Phil Keown
Engagement Lead
T: 020 7728 2394
E: philip.r.keown@uk.gt.com

Paul Eckersley
Manager
T: 0113 200 2525
E: paul.j.eckersley@uk.gt.com

James Renwick
Assistant Manager
T: 0113 200 2599
E: aparna.muthurajagopalan@uk.gt.com

Information Commissioner's Office

Internal Audit 2015-16: IT Asset Management Review – Phase 2

Last updated 21 February 2017

Distribution		Timetable	
For action	Head of Customer and Business Services	Fieldwork completed	17/02/2017
		Draft report issued	27/02/2017
For information	Senior Corporate Officer Audit Committee	Management comments	27/02/2017
		Final report issued	27/02/2017

Contents

Sections

Appendices

Glossary

ACCSEC	Accountable security (encrypted) devices
ALMO	Asset and Licence Management Officer
CESG	Communications Electronics Security Group (the UK Government's national technical authority for information assurance)
Custodian	Person responsible for managing encryption systems
IGSG	Information Governance Security Group – body that oversees information security
CMDB	Configuration Management Database - to hold data in relation to IT assets

This report is confidential and is intended for use by the management and Directors of ICO only. It forms part of our continuing dialogue with you. It should not be made available, in whole or in part, to any third party without our prior written consent. We do not accept responsibility for any reliance that third parties may place upon this report. Any third party relying on this report does so entirely at its own risk. We accept no liability to any third party for any loss or damage suffered or costs incurred, arising out of or in connection with the use of this report, however such loss or damage is caused.

It is the responsibility solely of ICO's management to ensure that there are adequate arrangements in place in relation to risk management, governance and control.

1 Executive Summary

1.1 Background

As part of the 2016-17 Internal Audit Plan, we have agreed with management and the Audit Committee to undertake a review to provide assurance over the process to manage IT assets. Following an incident involving a missing (secure) laptop, a review was requested by the Audit Committee over the controls over Accountable Security devices (called the "Cryptographic Controls" review). The ICO is also implementing a revised process to manage all IT assets going forward. This review focuses on how IT assets are managed and controlled but does not cover the specific requirements for compliance with CESG requirements.

1.2 Scope

The objectives of the review are to provide assurance over the adequacy of controls over the management of IT assets. The findings and conclusions from this review will support our annual opinion to the Audit Committee on the adequacy and effectiveness of governance arrangements. The review will be delivered in two phases:

1 An assessment of the design of the IT asset management processes to provide to identify opportunities for improvement (Phase 1) was carried out in November 2015.

2 This review (Phase 2) focusses on the operational processes based upon the new set of IT asset management controls reviewed in phase 1.

Our review considered the following risks:

- IT assets are missing and are unknown to ICO management
- The loss of an IT asset may contain sensitive information which could result in reputational damage
- Asset re-use / redeployment is poor leading to ICO purchasing additional assets and therefore increasing costs
- Unauthorised procurement lead to additional time spent managing and integrating the unauthorised asset

Further details on responsibilities, approach and scope are included in Appendix B.

1.3 Overall conclusion

Overall assessment – Design Effectiveness	
We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.	Green

Please refer to appendix B for further information regarding our overall assessment and audit finding ratings.

The table below details the key findings from our review.

1.4 Key findings

Risk / Process	High	Medium	Low	Imp.
IT asset management	-	-	3	-
IT asset procurement	-	-	-	-
IT asset usage	-	-	-	-
Total	**-**	**-**	**3**	**-**

There are no high or medium rated findings arising out of our review.

Further details of our findings and recommendations are provided in Section 2.

1.5 Basis of conclusion

Overall IT asset management within ICO is in a good state (other than the minor issues noted within this report). Processes are in place which are documented within a comprehensive asset management procedure. We also identified the following good practices:

- All IT assets are recorded with the details pertaining to that asset (such as classification, value, owner, location, serial number and asset number) when those assets are on ICO premises for the first time and a process is in place to ensure IT assets' information is kept up to date.
- All IT Assets are required to be tagged with the asset number.
- Procurement of IT assets is limited to members of IT management, to ensure control is maintained over the incoming IT assets.
- Renewal dates for licence agreements are documented and monitored by a traffic-light system (based on the number of days until renewal).
- All ICO laptops are encrypted.
- Mobile device management software is in use and is regularly monitored.
- Assets are disposed in a secure manner to prevent loss of confidential data.
- A project has been initiated to implement a new desktop and service management solution. This will include a configuration management database (CMDB) and asset identification on the network.

1.6 Acknowledgement

We would like to take this opportunity to thank the staff involved for their co-operation during this internal audit.

2 Detailed Findings

2.1 Asset management

1.	Low	Lack of documented procedures over management of software licences

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
We obtained the Asset Management Procedure; this was up-to-date and contained all relevant information in relation to management of physical IT assets from purchase, deployment and movement, through to disposal. There are however, no similar procedures in relation to management of software licences. Software licences are managed using a spreadsheet, which has a traffic-light system based on the number of days until renewal; this is monitored on a daily basis. Although this process is in place, this is not documented within a formal procedure. Where procedures are not documented there is a risk that procedures may not be followed in the absence of key staff leading to breach of licencing terms.	Procedures for the management of software licences should be documented either as part of the asset management procedure or within a separate procedure which is approved and communicated and subject to regular review.	*Agreed action: Document software license management procedure* *Date Effective: 31 March 2017* *Owner: Emma Deen/ Julie Tornetta*

2.	Low	Lack of formalised procedures over asset disposal

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
During the review, we were presented with a number of documented procedures in relation to asset management, management of cryptographic key materials, audit procedures and asset disposal procedures. All procedures are in the format of a formal policy that has been approved and contained a revision history. The asset disposal procedure however, was in the form of a PowerPoint presentation and lacked the same document/version controls i.e. approvals and revision status as the other procedures. Until policies are formally approved, then compliance with them is difficult to track and enforce.	Procedures for the disposal of IT assets should be reformatted in line with other formalised procedures that are approved and subject to regular review.	*Agreed action: Reformat disposals procedure* *Date Effective: 31 March 2017* *Owner: Emma Deen/ Julie Tornetta*

3.	Low	IT assets were not tagged.

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
The Asset Management process document requires that all assets require labelling with an asset tag. We undertook a physical inspection of five desks within the main office and two meeting rooms. Whilst all IT assets (including workstations, phones, mobile devices and monitors) within the office were tagged, we noted that monitors within the meeting rooms did not have an asset tag. Facilities explained that this was a legacy issue, as TV monitors were not previously classed as IT assets. There is a risk that not all assets are accounted for where they are not added to the register and clearly marked with an	All monitors within all meeting rooms should be tagged. Any new purchases of monitors by facilities should then also follow the asset management process and should be tagged.	*Agreed action: Asset tag meeting room monitors* *Date Effective: 31 March 2017* *Owner: Emma Deen/ Julie Tornetta*

3.	Low	IT assets were not tagged.

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
asset tag. This also increases the risk of theft.		

A Follow-up up of phase 1 findings

1.	Medium	Accurate and complete asset records are not in place

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*	Progress at phase 2
On a bi-annual basis, the ALMO conducts a physical audit of all IT assets except ACCSEC devices. ACCSEC devices are covered as part of the annual ACCSEC audit carried out by the Custodian to meet CESG requirements. The results of the physical audit are not being formally captured or reported to management. Additionally, although the non-ACCSEC assets are subject to a physical audit and the results of that audit are reconciled against the ICO asset register spreadsheet; there is no reconciliation against an independent source of asset information, such as an invoice or delivery note. Asset management policies states that should any issues be identified as part of the audit, these should be raised with the IT Helpdesk and decisions are made on next steps is made by the business based on the criticality of the incident. The policy does not state how this assessment of criticality should be carried out. Asset record keeping that is not operating effectively undermines the accuracy of a	The results of physical audits should be recorded within the asset register (when was the last physical audit conducted and by who) and shared with the IGSG. The incident management process over lost or stolen assets to include how to assess the criticality and therefore the appropriate action to take.	*Physical audit log to be added to asset register. Once each physical audit is complete, record to be copied from asset register and held as a stand-alone record of that periods' physical asset check. Reference to this to be added to the Asset Management procedure V1.0* *Asset Management procedure V1.0 to be updated to include risk assessment and action plan* *Date Effective: Complete by 31 January 2017 to enable phase II review of the operational processes referred to in 1.2 above.* *Owner: Emma Deen*	We observed the asset register - This now contains the date of the last physical audit date. All records of each audit are retained, these detail who conducted the audit. **Closed**

1.	Medium	Accurate and complete asset records are not in place

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*	Progress at phase 2
physical asset count which can in turn mean that assets that may be lost or stolen are not identified in a timely manner leading to damage to the ICO's reputation.			

2.	Low	Lack of guidance on non-project IT procurement

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*	Progress at phase 2
The ICO utilises the project management process to introduce new technology or make any significant changes to existing technologies. Under project management governance, purchases of equipment are made which are subject to management approval.IT assets that are not requested as part of a project (such as mice and keyboards) do not have a formal procurement process to follow. We identified that asset procurement can be initiated in three ways: 1. As a result of a new project 2. Replacing an asset as a result of end of life or damage 3. Other ad-hoc equipment requests Assets that are procured for a project will go through the formal project management governance and are approved by the project board. Other IT asset purchases are reviewed IT Service Team Manager and approved by	The process for non-project asset procurement should be documented and sets out what can be purchased, from where and who has the authority to approve such purchases.	*Non-project IT procurement process to be documented and shared with those with delegated authority* *Date Effective: 31 January 2017* *Owner: Emma Deen*	The Asset management procedures were updated in January 2017 to include Procurement advice and lost asset escalation process. **Closed**

2.	Low	Lack of guidance on non-project IT procurement

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*	Progress at phase 2
the Group Manager, Business Development. Most IT equipment purchases are raised with ICO's approved suppliers, Northgate or SEC. However, we noted that where purchases are made for low value items (such as a keyboard or a mouse), the purchase can be made with a different supplier. It is not clear what can be purchased outside of the formal IT procurement process or how. We were informed that where assets are not procured with approved suppliers (such as Northgate and SCC), ensuring that ICO's technical standards are being adhered to is the responsibility of Group Manager, Business Development.			

3.	Low	Monitoring of IT assets not connected to the network

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*	Progress at phase 2
Monitoring is not in place on all devices to identify ICO IT assets that have not been connected to the network for an appropriate period of time. Such devices may be candidates for redeployment or lack of connection may indicate that an asset has been lost or stolen. Management are reviewing their IT Service	Management should ensure that monitoring is in place to identify that ICO IT equipment is in active use.	*It was explained during the audit that ICO are limited in what they can do to monitor hardware use via network activity. We do not have direct control over this because of our contractual relationship with Northgate Public Services. Desktop management tools enable asset monitoring via Active Directory, which ICO cannot utilise.*	The previously agreed action has now been superseded as a project has been initiated to implement a new desktop and service management solution. Where possible this will include a CMDB and asset identification on the network. The project will

3.	Low	Monitoring of IT assets not connected to the network

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*	Progress at phase 2
Desk system solution and a new system could incorporate asset monitoring.		*The RSA portal reports enable us to monitor home working log in frequency. This will allow us to identify staff who have not logged in via their allocated device for an extended period of time. Report to be added to monthly monitoring.* *Replacement IT service desk requirement checklist to include system-monitoring abilities as a 'should have' requirement.* *Date Effective: 31 January 2017* *Owner: Emma Deen*	be completed by April 2017. **In Progress**

B Internal audit approach

Approach

Our audit will be carried out in accordance with the guidance contained within the Public Sector Internal Audit Standards (2013), and the Auditing Practices Board's 'Guidance for Internal Auditors'.

The objectives of the review are to provide assurance over the adequacy of controls over IT assets, in the following areas:

- Procurement of IT assets is limited to members of IT management, to ensure control is maintained over the incoming IT assets.
- All IT assets are recorded with the details pertaining to that asset (such as value, owner, location, serial number and asset number) and a process is in place to ensure IT assets' information is kept up to date
- Assets are regularly physically identified and asset records are reconciled
- ICO has the ability to determine market price for IT assets to ensure value for money
- Processes are in place to manage software licences (available licences are recorded, usage is regularly captured and available licences are used before purchasing new licences)
- Use of software is in line with licence agreement
- Renewal dates for licence agreements are documented) and responsibility for software licence renewal is in place
- Reporting of assets periodically to senior management
- A process is in place to ensure unauthorised equipment or assets are identified and that IT establish the underlying reasons why this has happened

We achieved our audit objectives by:

- agreeing the principles and benefits of effective risk management arrangements with management;
- meeting with key staff to gain an understanding of the arrangements in place, building upon the information we have already gained through our audit planning process;
- reviewing key documents that support the processes in place; and
- comparing existing arrangements with established best practice and other guidance.

The findings and conclusions from this review will support our annual opinion to the Audit Committee on the adequacy and effectiveness of internal control arrangements.

Additional information

Client staff

The following staff were consulted as part of this review:

- Christopher Goode, Asset and Licence Management Officer
- Julie Tornetta, IT Service Team Manager
- Emma Deen, Group Manager, Business Development

Documents received

The following documents were received during the course of this audit:

1 Asset management register
2 Software licence register
3 Asset management procedure
4 Example IT Asset changes email
5 Presentation on secure disposal to ICO staff
6 Homeworking kit process

Locations

We visited The Information Commissioner's Office, Wilmslow for this review.

C Overall assessment and audit issues ratings

Overall 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.

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

An instinct for growth™

grant-thornton.co.uk