

## **Audit Committee minutes**

Friday 6 June 2014

### **Members**

Neil Masom	Non-executive Director (chair)
Roger Barlow	Independent Audit Committee Member

### **Attendees**

Daniel Benjamin	Director Corporate Services
Simon Entwisle	Director of Operations
Christopher Graham	Information Commissioner and Chief Executive
Helen Heywood	Temporary Head of Finance
Phil Keown	Grant Thornton
James Edmands	National Audit Office
Henry Young	National Audit Office
Peter Bloomfield	Senior Corporate Governance Manager (secretariat)

## **1. Introductions and apologies**

- 1.1. There were apologies from Ian Watmore who was unable to attend. He had sent his comments on the papers to members of the committee.

## **2. Declaration of interests**

- 2.1. There were no declarations of interest.

### **3. Action points from the Audit Committee meeting of the 10 March 2014**

- 3.1. The minutes had been agreed previously by correspondence. Outstanding action points were considered in detail:
  - 3.1.1. Daniel Benjamin to consider development of an overarching efficiency indicator.

Daniel Benjamin and Simon Entwisle had discussed this. It was not considered to be a meaningful exercise given the wide range of very different work the ICO undertook.
  - 3.1.2. Daniel Benjamin to discuss the work needed to create a fully integrated assurance model with Grant Thornton.

This action was reported as having been cleared.
  - 3.1.3. Daniel Benjamin to ensure that the two outstanding recommendations were cleared as soon as possible.

The clearance of the two outstanding recommendations would be discussed under agenda item 5.
  - 3.1.4. Howard Munson to schedule re-visiting the governance review recommendations in 2015/16.

This action was reported as having been cleared.

### **4. Commissioner's update**

- 4.1. Christopher Graham provided an update on issues affecting the ICO. He had just attended the Spring Conference of EU Data Protection Authorities and highlighted discussion their on the recent "right to be forgotten" judgment and the loss of 200 million eBay subscriber details. Other issues affecting the ICO included the continuing ICO involvement in Care.data, and post legislative scrutiny of the Freedom of Information Act.
- 4.2. These issues provided the context for the more outward facing focus of the Commissioner's work over the next two years, especially given the general election in May 2015. And to support this there were going to be changes to the senior management team.
- 4.3. A new role of Deputy Chief Executive Officer was proposed to combine the roles of Director of Operations and Director of Corporate Services, deputising for the Commissioner in his role as Chief executive of the office. This would help continue the alignment of corporate services to business needs. The Deputy Commissioners would maintain

their focus on data protection and freedom of information and continue to deputise for the Commissioner in respect of his statutory responsibilities for the Data Protection and Freedom of Information Acts.

- 4.4. The change had meant that the current Director of Operations and Director of Corporate Services were at risk of redundancy. The Director of Corporate Services, Daniel Benjamin, had decided to take voluntary redundancy and would be leaving the ICO on 30 June. A slotting exercise had been undertaken, endorsed by members of the Remuneration Committee, Enid Rowlands and Andrew Hind. This had resulted in Simon Entwisle being confirmed as the new Deputy Chief Executive Officer from 1 July.
- 4.5. Christopher Graham also advised the Committee of the appointment of the new Head of Finance, Heather Dove, who would start on 28 July.
- 4.6. Christopher Graham expressed thanks for the work of Daniel Benjamin and Helen Heywood (the temporary Head of Finance).
- 4.7. The Commissioner explained that the heartbleed virus had not been specifically discussed at the Spring Conference. However, he did confirm that providing guidance on these sorts of issues was an important role for the ICO and that a recent blog on the issue had been well received.
- 4.8. The revised risk register was also considered. This had been developed from risks identified by Leadership Group and was deliberately high level, identifying risks in the areas of money, people and reputation.
- 4.9. Because of the high level nature of the risks more needed to be done on identifying sub-risks, mitigating actions and risk owners. There was also a need to link risks to the objectives in the ICO Plan. This reflected recommendations made in the Risk Management Horizon Scanning internal audit review (agenda item 6).
- 4.10. The need for the ICO to be able to identify risks associated with new technology was also identified, along with identifying opportunities.

**Action point 1: Peter Bloomfield to take account of the Audit Committee comments on the risk register when creating the next iteration of the register.**

**Action point 2: Peter Bloomfield to consider how to reflect opportunities as well as risks in the register.**

## **5. Outstanding audit recommendations**

- 5.1. There were two outstanding internal audit recommendations; one relating to the holding of a business continuity plan test and the other to making a decision on sample checks of notification fees. The latter recommendation was due to be cleared in July.
- 5.2. A test of the business continuity plan had not been held due to a lack of resources. The team was now fully staffed and a test would be held by the end of October.
- 5.3. The recommendation linked to holding an IT disaster recovery test had been cleared. Whilst the recovery had not been as quick as originally hoped valuable lessons had been learnt. It was also noted that after a power loss in April systems had been fully recovered within 24 hours. Annual disaster recovery tests were a contractual requirement.

## **6. Internal audit**

### Internal audit reviews

- 6.1. Grant Thornton introduced four internal audit reports for agreement:

#### IT service management

- 6.1.1. This audit had considered the management of good IT service delivery and incident management. There were five medium recommendations:

- until recently problems have not been managed proactively;
- a baseline of IT performance had not been established prior to the start of the contract;
- a disaster recovery test was a contractual obligation;
- there was a need for a database to detail what was in the contract; and
- there was a need to better manage software licence compliance.

#### IT contract management

- 6.1.2. The objective of this review was to establish the extent to which third-party services were being delivered according to contractual requirements. There was one medium recommendation relating to the number of deliverables still required from the contractor.

### Risk management and horizon scanning

6.1.3. This review considered how well the ICO identified emerging risks. There was one medium level recommendation relating to the already identified disconnect between risks identified and ICO Plan objectives.

### Follow up audit

6.1.4. The follow up audit had looked at arrangements for ensuring that recommendations were cleared. Arrangements were thought to be working well.

### Internal audit report 2013/14

6.2. Grant Thornton Introduced their internal audit annual report for 2013/14. This provided formal assurance to the Commissioner and the Audit Committee in the areas of risk management, corporate governance and internal controls.

## **7. External audit**

7.1. The NAO introduced their final audit completion report. The audit had gone well with good early engagement and they thanked Helen Heywood for the cooperation of the Finance Team. The audit work was almost complete with just the second stage review and pensions information outstanding. A clean opinion was provided.

7.2. The Committee was asked to review the findings set out in the report and to consider whether the unadjusted misstatements identified should be corrected. The Committee considered that the misstatements should not be adjusted as they were not material misstatements.

7.3. The key control issues arising from the audit and the NAO recommendations were then considered. In respect of the preparation of management accounts it was noted that management intended to replace the ICO's current outdated finance software this financial year.

7.4. The incorrect use of a Government Procurement Card was also noted.

### **Action point 3: NAO to consider the wording of the recommendation on use of Government Procurement Cards.**

7.5. The risk that notification fee income could be used to fund freedom of information activities was discussed. Management would be setting up an audit trail for changes

made to the apportionment model which controlled how money was split between the different ICO areas of work.

**Action point 4: Simon Entwisle to put in place processes to ensure that the audit trail for changes to the apportionment model are clear and readily accessible.**

7.6. Unpaid civil monetary penalties and the costs to the ICO of chasing payment, possibly unsuccessfully, were raised. It was thought that some government bodies retained some of the penalties paid to fund their recovery action. At the moment the ICO paid all of the money it recovered to the Treasury.

**Action point 5: NAO to provide the ICO with information about whether or not some organisations are allowed to retain some of the financial penalties paid to them to fund recovery work.**

7.7. It was agreed that the planned changes to the senior management team should be noted in the governance statement in the Annual Report and Accounts.

**Action point 6: Peter Bloomfield to add a brief note to the draft governance statement about the planned changes to the senior management team.**

7.8. The NAO was asked about references in the letter of representation to exit packages for junior members of staff.

**Action point 7: NAO to consider the wording of the letter of representation.**

7.9. The need to refer to certain benefits in kind in the remuneration report (included within the Annual Report and Accounts) was noted.

## **8. Audit Committee annual report 2013/14**

8.1. The draft Audit Committee Annual Report was discussed and amendments suggested.

**Action point 8: Peter Bloomfield to amend the report as discussed and to clear the final version via the Audit Committee chair.**

## **9. Governance statement 2013/14**

9.1. The draft governance statement (to be included within the Annual Report and Accounts) was considered. Minor

amendments were noted including the need to refer to the planned senior management team changes.

**Action point 9: Peter Bloomfield to finalise the governance statement.**

## **10. ICO annual report and accounts 2013/14**

10.1. The Committee considered the draft Annual Report and Accounts for 2013/14. There were a few minor amendments.

## **11. Internal audit plan 2014/15**

11.1. The internal audit plan for 2014/15 was considered in detail. The need to be flexible in choosing areas to audit was highlighted. Areas to keep an eye on included non-payment of civil monetary penalties, technological issues relating to data protection, and business and corporate planning.

11.2. Simon Entwisle gave an update regarding the Finance Steering Group which was being set up as part of the changes to the senior management team, and the planned for new Finance IT system. Some audit involvement in this might be useful towards the end of the year.

11.3. If there were changes to the audit plan the aim would be to keep within the overall envelope of agreed days.

## **12. Fraud report**

12.1. There were no incidents of fraud to report.

12.2. There was discussion as to the possible reporting of whistleblowing and security issues in addition to fraud.

**Peter Bloomfield to consider further the reporting of fraud, whistleblowing and security incidents and to report back to the next Audit Committee.**

## **13. Any other urgent business**

13.1. Christopher Graham thanked Neil Masom for his exemplary work as Audit Committee chair over the last four years. Neil was stepping down as a non-executive director in August.