Information Commissioner's Office

Internal Audit 2014-15: Integrated Assurance: Management Assurance

Last updated 9 December 2014

Distribution		Timetable	
For action	Director Chief Executive Officer	Fieldwork completed	10 November 2014
For information	Senior Corporate Governance Manager	Draft report issued	11 November 2014
For information	Audit Committee	Management comments	21 November 2014
		Final report issued	21 November 2014

Executive Summary

Background

Over the last two years we have discussed the concept of integrated assurance with ICO management. Some areas of the organisation have looked to apply the core principles of integrated assurance, identifying the assurances in place to safeguard information.

Discussions have taken place surrounding the merits of developing and deploying a fully integrated assurance map, however at this stage, given the size of the organisation and the way in which that the Executive Team is supported by a variety of management groups, it is not seen as beneficial.

We did agree though, that it would be worthwhile to review the different levels of management scrutiny and assurance over key areas of the organisation that support the work of Management Board and Executive Team.

This review has not been carried out as a risk based audit, nor have we sought to give an assessment. It will though underpin our annual opinion on governance.

Approach

We have worked with the Senior Corporate Governance Manager and Corporate Governance Officer to identify all the relevant management groups in place.

We have sought to understand the remit of relevant groups, and identify the agenda items that they have taken over the year that provide assurance over the continued operation of key controls in pursuit of the ICO's objectives.

Outcomes

Our review focussed on the operations of the Management Board, Executive Team, Information Rights Committee and Information Governance Steering Group. In our view, these form key second line of defence, i.e. management-led, commissioning and receiving assurances from across the organisation in respect of key strategic activities.

The work of these different governance entities covers key aspects of the ICO's internal and external operations, and includes the functions receiving and discussing the ongoing operation of activities surrounding:

Financial and strategic planning
Delivery of the ICO Plan
Risk management
Legislative changes
Decision making roles and responsibilities
IT Strategy
Organisational information and data security
Human Resources

That is not to say that these are the only management level assurances available across the ICO. Assurances are also received and reported from the Equality & Diversity and Health & Safety Committees and through the more recently established Finance Steering Group and IT Steering Group.

Further details of our findings are provided in Section 2.

Conclusion

The ICO has a well-developed network of second line, management-led, assurance functions. Their remits are clear and documented. They meet with sufficient frequency, with appropriate reporting lines through the organisation to ensure that key outputs and decisions required are reported and acted upon. Their agenda items are in line with their remit and they provide an opportunity for management to receive and challenge information on organisational activity in pursuit of the ICO's objectives.

Detailed Findings

Management Board

Management Board (MB) is responsible for developing ICO strategy, identifying where the organisation should be in three to 10 years' time and articulating the broad approach needed to reach this position. It monitors the progress made in implementing strategy, challenging performance and providing leadership where conflicts occur.

Key areas of activity that demonstrate the MB acting as the second line of defence include:

Assurance area	Activity
Financial management	Receipt and scrutiny of the ICO's income and expenditure position. Specific discussions in respect of IT Strategy, related IT project expenditure and notification fee income and the costs involved with data protection. Information also provided on the role of the new Finance Steering Group.
Risk management	Regular review of the ICO risk register and discussion of key ICO risks. This is also informed by the Information Commissioner's "forward look" item at each MB meeting. Further, specific discussions on the technological risks and their impact on information rights take place at MB and that the MB is assured based on the work of the Information Rights Committee.
Performance against the ICO Plan	Receipt and scrutiny of the ICO's ongoing performance against its strategic plan.
Review of decision making at committee/group level	Overview of the outcomes from an internal study surrounding the decision making processes and activities at committee/steering group level. There was also specific consideration of the terms of reference and role of the Remuneration Committee.

Executive Team

The Executive Team (ET) develops the ICO's corporate and business plans, budgets and significant strategies and ensures delivery against these plans and strategies. We have reviewed Executive Team (ET) minutes and papers for the last 12 months and have seen that ET has received and reviewed assurance in respect of the following key areas:

Assurance area	Activity
ICO direction and regulatory functions	ET receives regular papers from the Information Rights Committee or from the Deputy Commissioners. This includes updates on the ICO's approach to additional regulatory functions as well as information on proposed projects.
Budget monitoring	ET receives regular reports on the ICO's finances, and review and approve changes to agreed budgets. The key area of discretionary spend is IT projects, and specific attention is paid to this area. ET has also had a key role in improving arrangements in this area through the establishment of the Finance Steering Group and the IT Steering Group.
Risk management	Regular review of the ICO risk register and the key risk areas that affect the ICO's strategic and operational functions.
Human Resources	Discussions held around pay settlements and security checking of staff.
IT	Specific review of the ICO's IT Strategy and scrutiny of specific projects, such as the web rebuild project. Project monitoring includes oversight of IT expenditure and prioritisation of spend.
Succession planning	Specific consideration by ET of this risk. It was agreed that a sub-group of Leadership Group would be established to take this work forward.

Information Rights Committee

The Information Rights Committee (IRC) is in place to ensure a joined-up approach to the ICO's information rights policy objectives. Its role is to identify strategic information rights priorities and oversee cross-office programmes to achieve information rights objectives. The IRC is not responsible for the running of the ICO, it refers issues that come to it about the running of the office to managers or other corporate committees as appropriate.

We have reviewed its meeting minutes and relevant papers that have shown how it leads on information rights related activity, including:

The ICO's framework for developing policy across the ICO.
Changes to Data Protection policy following the Leveson Inquiry recommendations.
Reviewing the data handlers' audit self-assessment toolkit prototype.
The effectiveness of Civil Monetary Penalties.
Proposals on the use of privacy seals.
Discussion of policy research budget.

Information Governance Steering Group

The Information Governance Steering Group provides a dedicated forum to consider and make decisions about information governance matters and to support the work of the SIRO and the Information Governance Team. It is a decision making body which agrees changes in information governance policy and monitors progress towards the delivery of our information governance strategy. We have seen that it acts as the second line of defence, providing assurance in respect of the following:

Reviewing the work carried out by the IT Security and Physical Security working groups
Review of security incidents and internal IT security measures
Regular review of the Information Risk Register
Information Governance Business plan review
Review of Cabinet Office cyber security reports

Internal audit approach

Responsibilities

The Information Commissioner acts through his Board of Management and the Information Commissioner's Office ("ICO") discharges his obligations. Therefore references to the Information Commissioner and the ICO in this report relate to one and the same party.

It is the responsibility of the Information Commissioner to ensure that the ICO has adequate and effective risk management, control and governance processes.

HM Treasury's Corporate Governance in Central Government Departments (2011) states that boards of Public Bodies should determine the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The Board should therefore maintain sound risk management and internal control systems and should establish formal and transparent arrangements for considering how they should apply the corporate reporting and risk management and internal control principles and for maintaining an appropriate relationship with the organisation's auditors.

Please refer to our letter of engagement for full details of responsibilities and other terms and conditions.