Information Commissioner's Office

Internal Audit Annual Report 2015-16

Last updated 27 May 2016

Contents

Sections

Appendices

It is the responsibility of the management of the Information Commissioner's Office to ensure that there are adequate risk management, governance and control arrangements..

1 Executive Summary

1.1 Introduction

Grant Thornton UK LLP is the appointed internal auditor to the Information Commissioner for the period 1 April 2015 to 31 March 2016.

This report summarises the findings and conclusions of our work during the year together with our opinion and overall assurance commentary.

Our responsibilities and internal audit approach are set out in Appendix A.

1.2 Overall assurance

As the internal auditor to the ICO, our work in 2015-16 was carried out in accordance with the Internal Audit Plan approved by the Information Commissioner and the Audit Committee. The Plan was constructed in such a way as to allow us to make a statement of the adequacy and effectiveness of the ICO's risk management, control and governance processes.

In assessing the level of assurances to be given, we have taken into account:

- all audits undertaken during 2015-16
- any significant recommendations not accepted by management and the consequent risks *(there were none)*
- the effects of any significant changes in the organisation's objectives or systems *(there were none)*
- any limitations which may have been placed on the scope of internal audit *(there were none)*
- the extent to which resource constraints may impinge on our ability to meet the full audit needs of the ICO (*there were none – we tailored our audit team to provide the assurance and advisory skills required to deliver internal audit plan)*
- what proportion of the ICO's audit requirement has been covered to date *(the internal audit plan for the period has been completed in accordance with approvals from the Audit Committee)*
- the quality of our performance (summarised in section 3 of this report).

Control policies and procedures designed to address specified business objectives are subject to inherent limitations and, accordingly, errors may occur and not be detected.

In giving our opinion it should be noted that assurance can never be absolute. The most that we can provide to the Information Commissioner is a reasonable assurance that there are no major weaknesses in the ICO's risk management, control and governance processes

1.3 . Internal Audit Opinion

We are satisfied that sufficient internal audit work has been undertaken to allow us to draw a reasonable conclusion as to the adequacy and effectiveness of the ICO's risk management, governance and control processes.

There is nothing that has come to our attention, either as a result of audit activity we have undertaken since 31 March 2015 or by other means that affects the internal audit opinions we give as at the date of this report.

Risk management

Design effectiveness
Overall, we have concluded that, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management
Operating effectiveness
Those activities and controls that we examined were operating with sufficient effectiveness to provide reasonable but not absolute assurance that the related risk management objectives were achieved during the period under review.

Corporate governance

Design effectiveness
Overall, we have concluded that, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management
Operating effectiveness
Those activities and controls that we examined were operating with sufficient effectiveness to provide reasonable but not absolute assurance that the related risk management objectives were achieved during the period under review.

Internal controls

Design effectiveness
Overall, we have concluded that, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management
Operating effectiveness
Those activities and controls that we examined were operating with sufficient effectiveness to provide reasonable but not absolute assurance that the related risk management objectives were achieved during the period under review.

1.4 Management action on recommendations

Where deficiencies in control have been identified, either by management or Grant Thornton, we are satisfied on the basis of our own follow-up that management has taken, or has planned, appropriate action to implement our recommendations.

1.5 Use of this Report

This report is part of a continuing dialogue between the ICO and us. It is not, therefore, intended to cover every matter, which has come to our attention. For this reason we consider it inappropriate for the report to be made available to third parties and we do not accept responsibility for any reliance that third parties may place on it.

2 Review of 2015-16 work and basis of our opinion

2.1 Summary of our 2015-16 internal audit work

Our 2015-16 Audit Plan was based upon an agreed assessment of risk that focussed our initial work upon the most significant areas of business risk and core financial controls. It provided a means for determining audit priority and a judgement to be made on the frequency of visits.

Arising from our reviews, we made twenty five detailed recommendations to management to address weaknesses in the design and/or operation of controls, and/or take opportunities to improve the performance of the ICO's processes. Exhibit One highlights which elements of our annual assurance statement were informed by each review.

Note: One review, Core Operations (post Eagle) did not generate formal recommendations but did identify areas of improvement for management to consider.

Our detailed recommendations and management's responses can be found within the individual visit reports that we issued in 2015-16. Each has been discussed with the Audit Committee.

It is important to recognise that while the analysis of these recommendations set out later in this report can be used by the ICO to track implementation progress of recommendations in future periods, the number or grading of the recommendations cannot be taken as an indicator of relative performance in respect of controls, either with previous years, or with other similar organisations. The number of recommendations is a function of the improvement-focused nature of our audit approach, the particular areas approved for review by the Audit Committee this year, and the extent of change facing the ICO at the particular point in time our Plan was approved. In particular, the Amber rated reports provided advice and support to management on areas of improvement or change.

We believe that that, given the size and complexity of the ICO's activities and its on-going change agenda, an improvement-focused and effective internal audit function would be expected to identify development needs. The number of recommendations that we have made should not therefore be taken as pointing to any systemic problem in the ICO's control environment; rather it reflects a positive approach to audit and the development of the system of controls.

Our overall conclusions are based upon the conclusions of our individual assignments as summarised below. For the detailed findings of each of our reviews please refer to the individual reports.

2.2 Internal audit coverage

Review	Report date
Finance System Benefits Realisation	November 2015
Recruitment	August 2015
Staff Performance Management	November 2015
Core Operations (post Eagle)	May 2016
Core Financial Controls	April 2016
Follow Up	May 2016

2.3 Basis of opinion

Risk management

Our opinion on risk management is based on the outcomes of the reviews that we performed in five areas during the year (set out in Exhibit One overleaf) as well as our on-going discussions with management and Directors on how the ICO manages its risks and the involvement of the Management Board and the Information Commissioner in the management of risk.

The reviews that we have performed during the year that support our opinion on risk management are:

- Finance System Benefits Realisation
- Recruitment
- Staff Performance Management
- Core Operations (post Eagle)
- Core Financial Controls
- Follow up

Corporate Governance

Our opinion on corporate governance is based on the outcomes of business risk reviews that we performed in five areas during the year, as follows:

- Finance System Benefits Realisation
- Recruitment
- Staff Performance Management
- Core Financial Controls
- Follow Up

Internal control

As Exhibit One shows, our reviews in the following five business areas have considered the practical operation of the ICO's internal control arrangements:

- Finance System Benefits Realisation
- Recruitment
- Staff Performance Management
- Core Financial Controls
- Follow Up

Exhibit One: Outcomes of our 2015-16 reviews

Review Area	Recommendations					Review assessment	Review findings inform annual opinion		
	H	M	L	I	Total		Risk mgt	Corp Gov	Int. Control
Finance System Benefits Realisation	-	-	1	1	2	Green	✓	✓	✓
Recruitment	-	3	5	2	10	Amber		✓	✓
Staff Performance Management	-	3	2	-	5	Amber	✓	✓	✓
Core Operations (post Eagle)	-	-	-	-	-	n/a	-	-	-
Core Financial Controls	-	2	4	2	8	Amber	✓	✓	✓
Follow Up	-	-	-	-	-	Green	✓	✓	✓

3 Performance against plan

3.1 Audit plan and actual input

The 2015-16 Annual Audit Plan originally envisaged 47 days being required to deliver it but we agreed with management to increase that budget to 51 days. We have actually delivered our plan in 48.75 days.

Appendix A shows a detailed analysis of how the time was initially budgeted and ultimately spent, taking account of reallocations approved by the Audit Committee during the year. An analysis of the staff input by grade is provided below.

	Planned input		Actual input	
	Days	%	Days	%
Partner/Director	4.25	*8%*	2	*4%*
Associate Director	4.75	*9%*	4.75	*10%*
IT Audit Manager	3.5	*7%*	4	*8%*
Executive	28	*55%*	20.5	*42%*
Associate	10.5	*21%*	17.5	*36%*
Total	51	*100%*	48.75	*100%*

3.2 Other indicators of Performance

We have monitored our performance against the indicators agreed by the Audit Committee:

Indicator	Target	Actual Performance
Planning		
Preparation and submission of audit needs assessment (ANA) and audit plan to Audit Committee in time for agreement by the Information Commissioner before the commencement of work.	Usually to March meeting of Audit Committee	Draft prepared for March audit committee. Addition of potential reviews 2017-18 and 2018-19 was agreed by management prior to June audit committee
Evidence of involvement of Executive Team, Audit Committee and Management Board in developing the ANA and plan.	Planning process to be reported to and agreed with Audit Committee	Plan was prepared after consultation with the Executive Team, the Management Board and the Audit Committee.
Changes to plans agreed in advance by the Audit Committee [or Chair of Committee between meetings].	Changes to be agreed prior to work commencing.	Changes to the plan were agreed in advance of the work commencing by the Audit Committee.

Indicator	Target	Actual Performance
Provision of Service		
Actual time spent on delivering Plan is less than or equal to that agreed in the Plan.	Monitored through periodic progress reports. Changes to be agreed by Audit Committee.	Additional days were agreed with management to deliver work related to the Core Financials and Core Operations reviews.
Cost of service (excluding VAT)	£31,140	£31,040
Mix of staff reflects agreed balance of qualified / specialist / experienced staff.	Monitored through progress reports and annual reports.	Qualified staff mix was 64%
Response to request for ad hoc work are timely and appropriate.	Monitored by Committee on completion of ad hoc projects	We have not been asked to provide management with support during 2015-16 period.
Attendance at all Audit Committee Meetings	100%	100%
Reporting		
Reports set clear context for each audit and summarise strengths as well as weaknesses.	Report format has been developed in the light of previous discussions with the Audit Committee.	All reports include Executive Summary, which sets the context for the review. Areas of good practice are identified in the reports as well as areas for improvement.
Usefulness of outcomes / recommendations to the ICO	Action plans agreed for all internal audit recommendations	All actions agreed by the ICO
Draft reports to be issued within 20 working days of completion of fieldwork and closure meeting.	Each report to log timescales of key reporting events.	Core Operations (post Eagle) was delayed as a result of changing the focus of the review into a consultation with ICO stakeholders (data controllers or data subjects) and to accommodate unpredictable nature of such a review.
Final reports to be issued within five working days of receipt of final management comments.	Each report to log timescales of key reporting events.	All final reports issued within five working days of receiving final management responses.

3.3 Other work by Grant Thornton UK LLP

No additional work was provided during the year.

3.4 Acknowledgement

We would like to take this opportunity to thank the staff at the ICO for their assistance and cooperation during the audit.

3.5 Recommendation

We are pleased to present this report to the Audit Committee and recommend its acceptance by the Information Commissioner.

A Responsibilities and 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.

Our role as internal auditor to a Public Body is to provide an independent and objective opinion to the Accounting Officer on risk management, control and governance processes, by measuring and evaluating their effectiveness in achieving the organisation's agreed strategic objectives.

In common with most organisations, the control environment at the ICO depends on the competence of its staff and compliance with procedures.

Changes in staff, staff absences and, in extreme cases, collusion and/or deliberate actions by key individuals can corrupt the control environment. The day-to-day maintenance of the control environment depends on management control and supervision.

Our risk evaluations and tests are designed to ensure that controls and activities to manage risks are sound both in design and operation. Some of our conclusions are based on samples selected from the year's transactions. However, our conclusions should not be taken to mean that all transactions have been properly authorised and processed.

Internal audit approach

We have reviewed the controls policies and procedures employed by the ICO to manage the risks that it has identified to its business objectives as set out in the 2015-16 Annual Internal Audit Plan, approved by the Audit Committee. This report is made solely in relation to those business areas and risks reviewed in the year and does not relate to any of the other operations of the ICO.

Our approach complies with best professional practice, in particular, the Public Sector Internal Audit Standards (2013) and the Institute of Internal Auditors' guidance on risk-based internal auditing (2005).

In addition, we comply in all material respects with other Government guidance applicable to Public Bodies and have had regard to the HM Treasury guidelines on effective risk management (the 'Orange Book').

We adopted a risk based approach to our work which required us to:

- Establish the controls and activities in place to address the key business risks in each area under review
- Interview key staff to gain an understanding of the adequacy of controls and activities in place to manage the risks in each area under review
- Review certain key documents to confirm the existence and operation of the controls and activities identified
- Where applicable, perform tests to determine whether the controls and activities have operated as expected during the period.

Together these and other such procedures, as we considered necessary, enabled us to evaluate whether the control policies and procedures were suitably designed to meet the risk objectives and whether these control policies were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that those risk management objectives were achieved during the period reviewed. Some of our conclusions are based on samples selected from the year's transactions. However, our conclusions should not be taken to mean that all transactions have been properly authorised and processed.

B Analysis of time spent

Assurance Theme	Subject	Budget Days	Total days	Variance
Risk Management, Corporate Governance & Internal Control	Finance System Benefits Realisation	6	7.25	1.25
	Recruitment	7	6.25	-0.75
	Staff Performance Management	8	9.25	1.25
	Core Operations (post Eagle)	10	8	-2
	Core Financial Controls	10	9.5	-0.5
	Follow up	3	2.5	-0.5
Sub total		*44*	*42.75*	-1.25
Audit Strategy, Planning and Liaison, Attendance at Audit Committee and Annual Report		7	6	-1
Total		51	48.75	-2.25

C Definition of internal audit annual opinion and audit issue ratings

Internal audit annual opinion

Design effectiveness	Operating effectiveness
Overall, we have concluded that, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management	Those activities and controls were operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review
Overall, we have concluded that, except for the specific weaknesses identified by our audit, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management.	Except for the controls listed below those activities and controls that we examined were operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review.
Overall, we have concluded that, in the areas examined, the risk management activities and controls are not suitable designed to achieve the risk management objectives required by management.	Those activities and controls that we examined were not operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review

Audit report assessment

Rating	Description
Red	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which should be raised with Senior Management and the Audit Committee at the earliest opportunity.
Amber	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which require the attention of management to resolve and report on progress in line with current follow up processes.
Green	We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.

Audit issue rating

Within each report, every audit issue is given a rating. This is summarised in the table below.

Rating	Description	Features
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management	• Key control not designed or operating effectively • Potential for fraud identified • Non compliance with key procedures / standards • Non compliance with regulation
Medium	Important findings that are to be resolved by line management.	• Impact is contained within the department and compensating controls would detect errors • Possibility for fraud exists • Control failures identified but not in key controls • Non compliance with procedures / standards (but not resulting in key control failure)
Low	Findings that identify non-compliance with established procedures.	• Minor control weakness • Minor non compliance with procedures / standards
Improvement	Items requiring no action but which may be of interest to management or best practice advice	• Information for department management • Control operating but not necessarily in accordance with best practice

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

grant-thornton.co.uk