Internal Audit progress report – March 2016

The purpose of this report is to advise the Audit Committee of our progress in planning and delivering the 2016-17 Internal Audit Plan.

Progress to date

Since the Audit Committee last met, we have issued final reports for the reviews of Cryptographic Controls and phase one of the IT Asset Management, which had draft reports issued at the time of the December Audit Committee but were not issued as final in time for the Audit Committee.

We have completed Investigations, the second phase of IT Asset Management and the annual follow-up review.

There are three reviews that are in the process of being completed; the People Strategy (management actions are being agreed), Data Protection data law reform (draft report has been issued to management) and the Stakeholder review (report is in the process of being drafted). All reviews should be completed and final reports issued before the end of March 2017.

Status and progress of reviews

Completed reviews

Investigations

The review was completed as expected in December. We identified six opportunities for improvements but only one medium rated finding. The medium finding related to the initial communication to organisations or individuals of the investigation scope but as a matter of course the ICO do not communicate investigation timetables. In addition, when delays occur the person or organisation under investigation is not notified of the delay. We would expect that ideal target completion dates should be communicated at the outset of an investigation and those under investigation be notified of any significant delays to the process.

IT Asset Management – phase 2

The second phase of the IT Asset Management review was completed in February 2017 and identified no high or medium findings. The three low rated findings raised relate to improvements in documenting software licence management, formalising the asset disposal process and that not all assets were tagged.

Follow up review

The annual follow-up review of management actions that have been actioned during 2016-17 period was completed. We identified one low rated finding, concerning retention of evidence to support findings that are closed.

Reviews in progress

People Strategy

The report was agreed with management with little change made to the findings after the last update to the Audit Committee. There were two medium and two low rated findings. The medium findings relate to how ICO establish future demand for services and the impact that has on recruitment; and maturing the potential approaches that could be use used to recruit new staff. There is one finding, however, that management are finding difficult to commit to a date to achieve the action. The finding relates to who will lead staff retention improvements and when they will be in place. Management has stated that the lead is currently in the process of being recruited and therefore too early to set target dates. Internal Audit would suggest that a target date of when this could be achieved should be put in place. Once the new member of staff is in post and the date in not achievable, alternative plan is put in place.

Data Protection law reform

The review identified that whilst the preparation for change in data protection legislation is being co-ordinated, as a project might be managed, it is significant piece of business as usual activity. We identified a number of improvements that relate to how management could establish visibility of what to expect from the changes being planned, when and monitoring the success of activity more clearly. These are currently being agreed with management.

Stakeholders

The fieldwork for this review was completed late in February 2017 and the report is currently under Internal Audit quality review. A more detailed update will be provided for the next Audit Committee meeting in June 2017.

Overall summary of plan progress

Review	Scope	Timing	Days	Progress
Fines recovery	Review the process in place to recover fines issued to organisations that remain unpaid. The review will are cover how unpaid fines are identified, performance measures of fine payment are reported and the success of follow up activities to recover fines to ensure this process is efficient and effective.	Q2	6	Completed
Cryptographic Controls	CESG have defined a process to manage cryptographic controls to ensure encrypted data remains available if encryption keys become unavailable (through loss or corruption). The ICO are required to comply and demonstrate compliance by self-assessment. The audit will provide assurance over the compliance process to ensure that the self-assessment is robust and appropriate supervision is in place.	Q2	4*	Completed
GDPR project "Data Protection law reform project"	Provide assurance over the project to manage the impact of GDPR on the ICO, including governance over the change programme and interactions with other parts of the ICO. The review will include how the ICO have resourced the project and the activity to backfill project members' roles and the recruitment for the new activities as ICO takes responsibility for GDPR.	Q3	8	Reporting
IT Asset Management	Management are establishing policy and procedure to manage IT assets. The review will be delivered in two phases: 1. Review the policy and procedures to ensure the design of controls are likely to manage IT assets to ensure records are complete, accurate and will be kept up to date. 2. Once the procedures have been deployed, a second review will evaluate the controls in place and operating as expected.	Q2	11*	Completed
Investigations	The review will cover how the ICO manages investigations through communication with stakeholders, the use of frameworks, gathering intelligence and finally reporting on investigations. Where possible, we will benchmark against other regulators management of investigations.	Q3	9	Completed
People Strategy	People are a key part of the ICO and the management have established that the organisation needs to ensure it has "the right people, in the right place at the right time". The review will consider how staff performance is managed across the organisation and that managers are properly prepared to implement performance management to ensure consistency. The review will also consider the progress of recommendations made from the staff performance review in 2015-16.	Q3	8	Reporting
Stakeholder engagement	ICO is tasked with communicating key messages on data protection (and in the future data privacy) and access to information. A review will establish how those communications are prepared and published including thought leadership. The focus will be on how strategic activity is determined, agreed and approved, including consideration of the impact of GDPR on these activities. The review will also determine how the target audience is selected and the medium to use. How the ICO measures the success of such communication will also be assessed.	Q4	11.5	Reporting
Follow Up	Review of the arrangements to capture and implement audit recommendations in a timely manner.	Q4	3.5	Completed

* Additional review / budget agreed with management

www.grant-thornton.co.uk