ABERDEEN CITY COUNCIL

COMMITTEE	Audit and Risk
DATE	20th November 2014
DIRECTOR	Ewan Sutherland
TITLE OF REPORT	UK Information Commissioner, Data Protection Audit - Progress with Agreed Actions
REPORT NUMBER:	CG/14/132

1. PURPOSE OF REPORT

The purpose of this report is to update the Committee on the progress with implementing the actions agreed following the UK Information Commissioner's Office (ICO) Audit of the Council's Data Protection arrangements which was published in June 2013.

2. RECOMMENDATION(S)

that the Committee:–

(a) Note the progress with implementing the actions agreed following the Data Protection Audit; and

(b) Instruct officers to report progress with implementation of the actions to the Committee as appropriate until complete.

3. FINANCIAL IMPLICATIONS

There are no direct implications resulting from this report. It is the case, however, that costs could result from actions. It is also the case that breaches of data protection carry the possibility of financial penalty. The most recent fine applied to the Council being £100,000.

4. OTHER IMPLICATIONS

There are clear implications for the Council's management of risk as it relates to information. These are outlined at section 7 below.

5. BACKGROUND/MAIN ISSUES

The United Kingdom Information Commissioner's Office conducted an audit of the Council's data protection arrangements during 2013. Their report was published in June 2013 and contained a high number of agreed actions.

At the last meeting of this Committee officers provided an update on progress with the implementation of those actions. Since the last meeting, further progress has been made and an updated schedule of all outstanding actions is attached for the Committee's consideration.

6. IMPACT

The overall impact of implementation of the agreed actions is assurance of the Council's management of information and mitigation of risk as outlined in section 7.

7. MANAGEMENT OF RISK

There are clear risks associated with the creation and processing of data. The Council's Corporate Risk Register includes the following risk:-

"Risk that information is not managed effectively to support policy and decision making and statutory requirements."

Officers have currently evaluated the risk as having a "High" likelihood and a "Serious" impact.

The implementation of the agreed actions following the UK ICO Data Protection Audit and are a key mitigation of this. Once these have been fully implemented the likelihood of breaches should reduce.

There is a further risk of reputational damage associated with this report in the event of insufficient progress being made with implementation of the agreed actions.

Risk	Category	Cause	Impact
Risk that information is not managed effectively to support policy and decision making and statutory requirements.	Control	Not adhering to best practice attributes, standards and behaviours.	Breaches of data protection which result in i. censure and financial loss for the Council through ineffective processes for complying with statutory

			requirements; and ii. Insecure processing of data for the Council’s customers.
Controls	**Risk Class**	**Further planned mitigation**	
• Policy, procedures and processes; • Training / Induction • Audit & Inspection; • Self-reporting of breaches and CMT governance of these; • Information Management Strategy. • Corporate Records Management Approach.	Business	• Corporate gap analysis undertaken and improvement plan in place; • Actions from audits and inspections being taken forward; • Training - OIL course; • Compliance with Public Records (Scotland) Act from Jan 2013 - Development of Records Management Plans.	

8. BACKGROUND PAPERS

ICO Audit Report June 2013

9. REPORT AUTHOR DETAILS

Paul Fleming, Head of Customer Service & Performance
pfleming@aberdeencity.gov.uk
(01224) 523366

ICO Data Protection Audit Recommendations – Outstanding Actions

Introduction

Of the 36 recommendations accepted by Aberdeen City Council the implementation of 24 have been completed.

Recommendation	Agreed action, date and owner	Update August 2014	Lead Officer
A16. ACC should formalise an on-going DP targeted work plan, underpinned by a DP governance strategy, which is then periodically reviewed thereafter.	ACC accept this recommendation and will develop a targeted work plan which will be underpinned by the Information Management Strategy and Action Plan. The work plan will be reviewed in line with the Strategy at a bi-annual basis but will be monitored by the Steering Group referred to at A9above. OWNER: SIRO supported by appropriate officers TIMESCALE: within 6 months of Audit report being published.	Developments resulting from ICO recommendations have, in effect, been the prioritised work plan over the last 18 months. Following the approval of the Information Management Strategy (IMS) a proactive work plan will be put in place as part of the IMS Improvement programme priorities between January 2015 - March 2015	Fiona Smith
A19. ACC should consider implementing internal compliance checks, for example in the form of self-	ACC accept this recommendation. A checklist which is already in operation regarding clear desk practices will be reviewed and rolled out across all	As previously reported, implementation of this recommendation is overdue. The expected roll out of a clear desk policy checklist has not yet been possible as the draft checklist requires to be adapted to take account of revised working arrangements as part of the Smarter Working Programme.	Fiona Smith

assessments, to support overall DP compliance or areas where specific risk(s) may have been identified. Furthermore, compliance feedback should be collated and reviewed periodically in order to provide corporate oversight.	directorates to ensure compliance is effectively being monitored systematically and reported on. OWNER: SIRO supported by appropriate officers. TIMESCALE: checklist to be developed within 2 months of Audit report being published.	The IMGAG have agreed that the requirement for self-assessment and compliance monitoring in respect of DP compliance be included in the Information Management Strategy and be required by Committee in order to demonstrate the significance of this to all staff. Thereafter it is intended to include details of compliance and compliance monitoring within training for staff again to underline the significance of adherence as part of information management. In future, compliance checking will be tied into reporting considered by the IMGAG and reported to CMT on an exception basis. Officers have included work to map the internal controls across the Council within the 2014/15 Internal Audit Plan. It is anticipated that this will lead to a corporate approach to self-checks to support compliance with key policies and procedures and will include information management compliance.	Martin Murchie (re Internal Control Mapping)
B10. Introduce formal KPI's, overseen by CMT, to formally measure mandatory DP training completion.	ACC accept this recommendation and shall ensure that formal KPI's are devised and reported in accordance with A20 above. OWNER: SIRO supported by appropriate officers TIMESCALE: First report due second and quarterly thereafter.	Corporate reporting of mandatory training compliance via OIL (online) modules is reported monthly by HR to Directors. Directors are responsible for escalating any non-compliance issues. Training undertaken via other formats is currently being built into the corporate staff development system (YourHR) for Managers to update manually, but is currently not being monitored nor reported.	Dorothy Morrison / Fiona Smith
B11. Reporting improvements should be implemented concerning training completion compliance	ACC accept this recommendation and shall be exploring alternatives to ensure that it can easily identify those staff that have not undertaken training and	Work is currently underway to scope out including compliance monitoring as part of the Performance Review & Development function (PR&D) on YourHR (the Council's online HR portal). It is envisaged that a tool will be development by the YourHR team that will allow managers to see at a glance via YourHR who has completed the training in their teams / services.	Dorothy Morrison / Fiona Smith

monitoring, in order to simplify the identification of staff who have not undertaken mandatory training within an acceptable period.	improve reporting on a corporate basis. OWNER: SIRO with assistance from the Head of Human Resources and Organisational Development. TIMESCALE: within 6 months of the publication of the Audit report.	Immediate line manager oversight will enable close, local monitoring and early intervention to ensure that training is undertaken timeously. This function could also capture any refresher training etc in the same way. This function can also be used to prepare reports at section, service and corporate level. Implementation of this recommendation is behind schedule owing to the current work levels of the YourHR team. It is planned that the reporting function will be completed within 12 months of the publication of the Audit report.	
C4. ACC should adopt a protective marking scheme so as to provide clear benchmark guidance for appropriate security standards to apply to any data being processed. This would be consistent with SOCITM and HMG / Scottish Government guidance.	ACC will undertake an options appraisal to assess whether it will adopt a Protective Marking Scheme. OWNER: SIRO TIMESCALE: within 8 months of the Audit report being published.	As detailed in the February 2014 update, progress on implementing this recommendation has been delayed due to the wider issues in respect of the government marking scheme. IMGAG has decided to trial the ACC version of the new Government Classification Scheme (GCS) within SC&W and officers will report back to IMGAG on progress. However, the Joint Inspection of Children's Services has delayed the introduction into SC&W, it will start next month.	Steve Skidmore
C16. Protective markings should be applied to data and follow to 'end of life' including occasions of further processing by applications such as Business Objects.	ACC accept this recommendation and defers to its response at C4. ACC will investigate how it might achieve the "follow" function in relation to the processing of that data. OWNER: SIRO	See update to C4.	Steve Skidmore

	TIMESCALE: within 8 months of the Audit report being published.		
C17. ACC should adopt an asset ownership policy based on information assets rather than IT system or application. Owners should be responsible for assessing security standards to apply (including protective marking) and be responsible for whole life to destruction.	ACC accept this recommendation. Indeed, this recommendation accords with ACC's current Enterprise Architecture principles and work is currently on-going to develop ACC's data architecture layer which will include the recommended information. OWNER: SIRO TIMESCALE: December 2013	The creation of an Information Asset Register has commenced as part of the Corporate Information Management Strategy Improvement Programme (Committee approval 30 September 2014). Information Asset owners have been identified through the creation of a Business Classification Scheme by business function (Submission to Committee for approval 4 Dcember 2014). Asset ownership responsibilities will extend to technical (ICT) and physical systems (Branch office sites) management as well as information type (Data, record /class), access, security, retention and content (official / sensitive).	Paul Fleming / David McDowell
C21. ACC should adopt an integrated IS incident reporting process covering both ICT and paper assets so as to provide a common approach for staff to follow. In addition, ACC should adopt procedures to allow for the reporting of all IS incidents outside of normal office hours such as loss of ID badges.	ACC accept this recommendation and will take steps to consider how best to amalgamate the reporting process. OWNER: SIRO TIMESCALE: within 6 months of the Audit report being published.	A draft procedure in respect of an integrated IS reporting process covering both ICT and paper assets has been considered by CGSMT and will be submitted to CMT for final approval. Once approved the procedure will form part of the ACC Managers Handbook. In respect of the reporting of all IS incidents outside of working hours, the Council requires to give further consideration to how this can be delivered having regard to the level of risk posed and resource requirements to achieve it. This will be done by the end of 2014 also.	Steve Skidmore
C28. Access controls should be restricted	ACC accepts this recommendation. ACC will	Across the Council, the following arrangements now apply or are in the process of being implemented:	Mike Duncan / Simon Williams

by default to normal office hours when on-site security is available. Exceptions should then be made for staff required to work regularly outside of normal office hours.	review restricting access controls to normal staff hours; however past experience would suggest that due to the nature of the services undertaken by the building's occupiers, a large minority will then require access outside these hours (after discussion with their managers). Furthermore with the development of New Ways of Working such an approach may, in the passage of time, not be practical. OWNER: General Manager – Asset Manager & Facilities Manager TIMESCALE: Within 6 months of the Audit report being published.	1. All new starts are issued with access on a default setting of 7am – 8pm Monday – Friday. Any exceptions to the default are considered on a case by case basis. 2. All Directors and Heads of Service have 24/7 access to all corporate office buildings. 3. All services have been requested to advise of staff who, as part of their job role, require access out with the default hours. 4. All existing staff not advised by the service will have their access set to the default setting on a phased programme which is subject to the availability of the Security Co-ordinator Services feedback needs further review as many requested access which seemed excessive so the reduction not implemented as yet. Issuing of new badges to match new structure may delay the implementation of above even further. 5. Non routine access will be treated as an ad hoc request and will require a minimum of 48 hour's notice in order to change access settings.	
C31. As it was reported that ACC operate a 24hr CCTV facility CCTV cameras should be linked to this for real time observation. CCTV cameras should also be upgraded to a common standard of high resolution to ensure effectiveness and faulty cameras replaced.	ACC partially accept this recommendation. ACC shall review the specification of the existing CCTV cameras, costs involved in potentially upgrading and thereafter linking to the central CCTV Control. At present no budget has been identified. A complete review of costs involved against the actual risk requires to be undertaken. OWNER: Facilities Manager	As previously updated, the Housing & Environment Service have undertaken a survey of all CCTV, as such the timescale previously intimated within the audit response has been met. The detailed assessment of individual CCTV cameras has been completed. It is now being considered if all systems and images can be sent back to one central location or require to remain as stand-alone systems. It is proposed that a lead officer from Communities, Housing and Infrastructure directorate is identified to take this project forward.	Simon Williams

	TIMESCALE: Review of Requirement – 6 months IMPLEMENTATION: Subject to outcome of review		
C37. MFDs should be the standard default printer setting for all staff use and ACC should prioritise this planned change. The PIN system of user selected codes offers poor security and should be replaced by an ID proximity card authorisation system to comply with industry standard good practice.	ACC partially accept this recommendation. A) Proximity cards are being considered in connection with a new procurement exercise for multi-function devices once the current contract ceases in December 2014. B) In the interim, the Council will re-issue guidance to staff about how to set printing preferences to secure print and printer default settings will be reviewed OWNER: Facilities Manager/ Head of Procurement, IT Manager TIMESCALE: A) December 2014. B) within 4 months of Audit report being published.	A. A: As per previous update, on-going consideration is being given to the use of proximity cards in connection with the new procurement exercise for multi-function devices once the current contract ceases in December 2014. B. Regular reminders on the use of secure printing are distributed via the Zone and through e-mail cascade from Directorate Business Managers.	Sandra Massey