Audit Committee minutes
Monday 12 June 2017

Members:

Ailsa Beaton (chair)	Non-Executive Director
Roger Barlow	Independent Audit Committee member
Jane McCall	Non-Executive Director

Attendees:

ICO	
Paul Arnold	Deputy Chief Executive Officer
Heather Dove	Head of Finance
Internal Auditors	
Phil Keown	Grant Thornton
Paul Eckersley	Grant Thornton
External Auditors	
Matthew Atkinson	National Audit Office
David Eagles	BDO
Secretariat	
Peter Bloomfield	Senior Corporate Governance Manager
Caroline Robinson	Corporate Governance Officer

1. Introductions and apologies

1.1. There were apologies from Elizabeth Denham and Paul Keane who were unable to attend. Caroline Robinson was welcomed to this, her first, meeting.

1.2. Paul Arnold advised that, given recent changes in senior management responsibilities, Simon Entwisle (as former DCEO) would no longer be attending Audit Committee. The Committee thanked Simon for his contribution to the work of the Committee over the last twelve years.

2. Declaration of interests

2.1. There were no declarations of interest.

3. Minutes and action points from the Audit Committee meeting of the 7 March 2017

3.1. The minutes of the meeting of 7 March had been agreed in correspondence. There were no further amendments.

3.2. In respect of action points Paul Arnold updated the meeting.

3.3. The Department for Culture, Media and Sport consultation on fee changes had been delayed until July because of the general election. The delay did not affect the timescale for introducing the new fee structure. Paul Arnold confirmed that the ICO would be writing to data controllers on renewal of their current notification to explain the new fee structure. There would also be a continuation of the current exercise to encourage non-paying data controllers to pay.

3.4. The Committee agreed that the Management Board should be updated at its August meeting on the fee consultation and on steps the ICO was taking to ensure that data controllers paid the new fee.

Paul Arnold to update the August Management Board on the consultation on and timetable for the new fee structure and on how the ICO was to encourage payment.

3.5. There had been an action point for Paul Arnold to consider how best to publicise the fact that directors of companies which failed to pay a civil monetary penalty could be disbarred from being directors in the future. Paul Arnold advised that the matter had been highlighted in press releases on penalties.

Peter Bloomfield to provide copies of relevant press releases to the Committee.

3.6. Other action points would be discussed as part of subsequent agenda items.

4. Information and cyber security

4.1. Paul Arnold introduced a paper providing a high level analysis of ICO cyber security controls and how well the ICO complied with best practice. Paul Arnold advised that the ICO was aiming for the most suitable level of controls, and, whilst confident of ICO practices, the ICO was also committed to make sure it demonstrated that it had the most relevant accreditation. The report stated that the ICO would be actively considering ISO27001 accreditation by way of a scoping exercise this calendar year, with the implementation of any new controls and associated processes then expected from later this financial year.

4.2. The office was currently recruiting to a new Risk and Governance role and the appointee would be responsible for taking the scoping exercise forward. The Committee asked whether the process ought to be brought forward so that decisions were made before the GDPR came into force in May 2018. Paul Arnold explained that, whilst the ICO aimed to be an exemplar in good information rights handling, it also needed to act proportionately. Paul Arnold confirmed that the scoping exercise would assess whether ICO27001 was something we would expect to see in place for all those we regulated. It was not a must have addition for the ICO other than in response to a considered assessment of information risk or business need.

4.3. The Committee appreciated the importance of the scoping exercise in ensuring a measured approach, but were keen to see this completed at the earliest available opportunity.

Paul Arnold to bring a paper to Management Board in November on decisions to seek ISO27001 accreditation and the cost of doing so.

5. ICO approach to the recovery of unpaid civil monetary penalties

5.1. Heather Dove introduced a paper detailing the ICO approach to unpaid civil monetary penalties.

5.2. The cost of recovery was between £3k and 5k per case. Allowing the ICO to retain its costs arising from the recovery process had been considered previously but the ICO could not currently do so.

5.3. The Committee suggested that, where it was thought a data controller was likely to default, the ICO should expedite

matters rather than undertaking a long, and probably unnecessary, process.

5.4. On the matter of the ICO instructing third parties to help in the recovery of penalties, the Committee suggested that the criteria be reviewed. For example it felt that all debt over a certain limit should be chased.

Heather Dove to review the criteria on making use of external parties in the collection of unpaid penalties.

The steer from the Audit Committee was that the ICO should be aggressive in chasing unpaid penalties. It was agreed that the matter ought to be discussed at the next Management Board.

Heather Dove to bring a paper in conjunction with Investigations to the August Management Board to get a clear steer regarding the ICO's approach to the recovery of monetary penalties.

6. Risk and opportunity management

6.1. The new format risk and opportunity register was presented for information and discussion. Paul Arnold advised that the register was still in the process of being developed. He highlighted the risk of delays in legislation to implement the GDPR and Law Enforcement Directive as being high.

6.2. The Committee considered it worthwhile grouping risks around resources, people capacity and recruitment and retention. These issues were to be discussed at the next Management Board.

6.3. The internal auditors liked the format of the new register and the appetite statement. They suggested that, as use of the risk appetite develops, there was a need to be aware of the difference between risk appetite and tolerance of risk. They also agreed that grouping similar risks was useful along with linking risks to the ICO's aims.

6.4. The internal auditors also suggested that there needed to be clarity as to whether risk status was before or after mitigating actions. Risks should also be linked to ICO aims, and further mitigating actions needed to be identified where necessary.

6.5. There was also discussion as to whether there was any differentiation needed between implementation of the GDPR and of the Law Enforcement Directive.

Peter Bloomfield to amend the risk register to reflect differences in risk for the GDPR and LED.

7. Outstanding audit recommendations

7.1. The register of outstanding audit recommendations was presented for information. Most internal and external audit recommendations had been cleared by the given time.

7.2. There was one late investigations review recommendation.

Peter Bloomfield to check the investigations review recommendation to see if it had been cleared.

7.3. The Management Agreement had not as yet been formally signed off by the DCMS.

Peter Bloomfield to liaise with Ailsa Beaton about writing to the DCMS about the delay in sign off for the Management Agreement.

7.4. Heather Dove introduced discussion on an outstanding action (relating to both internal and external audits) on changing the passwords on the finance system. The ICO's view was that, rather than making the change as initially agreed, a fuller review of the implications of doing so was needed.

7.5. The internal auditors advised that the ICO position is not unique in terms of system maintenance and that it would be useful to seek assurance from the provider as to what controls they have over use of the password and the making of changes to the system.

7.6. The Committee considered that they needed more information on this matter before making a final decision; for example on the use of the password and controls around this use.

Heather Dove to come back to the September Audit Committee with more information on the use and controls relating to the finance system password.

7.7. There was discussion as to how the ICO followed up on outstanding audit recommendations. It was agreed that the internal and external audit recommendations be included in Steering Group action logs as appropriate to provide the right level of visibility and oversight.

Peter Bloomfield to ensure that audit recommendations are added to the Steering Group action logs.

8. Internal audit

Investigations review

8.1. The Investigations Review was introduced by Grant Thornton. The actions had been reviewed following discussion at the previous Audit Committee.

8.2. There had been a delay in signing the review off. Agreement of the final wording by email had caused the delay.

Internal audit annual report 2016/17

8.3. Grant Thornton provided their report – giving an overall clear opinion for 2016/17. The GDPR review is included in the overall opinion although the report has not itself been received.

Internal audit plan 2017/18

8.4. The internal audit plan for 2017/18 was re-submitted to confirm the final version. It will be reviewed as the audits progress.

8.5. The possibility of a cyber security review was raised by the Committee. This was partly dependent on discussion at the August Management Board on the matter.

9. External audit

9.1. David Eagles introduced the external audit completion report for 2016/17. The report included an update on the current audit position and on significant financial statement risks relating to management overrides and the ICO being a going concern. There were no issues of concern reported.

9.2. The committee thanked both the ICO and BDO for their work on the accounts.

10. Audit Committee Annual Report 2016/17

10.1. Peter Bloomfield introduced the most recent version of the Audit Committee's Annual Report 2016/17 which provided formal assurance to the Commissioner on the management of the ICO. The draft reflected the internal and external audit opinions.

10.2. The wording of the report was agreed subject to checks on the final number of audits, and cleared recommendations.

Peter Bloomfield to check and finalise the Audit Committee annual report and to ensure it is published on the website.

11. ICO Annual Report and Accounts 2016/17

11.1. A near final draft of the ICO Annual Report and Accounts 2016/17 was presented for any comments from the Committee and auditors. It was due to be sent to the designers within the next few days.

11.2. There was a question as to whether pension transfers into the Civil Service Pension Scheme should be included.

11.3. For consideration in future it was considered useful if the ICO could detail lessons it learnt from complaints it received about itself.

11.4. Various other comments were received on the draft and the NAO confirmed it would be sending more detailed comments through shortly.

Peter Bloomfield to amend the draft Annual Report and Accounts and to re-circulate it to the Committee and auditors as soon as possible after the meeting to allow an agreed version to go to design by the end of the week.

12. Fraud, whistleblowing and security

12.1. The standing report on fraud, whistleblowing and security was presented for information. The number of minor data breaches remained a concern.

13. Audit Committee terms of reference

13.1. The revised Audit Committee terms of reference were brought to the Committee for information.

14. National Audit Office guidance

14.1. The Committee had requested that relevant National Audit Office guidance be brought to the attention of the Committee on a regular basis, along with details of the action being taken by the ICO in response to the guidance where appropriate.

14.2. Peter Bloomfield advised that the National Audit Office itself published a half yearly summary of guidance of interest to Audit Committee and this report would be timed to make use of this summary.

15. Any other business

15.1. It was agreed that the accounting treatment of the loan from DCMS next year would be discussed at the next Audit Committee.

16. Internal audit re-procurement

16.1. The Audit Committee was updated on the re-procurement of the internal audit function, in the absence of the auditors.