Information Commissioner's Office

Audit and Risk Committee
Internal Audit Annual Report 2022/23

Prepared by: Mazars LLP

Date: April 2023

Contents

01 Introduction

02 Audit Opinion

03 Internal Audit Work Undertaken in 2022/23

04 Internal Audit Plan 2022/23 vs Budget

05 Benchmarking

06 Performance of Internal Audit

Appendices

A1 Implementation of Recommendations

A2 Definitions of Assurance

mazars

01 Introduction

Mazars LLP are the appointed internal auditors to the Information Commissioner's Office (ICO). This report summarises the internal audit work undertaken by Mazars in 2022/23, the scope and outcome of work completed, and incorporates our annual statement on internal controls assurance.

The report should be considered confidential to the ICO and not provided to any third party without prior written permission by Mazars.

Scope and purpose of internal audit

The purpose of internal audit is to provide the Audit and Risk Committee, with an independent and objective opinion on governance, risk management and internal control and their effectiveness in achieving the ICO's agreed objectives. It also has an independent and objective advisory role to help line managers improve governance, risk management and internal control.

The opinion for 2022/23 is included in **Section 02** and forms part of the framework of assurances that is received by the ICO. Internal Audit also has an independent and objective consultancy role to help line managers improve risk management, governance and control. Our professional responsibilities as internal auditors are set out within the Chartered Institute of Internal Auditors (CIIA) and the Internal Audit Charter.

Responsibility for a sound system of internal control rests with the Management Board and work performed by internal audit should not be relied upon to identify all weaknesses which exist or all improvements which may be made. Effective implementation of our recommendations makes an important contribution to the maintenance of reliable systems of internal control and governance.

Internal audit should not be relied upon to identify fraud or irregularity, although our procedures are designed so that any material irregularity has a reasonable probability of discovery. Even sound systems of internal control will not necessarily be an effective safeguard against collusive fraud.

The report summarises the internal audit activity and, therefore, does not include all matters which came to our attention during the year. Such matters have been included within our detailed reports to the Audit and Risk Committee during the course of the year.

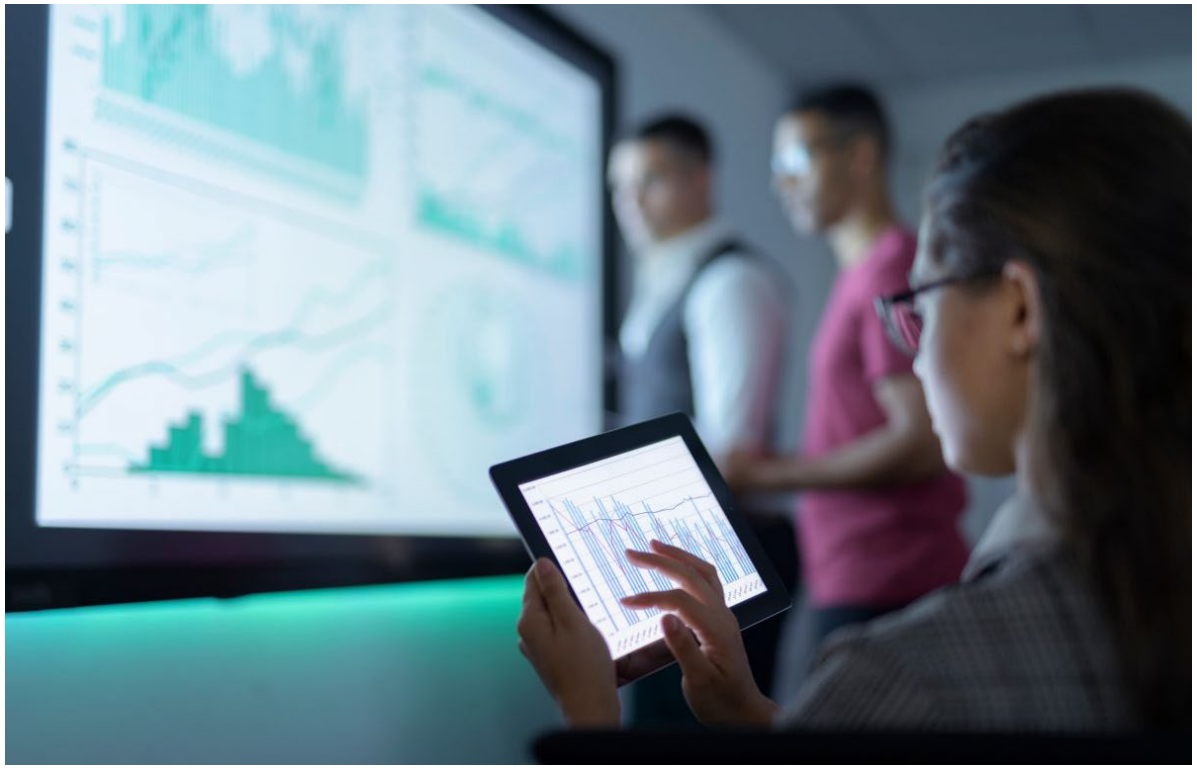
Performance against the Internal Audit Plan

The original Internal Audit Plan for 2022/23 provided for 91 days of internal audit work. At the request of management, Mazars conducted a Civil Monetary Penalty Recording audit in addition to the original 2022/23 Audit Plan. As agreed with management and the Audit & Risk Committee, the People Strategy and the IT Strategy audits were removed from the Audit Plan during the year. We are pleased to confirm that we completed the rest of the audit work scheduled.

Further details of performance against the Internal Audit Plan and work completed is included in **Section 03** and **Section 04**. We have undertaken a benchmarking exercise in **Section 05** of assurance ratings and recommendation gradings given compared to prior years. **Section 06** is a summary of the performance of internal audit.

Acknowledgements

We are grateful to the staff throughout the ICO for the assistance provided to us during the year.



Sampling methodology

As part of our auditing methodology we use a range of sampling techniques to provide a robust basis for our audit opinions. Where possible we favour conducting whole data set testing using the analytics software IDEA.

Where this is not possible or practical, we look to conduct sampling through use of random number generators, stratified or systematic sampling as appropriate to ensure that our findings are both representative and relevant. Sample sizes are driven by the level of assurance being provided and where not dictated as part of the audit scope are at the discretion of the internal auditor in conjunction with the Engagement Manager.

02 Audit Opinion

Remote Working

Audits were mostly completed remotely, with walkthroughs and client interviews held virtually and all evidence being requested and provided digitally. The annual internal audit opinion provided below reflects the audit plan agreed and is not limited in scope, to the extent that the assurance provided by internal audit can only ever be reasonable, not absolute.

Our opinion

On the basis of our audit work, our opinion on the framework of governance, risk management, and control is **Substantial** in its overall adequacy and effectiveness.

Certain weaknesses and exceptions were highlighted by our audit work. No 'High' priority findings have been raised, however, Limited Assurance was provided in respect of Corporate Charge Card processes. These matters have been discussed with management, to whom we have made several recommendations. All of these have been, or are in the process of being addressed, as detailed in our individual reports. An internal audit of Risk Management was completed in the year with a Substantial Assurance opinion given.

The ICO has continued to perform well with the implementation of recommendations, with 100% of recommendations closed.

Scope of Opinion

In giving our internal audit opinion, it should be noted that assurance can never be absolute. The most that the internal audit service can provide to the ICO is a reasonable assurance that there are no major weaknesses in risk management and internal control processes.

The matters raised in this report are only those which came to our attention during our Internal Audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

In arriving at our opinion, we have taken the following matters into account:

- The results of all audits undertaken as part of the plan;
- Whether or not any 'High' or 'Medium' recommendations raised have not been accepted by Management and the consequent risks;
- The extent to which recommendations raised previously, and accepted, have been implemented;
- The effects of any material changes in the ICO's objectives or activities;
- Matters arising from previous reports to the ICO;
- Whether or not any limitations have been placed on the scope of internal audit;
- Whether there have been any resource constraints imposed upon us which may have impinged on our ability to meet the full internal audit needs of the ICO; and
- The proportion of the ICO's internal audit needs have been covered to date.

Further detail on the definitions of our opinions raised in our reports can be found in Appendix A2.

Reliance Placed on Third Parties

Internal audit has not placed any reliance on third parties in order to assess the controls operated by the ICO. Our opinion solely relies on the work we have performed and the results of the controls testing we have undertaken.

Follow Up

We follow up on all IA recommendations to ensure Management have addressed and implemented appropriate actions to address those recommendations. Further detail on the number of open and closed actions can be found in **Appendix A1.**

03 Internal Audit Work Undertaken in 2022/23

The audit findings in respect of each review, together with our recommendations for action and the management responses are set out in our detailed reports.

We undertook six in-depth audit reviews, covering a number of important control systems, processes, and risks. The results of this work are summarised below. We also completed follow up reviews of implementation of recommendations. The results of the follow up reviews are included in Appendix A1.

Audit area	Assurance level	Recommendations				Accepted	Not accepted
		High	Medium	Low	Total		
Risk Management	Substantial	-	2	4	6	6	-
Core Financial Controls – Corporate Charge Cards	Limited	-	6	-	6	6	-
Procurement and Contract Management	Adequate	-	6	4	10	10	-
Guidance Development	Substantial	-	-	1	1	1	-
Case Management	Adequate	-	3	4	7	7	-
Civil Monetary Penalty Recording	Substantial	-	-	2	2	2	-
Total		-	17	15	32	32	-

04 Internal Audit Plan 2022/23 vs Budget

The original Internal Audit Plan was for a total of 91 days, 80.75 days of internal audit work was delivered. Two audits were removed from the Plan during the year and reported to the Audit and Risk Committee. The IT Strategy and People Strategy audits were merged to form a review of the proposed Culture, Capability and Capacity Strategy (now called the High Performance Strategy). Following initial planning calls, it was agreed with management that the timing of the review would not be suitable given the current stage of development of the strategy. An additional audit on Civil Monetary Penalty Recording was added to the plan. This was requested by management and agreed with the Audit and Risk Committee in October 2022.

Audit area	Planned days	Actual Days	Difference	Status
Risk Management	8	8	-	Final Report
Core Financial Controls – Corporate Charge Cards	7	7	-	Final Report
IT Strategy	8	-	-8	Removed from plan
Procurement and Contract Management	10	11	+1	Final Report
Guidance Development	8	8	-	Final Report
People Strategy	8	3*	-5	Removed from plan
Case Management	10	10	-	Final Report
Civil Monetary Penalty Recording	-	5	+5	Final Report – Addition to plan
Cyber Security (Follow Up)	17	12.75	-4.25	Final Report
Follow Up	5	6	+1	Final Report
Management and Control	10	10	-	Fully Utilised
Total	**91**	**80.75**	**-10.25**	

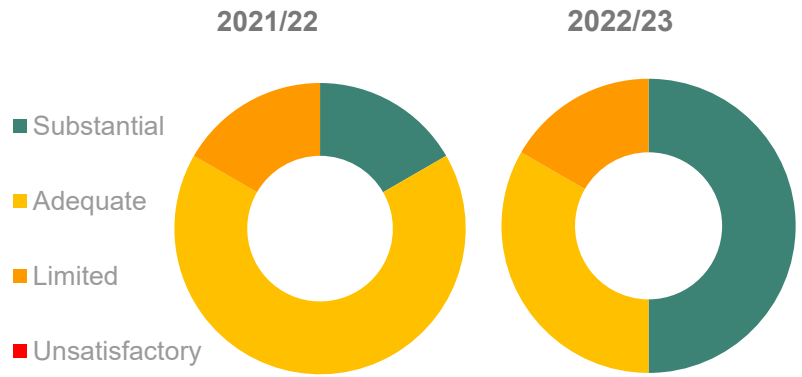
* Three days for the People Strategy were invoiced due to planning time spent and a late notice cancellation. This was agreed with the Director of Corporate Affairs & Governance.

05 Benchmarking

This section compares the Assurance Levels (where given) and categorisation of recommendations made at the ICO.

.

Comparison of Assurance Levels

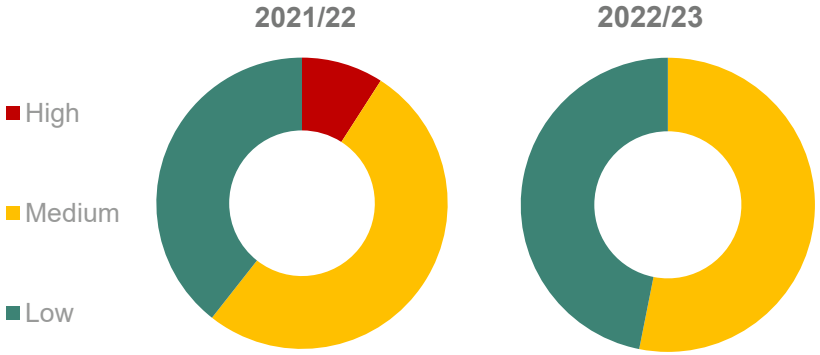


Of the six strategic audits conducted in 2022/23, one was rated Limited, two were rated Adequate, and three were rated Substantial.

In 2020/21, there were also six strategic audits completed. One review received Substantial assurance, four received Moderate assurance and one received Limited assurance. There has been an increase in Substantial assurance opinions given in 2022/23.

It should be noted though that the areas of review will not typically be the same given the risk based nature of the Internal Audit Plan year on year that caution should be exercised in comparing years.

Comparison of Recommendation Gradings



The total number of recommendations made in 2022/23 was 32. The figure in 2021/22 was 33. There have been no High priority recommendations raised this year.

As noted above, the areas of review each year will not typically be the same.

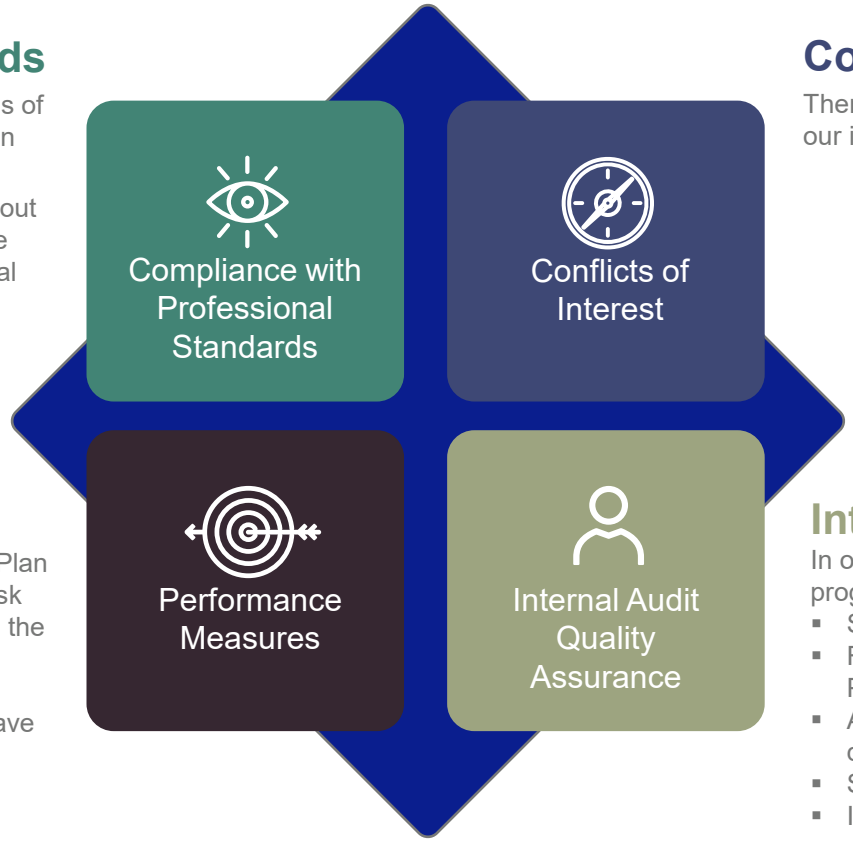
06 Performance of Internal Audit

We have provided some details below outlining our scorecard approach to our internal performance measures, which supports our overall annual opinion.

Compliance with Professional Standards

We employed a risk-based approach to determining the audit needs of the ICO at the start of the year and use a risk-based methodology in planning and conducting our audit assignments.

In fulfilling our role, we abide by the three mandatory elements set out by the Institute of Internal Auditors. Namely, the Code of Ethics, the Definition of Internal Auditing and the Standards for the Professional Practice of Internal Auditing.



Conflicts of Interest

There have been no instances during the year which have impacted on our independence and/or lead us to declare any interest.

Performance Measures

We have completed our audit work in accordance with the agreed Plan and each of our final reports has been reported to the Audit and Risk Committee. We have received positive feedback on our work from the staff involved in the audits.

Regular planned discussions on progress against the Audit Plan have taken place with the Audit and Risk Committee.

Internal Audit Quality Assurance

In order to ensure the quality of the work we perform; we have a programme of quality measures which includes:

- Supervision of staff conducting audit work;
- Review of files of working papers and reports by Managers and Partners;
- Annual appraisal of audit staff and the development of personal development and training plans;
- Sector specific training for staff involved in the sector;
- Issuance of technical guidance to inform staff and provide instruction regarding technical issues; and
- The maintenance of the firm's Internal Audit Manual.

Appendices

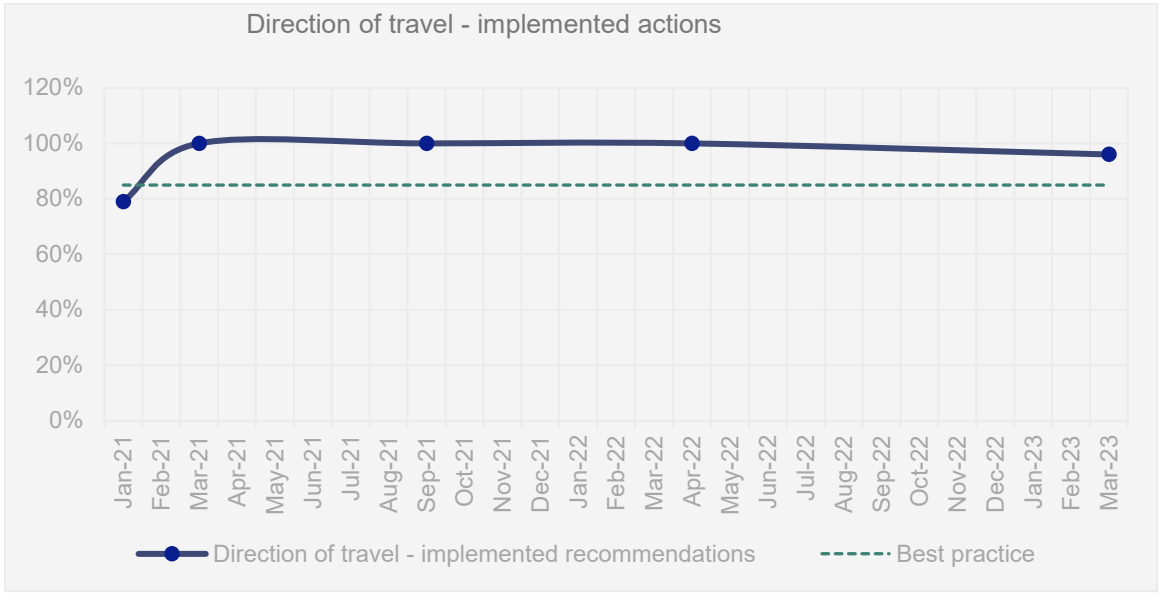
A1 Implementation of Recommendations
A2 Definitions of Assurance

A1 Implementation of Recommendations

During the course of the year, the Mazars Cyber Advisory Team reported on progress against the 2021/22 Cyber Security recommendations to the Audit and Risk Committee. Two update reports were presented (April 2022 and October 2022). The seven remaining actions were reviewed as part of the March 2023 Follow Up.

The following table provides a status of agreed audit actions reviewed in the March 2023 Follow Up. The ICO has continued to perform well with the implementation of recommendations, with 96% of recommendations implemented and **100% of recommendations closed.**

	Implemented	Overdue	Propose to close
High	-	-	-
Medium	15	-	-
Low	7	-	1
Total	**22**	**-**	**1**
%	**96%**	-	**4%**
Recommendations closed	**100%**		



A2 Definitions of Assurance

Assurance Gradings

We use categories to classify our assurance over the processes we examine, and these are defined as follows:

Level	Description
Substantial	The framework of governance, risk management and control is adequate and effective.
Adequate	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control..
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Unsatisfactory	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Recommendation Gradings

To assist management in using our reports, we categorise our recommendations according to their level of priority, as follows:

Priority	Description	Action required
High	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium	Weakness in governance, risk management and control that if unresolved exposes the organisation to a high level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low	Scope for improvement in governance, risk management and control.	Remedial action should be prioritised and undertaken within an agreed timescale.

Annual Opinion

For annual opinions we use the following classifications within our audit reports:

Opinion	Definition
Substantial	The framework of governance, risk management and control is generally adequate and effective.
Moderate	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Unsatisfactory	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Contacts

Peter Cudlip
Partner, Mazars
Peter.Cudlip@Mazars.co.uk

Hannah Parker
Associate Director, Mazars
Hannah.Parker@Mazars.co.uk

We take responsibility to the Information Commissioner's Office for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.