urgent and immediate

- Advise Comms of message for website if necessary.
- Cover emergency line
- Contact IA/AA/Co-ordinators/Board members expecting actions on the day
- Notify IA/AA/Co-ordinators/Board members/transplant units/NHSBT
- Maintain offline T-Number system.

Usual timescale

- Advise SMT and Comms as necessary.
- Maintain provision of advice and guidance

Recovering from a Critical Incident

- Ensure EDRMS & CRM are updated, and relevant parties are advised of CRM T-Number.
- Ensure hard copies are scanned, stored and originals securely destroyed or filed.
- Notify IA/AA/Co-ordinators/Board members/transplant units/NHSBT

Transplants contacts

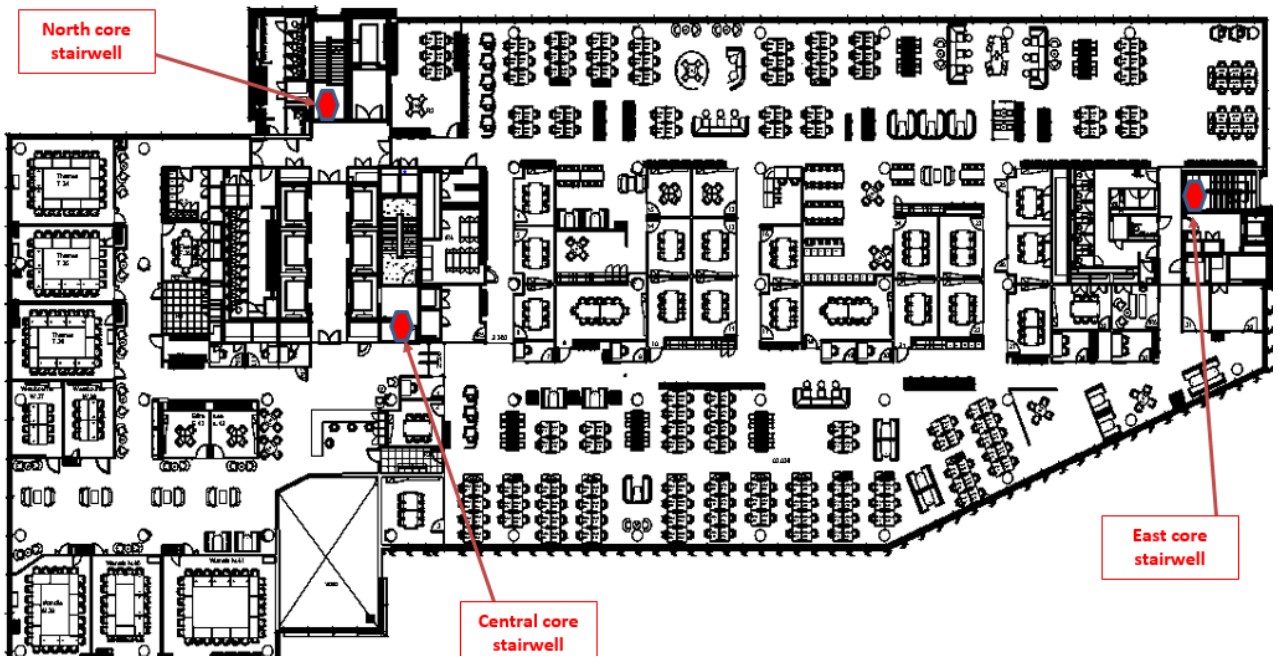
NHSBT Telephone	information withheld	information withheld	information withheld
NHSBT Organ Donor Line	information withheld		
Transplants and health law	information withheld		

Managing Critical Incidents – All Role Owners	
Urgent and immediate	**Usual timescale**
• Alert Role owners. SMS broadcast to role owners and include details of how and when to meet (e.g., conference call at 9am) • Go through First Meeting Checklist	• Arrange for a meeting with all role owners. • Go through First Meeting Checklist

Communicating during a Critical Incident		
Group	**Urgent and immediate**	**Usual timescale**
HTA staff Heads Role Owners SMT	**All Staff Role Sheet** – Role owner contact numbers **IT Role** – SMS Broadcast **Any role** – Portal Incident Page **HR Role** – Individual Mobiles **Teams Meeting** – Send invitation or add to call	**Comms Role** – Newsletter **CEO –** Weekly Exchange Call Outlook Meeting Requests All Staff Meeting All staff phone list
Board Members	information withheld	Name of Board secretariat Board Secretary
Licensed Establishments	**Comms Role –** HTA Website **Comms Role –** Mail Chimp **Other Roles –** Message/Content **IT Role –** HTA Portal **IT Role –** CRM Advanced Finds	
Public	**Comms Role –** HTA Website **Comms Role –** Social Media **Comms Role –** Mail Chimp **Other Roles –** Message/Content	

First Meeting Checklist	
1. Who is needed? Think about which roles should be included. Should anyone else be included? 2. Who should be the critical incident owner? The incident owner will be responsible for managing the incident and making sure actions and decisions are logged. The incident owner is not responsible for decisions. 3. Agree communication channels and frequency. 4. What is known about the critical incident? 5. Who is affected by the incident? 6. Do we need to take any immediate action? 7. Do we need to let anyone know about the incident?	**All Critical Incidents** SMT Role Communications Role CIRP Admin Role HR Role **IT / Phone Related** +IT Role +Finance Role **Licensing / Regulation/Transplant Related** + Regulation Role + Board and Planning Role + Transplants Role **Building Related** +Accommodation Role +Fire Wardens

2 RP Building Evacuation Plan



Revision history

Reference: HTA-BCP-03

Author(s):

Reviewed by: **Head of Finance**

Approved by:

Owner: Dr Colin Sullivan

Distribution: All Staff and Authority

Protective Marking: OFFICIAL

- April / Version: 21.0
- May / Version: 21.0 – reviewed by HoF. Updates to contact details and removal of business continuity references not required. Updated links to relevant documents.

HTA Policy

Business Continuity/Disaster Recovery Plan

Purpose

1. The purpose of this document is to provide the Human Tissue Authority (HTA), its staff and Authority Members with an action plan so that it can manage any possible threats (disruptions) to the organisation from both internal and external influences. These threats can take the form of systems failures or external emergencies such as natural disasters (fire, flood), terrorism or infectious disease.

Introduction

2. This disaster recovery and business continuity plan has been prepared with the aim of ensuring that the Human Tissue Authority is able to respond rapidly and efficiently to serious business disruption. This plan consists of the arrangements, procedures, and documents for reference in the event of a serious interruption to HTA's business. Its aim is to minimise disruption of essential activities and the consequential financial impact and to allow activities to return to normal as soon as possible.

3. Whilst it is impossible to predict every type of incident this plan provides a pragmatic framework to use by the Business Continuity Team (BCT) in the event of an incident such as fire, flood, bomb or terrorist attack, power and/or communication failure or any other emergency that may impact upon the daily operations of the HTA.

4. The main purpose is to:

   - Ensure members of the BCT are aware of and understand their responsibilities;
   - Provide a process for emergency incident notification;
   - Giver guidance on recovery planning, maintenance, and testing;
   - Ensure that there is a well-rehearsed, communications plan and communications channels are effectively maintained and utilised;
   - Minimise disruption, cost and operational impact;
   - Protect HTA's public image and minimise legal consequences, such as losing data if services crash, missing freedom of information deadlines due to non-availability of data.

Scope

5. This plan covers any incident that could seriously interrupt HTA's business for example:

    - Unavailability of premises for more than 7 working hours due to incidents such as fire, flood, or electrical outages;
    - Serious injury to, or death of, staff or visitors whilst in the offices;
    - Significant chemical contamination of the office or surrounding environment;
    - Staff prevented from accessing or leaving the HTA's offices due to external factors such as bad weather or transport issues;
    - Terrorist attack or threat affecting transport networks;
    - Theft or criminal damage to the extent that the ability to function is compromised;
    - Significant cyberattacks or severe disruption to the IT network and systems;
    - Significant cyberattacks or severe disruption to the HTA's website and other on-line information services;
    - Illness or epidemic affecting a significant number of staff;
    - Simultaneous resignation or loss of a number of key staff;
    - Widespread industrial action;
    - Significant fraud, sabotage, or other malicious acts.

6. Upon identification of an incident, the level of criticality is assessed by the BCT utilising the table found on page 9.

7. The plan provides for the recovery of priority business operations in accordance with predetermined time frames and for the resumption of other business operations as required and finally, a return to a permanent operating environment.

8. Individual building evacuation procedures are covered separately both through onsite visible documentation and the fire evacuation processes as agreed with building management.

9. HTA staff and visitors should await specific direction from the BCT or the recognised communication channels before taking action, for example attempting to re-enter the office. Managers should assess resulting business continuity issues within their specific areas.

Key elements to ensure business continuity

10. Several elements are in place to enable an effective and rapid response to a business-critical incident in order to mitigate possible damage.

11. The HTA's primary mitigation in relation to business continuity is the ability of the organisation to work remotely from its physical office. These processes are established ways of working and have been rigorously tested during the COVID19 pandemic.

12. The electronic file infrastructure is stored in the cloud (Azure). If either the office location is disabled, HTA's file information system remains accessible to staff via remote access.

13. Members of the BCT and senior management team can make necessary payments and purchases using Government Procurement Cards (GPC).

14. The text alert system is effectively maintained and *will* contain up to date information. Text will be used as the main method of communication (alongside email) to relay high level updates instantly.

15. The BCT will meet either in HTA office space (if possible) or they can meet virtually by using MS Teams or Zoom to plan next steps.

16. Our website is hosted *externally* and therefore maybe utilised to provide a notice board for staff and advice and information for stakeholders and the outside world.

17. This plan should be held by members of the BCT, their deputies and other members of the senior management team in a format that is accessible in the absence of network or intranet links. This can be in pdf downloadable format to personal devices such as phone or tablet. Otherwise it should be held as paper copies, one at home and one in the office.

18. Building management and security are provided with details of the BCT lead(s) and in the event of an out of hours incident the FM team lead for the floor will contact the designated HTA staff member.

Business impact analysis

19. The HTA is a regulator that performs activities under the Human Tissue Act 2004 and associated regulations including the Human Tissue (Quality and Safety for Human Application) Regulations 2007. The HTA makes consent the fundamental principle underpinning the lawful storage and use of body parts, organs and tissue from the living or the deceased for specified health-related purposes and public display. It also covers the removal of such material from the deceased. It lists the purposes for which consent is required (the Scheduled Purposes).

20. The critical functions that need to be maintained are:

    - processing and approval of organ and bone marrow from living donors donations for transplantation;
    - notification of establishments in case of adverse events related to tissue or cells used for human application;
    - provision of advice and guidance (via telephone / email); and
    - licensing / inspection of establishments that store human tissue for scheduled purposes, as defined under the Human Tissue Act and associated regulations;

- licensing of emergency mortuaries in mass fatality situations.

21. These are considered business critical functions because of the high risk / potential risks created should they be disrupted, e.g., patient safety.

Business Continuity Threat	Risk Level			Business Continuity action			
	Grade 1-5 Most - least likely	Grade 1-5 Most - least prepared		HTA Location only		Greater than HTA	
				Short-term 1-5 days	Long term 5 days plus	Short-term 1-5 days	Long term 5 days plus
Building							
Damage to the building (2nd Floor) – 2 Redman Place	4	1		Staff work from home	Staff work from home	Staff work remotely / possibly source alternative DHSC site	Staff work remotely / possibly source alternative DHSC site
Telecoms system failure – MS365	5	4		N/a as this would be a global incident	N/a	N/a	N/a
General energy outage to the area (Stratford)	2	4		Staff encouraged to work from home	Staff work from home	Staff work remotely	Staff work remotely
General access to 2 Redman Place denied due to environmental issue	3	1		Staff work from home	Staff work from home	Staff work remotely	Staff work remotely
Employee Health and safety incident	3	1-2					
Terrorist incident/threat – local area	5	2-3		Staff work from home	Staff work from home	Staff encouraged to work from home	Staff encouraged to work from home

Terrorist incident/threat – wide area	5	2-3	Staff work from home	Staff work from home	Staff work from home	Staff work from home
Inability to leave 2 Redman Place	5	2-3	Emergency team to ensure all staff accounted for	Emergency team to ensure all staff accounted for		

Business Continuity Threat						
	Risk Level		**Business Continuity action**			
	Grade 1-5	**Grade 1-5**	**HTA Location only**		**Greater than HTA**	
	Most / least likely	**Most / least prepared**	**Short-term 1-5 days**	**Long term 5 days plus**	**Short-term 1-5 days**	**Long term 5 days plus**
IT RELATED						
IT failure – network issues	4	2	Restore from backups			
Telecoms system failure – MS365	5	4	N/a as this would be a global incident	N/a	N/a	N/a
IT failure – data loss	4	2	Restore from backups	Restore from backups	This would mean data centres are down across Europe and little can be done	
Business related						
Transplant related issues – processing /approval of cases	2	1	Low risk as staff can access remotely	Low risk as staff can access remotely	Low risk	Low risk

Unable to process Licence applications	4	2		Impact is negligible – remote access	Impact is negligible – remote access		Access to CRM remotely	Access to CRM remotely
Unable to conduct on-site visits	4	1		Impact is negligible – remote access	Impact is negligible – remote access		Implement Virtual Regulatory Assessments (VRAs)	Implement Virtual Regulatory Assessments (VRAs)
Unable to receive reports of serious adverse events or reactions (SAEARs and HTARIs))	4	1		Impact is negligible – remote access	Impact is negligible – remote access			

Business Continuity testing

22. As our material mitigation for business continuity is remote working, we gain assurance of effectiveness via day-to-day operations and regular system testing.

23. The HTA will undertake an annual test of its business continuity cascade to ensure that all staff can be notified immediately of any business continuity issues.

24. Remaining premises-based testing will be undertaken in line with wider evacuation procedures and testing across all 5 ALB’s who utilise the 2nd Floor of 2 Redman Place and the wider building management testing regime.

25. This testing protocol, and any actual business continuity responses, will be catalogued and reviewed for lessons learned and these will be incorporated in future iterations of this policy.

Roles and Responsibilities

26. The table below details individual responsibilities

Role	Responsibilities
Senior Management Team (SMT)	• Awareness and understanding of the BCP • Provision of appropriate resource to maintain and continually improve systems to support business continuity • Ensure information governance standards continue to be applied to data and information during an incident • Provide support and assistance to the BCT where required • Act as a conduit for communication in the event of an incident
Heads of Service	• Maintain awareness of business continuity activity within their teams • Act as a conduit for dissemination of information, guidance, programmes of activity to management and staff
Staff	• Maintain awareness of the BCP • Alert a relevant senior staff member of potential or actual risks to business continuity • In the event of an incident, await management instruction • Ensure information governance standards continue to be applied to data and information • Ensure the text messaging system contains up-to-date telephone number (ideally mobile).
Business Continuity Team	• Assess the nature of the incident and decide upon the level of response as per table on page 9 • Ensure that where possible, the business of the HTA is maintained, and the organisation continues to meet the needs of its stakeholders • Manage any on-going incident on a day-to-day basis • Decide priorities and on the deployment of available resource • Decide which communication channels to use and when • Keep staff and stakeholders as informed as possible • Review actions taken following an incident and update procedures and BCP if required.

BCT Membership

27. The business continuity team (BCT) consists of a core group of people critical to the support functions and services the HTA. These are:

Key Contacts and Responsibility	
Chief Executive (CEO) - Chair Responsible for the safety of the organisation and making final decision.	information withheld
Director of Resources Responsible overall for estates, facilities management. First point of contact **DN: deputy for CEO**	information withheld
Director of Data, Development and Technology Responsible for agreeing communication to staff and the press. Responsible for overall IT disaster recovery including HTA IT systems, website and web-based services hosted for the HTA	information withheld
Head of Human Resources Holder of staff records	information withheld
Chief Information and Technological Officer First point of contact for IT related incidents. Liaising with IT Service providers	information withheld
Head of Communications Ensuring the agreed messaging to staff and the press is disseminated	information withheld

Deputies	
Head of Finance and Governance	information withheld
IT Operations Manager[1]	information withheld

28. The nature of the incident will dictate the composition of the BCT; therefore, members may not be required to attend all meetings and additional members may need to be co-opted (deputies). Membership will be determined by the Chair in light of the circumstances.

[1]Is on an FTC and may need to be replaced at end of contract

29. Deputies may be called upon to stand in if a member is unavailable and should be made aware of this responsibility.

30. Responsibility for the co-ordination and planning of meetings and actions, lies with the Director of Resources

31. In the event of an incident, the Director of Resources or the most senior manager on site should be informed by building management and/or security team. The BCT will be called together and proceed to issue instructions as to which actions should be taken and communications to staff. The BCT will ensure that appropriate support is available to staff should a traumatic incident occur.

Out of hours contact information

Staff contacts

Name	Title	Contact details
Colin Sullivan	Chief Executive	information withheld
Richard Sydee	Director of Resources	information withheld
Louise Dineley	Director of Data, Technology and Development	information withheld
Nicky Harrison	Director of Regulation	information withheld
Information withheld	Head of Human Resource	information withheld
Information withheld	Chief Information and Technological Officer	information withheld

Building contacts – 2 Redman Place

Name	Title	Contact details
Information withheld	Reception Manager	information withheld
Information withheld	Engineering Supervisor	information withheld
Information withheld	Head of Security	information withheld
Information withheld	Building Manager	information withheld

Tenant contacts – 2 Redman Place

Tenant	Contact	Contact details
Care Quality Commission	information withheld	information withheld

Human Fertilisation and Embryology Authority (HFEA)	information withheld	information withheld
Health Research Authority (HRA)	information withheld	information withheld
National Institute for Health and Care Excellence	information withheld	information withheld

32. In the event of an out of hours incident the above named contacts will be called in succession until a contact is made. Once contact is made, the building management or security will inform the BCT member of:

- The nature of the incident
- How this will affect the HTA
- What action is being taken
- Estimated timescales to resolution
- Whether a HTA representative will be required on site
- When a further update will be provided

33. The initial point of contact will note the information provided and contact the Director of Resources (or Deputy in his absence).

34. The Chief Executive and the Director of Resources will make an initial assessment and assist in formulating an initial plan.

35. The Director of Resources will determine if the issue is significant enough to require formation of the BCT. Should this be the case a time and place for the BCT to meet will be decided.

Communication Strategy

36. The BCT will be responsible for approving the appropriate statements for internal and external communication. The communications team will manage contact with the media and external parties in conjunction with SMT. Should a Director or the BCT need to speak with the media about the incident, the Head of Communications will assist in making any release statements.

37. The BCT will keep staff and stakeholders as informed as possible during the incident and recovery phase.

38. The HTA BCT in the event that MS 365 is unavailable, will use WhatsApp or normal text messaging to keep BCT members up to date with ongoing incidents. The incident will remain live until a BCT member has confirmed that the incident has been resolved. If a BCT member is not contactable (say due to annual leave) they should add a deputy to the WhatsApp or other group system for the duration of their absence. They must contact the group to advise of their absence and who to contact should an incident arise that requires their team's input. On return to work, the deputy should be removed from the group.

39. The BCT will use the text alert system to update all staff as necessary. The internal communications team will send messages directly to staff. The messages will be short updates including key information within the 160-character text limit. Reminders to update the text service with mobile numbers are circulated regularly to staff and included in the induction programme.

40. Updates can be posted to external audiences or to staff unable to access emails from home or the text alert system using the HTA website and social media channels, Twitter, or Facebook.

Level of criticality of incidents and corresponding actions

41. The table below summarises the impact of various types of disruption on a scale of **1** (disruptive/inconvenient) to **5** (major impact on the HTA). These are examples. The scale of the incident will determine the course of action to take. If the criticality of the incident is at level 3 or above, a meeting of the BCT is essential.

Incident	Impact	Impact Rating	Key Action
IT – loss of use of MS[2] 365 which includes Telecoms and access to Azure (this would be extremely rare and out of our control)	Very severe disruption	5	Convene BCT. Liaise with Microsoft. Communicate with staff via text message system as to duration.
Premises – long term loss of access to 2 Redman Place	Disruption	3	Convene BCT. Communicate instruction for staff to work from home till further notice Move to online Staff/Committee meetings. Assess number of staff who may need access to an office environment.
Power – long term loss of power to the building	Disruption	3	Convene BCT. Contact building management or security.

[2] Microsoft have a service agreement 99.9% guaranteed up-time and two data centres where replication of servers takes place.

Incident	Impact	Impact Rating	Key Action
			Communicate with staff via text message system. Use externally hosted website to advise stakeholders. Where possible move imminent committees to virtual.
Staff – temporary loss of staff due to a pandemic, either through illness, social distancing, or redeployment to assist with national emergencies, impacting the ability to deliver critical business systems	Severe disruption	4	Convene BCT. Communicate with staff via text message system. Identify priority work and allocate resources accordingly.
Significant or prolonged loss of website or website services	Severe disruption	4	Convene BCT. Ensure the website recovery plan has been initiated. Communicate with staff via email.
Power – temporary loss of use (1 day)	Minor disruption	2	Convene BCT Communicate with staff via text message system. Advise of alternative ways of working from home.
Telecommunications – temporary loss of use (1 day)	Inconvenient	1	Liaise with building management and IT. Communicate with staff via text and email.

Ownership, maintenance, and distribution

42. The Business Continuity Plan will be owned by the BCT who will also be responsible for change control, maintenance, and testing of the plan annually.

43. Each BCT member and their appointed deputies should keep two hard copies of the BCP allocated to them. One at home and one in the office. It is also advised that a PDF version is saved on personal mobile devices. The plan should be reviewed and updated annually. The responsibility for ensuring this falls to the Director of Resources and operationalised by the Corporate Services Manager.

44. A version of this document will be available on WAVE (intranet).

Revision history

Reference: **BCP-004**

Author(s): Head of Finance

Reviewed by: Director of Resources

Approved by: SMT

Owner: Director of Resources
Distribution: BCT/Staff

Protective Marking: OFFICIAL

- (20 May 2021 / Version 1.0: Created)
- (10 June 2021 / Version 1.1: Approved by SMT)
- (27 Aug 2021 / Version 1.2: Adjustment to levels of criticality)
- (09 Jan 2022 / Version 1.3: Update contact details)

Audit and Risk Assurance (ARAC) meeting

Date: 9 June 2022

Paper reference: 21/22

Agenda item: 9

Author: Morounke Akingbola
Head of Governance and Finance

OFFICIAL

Declaration of Interests, Gifts and Hospitality policy

Purpose of paper

1. The purpose of this paper is to present to the Audit, Risk and Assurance Committee the Anti-fraud Policy.

Decision making to date

2. The SMT reviewed the above policy at its meeting on the 18 May 2022.

Action required

3. The Committee are requested to note the updates and amendments to the policy as detailed below:

- para 2 - effective date of Bribery Act added;
- para 5 - Authority changed to Board;
- para 8 - amendment to Director of Finance to Resources;
- para 10 has been added and refers to adherence to professional standards as set out in the Ethical Code of CIPS;
- para 11 - last sentence refers to Board Member declarations
- para 28 - last sentence in bold added

- para 29 - amended to show Gifts Register to be presented when there are items added, else it will be stated that there are no additions and
- para 31 - has been added and refers to staff training.

4. The Committee are requested to approve the review period of 2 years (para 33) and approve the updated policy.

Annex A- HTA-POL-051- Declaration of Interests, Gifts and Hospitality Policy (AUD 21a/22)

Annex B- Gifts and Hospitality Register (AUD21b/22) Financial year 2021/22

HTA Policy

Declaration of Interests, Gifts and Hospitality Policy

Purpose

1. The aim of this policy is to enable the HTA to demonstrate both to the public at large and others in the sectors we regulate that its processes and decisions are objective and consistent, and to protect staff from unfair accusations of concealed interests.

2. All employees of the HTA should be aware of the Bribery Act 2010 which came into effect on 1 July 2011. This act creates specific offences of bribing, and being bribed, which apply to any function of a public nature; any activity performed in the course of a person's employment; and any activity performed by or on behalf of a body of persons.

3. All employees must ensure that they do not solicit or accept any financial or other advantage which results in the improper performance of their duties as an HTA employee.

4. This policy provides guidelines for the management of the registering of staff interests, and the accepting or refusing of gifts, taking into account the terms of the guidance to public bodies.

Scope

5. This policy applies to full time and part time employees on a substantive or fixed-term contract, Board Members and to associated persons such as secondees, agency staff contractors and others employed under a contract of service.

6. The Gifts and Hospitality Register will not be routinely published by the HTA, however, information contained in the register may be disclosed pursuant to any request for disclosure made under the Freedom of Information Act 2000.

Principles

7. It is acknowledged that in their role as employees of the HTA that individuals may be exposed to a number of potential conflicts of interests.

   - Direct pecuniary interest – the most clear-cut situation where common law requires that executives with a direct pecuniary interest should not participate in the discussion or determination of matters.
   - Indirect pecuniary interest – again, common law requires that members of staff show consider whether participation in the preparation of items for discussion or discussion of a matter would suggest a real danger of bias. This should be interpreted in the sense that a member of staff might unfairly influence the case of a party to the matter under consideration. In considering whether a real danger of bias exists in relation to a particular decision, members of staff should assess whether they, a close family member, a person living in the same household as the HTA staff member, or a firm, business or organisation with which the member of staff is connected are likely to be affected more than the generality of those affected by the decision in question. (A 'close family member' is regarded here as personal partners, parents, children, brothers, sisters, and personal partners of any of these.)
   - Professional/personal interests – These are more subjective, but it is just as important that they are declared. This would include involvement with a charitable trust or professional organisation within sectors or related clinical or scientific fields. Professional and personal interests are taken to include those not only of the individual staff member, but also interests of close family as defined above. It would also be necessary to make a declaration when asked to participate in preparing documents about specific issues for HTA Authority Members to discuss, if a member of staff has a close personal friend or previous association.

8. If in doubt, individuals are advised to declare the potential interest or at least consult the Director of Resources or relevant Director as soon as they are asked to participate in the preparation of an item for HTA or sub-Committee consideration. Anyone who is unclear about whether a particular interest constitutes a conflict of interest should discuss this with their line manager or Head of Finance in the first instance. The guiding principle is when in doubt it is better to ask for a record to be made, than not.

Declaration of Interests

9. Staff should declare if they, their partners, family members or a close friend have financial, professional, or personal interests in: -

- Organisations licenced by the HTA, or other organisations involved the use, procurement of human tissue
- Companies or individuals providing services for or bidding for contracts with the HTA.

10. All staff who are in contact with suppliers and contractors (including external consultants), and in particular those who are authorised to sign Purchase Orders, or place contracts for goods, materials, or services, are expected to adhere to professional standards as set out in the Ethical Code of Chartered Institute of Purchasing and Supply (CIPS).[1]

11. The Head of Finance periodically asks members of staff to update their details of personal and professional interests and will e-mail a form for completion and return (see appendix A). Any additional interests arising during the year should be e-mailed to the Head of Finance for inclusion in the Register of Interests. Board Members will be requested to provide updates also during the annual reporting process (December through March).

Policy Statement

12. You must declare all offers of gifts and hospitality, made to or by you, regardless of value, in your role at the HTA. **All such offers must be declared whether accepted or declined**. Offers of gifts and hospitality may include items ranging from diaries, wall charts, and boxes of chocolates, to free international travel and accommodation.

13. Declarations must be recorded on HTA's Gifts and Hospitality Register (the register). The register is maintained by the Director of Resources and is potentially publicly available through Freedom of Information requests.

14. It is your responsibility to ensure that you are not placed in a position that risks, or appears to risk, compromising your role or the HTA's public and statutory duties. You should not secure valuable gifts and hospitality by virtue of your role at the HTA. You should not accept or provide any gift or hospitality while acting in an official capacity, if acceptance/provision will give the impression that you have been influenced/are deemed to be influencing the activity or work of the HTA.

15. This Policy also applies to spouses, partners, or other associates if it can be argued or perceived that the gift or hospitality is in fact for your benefit.

[1] The code can be found at: https://www.cips.org/who-we-are/governance/cips-code-of-conduct/

16. In exercising judgement as to whether to accept a gift or hospitality, the question should be asked what the public perception would be if the information were published given your role and circumstances.

Receiving gifts

17. Staff are permitted to keep small, low value gifts e.g., promotional pens/mugs/calendars etc. All other gifts should be declined unless it is felt that to do so would cause embarrassment to the HTA. For example, to refuse a gift from an international delegation may cause embarrassment to both the HTA and the delegation.

18. All other gifts should be passed to the Director of Resources who, in conjunction with the Chief Executive, will decide on the most appropriate action, which may include:

    - returning the good to the supplier;
    - sharing the gift with all staff;
    - retaining the good within the HTA;
    - donating the gift to charity; or
    - Allowing the member of staff to keep the gift.

Accepting offers of hospitality – genuine business reasons

19. Hospitality offered should only be accepted where there is a direct link to working arrangements and a genuine business reason can be demonstrated, for example:

    - attendance or speaking at a conference, which provides complimentary subsistence;
    - attending a free training course; or
    - attending a reception for networking purposes.

20. It is recognised that, in the course of carrying out your duties, you will need on occasion to ensure good relationships with existing and future contractors and stakeholders and that this may involve for example, the receipt of modest working lunches and dinners. These are acceptable where there is a genuine business reason.

21. Hospitality invitations to events, which are purely social events, should be considered very carefully before accepting; in such circumstances, it may be much more difficult to substantiate a genuine business reason. All invitations should be recorded in the register whether received or declined.

Gifts and hospitality offered by the HTA

22. HTA staff must be mindful that the value of all gifts and hospitality offered by the HTA are sourced from public funding, and the expectation is that such funding will be used for legitimate purposes and in keeping with value for money considerations.

23. In exceptional circumstances, it may be appropriate for the HTA to provide a gift of up to £50.00 in value, for example: providing a nominal gift to someone who spoke at an HTA conference free of charge.

24. It is acceptable for the HTA to provide modest hospitality in the way of working lunches and/or dinners to existing and potential contractors and stakeholders subject to a genuine business reason.

Declaration

25. You should make your declaration as soon as possible after the offer or receipt of gifts or hospitality. All declarations are to go to the Head of Finance and Governance in the required format as shown below. The Head of Finance and Governance will record the declarations in the register. The register is an annual document and will be broken down and filterable by financial year. It is recommended that you make your declaration by email and retain a copy for your personal records.

26. Your declaration will need to include the following information:
    - the date of any offers of gifts or hospitality, and the date of events where relevant;
    - the name, job title and the organisation of the recipient/provider;
    - the nature and purpose of the gift or hospitality received or declined;
    - the name of any other organisation involved;
    - the estimated value of the gift or hospitality.

For example:

Date received	12 Dec. 2016
Recipient (Name & Directorate)	Jane Brown
(Resources)	
Received from (Name, position & organisation)	Josh Sergeant
(AAA Ltd)	
Description of Gift/Hospitality received	Lunch
Value £ (Estimate if unknown)	Approx. £15.00
Reason given for providing gift/hospitality	Working lunch provided during contract discussions

27. Personal data of HTA employees processed by the implementation of this document will be done so in accordance with HTA-POL-108 HTA HR Privacy Policy. Personal data of non-HTA employees processed by the implementation of this document will be done so in accordance with the HTA's Privacy Notice.

28. You should consult the Director of Resources or Head of Finance and Governance for any guidance required on this Policy**. If you have any doubt about whether an item should or should not be accepted, you are advised to decline and declare it**.

Monitoring

29. The register will be reviewed quarterly by the Resources Directorate and provided to the Audit and Risk Assurance Committee in full only when there are items added to the register, otherwise it will be confirmed by the Executive if there are no items.

30. Staff will be reminded periodically of their requirement to declare gifts and hospitality provided/accepted/declined in accordance with this Policy.

Training

31. Staff will be required to undertake annual training via the Astute Learning platform.

Policy breach

32. Staff who fail to declare the acceptance/provision/decline of hospitality and gifts in accordance with this policy may be subject to disciplinary action under the HTA's Disciplinary Policy.

Review

33. This document will be reviewed every two years.

Other policies of relevance and references

- Whistleblowing Policy
- Anti-fraud, Bribery and Corruption Policy
- Chartered Institute of Purchasing and Supply Ethical Code of the Chartered Institute of Purchasing & Supply (March 2013)

Declaration of Interest **Annex A**

HUMAN TISSUE AUTHORITY

HTA STAFF – REGISTER OF INTERESTS

As a public body, the HTA is required to demonstrate that it has well defined and transparent arrangements for handling conflicts of interest, whether real or perceived. The HTA must be able to demonstrate both to the public at large and other stakeholders that its processes and decisions are objective and consistent.

An important mechanism for ensuring and demonstrating this objectivity is the maintenance of a register of interests. The Standing Orders require the Chief Executive to establish a register for Members of the Authority and staff. Members' register of interests is publicly available on the HTA website. A similar register of interests has been established for all staff. This register whilst not published on our website is available for inspection.

Members and staff should declare if they, their partners, relatives, or friend (as far as is known or might be considered significant) have financial, professional, or personal interests in: -

- establishments licensed by the HTA, or other organisations affected by the work of the HTA;
- Companies or individuals providing services for or bidding for contracts with the HTA.

If staff are in any doubt whether to declare an interest, this should be discussed with their manager or the Head of HR. It is better to declare something when in doubt.

Declaring an interest does not imply any inappropriate behaviour by staff, nor adversely affect your employment. There may be occasions when you are asked not to work on a specific issue if there is a conflict of interest as it is part of ensuring public confidence in the fairness and transparency of the HTA's decision making.

Please complete the form overleaf detailing any relevant interests including a "nil return."

We will be repeating this request for declarations in November and April (financial year-end). In the meantime, if your circumstances change, and a new interest arises that should be declared, please e-mail the Head of Finance and Governance at: morounke.akingbola@hta.gov.uk.

Name____

Address____

Please complete Box A or Box B

BOX A ☐ **I / my partner / relatives or friend (as far as is known or might be considered significant) have the following financial, professional, or personal interest in: -** * Delete as appropriate If not self, please state name of person with interest and relationship ____ **Establishments licensed by the HTA, or other organisations affected by the work of the HTA (please give details)** **Companies or individuals providing services for or bidding for contracts with the HTA (please give details)**
BOX B ☐ **I have no interests to declare**

Signed_______________________________________ **Date** _________________

Revision history

Reference: HTA-POL-051

Author(s): Head of Finance and Governance

Reviewed by: SMT

Approved by: Audit, Risk and Assurance Committee (ARAC)

Owner: Director of Resources
Distribution: Staff and HTA Board

Protective Marking: OFFICIAL

- Oct-19/ Version 1.3: No amendments)
- Nov-20/ Version 1.4: Minor amendments)
- August-21/ Version 1.4: Minor additions included reference to other policies)
- May-22/ Version 1.5: Few amendments made, and section added (section 10)

AUD21b/22 **Register of Gifts / Hospitality Received and Provided**

Version: HTAG0001
Jun-22

DIVISION / DEPARTMENT:	**HTA**
FINANCIAL YEAR(s):	**2021/22 - onwards**

	Details of the Gift or Hospitality						**Provider Details**			**Recipient Details**	
Type	**Brief Description of Item**	**Reason for Gift or Hospitality**	**Date(s) of provision**	**Value of Item(s)**	**Location where Provided**	**Action on Gifts Received**	**Name of Person or Body**	**Contact Name**	**Relationship to Department**	**Name of Person(s) or Body**	**Contact Name**

Audit and Risk Assurance (ARAC) meeting

Internal Audit – Confidential

Audit and Risk Assurance (ARAC) meeting

Audit Tracker – Confidential

Audit and Risk Assurance (ARAC) meeting

External Audit – Confidential

Audit and Risk Assurance (ARAC) meeting

Date: 9 June 2022

Paper reference: AUD 25/22

Agenda item: 15

Author: Richard Sydee, Director of Resources

OFFICIAL

ARAC Committee Effectiveness Review

Purpose of paper

1. To provide ARAC with a summary of responses to the ARAC Committee effectiveness questionnaire

Decision-making to date

2. This paper was approved by the Director of Resources on 26 May 2022.

Action required

3. ARAC Members are asked to:
   - Note the summary comments
   - Consider any actions in relation to the ARAC timetable and the approach to the induction of new members, and a consideration of when the next review might be scheduled

Background

4. Following the last ARAC meeting members were issued with a questionnaire to provide feedback on the effectiveness of ARAC meeting. The questionnaire

posed 15 questions within 4 sections and feedback against each of these sections is summarised below.

Membership, independence, objectivity & understanding

5. Responders reported having a good understanding of the terms of their appointment to ARAC and any conflicts or declarations of interest are correctly noted, and action taken if appropriate. It was agreed by all responders that attendance from the Executive team is appropriate and that by and large there was sufficient time to discuss issues with internal and external audit without HTA employees present – although it was suggested this could perhaps be more structured.

Role and scope of the committee

6. All responders agreed that this was appropriate and that there was regular review and discussion of audit issues, risk registers, cyber security and HTA policies. Improvements to risk and cyber reporting were acknowledged and welcomed although the need for the detailed risk mitigation matrix to come regularly was questioned.

7. It was also noted that there had been improvements in tracking and resolving audit recommendations, but that this could and should continue to improve.

Organisation of meetings

8. Responses indicated general satisfaction with papers and the cycle of business and that there is sufficient time and coverage to ensure members can raise all issues they would like to discuss. It was noted that there are sometimes late revisions or additions to papers, which does impact on members time in terms of scheduling the review of papers, this is clearly an area for further improvement over the coming year.

9. Members would like to see a resumption of the deep dives and more timely advice to ARAC on emerging pressures on the organisation.

Other reflections

10. Members felt the ARAC meetings was open with good challenge and discussion between the members, executive and internal and external auditors. It was noted that training had not been a regular part of the ARAC timetable, and this should be considered in the areas that are frequently discussed at ARAC (Rick, Cyber Security and Corporate Accountability), particularly so given the recent changes to membership of the Committee.

11. We should continue to build on the improvements outlined above in relation to risk and cyber reporting and resolving audit recommendations and overall maintain and build on the contribution of ARAC to the HTA.

Audit and Risk Assurance (ARAC) meeting

Date: June 2022

Paper reference: AUD 26/22

Agenda item: 16

Author: Sandra Croser

OFFICIAL

Equality Diversity and Inclusion

Purpose of paper

1. The purpose of this paper to is report how the HTA is working to improve our Equality, Diversity, and Inclusion (EDI) representation across the HTA and encouraging a workforce that is also representative of the wider UK environment in which we operate

2. This paper has been developed for ARAC in response to the GIAA audit response delivered in January 2022. However, as RemCo will have a remit to support the CEO in People matters, it is expected that EDI will be reported to RemCo on an annual basis going forward. There are of course people related risks that ARAC has an interest in, and in that regard please note the most recently developed people risk form the Strategic Risk Assessment at Annex A, which references the importance of a facilitating a diverse workforce.

3. The HTA is committed to encouraging diversity across all activities and processes. We continue to build EDI awareness into all aspects of our operational and strategic objectives. All HR related policies contain an EDI statement of intent and all benefits, including flexible working and remote working are available to all colleagues as they join the HTA. Great care is taken to ensure fair and equitable practices are adopted to support colleagues throughout the employment lifecycle.

4. Our Recruitment process is designed with anonymity at the first long listing stage. This enables hiring managers to assess the skill and suitability to the role without further context to any of the protected characteristics including sexual orientation, gender, race, nationality, or ethnicity. We offer all candidates the option to request accommodations during the recruitment process and have received positive feedback as to the nature of our inclusive recruitment practices.
   We continue to monitor our job descriptions and job adverts to ensure we use inclusive language and reduce the potential impact of unconscious bias.

5. The HTA gained both the Race at Work and the Disability Confident accreditations in 2019/20 and promote these on our HTA website, our recruitment documentation, and all internal communications.

6. We have also recently introduced a Candidate Recruitment pack to support the job description and advert. This provides prospective candidates with a broad understanding of who we are and what we stand for. This includes our organisational EDI statement and accredited badges.

7. Our HTA handbook, launched in 2021, sets expectations for new and existing colleagues of what they can expect from the HTA and just as importantly what the HTA expects from them across all topics and including EDI.

8. We have Wellbeing and Diversity pages on Wave owned by HR and that are regularly updated to reflect topical ‘awareness days or trending research and training opportunities. We also hold many social events that incorporate EDI such as Diwali, Chinese New Year and St Georges day to name a few. Very regularly links are provided in the weekly newsletter directing colleagues to the various events and material available on Wave, keeping the awareness and momentum top of mind.

9. It is important to us that all colleagues know who to go to in addition to their Line Manager, for advice or guidance regarding EDI. The EDI page on Wave clearly displays our CEO as the HTA Senior Sponsor for EDI and HR colleagues as the named champions.

10. EDI has been incorporated into the quarterly mandatory training programme including topics of Challenging Unconscious Bias, Managing and Identifying Stress, and Respect in the Workplace etc, to further support our EDI policy and practices across the HTA.

11. Additionally, we have created, launched, and updated HR policies that support colleagues through many of life changes, including but not limited to Remote working, Flexible working, Trans Equality, Menopause and Equality, Diversity, and Inclusion.

12. We encourage Leaders across the HTA to start team meetings with a wellbeing check in and Line Managers add this to all 1:1 meetings. This encourages colleagues to discuss areas of concerns and raise topics they would like to better understand.

13. Over the last 2 years, we have held a number of Listening events, the last one was well attended with the topic of 'Time to Talk' highlighting mental health awareness which coincided with a national Time to Talk event. This was designed to encourage colleagues to discuss their experiences and share tips with what works for them. We have also held a Diversity and Inclusion session where colleagues shared experiences related to discrimination or exclusion. The next session planned for June, has a topic of Neurodiversity. Colleagues will discuss the impact on them in living with various neurodiverse challenges and how the HTA can raise awareness of and help to reduce stigma of learning and thinking differences.

14. Lastly, we are building an EDI shared network across the sector taking advantage of scale and enabling us to provide a wide variety of support groups to the HTA by tapping into existing groups and networks. We will also lead and own specific groups so contributing to the wider network. Our CEO is leading this initiative and the first meeting was held at the end May.

15. Below is a breakdown of the statistics related to EDI, where the data is available previous recorded statistics have also been included to provide guidance as to the progress made:

    a. Nationality:
    The majority of our colleagues are British or have a dual British nationality. There are a small number of colleagues who have chosen not to identify their nationality and the remainder represent a small number of different European nationalities. We don't currently have any colleagues with a nationality from outside of Europe.

Nationality	British/ Dual	European	Non-European	Undefined
January 2020	81%	8%	2%	8%
31 May 2022	83%	8%	0%	8%

b. Ethnicity:
The HTA is predominately white British. However, we have made some progress with a more diverse ethnic demographic, although it should be noted that we still have 14% of colleagues choosing not to define their ethnicity within our systems.

Ethnicity	White British	Non-White British	Other	Undefined
January 2020	60%	8%	10%	14%
May 2022	64%	23%	0%	14%

c. Gender:
Currently all HTA colleagues self-identify as male or female. For future reporting, if colleagues identify as non-binary or Agenda, it may be necessary to adapt the report in order to protect the identity of colleagues.

As with many organisations within our sector, we have more colleagues that identify as female than male. However, the trend does demonstrate we are moving towards a more gender balanced population

Gender	Male	Female
January 2020	26%	74%
May 2022	34%	66%

Recommendation

16. ARAC members are asked to note report how the HTA is working to improve our Equality, Diversity, and Inclusion (EDI) representation across the HTA and encouraging a workforce that is also representative of the wider UK environment in which we operate. Going forward, these will be issues discussed primarily at the revised Remuneration and People Committee.

Annex A

June 2022

Strategic Risk Register

People Risk (4)

The People Strategy needs to reflect and support the HTA Objectives by facilitating the recruitment and development of a highly skilled and diverse workforce.

The strategy will include support for a robust, fair, and equitable recruitment process that facilitates the most effective utilisation of headcount against the agreed deliverables. A formal assessment of future capability needs and how these should be met will also support effective internal resource deployment and identification of future skill sets required. Succession planning will be developed as part of the workforce model.

The strategy will include a regular review of processes and procedures with relevant colleague training and awareness provided to ensure appropriate adherence to the relevant policies and governance compliance.

The People strategy will also encourage and support colleague Wellbeing programmes that not only meet our duty of care, but also reinforce and recognise the relationship between appropriate support and colleague engagement.