ABERDEEN
CITY COUNCIL

Internal Audit Report

Commissioning

Information Governance

Issued to:
Andy MacDonald, Director of Customer Services
Martin Murchie, Chief Officer – Business Intelligence and Performance Management
Fraser Bell, Chief Officer – Governance
Jonathan Belford, Chief Officer – Finance
Caroline Anderson, Information and Data Manager
External Audit

Date of Issue: February 2020 **Report No. AC2020**

EXECUTIVE SUMMARY

The Council's Corporate Information Policy defines the Council's information as all information and data created, received, maintained or used by or on behalf of the Council, in any format and of any age.

The Council's Corporate Risk Register includes risk Corp-005 which is defined as "Information governance protocols and processes do not provide the appropriate framework to facilitate optimum information management in support of decision making and resource allocation based on a Business Intelligence culture".

The objective of this audit was to provide assurance that the controls in place for mitigating the risks identified in the Corporate Risk Register (Corp005) are adequate and operating as expected. In general, this was found to be the case.

Comprehensive and clear policies, procedures and mandatory training are in place. In addition, the Corporate risk and related controls are being assessed monthly by the Information Governance Group, chaired by the Council's Senior Information Risk Owner, and by Corporate Management Team, and reviewed annually by Committee. Information Governance controls were comprehensive and control assessments were, in general, supported.

1. INTRODUCTION

1.1 The Council's Corporate Information Policy defines the Council's information as all information and data created, received, maintained or used by or on behalf of the Council, in any format and of any age. The policy recognises the crucial role that the proper use and governance of Council information and data plays in:

- delivering outcomes for the people, place and economy of Aberdeen;
- respecting privacy and fostering trust;
- demonstrating accountability through openness and ensuring compliance with Data Protection, Freedom of Information, Environmental Information, Re-Use of Public Sector Information and Public Records law;
- enabling and supporting staff in the proper use and governance of Council information and data;
- building the Council's corporate memory and the memory of the people and place of Aberdeen.

1.2 The Council's Corporate Risk Register includes risk Corp-005 which is defined as "Information governance protocols and processes do not provide the appropriate framework to facilitate optimum information management in support of decision making and resource allocation based on a Business Intelligence culture".

1.3 The objective of this audit was to provide assurance that the controls in place for mitigating the risks identified in the Corporate Risk Register (Corp005) are adequate and operating as expected.

1.4 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Martin Murchie, Chief Officer – Business Intelligence and Performance Management and Caroline Anderson, Information and Data Manager.

2. FINDINGS AND RECOMMENDATIONS

2.1 Written Policies and Procedures

2.1.1 Comprehensive written policies and procedures which are easily accessible by all members of staff can reduce the risk of errors and inconsistency. They are beneficial for the training of current and new employees and provide management with assurance that correct and consistent instructions are available to staff. This is important in the event of an experienced employee being absent or leaving, and they have increased importance where new systems or procedures are being introduced.

2.1.2 Policies in place covering the Council's information governance arrangements, include: the Corporate Information Policy, which details the policy on the use and governance of the Council's information and data; the Corporate Protective Monitoring Policy, which details the means of collecting, analysing and reporting on threats to the Council's information and data; the Corporate ICT Access Control Policy, which details the expected controls and employee behaviour, to avoid unauthorised access to Council information and data; and the Corporate ICT Acceptable Use Policy, which defines employee responsibilities when using Council ICT equipment, networks and systems.

2.1.3 Procedures available in relation to information governance include: the Managing Information Handbook (Council's minimum standard for managing information including legislative requirements), Freedom of Information and Environmental Information Procedures; Bond Governance Insider Protocol to ensure compliance with the Market Abuse Regulations as a result of the Council's bond issue on the London Stock Exchange; the Information Asset Owner Handbook, covering requirements for senior business managers in relation to the information assets they are responsible and accountable for; the Corporate Records Retention and Disposal Schedule; and the Corporate Information Security Incident Reporting Procedure (information security incident and near miss reporting requirements).

2.1.4 Policies and procedures were available on the Zone and were comprehensive, clear and current.

2.2 Training

2.2.1 It is mandatory for all employees to complete the on-line interactive learning (OIL) based course "Information Governance" on an annual basis. The course is comprehensive, covering the Council's information governance policy and procedural requirements, and the related legislation. The Service has advised that completion of the course by employees is monitored by Chief Officers and Corporate Management Team (CMT) Stewardship on a monthly basis using the People Performance dashboard, which includes exception reporting of staff who have not completed Information Governance training as required. The "edited" People Performance dashboard was first reported to CMT Stewardship on 28 November 2019.

2.2.2 Data is extracted from the payroll system and online learning system by People and Organisation (P&O) on a monthly basis and sent to Business Intelligence and Performance Management (BI&PM) to be uploaded into the PowerBI based People Performance dashboard. The dashboard displays the number of staff who have not completed the mandatory Information Governance training by Cluster and by month, excluding staff that are on sick leave or maternity leave and those who have commenced employment with the Council in the last month.

2.2.3 The "unedited" dashboards available to Chief Officers are specific to each Chief Officer's Cluster and enable details to be reviewed of staff who have not completed the training as required for follow up purposes. An instruction on the use of the dashboard was issued to Chief Officers on 14 June 2019 by email. This explained the process for exporting details of staff who have not completed mandatory training for the purposes of disseminating details of non-compliance to third tier managers. Whilst the instruction is clear, the process of dissemination of information by Chief Officers requires manual intervention. BI&PM advised that it is possible to report to third tier managers directly via the dashboard. Granting third tier managers access to the dashboard for the staff they manage would facilitate the follow up process for non-compliance by staff.

2.2.4 BI&PM requires 350 PowerBI licenses in order to roll out the People Performance dashboard to third tier officers. A business case for a revised Microsoft Enterprise Agreement (MEA) covering the period 1 April 2020 to 31 March 2023 was approved by the Strategic Commissioning Committee on 30 January 2020; D&T advised this covered the PowerBI license requirements for rolling out the dashboard to third tier managers.

2.2.5 Whilst the People Performance dashboard is a useful means of identifying staff who have not completed mandatory training the position available via the dashboard as at 20 January 2020 was historic (30 November 2019) since this was the last data provided by P&O. BI&PM advised that the intention is to provide “real time” data via the dashboard when a new online learning platform is brought into use.

2.2.6 The Employee Data Forum is responsible for managing and driving a coordinated approach to improvements required to the governance, architecture, performance reporting and improvement arrangements for employee related information and data assets. The group is co-chaired by the Chief Officer – Business Intelligence and Performance Management and the Chief Officer – People and Organisation. People Performance was an agenda item on the January 2020 meeting of the Employee Data Forum and it was agreed that Business Intelligence and Performance Management would collaborate with Digital and Technology to automate updates of employee data, including exception reporting in relation to Information Governance training completion. The Chief Officer – BI&PM has advised progress will be monitored by the Employee Data Forum.

2.2.7 The Data Protection page of the Zone includes a link to the available OIL based Information Governance course and training slides covering: changes to data protection law (as a result of the General Data Protection Regulation); Information Asset Owner responsibilities; and privacy notices. The Data Protection page also indicates face to face data protection training can be delivered on request by contacting the Council’s Data Protection Officer.

2.2.8 Information Governance advised that a briefing is also provided at monthly Corporate Employee Induction sessions, to ensure all new staff are aware of the relevant policies and procedures and the Information Governance OIL course.

2.3 Information Governance Controls

2.3.1 The Corporate Risk Register risk Corp 005 Information Governance identifies a number of relevant potential impacts of information management failing to support decision making and resource allocation, including: unlawful disclosure of sensitive information; individuals placed at risk of harm; service disruption; financial penalties; and prosecution. To mitigate these, Corp 005 identifies the following controls:

- Clear policies, systems and processes in place for ensuring appropriate management, governance and use of information;
- Mandatory information governance training for all staff with regular exception reporting;

- Clear roles and responsibilities assigned and embedded for all staff for managing & governing information assets across the Council;
- Information Governance Board led by SIRO provides robust corporate oversight of information assurance arrangements;
- Effective monitoring and reporting of corporate and information asset level information governance arrangements is in place;
- Data Forums;
- Data Protection Officer directly influences information governance;
- Effective Governance in place around Bring Your Own Device Arrangements;
- Enabling functionality of digital / technology systems are fully assessed and compliant.

2.3.2 All of the above controls have been assessed by management, in November 2019, as fully effective with the exception of the final control relating to digital / technology systems which has been assessed as partially effective. Internal Audit reviewed these controls to determine if the fully effective control assessments were correct and action was being taken in a timely manner to implement the partially effective control.

Policies, procedures and training (including roles and responsibilities)

As covered in section 2.1 and 2.2 above, policies and procedures are comprehensive and clear covering roles and responsibilities in relation to information use and governance (the Managing Information Handbook and the Information Asset Owner Handbook) and mandatory information governance training is in place for all staff.

Information Governance Board led by SIRO / monitoring and reporting arrangements

2.3.3 The Information Governance Group's (IGG) terms of reference state that the group's purpose is "to drive the corporate, information-governance agenda, setting standards, monitoring compliance and maintaining ethical practice, holding to account the organisational roles and responsibilities that provide CMT with the assurance that effective control mechanisms are in place within the organisation to manage and mitigate the Council's information risks".

2.3.4 According to the Corporate Information Policy, the Senior Information Risk Owner (SIRO), is accountable to the Chief Executive for the management of the information risks across the Council. The SIRO (Chief Officer – Governance) chairs the Information Governance Group and other core members include: the Chief Officer – Business Intelligence and Performance Management; the Chief Officer Digital and Technology; the Information and Data Manager; and the Data Protection Officer.

2.3.5 A sample of IGG minutes from between May and November 2019 was reviewed by Internal Audit. The group is meeting monthly to discuss relevant information governance matters, including to agree the most recent Corporate risk Corp 005 position reported by the Information and Data Manager. Other items discussed by the IGG included: the information governance assurance cycle; the information governance quarterly report; data breaches and incidents; and cyber security risks and controls (corporate risk 006).

2.3.6 The purpose of the information governance assurance cycle is to provide assurance to the SIRO that the Council's information asset owners have appropriate controls and measures in place at an information asset level across the organisation. A key part of the cycle is the identification of where action is required to bring assurance to an appropriate level and to manage and monitor the completion of any such actions, i.e. via the information governance group or, where applicable, CMT.

2.3.7 The Corporate Information Policy defines Information Asset Owners as senior business managers responsible and accountable for the specific, defined information assets within their remit, in accordance with the Council's Information Asset Owner Handbook (the Handbook). The Handbook defines an Information Asset as an identifiable collection of data stored in any manner, at any location, which is recognised as having value to the Council for the purposes of performing its business functions and activities. All collections of information containing personal information must be managed as Information Assets.

2.3.8 Information Asset Owners are required to provide assurance to the SIRO on the use, management and governance of their information assets, to enable the SIRO to report to the Chief Executive. A checklist is available in the Information Asset Owner Handbook which details expected actions by the Information Asset Owner in order to provide this assurance, including:

- the Information Asset Register is up to date;
- Privacy Impact Assessments have been completed where required in relation to data protection;
- contractual arrangements are in place with third parties involved in processing, hosting or supporting the Information Asset;
- it is known who has access to information and why;
- appropriate disaster recovery and business continuity arrangements are in place;
- the Information Asset Owner is satisfied with the technical and physical measures in place to secure and protect the Information Asset; and
- risks in relation to Information Assets are actively managed with risk registers updated as appropriate.

2.3.9 Information Asset Owners are required by the Handbook to register and keep up to date entries relating to their information assets in the Council's Information Asset Register. This is the main means by which assurance over information assets is obtained.

2.3.10 Information Governance and Digital and Technology (D&T) are collaborating to develop a database which is more focused on the flow of data. This will include all relevant details for each Information Asset, including the means by which data is captured; the relevant privacy notice to notify the public of data being captured; the system used to store and process the data; adequacy of technical and physical measures to secure Information Assets; and the reasons, means and legal basis for processing.

2.3.11 A recommendation was agreed as part of Internal Audit report AC1912 "Data Security in a Cloud Based Environment", for the Service to liaise with D&T to establish a revised Information Asset Register that reflects all Council systems, describing the nature of the data held in Council systems and the adequacy of technical and physical measures to secure that data. The Service has advised that the Information Asset Register will be updated to include the adequacy of technical and physical measures to secure data by February 2020.

2.3.12 The fully effective status of Corporate Risk 005 control "Effective monitoring and reporting of corporate and information asset level information governance arrangements is in place" did not reflect the fact the Information Asset Register is being developed as described in paragraph 2.3.11. Business Intelligence and Performance Management has since updated the control assessment to "partially effective" and established an Assurance Action to update the Information Asset Register as agreed in Internal Audit report AC1912. BI&PM advised that the updated position is due to be reported to CMT Stewardship on 20 February 2020 with progress to date of 50% and a completion date of 28 February 2020.

Data Forums

2.3.13 The Council's Business Intelligence & Performance Management Cluster has established six Data Forums to drive development and improvement of the Council's data capabilities and governance arrangements. These are arranged by data entity rather than by organisational structure to enable relevant stakeholders to contribute to the data projects and related improvements. These data forums are as follows:

- Employee Data
- Children & Young People Data
- Governance Data
- Asset Data
- Finance & Procurement Data

2.3.14 The Data Forums are required to provide the Information Governance Group with the assurance that effective control mechanisms are in place within the organisation to manage and mitigate the Council's corporate information risks. The core members include: the Chief Officer(s) relevant to the Data Entity; the Chief Officer – Business Intelligence and Performance Management; the Information and Data Manager; the Data Protection Officer; and the relevant Information Asset Owner(s). The Chief Officer – Business Intelligence and Performance Management, the Information and Data Manager, and the Data Protection Officer are members of the Information Governance Group, meaning relevant issues can be reported to the IGG and CMT as required.

2.3.15 It was reported to the November 2019 Information Governance Group that actions arising from the annual assurance cycle will be consolidated into action plans to be managed and monitored through the relevant Data Forum. Pro-forma action plans have been prepared and owners have been assigned to Data Forum Action Plans which cover: local procedures; retention and disposal; privacy notices; data protection impact assessments; information sharing and incidents and breaches.

Data Protection Impact Assessments

2.3.16 As well as via the Data Forums and annual assurance cycle, the Information Governance Group identifies new and emerging Information Governance risks via Data Protection Impact Assessments. The Information Asset Owner Handbook requires a Data Protection Impact assessment to be completed where information assets contain personal data and there is to be a change in the way the information is collected, stored, used, managed or processed. Instances were identified in June 2019 in Internal Audit report AC1912 "Data Security in a Cloud Based Environment" where DPIAs were not completed as required. Recommendations were agreed to address this.

Data Protection Officer

The Data Protection Officer influences information governance in a number of ways. As stated above in paragraphs 2.3.4 and 2.3.13, the DPO is a member of the Information Governance Group and the Data Forums. In addition, the DPO monitors data breaches for the purposes of reporting to the Information Commissioner's Office and Information Governance Group. The Data Protection Officer is also required to review all Data Protection Impact Assessments prior to approval by the relevant Information Asset Owner / Chief Officer (as appropriate).

Bring Your Own Device Arrangements

2.3.17 A Bring Your Own Device policy was reported to the Operational Delivery Committee in September 2019. This covered the use of employee owned Information Technology devices to access Council information, data, systems, and any other ICT resources. The

Committee approved the policy with a request that a Service Update be issued to Members after 12 months on how successful the policy has been with take up rates and details of any possible cost savings. The policy is clear and details Chief Executive, Director, line manager, Digital and Technology, and user responsibilities.

Functionality of digital / technology systems

2.3.18 The control "Enabling functionality of digital / technology systems are fully assessed and compliant" was reported to the November 2019 Information Governance as partially effective. A related assurance action was included in the November corporate risk register as required with an update from the relevant responsible officer. The related action is to assess the extent of digital records requiring long term preservation and create a digital repository to address the issue of long term storage.

2.3.19 The progress was reported as 20% with an original due date of 31 March 2019 and an amended due date of 31 December 2020. Data is being gathered on the number of Council digital records; an options appraisal is underway regarding a suitable digital repository; and guidance is being drafted on the fundamentals of digital preservation. The delay is due to the work involved being underestimated.

2.4 Performance Reporting

2.4.1 The Information Governance Group provides a quarterly report to the Information Governance Group on Information Governance Management and an annual report to CMT and the Audit, Risk and Scrutiny Committee. These reports cover a range of information governance statistics, including numbers of: data protection requests; data protection breaches; freedom of information and environmental information requests; cyber incidents; and physical incidents, e.g. loss of ID badges.

2.4.2 The 2019/20 quarter 1 performance report was reported to Information Governance Group on 6 August 2019 and the annual report for July 2018 to June 2019 was reported to CMT on 29 August 2019 and noted by the Audit, Risk and Scrutiny Committee on 25 September 2019.

2.4.3 Whilst these Information Governance reports are otherwise comprehensive and clear, it was noted that the Audit, Risk and Scrutiny Committee is no longer receiving an update on Information Governance training completion statistics for Council employees as part of the Information Governance report. The Service has advised that Information Governance training completion rates will now be reported to Staff Governance Committee.

2.4.4 The Corporate Risk Register, including Corporate Risk 005 Information Governance, is reported to Corporate Management Team monthly following review by the Information Governance Group; Internal Audit confirmed this was taking place as expected. The Audit, Risk and Scrutiny Committee received an annual report on the Corporate Risk Register and Corporate Assurance Map in September 2019. This also covered Corporate Risk 005 Information Governance, including the assessment of Information Governance controls.

AUDITORS: D Hughes
A Johnston
C Simpson