**HEALTH RESEARCH AUTHORITY**

**AUDIT AND RISK COMMITTEE MEETING**

**Minutes of the Health Research Authority (HRA) Audit and Risk Committee meeting, held on 01 February 2016 from 1.00pm – 4.00pm in**

**Room 136B, Skipton House**

|  |  |
| --- | --- |
| **Present** | **Initials** |
| Present:Graham Clarke HRA, Non-Executive Director *(Chair)*Deirdre Kelly HRA, Non-Executive Director Nalin Thakker HRA, Non-Executive DirectorMarc Taylor HRA, Audit and Risk Committee MemberIn attendance:Karen Williams HRA, Director of Finance, Procurement and EstatesTeresa Allen HRA, Interim Assistant Chief ExecutiveIan Cook HRA, Director of Corporate ServicesZafir Ali Health Group Internal Audit, Head of Internal AuditGareth Davies MazarsMadeline Dugmore National Audit OfficeJane Martin HRA, Quality Assurance ManagerStephen Robinson HRA, Corporate SecretaryCollette Rowe HRA, Senior Finance Manager Hilary Tulloch HRA, PA to Chief Executive | GCDKNTMTKWTAICZAGDMDJMSRCRHT |
| **Item** | **Item details** | **Action** |
|  | **Welcome**GC welcomed Karen Williams, HRA Director of Finance, Procurement and Estates to the Committee. |  |
| 1. | **Apologies**Stephen Tebbutt HRA, Head of Corporate Governance Ilga Eile-Parker National Audit OfficeKeith Illingworth Mazars  |  |
| 2. | **Conflicts of interest**None to note |  |
| 3. | **Minutes of the last meeting held on 01/06/2016**The minutes of the previous meeting were accepted as a true and accurate record. |  |
| 4. | ***Action Log***HRA Standing Orders, Reservation and Delegation of Powers and Standing Financial Instructions; and HRA Delegation of Financial PowersThe Committee agreed to carry this action forward for ST to update.Audit recommendations tracker Suggestions to improve and streamline the tracker. Has been actioned.Can be closed.HRA Governance Arrangements and Board EffectivenessCarry forward to around mid-year when new membership have had sufficient experience of the committee to contribute Assurance MappingTo be kept open.External Audit meeting with NEDsTo be scheduled prior to next audit meeting. To be kept open.HRA Information Systems Strategy Development Advisory ReportTA advised that Draper and Dash have just started work to look at IS need across the business and will potentially work collaboratively with 3rd parties. This work is distinct from the IT Strategy review. Will come back in 3 months to update. To be kept open.Audit Recommendations TrackerCR apologised for not updating out of session but confirmed that the high rated recommendation had been closed with good progress having been made against the medium rated recommendation.  The update on progress could be seen on the audit tracker and recommendations summary. Carry forward to next meeting 26 AprilHRA Corporate Risk Register September 2016The committee noted that the HRA Approval risks still remained so in the absence of ST agreed to carry this forward to next meeting 26 April. | **ST** |
| 5. | **External Audit update**GD advised that the paper had previously been circulated in November and that internal visits to the HRA and planning and testing work had been completed. He also confirmed that the Audit approach was similar to last year with no significant change from audit or accounting perspectives, that the handover from Moore Stephens had been undertaken efficiently and that Mazars was not new to NHS or DH working practices. KW advised that there had been considerable change within Finance last year but consolidation was the priority for this year.With regard to the NAO statements in Appendix 6, TA confirmed that ST was progressing work to examine risks across ALB’s through the DH ALB Risk Management Forum. |  |
| 6. | **Progress report: Delivery of HRA Internal Audit Plan 2016/17**ZA reported that delivery of the programme was on time and thanked HRA management for timely delivery. He advised that 3 review ToRs had been agreed and work has commenced on them. All was on track therefore for completion of the programme by the end of March 2017.GC asked whether other ALBs rush to complete internal audit by year end causing resourcing problems. ZA confirmed that in some ALBs they do for internal reasons but that this will not affect the HRA.ZA confirmed that the audit programme was synchronised to the financial year and therefore runs from April to March.  |  |
| 7. | **Final Audit Reports from HGIAS** 1. Cyber Security Audit report

ZA stated that the report author had planned to attend but apologised that she could not now attend. He reported that the audit had resulted in a limited rating but was pleased to report that HRA management had been responsive and had instigated actions to progress the recommendations.NT asked if the HRA was aware of the information it had in its possession. SR advised that the HRA implements the standard NHS Information Governance framework that consists of SIRO, IAOs and IAAs and advised that an annual information asset review is conducted. At present 16 information assets had been identified ranging from simple excel spreadsheets for contact databases to IRAS and HARP. Risks are identified within the review and appropriate action plans developed to mitigate those risks. GC noted that no information risks were on the corporate risk register. SR replied that the Information Governance Steering Group regularly reviewed information risks but that none were deemed to be above a 12 rating so would not appear on the register. DK asked why ethical hacking was not undertaken and suggested that we should look to commissioning that work. It was noted by the Committee that industry standard penetration testing is undertaken annually but if ethical hacking testing was appropriate for IRAS / HARP, management would undertake it as suggested.TA advised that the main assurance for system security was undertaken through the procurement contract with BGO with Gaynor Collins-Punter as the manager. NT asked how an attack on IRAS would be dealt with. SR advised that the current host of the system, Rackspace was fully accredited and had appropriate systems in place to prevent such attacks. It had responded quickly to a previous DDOS attack resulting in minimal system down time. The Committee noted that the hosting arranging for IRAS / HARP were under review.DK asked how vulnerable to phishing the HRA is. IC advised that we do have guidance on how to deal with phishing but this problem related primarily to the NHS Mail / ATOS system, not IRAS / HARP.MT noted that the report had indicated that there are gaps in staff training and suggested that there needs to be broader thinking as to what the training needs are and what the risks might be. SR advised that the HRA currently uses the Civil Service Learning packages which are accredited for all Civil Servants but concurred that in light of the report a review of training should be conducted to see if the HRA can commission alternative training. JM also noted that T&Cs for volunteer members were clear on requirements regarding information management and confidentiality.GC asked if HRA’s information risk had been assessed from a DH perspective. SR advised that the HRA works closely with the DH Information Governance team and have been classified as Tier 3, low information risk organisation as we carry very limited sensitive PI information – for example most of the HRAs sensitive information relates to staff but SBS holds the majority of that information. He also stated that the DH sought assurance of this through an annual process consisting of completing a comprehensive questionnaire that follows the HMG Security Policy Framework. DK suggested that external help may prove useful and that NHS Digital may be in a position to provide this help. TA agreed that this could be useful to investigate. 1. **Payroll Audit report**

ZA advised this audit had been requested by DC and resulted in a moderate rating. DK asked how much of the audit work related to BSA. ZA confirmed that the audit had only looked at HRA processes.NT noted that the audit had only sampled a small number of records but problems were still found. Could this be indicative of widespread problems? ZA replied that the majority of the recommendations were rated low with only 2 mediums and that evidence of good practice had been found, so whilst problems had been found, they were not indicative of a serious lapse of control. Management had also accepted and actioned all recommendations. KW advised that BSA had also taken steps to tighten their processes.1. **Risk Management Audit report**

ZA advised that the audit had found lots of good practice and that all the recommendations were low.A discussion on risk appetite ensued and it was agreed that the Board should embark on a process of defining the HRA’s risk appetite. DK suggested and the committee concurred that a good way forward would be to hold a seminar to examine the issues. It was suggested one way of approaching it could be defining tolerance by risk category i.e. financial, business, staff, IT etc. and setting a base line of risk that would not be tolerated.ST will be asked to progress this.1. **Records Management Audit report**

ZA reported that the audit had looked at records management policies and procedures and that a moderate rating had been achieved. NT expressed concern that no records themselves were examined and that interviews were conducted by phone and therefore the audit had been limited in scope. ZA advised that this was due to the allocated audit budget and agreed to review the approach for any future audit.MT advised that a new general data protection regulation could be in place in a year so suggested that this area should be flagged up for another review to ensure compliance with the new law.GC concurred and advised that it should be noted that the committee will want to revisit this at some point in the future.  |  |
| 8. | **Audit recommendations tracker**The Committee welcomed the new format.CR reported that a number of recommendations are now closed which were outstanding at the last meeting. ZA agreed that there was an improvement in number of high recommendations falling. DK asked whether the recommendations do make a difference. ZA replied that in his view acting on the recommendations does improve the control environment and therefore reduces organisational risk. IC concurred stating that the HRA is not forced to accept recommendations but that once agreed and implemented, in the main they do add value. KW urged that proportionality between the number of recommendations and the resources available to address the actions be maintained so that the organisation does not suffer overload. The Committee noted that this was a key consideration.GC observed that this work contributed to providing the necessary Board assurance and asked about the status of the assurance mapping work. SR stated that this work was being undertaken by ST, JM and her team who were looking to produce a proposal by April. The map itself would be a large piece of work but once set up will prove to be a useful tool to support the Board’s assurance requirements. |  |
| 9. | **HRA Internal Audit Annual Plan 2017-18** TA observed that the timing of the audits is important to ensure that improvements have been completed i.e. the SIP work, and suggested it might be best to delay final approval of the proposed plan.GC commented that the scope and topics of the proposed audits was right but agreed that flexibility would be required in the actual commencement of the audits.MT observed that the CAG function audit needs expressing as an implementation style audit and that 7 could be more about preparedness. |  |
| 10. | **HRA Corporate Risk Register Quarter 3 16/17**GC asked that concern be noted that there is no movement of risk scores. The Committee will expect movement in the future. It was also noted that the HRA Approval risks had not been reviewed as requested.TA advised that EMT had reviewed the HRA Approval risks and that actions had been taken which would be presented in the next iteration of the report. She agreed that no movement was of concern but this was also being addressed by EMT.  |  |
| 11. | **Deep Dive on Risk: Amendments**JM and CC gave a presentation on the issues surrounding the backlog of amendments following the implementation of HRA Approval.DK offered congratulations on a clear presentation and asked 3 questions:1. Why had the ‘odd’ behaviour of applicants not been anticipated? Was it a communications issue?
2. What was the reputational damage to the HRA?
3. Why had there been a delay between identification of the problem and the implementation of a task force?

JM replied that there had been a disconnect between what the HRA thought it had communicated to stakeholders and what those stakeholders thought they were being told. Whilst the HRA had requested that ALL amendments be sent through it had actually meant only those that were necessary. As a result there was confusion as to what was expected so people erred on the side of caution and sent through every amendment. This is a real learning point for future communications – making sure there is a precise, unambiguous clarity of message, building in appropriate stakeholder involvement and understanding their positions are all vitally important. Acting on these lessons would also help mitigate reputational damage.JM also stated that whilst the roll out of HRA Approval had been piloted and staggered to ensure a lot of learning, and fine tuning prior to roll-out had been achieved, this had not been possible for amendments and again, was a real learning point.NT suggested that this could have been the result of a ‘fading out’ of critical issues as the main concentration and devotion of resources had been applied to implementing HRA Approval and not amendments. JM concurred that this could have been the case and that there were 3 things that contributed:1. Amendments were too ‘complicated’ so enough time and expertise was not devoted to preparation;
2. No additional resources were available as the original Business Plan had not been able to determine resource requirement accurately at such an early stage in development; and
3. Timings were imposed rather than opted for i.e. CRN needed to decommission its CSP systems and applied huge pressure, DH was also applying time pressures and resolving devolved administrations constraints delayed necessary changes.

With regards to reputational damage, JM agreed that this had been huge but that significant steps had been taken to restore the reputation and that these appear to be having the desired effect. The HRA was working hard through all its stakeholder groups to get back to where we were. In response to the time taken to respond to the crisis, JM observed that there had been an underestimation of the volume of amendments in the period immediately after implementation, and therefore the team to deal with them. In responding to the crisis, JM stated that there were several problems that led to delays. One was a lack of interconnectedness between initiatives. For example, whilst the website carried the majority of the communications, it has been acknowledged as being deficient in many areas and required improvement but there were insufficient resources to address this. Additionally, the IT systems had not been built around amendment processes, so in many instances work arounds needed to be developed and were not initially optimal. There is also an acknowledged lack of capacity to be able to respond to significant change requirements rapidly.Another problem was not being able to draw support from the rest of the organisation when necessary, so when the crisis occurred, it was difficult to get appropriate help from elsewhere. Other staff required additional training and considerable change management support, which had not been anticipated and led to delays. The lessons learnt from these are that contingency, resource and process planning are vital elements that need to be incorporated in early scoping and planning work. It was acknowledged that it is harder to respond to external timing pressures, but maybe pushing back harder might be a consideration worth noting.DK expressed her thanks to the team for their hard work in clearing the backlog, especially during the summer. |  |
| 12. | **Business Case for ICT spend approval**KW informed the Committee that approval for this BC was sought to move the new contract for hosting the business critical IRAS / HARP systems from Rack space to Crown Hosting Data Centre. The Committee requested more background as to why the Crown Hosting Data Centre uses Ark Data Centres. In response to a question, KWinformed the Committeethat the procurement process had been undertaken through DH procurement and that the BC template was one used by them.The Committee requested that more details be provided and that the proposal should be brought back for approval. | **KW** |
| 13. | **Review of HRA registers**The Committee noted and accepted the report. |  |
| 14. | **iCasework Lessons learnt Update**The Committee agreed to defer this to the next meeting. | **ST** |
| 15.  | **Out of session items**Noted. |  |
| 16. | **Any other business**MT raised the subject of expenses for REC committee members, suggesting that a review is required. He also suggested that there should be more opportunities for volunteer members to take part in training face to face rather than on line as this would be of more benefit to members. MT queried if the systems in place were appropriately capturing the value of the HRA’s volunteer membership, the good will that the HRA relies on and any potential risks.MT observed that whilst the HRA surveys staff on a number of issues, he was unaware if this took place for the HRA’s volunteer membership and members’ views may not be visible to HRA management and the Board. MT advised key issues may not therefore be captured appropriately on the HRA’s risk registers. The Committee recognised the importance of the HRA’s volunteer membership and agreed to discuss further at its next meeting in April. | **ST** |
| 17. | **Date of next meeting**Wednesday 26th April 2017 – HRA 1, Ground Floor, Skipton House |  |