Governance, Risk and Best Value Committee

10.00am, Tuesday 28 August 2018

Internal Audit: Review of General Data Protection Regulation (GDPR) Readiness Programme

Item number	7.10
Report number	
Executive/routine	
Wards	
Council Commitments	

Executive Summary

The purpose of this paper is to present the outcomes of the Internal Audit (IA) review of the Council's GDPR Readiness Programme to the Committee.

This specialist review was included in the 2017/18 Internal Audit plan and was performed by PwC as part of the existing Internal Audit co-source arrangement.

Whilst the review confirmed that the Programme was appropriately designed to identify key GDPR readiness risks and control gaps across the Council and identified a number of areas of good practice; it also noted the risks associated with Information Governance Unit (IGU) resourcing levels which could limit the necessary capacity to complete Programme activities and provide ongoing assurance of the Council's progress towards full GDPR compliance.

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Report

Internal Audit: Review of General Data Protection Regulation (GDPR) Readiness Programme

1. Recommendations

1.1 The Committee is recommended to note:

1.1.1 the outcomes of the GDPR Readiness Programme internal audit review;

1.1.2 the Council wide potential GDPR risks associated with Information Governance Unit (IGU) resourcing levels; and

1.1.3 that the Corporate Leadership Team will review the adequacy of IGU resource allocation as part of the change strategy and financial planning arrangements, scheduled for September 2018.

2. Background

GDPR Readiness Programme

2.1 The GDPR came into effect on 25 May 2018 and the Information Commissioner's Office (ICO) has stated that it expects organisations to have established plans detailing the actions they need to implement to achieve compliance with the new regulations, with focus on addressing known legacy issues.

2.2 To meet this expectation, the Council's Information Governance Unit (IGU), within the Strategy and Insight Division, developed a risk based GDPR readiness programme (the Programme), with the objective of assessing the extent of GDPR readiness across the Council.

2.3 A total of 12 GDPR 'high risk' and 18 'medium risk' Service Areas were identified by the Programme.

2.4 GDPR readiness across these Service Areas was assessed by completion of questionnaires and "Survey Interviews". This approach was designed to assess the gap between existing data protection processes and controls in comparison to those required by the GDPR; the appropriateness of data protection responsibilities; and compliance with the Council's information governance policies.

2.5 Following completion of these interviews, Service Area action plans were created by the IGU detailing actions required to address the gaps identified and associated risks. Actions were recorded and are to be implemented by individual Service Areas, with implementation progress monitored by IGU.

2.6 Service Area action plans were then consolidated into Council wide Programme outcomes detailing the Council's current levels of compliance with GDPR; the gaps to be addressed; and identifying a number of corporate GDPR risks.

2.7 These outcomes were shared with Service Areas; Risk and Assurance Committees; Divisional Management Teams; the Council's Corporate Leadership Team (9 May 2018) and will be shared with appropriate Executive Committees.

Scope of the IA Review

2.8 This specialist review was performed by PwC under the terms of the current Internal Audit Co Source agreement.

2.9 The scope of the review assessed the adequacy of the design of Programme, considering whether it was appropriately designed to identify key GDPR readiness risks across the Council, and ensure that appropriate action plans were developed to support the move towards GDPR compliance.

2.10 The benchmarking used to support this assessment were comparison to the 12 GDPR preparation steps published by the Information Commissioner's Office (ICO); the guidance issued by the European s.29 Working Party Group; and good practice adopted by other organisations.

2.11 This audit was performed in conjunction with the Programme, with our work performed between March and May 2018. IA selected a sample of 4 'high risk' and 1 'medium risk' Service Areas as the basis for our assessment on the design of the Programme in addition to review of relevant Programme and operational information governance documents.

3. Main report

3.1 Our review confirmed the Programme was appropriately designed to identify key GDPR readiness risks and control gaps across the Council, with high risk Service areas prioritised and significant focus on awareness and training which will help support the move towards GDPR compliance. Additionally, a number of areas of good practice were identified

3.2 Whilst the Programme has been appropriately designed, we noted that Programme delivery has been impacted by resourcing challenges. This presents a risk to the Council in relation to the capacity to complete the Programme; specialist (second line) oversight of completion of Service Area GDPR actions; supporting and providing oversight of resolution of relevant corporate risks with GDPR impacts (for example third party contracts and shadow IT); providing an ongoing view of the Council's progress towards full GDPR compliance; and capacity to support ongoing and increasing volumes of operational IGU activity generated as a result of the new regulations. This risk is reflected in the High rated finding included in the draft report.

3.3 We also identified the need for enhanced IGU scrutiny of Data Privacy Impact Assessments (DPIAs) prepared by Service Areas to confirm that data held in systems

is aligned with GDPR data minimisation principles. This risk is reflected in the Medium rated finding included in the draft report.

3.4 At their meeting on 1 August 2018, the Corporate Leadership Team decided to consider that IGU resourcing requirements would be considered as part of the change strategy and financial planning process in September 2018. Consequently, a date of 31 October 2018 has been allocated to the high rated finding included in the report.

4. Measures of success

4.1 Appropriate management actions have been agreed and will be implemented to address the GDPR risks identified.

5. Financial impact

5.1 Not applicable.

6. Risk, policy, compliance and governance impact

6.1 A high rated finding has been raised reflecting the GDPR risks associated with IGU resourcing challenges.

7. Equalities impact

7.1 Not applicable.

8. Sustainability impact

8.1 Not applicable.

9. Consultation and engagement

9.1 The Corporate Leadership Team (CLT), the Head of Strategy and Insight; Democracy, Governance and Resilience Senior Manager; the Records and Information Compliance Manager have been consulted and engaged.

10. Background reading/external references

10.1 None.

Lesley Newdall

Chief Internal Auditor

E-mail: lesley.newdall@edinburgh.gov.uk | Tel: 0131 469 3216

11. Appendices

Appendix 1: Internal Audit Report - Review of the General Data Protection Regulations Readiness Programme

The City of Edinburgh Council

Internal Audit

Review of the General Data Protection Regulations Readiness Programme

Final Report

8 August 2018

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2017/18 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2017. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there is a number of specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

1. Background and Scope

Background

After four years of political negotiations and lobbying, the EU agreed the final wording of the General Data Protection Regulation ("GDPR") in December 2015. The new regulation introduced changes from the previous Act (the Data Protection Act 1998) but also related legislation. Those changes included increased financial sanctions for non-compliance, and this impacts every entity that stores or processes the personal data of EU citizens, both within and outside of the EU.

The GDPR came into effect on 25th May 2018 and it is expected that organisations will have established plans detailing the actions they need to implement to achieve compliance with the new regulations, with focus on addressing known legacy issues.

The adoption of the GDPR presents numerous challenges. The key issues to be aware of include:

- demonstrating compliance with the new rules (or the "Accountability Principle"). Under this principle, the assumption that organisations are complaint with the law has been removed. The burden of proof to demonstrate compliance with the law is now the responsibility of the organisation. For example, one of the documents required to demonstrate compliance is the Record of Processing, required by Articles 5(2) and 30 of the GDPR;
- changed approach for public authorities regarding consent and consent management; and
- changes to Subject Access Requests (SARs) timescales and mandatory reporting of certain breaches.

The City of Edinburgh Council's (The Council's) Information Governance Unit (IGU), within Strategy and Insight, has developed a risk based GDPR readiness programme, with the objective of assessing the extent of GDPR readiness across the Council.

The IGU assessed GDPR readiness by conducting questionnaires and "Survey Interviews" across the Service Areas. This approach was designed to assess the gap between existing data protection processes and controls against those required by the GDPR. In addition, the interviews also assessed the appropriateness of data protection responsibilities and compliance with the Council's information governance policies.

Following the completion of these interviews, Service Area action plans were created by the IGU team to address the gaps identified and associated risks. Actions were recorded and are to be implemented by individual Service Areas, with implementation monitored by IGU with appropriate reporting.

Programme outcomes will be shared with Service Areas, Risk Committees, Senior Management Teams, the Council's Corporate Leadership Team, and relevant scrutiny committees. This will ensure high levels of awareness regarding significant gaps identified and the extent of work required to achieve GDPR compliance.

Scope

The scope of the audit assessed the adequacy of the Council's GDPR readiness programme in comparison to the 12 steps for GDPR preparation published by the UK Information Commissioner's Office. It assessed whether the programme was appropriately designed to identify key GDPR readiness risks across the Council; ensure that appropriate action plans were developed to support the move towards GDPR compliance and address the following Corporate Leadership Team (CLT) risk:

- **Information Governance -** A loss of data from the Council's control could result in fines, claims, loss of public trust and reputational damage. This risk takes into account the new requirements arising from the New General Data Protection Regulation due to take effect in May 2018.

This assessment was made against good practice adopted by other organisations; the guidance issued by the European s.29 Working Party Group; and the UK Information Commissioners Office (ICO).

This specialist review was performed by PwC under the terms of the existing Internal Audit Co Source agreement.

This audit was undertaken alongside the GDPR readiness programme, with work performed between March and May 2018, enabling the IA team to jointly attend relevant meetings scheduled by the IGU team.

Limitations of Scope

Work performed by the IA team did not include the following areas in scope:

- Our review was limited to the design of the GDPR readiness Programme and did not cover control effectiveness. Consequently, no detailed testing or deep dives into specific Service Areas was performed to confirm the accuracy of IGU gap analysis assessments;
- Interviews and meetings with Service Areas were limited to those Service Areas assessed as high risk, or where further information is required to clarify maturity;
- Only those processes and policies within the control of the Council were included in scope. No work was performed to assess the extent of third party supplier compliance with GDPR requirements; and
- This work does not guarantee that the organisation will be fully compliant with GDPR requirements.

For the full terms of reference see Appendix 2.

Approach

During the review planning process, the following documents were requested and reviewed:

1. GDPR Project Plan
2. Project Status Reports to the CLT (Corporate Leadership Team)
3. Records Retention Guidance
4. Data Sharing Agreement Template
5. Full Privacy Notice (in draft form).

The approach applied by the IGU was to hold 'gap analysis' meetings with Service Areas. These meetings were prioritised on the basis of GDPR risk assessments where Service Areas were assessed as either 'high', 'medium' or 'low' risk. The risk rating was based of the volume and quality of personal data they were likely to process. Service Areas assessed as 'low risk' did not handle personal data.

This resulted in a total of 12 'high risk' and 18 'medium risk' Service Area gap analysis meetings for IGU to complete. IA decided to prioritise high risk areas as these were the main areas of concern for the project and selected the following sample of 4 'high risk' and 1 'medium risk' Service Areas:

1. Community Safety (High Risk)
2. Access to Housing (High Risk)
3. Special Schools (High Risk)
4. HR (High Risk)
5. ICT Programmes (Medium Risk)

The gap analysis meetings were conducted as a series of interview questions by the IGU team and it was agreed that the IA team would attend the meetings noted above so that proceedings could be observed. The aim of the IGU team's questions was to understand the risks associated with departments' data processing activities in relation to the GDPR.

Following completion of the interviews, two key documents were produced by the IGU:

- A Service Area Record of Processing (which feeds the Council wide Record of Processing); and
- A report detailing any identified risks in the Service Area's systems or processes. Each risk was assigned a RAG-status (high, medium, and low) and an action plan was developed alongside the department to mitigate the identified risks.

Following attendance at these meetings, the IGU provided IA with the subsequent gap analysis reports developed for these Service Areas, and the accompanying Record of Processing for review.

Additional meetings were held with the readiness programme and a further documentation requested. This included information on Breach reporting; volumes of Subject Access Requests (SARs); the Data Protection Impact Assessments (DPIA) process; and the latest CLT updates.

Collectively this additional selection was examined and further questions were compiled and addressed in a meeting with the IGU.

2. Executive summary

Total number of findings

Critical	-
High	1
Medium	1
Low	-
Advisory	-
Total	**2**

Summary of findings

The Council's approach to GDPR readiness was appropriately designed to identify key GDPR readiness risks and control gaps across the organisation. High risk Service areas have been prioritised and there has been significant focus on awareness and training throughout the programme, which will help ensure appropriate action plans are developed and implemented to support the move towards GDPR compliance.

Whilst the GDPR readiness gap analysis was completed by the end of April (as noted in the update provided to the Corporate Leadership Team on 9 May), we observed that the programme had fallen behind the original planned timelines of end of March, which would have ensured resolution of any significant (High rated) control gaps identified in high risk Service Areas two months in advance of GDPR regulations becoming effective on 25 May 2018.

A total of 70 High priority GDPR findings were identified by IGU by the end of April, enabling Service Areas to implement mitigating actions by 25 May. IGU has not obtained formal confirmation from Service Areas that all actions were fully addressed prior to 25 May.

As a result of these delays timeframes for the completion of other work streams within the programme, including addressing medium and low risk issues and the completion of the Data Protection Impact Assessment (DPIA) process, have been extended.

Delays in completion of the Programme are directly attributable to resourcing challenges within the Information Governance Unit (IGU). This presents a risk to the Council in relation to the capacity to complete the Programme; specialist (second line) oversight of completion of Service Area GDPR actions; supporting and providing oversight of resolution of relevant corporate risks with GDPR impacts (for example third party contracts and shadow IT); providing an ongoing view of the Council's progress towards full GDPR compliance; and capacity to support ongoing and increasing volumes of operational IGU activity generated as a result of the new regulations.

While Service Areas work through the improvement actions identified by the Gap Analysis, and respond to risks identified through other Programme workstreams (for example third party; contract; and shadow IT risks), there is a risk that the ICO may conclude the Council cannot demonstrate that it has fully complied with its statutory responsibilities.

Additionally, we noted that Data Privacy Impact Assessments (DPIAs) are based on information provided to the IGU by Service Areas, and there is a need for the IGU to improve the level of scrutiny and assurance over the information provided in relation to data held in system fields to ensure compliance with GDPR data minimisation principles and individual rights.

The Programme also confirmed that DPIAs have not yet been completed for all systems used across the Council, notably for historic legacy and shadow IT systems (systems that are not hosted and supported by the Council). The need to complete DPIAs for these systems has been reflected in service area GDPR action plans.

Consequently, two findings (one High and one Medium) have been raised.

Good practice

During the course of our work, IA identified the following of areas of good practice:

- The ICO has made a number of remarks in relation to data privacy and the public sector with regards to the coverage of training within organisations. The GDPR readiness programme has taken a proactive stance on the issue, hosting a significant number of privacy workshops (entitled Cake and Compliance) with records of attendance. In addition to the workshops, high quality training material (the "teach yourself GDPR" booklet) has been developed with accessible, clear messages. A GDPR-specific e-learning module was in development during the course of our review, and has now been launched. Information Governance training modules are mandatory for all new joiners and the project is proactive in monitoring employee completion with detail included in project updates to CLT. An internal survey was launched in February to assess levels of awareness around GDPR across Council services. Of the 567 responses received, 80% of respondents confirmed knowledge and awareness of GDPR.
- The Programme also completed a review of existing data and records management policies and procedures; provided guidance and templates (for example privacy notice templates) to support Service Areas with their readiness activities; and reviewed and revised existing Breach procedures and reporting.
- The Council has appointed a Data Protection Officer (DPO) at a level that reports to the CLT, which is the highest level of corporate governance within the Council. The level of this appointment would therefore seem to be appropriate given the nature of the role.
- The project identified GDPR "champions" within Service Areas. This helps to embed a privacy aware culture; enforces the 'tone from the top' as well as personal responsibility for compliance amongst employees; and provides advocacy and support to the project team. This will be essential in ensuring business as usual activities are successfully performed. During the gap analysis interviews, it was also noted that many of the employees engaging in the interviews were knowledgeable and forthcoming around the activities required to move towards GDPR compliance. This, in part, demonstrates the success of the previously mentioned awareness campaign as well as demonstrating a culture that is sensitive to the issues surrounding data protection.
- The DPIA (Data Protection Impact Assessment) form and procedure has been designed to help embed the Privacy by Design & Default principles published by the ICO. The IGU plan to utilise this procedure on all recorded high risk processes, to help highlight any gaps and allow Service Areas to take suitable remedial action. Use of DPIAs in this way is a step further than the legislation requires, with the GDPR requiring a DPIA for new processes only. As a result, this action will help highlight further risk across the Council's processing activities.

3. Detailed findings

1. Programme Progress and Information Governance Capacity

Findings

The Information Governance Unit (IGU) is currently reliant on temporary employees (one secondment, one fixed term contract), and does not have sufficient resources to support completion of the GDPR readiness programme in addition to ongoing operational activities. Volumes of operational activities have already increased and are likely to increase further as a result of the enhanced GDPR requirements.

It is acknowledged that management is aware of IGU resourcing risks, and that these have been escalated to the Corporate Leadership Team in the Data Protection Reform Paper presented on 9 May 2018.

GDPR Readiness Programme

The original plan set out by the IGU team was to have all high risk Service Area actions identified from the gap analysis by the end of March, providing sufficient time for Service Areas to address all High rated findings by May 25th. The March timeframe objective was not achieved due to the following key factors:

- Whilst the IGU highlighted their additional resourcing requirements early in the Programme planning process, there were significant recruitment delays. As a result, other work streams of the project were delayed by up to two months. This has had a subsequent impact on completion of the GDPR gap analysis;
- The timescales initially proposed for the gap analysis (influenced by the recruitment challenges) were not sufficient to conduct a scoping exercise of this magnitude;
- As a result of these factors, the recommendations following the gap analysis process have taken longer to produce than initially scoped by the IGU. Whilst there was ongoing engagement and communication with Service Areas, 2 out of 4 of the Service Areas included in our sample did not receive final reports detailing their high risk GDPR actions until April. Consequently, the time allocated for Service Area implementation of actions required to remediate against the High risks highlighted by the scoping exercise was substantially reduced;
- An impact of the delay to the gap analysis work was that the validation process, to monitor how services responded to improvement actions, could not commence in earnest until May, which was later than was initially planned.

IGU Operational Responsibilities

The IGU confirmed that they perform a number of operational activities, including processing Subject Access Requests (SARs); data protection breach investigations; assessment of DPIAs and information sharing agreements; and other general enquiries. We noted that there has been a significant increase across these areas since the start of the calendar year, with this expected to intensify following the 25th May. Going forward, the IGU workload will include supporting and monitoring Service Area implementation of high; medium; and low rated control gaps identified from the Gap Analysis interviews and other scoped activity such as Data Protection Impact Assessments (DPIAs).

Based on comparative figures for January to April 2017 and January to April 2018, we noted the following:

- Data Protection breach volumes - have more than trebled, rising from 17 to 60. This increase in breaches is particularly challenging from both the perspective of the Council's processes as well as the increased pressure of a 3-day turnaround required by the GDPR;
- Data Protection Impact Assessments and Data Protection requests for personal data from other agencies (e.g. Police Scotland and HMRC) have increased from 27 to 55 and 303 to 486 respectively; and
- Volumes of Subject Access Requests have increased from 111 to 152.

Whilst the Information Rights Team within IGU manages the SARs process to ensure that a compliant approach is consistently applied, increased volumes of SARs will also impact Service Areas who are asked to locate and provide all relevant information; and express any concerns they may have about disclosure. The time taken to complete SARs varies for all teams involved, depending on the complexity of the request.

Business Implication	Finding Rating
• While Service Areas have confirmed that improvement actions are being addressed, this cannot be confirmed until the Programme validation process is complete; • Whilst there was already an expectation that outstanding medium and low risk actions would remain, the timelines for the completion of these actions may now be significantly extended to accommodate the remediation of the higher risk activities; • Any further increases in breaches or subject access requests may mean the Council is not able to respond to them with the appropriate rigour or within the appropriate timeframes noted in the GDPR; • Other work streams that require significant work, such as the Data Protection Impact Assessment (DPIA) schedules, may not be completed in the proposed timeframes. This may lead to additional re-planning and dependent activities being further delayed putting the Council in an indefensible position with the regulator; and • Insufficient capacity to manage ongoing operational activities including the ability to respond to SARs with the required one month time frame, or an inability to investigate breaches and appropriately report these to the ICO.	**High**

Action plans	
Recommendation	**Responsible Officer**
1. IGU resourcing should be reviewed to ensure that it remains adequate to support completion of the GDPR readiness programme and support completion of ongoing operational activities, taking into account anticipated increases in volumes. 2. The GDPR readiness programme and delivery timeframes should be reviewed and rebased to assess additional risks created as a result of project delays, as well as activities to mitigate against these risks.	Laurence Rockey, Head of Strategy and Insight
Agreed Management Action	**Estimated Implementation Date**

1. a) The project resource available to the IGU has been reviewed and augmented. The secondment has ended, but the fixed-term contract has been extended to December 2019; b) Operational activities will be subject to review and a report made to CLT on longer term resource impacts for the IGU and service areas in meeting statutory requirements; and 2. The GDPR Action Plan will be revised to reflect outstanding work, taking into account revised project resource (see above). The GDPR Project will continue to be monitored and any associated risks resulting from operational pressures will be reported through the Council's Change Board.	1. a) Complete 1. b) 30 September 2018 2. 31 August 2018

2. Field Level Documentation to support evidencing compliance with data protection principles (including data minimisation)

Findings

Data protection principles (which include the new GDPR data minimisation principles) require organisations to ensure that they only collect, process, and retain personal data required for their specific purposes; that they have sufficient personal data to properly fulfil those purposes; and that data held is periodically reviewed with anything not required deleted.

A good practice approach that ensures organisations have a complete record of all personal data held is to create and maintain a record of all data entered into the fields within all systems used, that could be linked with the GDPR record of processing. This approach can help to provide assurance in relation to compliance with data protection principles and individual rights.

It is noted that the GDPR Readiness programme did not include plans to create and maintain a record of data held at field level within systems, however details of data at field level is included in Data Protection Impact Assessments (DPIAs) completed by Service Areas for all new systems and system changes.

DPIAs are completed by Service Areas and include a narrative response to questions on the data held in system fields. This is not subject to independent review or validation by Information Governance (IGU).

Additionally, there is currently a backlog of DPIAs to be completed by Service Areas and approved by the Board for both historic legacy and shadow IT systems (systems that are not supported by the Council). Consequently, existing DPIAs do not provide a comprehensive and complete record of personal data at field level held across the Council, and the Programme has been unable to confirm full compliance with data minimisation requirements.

It is acknowledged that the requirement to complete DPIAs for legacy and shadow IT systems is included in relevant Service Area GDPR action plans.

Business Implication	Finding Rating
• Personal data at field level provided by Service Areas for inclusion in DPIAs may be incomplete or inaccurate; and • Inability to confirm compliance with data protection (including GDPR Data Minimisation) principles until all outstanding DPIAs have been completed.	**Medium**

Action plans	
Recommendation	**Responsible Officer**
1. IGU should request additional information form Service Areas to support DPIA submissions (for example system screen shots) enable effective scrutiny; 2. Where there is a lack of clarity in the content of DPIAs in relation to data held at field level and the process to be applied to support data minimisation, IGU should perform a review of the system in conjunction with the Service Area and make appropriate recommendations to change the content of the DPIA; and 3. Management should consider recording details of information held at field level within systems on the Information Asset Register to provide a comprehensive view.	Laurence Rockey, Head of Strategy and Insight
Agreed Management Action	**Estimated Implementation Date**
1. DPIA guidance will be revised to encourage the provision of evidence, when appropriate, as part of the DPIA submission, including field level descriptions; 2. The IGU is currently developing a risk-based methodology to ensure DPIA actions are implemented, and that processing is compliant with data protection principles, including data minimisation; and 3. As part of the continued development of the Council's Information Asset Register, options will be considered around field level descriptions and a report presented to the Council's Senior Information Risk Owner.	1. 31 October 2018 2. 31 December 2018 3. 31 December 2018

Appendix 1 - Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***; or*** • ***Critical*** impact on the reputation or brand of the organisation which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences***; or*** • ***Significant*** impact on the reputation or brand of the organisation.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation or brand of the organisation.
Low	A finding that could have a: • ***Minor*** impact on the organisation's operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the organisation.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Appendix 2 – Terms of Reference

Resources

Terms of Reference – Internal Audit of General Data Protection Regulations readiness

To: City of Edinburgh Council Corporate Leadership Team
Laurence Rockey, Head of Strategy and Insight

From: Lesley Newdall, Chief Internal Auditor Date: 7th February 2018

This review is being undertaken as part of the 2017/18 internal audit plan approved by the Governance, Risk & Best Value Committee.

Background

After four years of political negotiations and lobbying, the EU agreed the final wording of the General Data Protection Regulation ("GDPR") in December 2015. The new regulation will introduce widespread changes to current law (which is primarily the Data Protection Act 1998 but also related legislation); will greatly increase financial sanctions for non-compliance; and will impact every entity that stores or processes the personal data of EU citizens, both within and outside of the EU.

Organisations have until the 25th May 2018 to implement all the necessary changes to systems and operations to meet the new compliance requirements.

The adoption of the GDPR will present numerous challenges. The key issues to be aware of include:

- demonstrating compliance with the new rules;
- procedures surrounding consent and consent management; and
- changes to SARs and disclosing breaches.

The City of Edinburgh Council's (The Council's) Information Governance Unit (IGU) within Strategy and Insight has developed a risk based GDPR readiness programme that will assess the extent of GDPR readiness across the Council.

The main objective of the Council's GDPR readiness programme is to identify gaps between current Service Area data protection arrangements and the new GDPR requirements, and the extent of compliance with changes to current legislation following the enactment of the draft Data Protection Bill.

The programme is also designed to assess appropriateness of all data protection responsibilities (including the new elements set out under GDPR) and compliance with current Council information governance policies.

Work has already commenced with survey work across Service Areas to identify gaps scheduled to conclude by 31st March. This will result in development of implementation plans to address the gaps identified, with actions implemented by Service Areas on an ongoing basis.

Programme outcomes will be shared with Service Areas; Risk Committees; Senior Management Teams; the Council's Corporate Leadership Team and relevant scrutiny committees to ensure that they are fully aware of any significant gaps identified and the extent of the work required to ensure ongoing GDPR compliance.

Scope

The objective of this audit is to assess the Council's approach towards GDPR readiness against good practice adopted by other organisations, and the guidance issued by the European s.29 Working Party Group and the UK Information Commissioners Office (ICO), identifying any gaps in the current approach that will need to be addressed to support the move towards GDPR compliance and address the following Corporate Leadership Team (CLT) risk:

- **Information Governance** - A loss of data from the Council's control could result in fines, claims, loss of public trust and reputational damage. This risk considers the new requirements arising from the New General Data Protection Regulation due to take effect in May 2018.

The scope of the audit will assess the adequacy and effectiveness of the Council's GDPR readiness programme to confirm whether it has been appropriately designed to identify key GDPR readiness risks and existing control gaps across the Council, and ensure that appropriate action plans are developed and implemented to support the move towards GDPR compliance.

This specialist review will be performed by PwC under the terms of the existing Internal Audit Co Source agreement.

This audit will be undertaken alongside the GDPR readiness programme, with work performed between March and May 2018, enabling PwC to jointly attend relevant meetings scheduled by the IGU team.

Limitations of Scope

Work performed by PwC will not include the following areas in scope:

- Only those processes and policies within the control of the Council are included in scope;
- No work will be performed to assess the extent of third party supplier compliance with GDPR requirements;
- We will not be conducting any third party assurance work, and we will not be performing any detailed end to end testing with respect to the effectiveness of controls in place;
- Interviews and meetings with Service Areas will be limited to those Service Areas assessed as high risk, or where we require further information to clarify maturity;
- The documentation or evidence reviews will be conducted at a desktop project plan level only, and will not involve deep-dive findings into specific service areas; and
- Our work cannot guarantee that the organisation will be fully compliant GDPR requirements as the legislation and supporting guidance has not yet been finalised.

Approach

Our review will be completed using the following approach:

1. We will undertake a detailed review of the Council's GDPR readiness programme plan, governance framework and resourcing model for delivery to identify any gaps in the plan against general good practice;
2. We will discuss with the GDPR readiness project management team how the Council has addressed the specific cultural and structural considerations in moving towards a position of GDPR compliance;

3. We will undertake a review of a subset of key documents that have been produced IGU to date; and
4. Follow-up of previously raised Internal Audit recommendations where these are aligned with our scope.

We will consider whether and how effectively the Council's GDPR readiness programme addresses each of the sub-processes and focus areas listed below:

Sub-process	Focus Area

Vision & Strategy	We will:
	• Review the organisation's GDPR readiness programme against the 12 points stated by the ICO to confirm that the following areas are assessed as a minimum:
	  ○ Data Protection Governance, assignment of necessary Roles and Responsibilities, and Target Operating Model implementation;
	  ○ Data Protection policies and procedures;
	  ○ Privacy Impact Assessment procedures;
	  ○ Information Risk Management policies and procedures
	  ○ Personal data discovery and data repository creation to support necessary data processing on a lawful basis;
	  ○ Personal data governance enhancements, and retention compliance procedures;
	  ○ Training enhancement, & ongoing corporate awareness strategy;
	  ○ Consent and privacy notification enhancements, plus data subjects rights compliance;
	  ○ Security of Personal Data (including transfer of sensitive personal data to partnerships and third parties) plus mandatory breach identification and notification procedures;
	  ○ Subject Access Request procedure enhancements; and
	  ○ Third party supplier management (due diligence and ongoing assurance) procedures, and contractual enhancements.
	  ○ Adequacy and effectiveness of system access rights where systems hold personal sensitive data.
	• Determine how the Council has assessed whether it is a data controller (or where applicable joint /common) or a data processor for all personal data processing activity, specifically taking into account the corporate binding and structure; and
	• Determine whether the GDPR readiness programme includes completion of an effective end to end data protection and GDPR controls assessment, to understand the level of implementation activity required to achieve GDPR compliance

Awareness	We will: • Conduct a high-level review the progress of any GDPR communication and awareness plans that have been developed, which are intended to inform all employees of the impact of the GDPR on their individual roles and responsibilities
Data Protection Governance, and assignment of necessary Roles and Responsibilities	We will: • Consider if a clear & defined Data Protection governance structure is in place; • Confirm whether the organisation's Data Protection programme is sponsored by executive or board level management; • Confirm that accountability for Data Protection compliance has been assigned to an appropriate individual with relevant skills and experience within Service Areas; • Confirm that responsibility for day to day, data protection operational compliance been assigned to an appropriate individual; and • Confirm whether clear reporting lines for the Data Protection Officer have been defined.

Data Protection policies and procedures	We will: • Discuss whether up to date data protection, information security, information governance, data protection impact assessments and information classification and handling policies & procedures are in place; and if existing procedures are updated • Confirm that the GDPR readiness programme will assess existence and adequacy of procedures are in place to ensure policy provisions are incorporated into Service Area processes; • Confirm that the organisation has policies and procedures for data protection by design and by default; and • Confirm that the GDPR readiness programme includes an independent assessment to identify technical and organisational controls required to achieve compliance.
Information Risk Management policies and procedures	We will: • Understand the approach to information risk management documentation and implementation, including assessing the risk to data subjects of their data being compromised; • Review the extent to which the organisation has formally assessed its risk appetite in relation to GDPR compliance; • Confirm the inclusion of data protection compliance (and GDPR readiness) in the organisation's corporate risk register; and • Confirm that departmental data protection and/or information security risk registers are maintained.
Data Discovery	We will: • Understand the extent to which the organisation has a complete understanding, and documented inventory, of the personal data processed, and associated processing purposes, in order to comply with Article 30 of the GDPR.

Internal Audit Team

Name	Role	Contact Details
Lesley Newdall	Chief Internal Auditor	lesley.newdall@edinburgh.gov.uk
Iain McMichael	Senior Auditor	iain.g.mcmichael@pwc.com
Dash Peruvamba	Auditor	adarsh.s.peruvamba@pwc.com

Key Contacts

Name	Role	Contact Details
Laurence Rockey	Review Sponsor	lawrence.rockey@edinburgh.gov.uk
Kevin Wilbraham	Key Contact	kevin.wilbraham@edinburgh.gov.uk
Henry Sullivan	Key Contact	henry.sullivan@edinburgh.gov.uk

Sarah Hughes-Jones	Key Contact	sarah.hughes-jones@edinburgh.gov.uk

Timetable

Fieldwork Start	29 January 2018
Fieldwork Completed*	02 April 2018
Draft report to Auditee*	9 April 2018
Response from Auditee*	16 April 2018
Final Report to Auditee*	23 April 2018
Final report available for presentation to the Governance, Risk and Best Value Committee*	June 2018

* Agreed timescales are subject to the following assumptions:

- All relevant documentation, including source data, reports and procedures, will be made available to us promptly on request.
- Staff and management will make reasonable time available for interviews and will respond promptly to follow-up questions or requests for documentation.
- The subset of stakeholders selected for follow-up discussions will be available to conduct these discussion week commencing 29h January 2018.
- As stated in the scoping section, the timelines for meetings will be fluid and dependent on key staff availability.