Audit and Risk Committee minutes

17 January 2023

Details of attendees are provided at the end of the minutes.

1. Introductions and apologies

1.1. Ailsa Beaton welcomed Darren Hall of the Government Internal Audit Agency, who was joining his first Audit and Risk Committee meeting. GIAA would be taking over responsibility for internal audit services from the 2023/24 financial year. She also welcomed Fiona Wilcock to her first meeting.

1.2. There were apologies for absence from Peter Cudlip.

2. Declarations of interests

2.1. No declarations of interests were made.

3. Matters arising from the previous meeting

Minutes

3.1. The minutes of the previous meeting had been approved as a correct record.

Actions

3.2. The updates on actions from previous meetings were noted. Chris Braithwaite explained that the Governance team was currently reviewing the items due to come to the Committee's April meeting, which may need to be extended. He explained that he would email the Committee with an update on this in the next couple of weeks.

4. Deputy Chief Executive Officer's update

4.1. Paul Arnold provided an update on recent activities related to the Committee's remit, reflecting on the work that had been completed across the organisation in 2022 and the delivery that was planned for 2023, with particular reference to the creation and delivery of ICO 25. He explained that Executive Team was due to review the organisation's target operating model, and consultations on proposed organisational design would take place from February.

4.2. He also provided an overview on progress with legislation which was relevant to the ICO's powers and structure, particularly the Data Protection and Digital Information (DPDI) Bill. He explained

that a report providing further detail on this would be considered by Management Board on 23 January.

4.3. He assured the Committee that management was reviewing the plans in place to ensure that the ICO would continue to provide all of its services during the upcoming PCS strike action.

4.4. In response to a question regarding the DPDI Bill, he explained that, at present, the expectation was that the transition period for any governance changes to the organisation as a result of the DPDI Bill would take place during John Edwards' term as Commissioner.

5. Business continuity strategy statement – Annual review

5.1. Jo Butler presented a report setting out the outcome of the recent annual review of the business continuity strategy statement. She also provided an overview of the preparations to ensure resilience during the upcoming strike action.

5.2. The Committee commented on the importance of regular testing of the business continuity plan and asked when full business continuity tests were planned. Jo Butler explained that testing was scheduled to take place over the summer, and this was likely to include testing of specific departmental responses plans as well as a test of an incident which impacted the whole business.

5.3. The Committee asked whether the response to the recent water damage at Wycliffe House had provided any lessons learned about business continuity preparedness. Jo Butler explained that this incident had been managed well and had demonstrated that there was a lot of good practice and preparedness in place. A lessons learned exercise had taken place following the incident and some minor improvements had been identified, primarily around internal communications. These were already being implemented.

6. Ransomware Desktop assessment/playbook

6.1. Mike Fitzgerald provided an oral update on the outcomes of a recent ransomware desktop assessment exercise. He explained that this had been facilitated by an external provider. The assessment had been positive, particularly in relation to clarity on roles, responsibilities and responses, as well as the level of technical capabilities. The main area for development had been ensuring sufficient coverage and clear decision-making within the incident response team, including named deputies being identified in the event that key staff were unavailable. A fully updated

response plan reflecting the lessons learned from the exercise would be completed by the end of January.

6.2. The Committee asked what procedures were in place to ensure that the ICO had the latest intelligence of current attack types, to ensure that it was prepared for these. Mike Fitzgerald explained that as well as intelligence of breaches reported to the ICO as a regulator, they had regular contact with DCMS and Microsoft regarding emerging threats, and also had a third-party provider which monitored forums for developing threats.

6.3. The Committee agreed that it should receive regular assurance reports on business continuity and cyber security activities.

ACTION: Mike Fitzgerald and Jo Butler to provide the Committee with six-monthly assurance reports on business continuity and cybersecurity preparedness. Due date: 19/6/23, ongoing thereafter.

7. Security report

7.1. Mike Fitzgerald presented a report providing information of security matters over the last quarter.

7.2. The Committee commented that the report gave good assurance that the systems in place were operating as intended.

8. Risk and opportunity management

Risk Management policy review

8.1. Louise Byers presented a report setting out proposed changes to the Risk Management Policy and Risk Appetite Statement, ahead of this being considered by Management Board in March. She explained that the proposed changes to the policy had primarily arisen from the awareness-raising that the team had completed and were aimed at making the policy document as understandable and as useful as possible to all staff.

8.2. The Committee welcomed the report and updated policy. The Committee also welcomed the resources which Management Board devoted to reviewing the risk appetite on an annual basis. The Committee also suggested that it would be useful to develop case studies to demonstrate how the risk appetite was applied. Louise Byers confirmed that these were being developed.

8.3. The Committee commented that it may be useful to complete a deep dive into target risk scores at a future meeting once the Risk Appetite had been reviewed, potentially at the June meeting. Jo

Butler explained that review of target scores, and particularly whether the planned mitigations were sufficient to achieve those scores, was a focus of each of the corporate risk review meetings. She confirmed that she could bring a report to the Committee's June meeting with further information.

8.4. The Committee asked whether any work had been undertaken to review whether decisions were consistently being taken in alignment with the risk appetite. Jo Butler explained that as part of the current review of the risk appetite and review of risks in light of ICO 25, work was currently underway to review decisions which may not have been taken in alignment with the risk appetite or may have been taken differently in light of changes to the risk appetite. Further information on this could be included in the report to the Committee's June meeting. Louise Byers commented that there was still more to do to fully embed the risk appetite into decision-making across the organisation.

ACTION: Jo Butler to bring a report to a future meeting providing further information on: how planned mitigations will achieve risk target scores; findings of work to review how consistently the risk appetite was being followed; and work to embed the risk appetite into decision-making. Due date: 16/10/23

Corporate risk review outcomes

8.5. Louise Byers presented a report setting out the outcomes of the most recent review of corporate risks, as well as the work being done to review the risk register in light of the ICO 25 objectives. The Committee noted the report.

9. External audit

9.1. Robert Buysman, Michelle Hopton and Laura Charmant presented a report setting out the plan for external audit of the 2022/23 accounts.

9.2. The Committee discussed the timeline for the external audit, which called for completion of fieldwork by mid-May, but only provided for an audit completion report on 14 July, rather than this being completed in time for Audit and Risk Committee on 19 June. Ailsa Beaton explained that her expectation as Chair, and what the Committee had agreed the previous year, was that the ACR should be completed in time for the June Audit and Risk Committee. This would ensure that the Committee was able to consider the final

annual report and financial statements, to allow them to recommend the report to the Commissioner for signature and achieve a target laying date of 4 July.

9.3. NAO and Deloitte clarified that the audit completion report referred to in the report was final certification by the Comptroller and Auditor General; they confirmed that the report to Audit and Risk Committee in June would reflect completed fieldwork and ensure that the Committee was able to review the final version of the annual report and financial statements. They also confirmed that would review the timeline to enable certification and laying of the annual report in early July.

ACTION: Deloitte and NAO to confirm the timeline for completing external audit work in order to ensure that the Audit and Risk Committee can review the final annual report on 19 June 2023. Due date: 24/4/23

9.4. The Committee was not aware of any concerns in relation to the questions for the Committee set out in the report. They were not aware of any instances of fraud or suspected fraud, although highlighted the discussion at the previous meeting regarding no fraud being reported being a potential concern. The Committee would receive a report on this in June.

10. Annual report and financial statements approach

10.1. Louise Byers presented a report setting out the approach to be taken for development of the annual report and financial statements.

10.2. The Committee asked for confirmation that there was sufficient resilience in the teams involved in the work for the annual report and audit to ensure delivery in the event of any absences. Louise Byers and Deloitte confirmed that they were content with the current levels of resilience in these teams.

11. Finance

Most recent income and expenditure report

11.1. Angela Donaldson presented a report setting out the financial position as at end of November. She explained that the ICO was awaiting confirmation from DCMS regarding additional funding or authority to utilise reserves to cover the current budget deficit but anticipated this being granted.

Changes to accounting standards

11.2. Angela Donaldson confirmed that there were no changes to accounting standards to be considered as part of preparation of the financial statements.

Single tender contract awards

11.3. Angela Donaldson presented a report informing the Committee of a single tender contract which had been awarded since the Committee's last meeting.

12. Internal audit

12.1. Hannah Parker presented a report providing an update on progress with delivering the internal audit for 2022/23. She highlighted the busy quarter 4 for the audit programme, with two audits currently ongoing and two audits taking place during February. Louise Byers assured the Committee that the ICO was working closely with Mazars to ensure that the audits in quarter 4 were completed on schedule. The Committee welcomed this update. The Committee requested that they be informed of any delays to delivery of these audits.

ACTION: Chris Braithwaite to provide the Committee with updates in the event of any delays to delivery of the remaining internal audits. Due date: 24/4/23

12.2. Hannah Parker reported that the Case Management audit report was currently being finalised and would be presented to the Committee's April meeting.

13. Corporate Charge Cards Audit Progress report

13.1. Angela Donaldson presented a report providing an update on the progress implementing the recommendations from this audit.

14. Outstanding audit recommendations

14.1. Chris Braithwaite presented a report setting out the current status of outstanding internal audit recommendations.

15. Fraud and Whistleblowing report

15.1. Chris Braithwaite presented a report providing information on fraud or whistleblowing disclosures over the last quarter.

16. Any other business

Lee Parfitt

16.1. Ailsa Beaton highlighted that this was Lee Parfitt's last meeting as part of the Next-Generation NEDs programme and thanked on

behalf of the Committee Lee for his attendance at meetings for the last year. Lee thanked the Committee for enabling his attendance over the year which had been extremely valuable to him and had assisted him in gaining a role as a trustee at a charity.

16.2. Ailsa Beaton informed the Committee that a new member of the Next-Generation NEDs programme would be joining the Committee from its April meeting.

Attendance

Members

Ailsa Beaton (Chair)	Non-Executive Director
Ranil Boteju	Non-Executive Director
Jayne Scott	Independent Audit Committee member

Attendees

ICO	
Angela Donaldson	Director of Finance
Joanne Butler	Head of Risk and Governance
Louise Byers	Director of Corporate Risk and Governance
Mike Fitzgerald	Director of Digital, IT and Business Services (for items 6 and 7)
Paul Arnold	Deputy Chief Executive Officer and Chief Operating Officer
Internal auditors	
Hannah Parker	Mazars
Darren Hall	Government Internal Audit Agency
External Auditors	
Robert Buysman	National Audit Office
Curtis Hodgson	National Audit Office
Laura Charmant	Deloitte
Michelle Hopton	Deloitte

Secretariat

Chris Braithwaite	Corporate Governance Manager
Fiona Wilcock	Corporate Governance Officer

Observer

Lee Parfitt	Next Gen NEDs Programme