Policy and Sustainability Committee

10.00am, Tuesday, 1 October 2019

Internal Audit – GDPR (Gap Analysis) Follow-up and Quality, Governance and Regulation – referral from the Governance, Risk and Best Value Committee

Executive/routine
Wards
Council Commitments

1. For Decision/Action

1.1 The Governance, Risk and Best Value Committee has referred the attached GDPR (Gap Analysis) Follow-up and Quality, Governance and Regulation Audits to the Policy and Sustainability Committee for review and scrutiny.

Andrew Kerr

Chief Executive

Contact: Jamie Macrae, Committee Officer

E-mail: jamie.macrae@edinburgh.gov.uk | Tel: 0131 553 8242

Referral Report

Internal Audit – GDPR (Gap Analysis) Follow-up and Quality, Governance and Regulation – referral from the Governance, Risk and Best Value Committee

2. Terms of Referral

2.1 The Governance, Risk and Best Value Committee on 13 August 2019 considered a report by the Chief Internal Auditor, Internal Audit Annual Opinion for the year ended 31 March, which detailed the outcome of the audits carried out as part of the Council's 2018/19 Internal Audit annual plan and the status of open Internal Audit findings as at 31 March 2019.

2.2 The Governance, Risk and Best Value Committee agreed:

2.2.1 To note the Internal Audit opinion for the year ended 31 March 2019.

2.2.2 To request that the Chief Executive, Executive Directors and Chief Officer of the Edinburgh Health and Social Care Partnership, supported by the Chief Internal Auditor, report to the relevant Executive Committee at the earliest opportunity and the subsequent Governance, Risk and Best Value Committee setting out clear plans to ensure the closure of all historic and overdue internal audit management actions to enable an improvement to the overall Internal Audit Opinion for 2019/20.

2.2.3 To refer all audits with a red finding to the next meeting of the appropriate Executive Committee for their consideration and that action plans would be reported back to the Governance, Risk and Best Value Committee.

2.3 This report therefore refers the GDPR (Gap Analysis) Follow-up and Quality, Governance and Regulation audits to the Policy and Sustainability Committee for consideration.

3. Background Reading/ External References

3.1 Internal Audit Annual Opinion 2018/19 – report by the Chief Internal Auditor

3.2 Governance, Risk and Best Value Committee – 13 August 2019 – Webcast

4. Appendices

Appendix 1 – Internal Audit – GDPR (Gap Analysis) Follow-up

Appendix 2 – Internal Audit – Quality, Governance and Regulation

The City of Edinburgh Council

Internal Audit

Final Report

GDPR (Gap Analysis) Follow-up

8 August 2019

CW1805

Overall report rating:

Generally adequate but with enhancements required	Areas of weakness and non-compliance in the control environment and governance and risk management framework that that may put the achievement of organisational objectives at risk

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2018 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

Legislative requirements

The General Data Protection Regulation (GDPR), together with the UK Data Protection Act 2018, introduced widespread changes to data protection legislation on 25 May 2018. These included increased financial sanctions for non-compliance, and stronger direction in relation to roles and responsibilities and how personal data should be processed and stored by organisations both within and outwith the EU.

In advance of the 25th May 2018, organisations processing and storing personal data were expected by the Information Commissioner's Office (ICO) to conduct a programme of work to prepare for the new legislation. This included performing a gap analysis to identify areas of non-compliance and risk, and ensuring that appropriate implementation plans and supporting timeframes were established by 25h May 2018 to address the gaps identified.

GDPR Readiness Programme

The City of Edinburgh Council's (The Council's) Information Governance Unit (IGU) within Strategy and Communications developed and implemented a risk based GDPR readiness programme (the Programme) that assessed the extent of GDPR readiness across the Council. This programme included 20 workstreams addressing all areas of preparations for the new legislation. At a corporate level, these included establishing roles and responsibilities, new and revised guidance and procedures, establishment of new documentation such as the Record of Processing, privacy notices, and revised contract provisions, as well as an extensive communications and training programme.

One of the workstreams was a service gap analysis which identified areas of improvement to support services in achieving better compliance.

Outcomes of the 2017/18 GDPR Readiness Programme Internal Audit review

The 2017/18 audit of the of the GDPR readiness programme (performed between March and May 2018) confirmed that 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.

The review also highlighted that completion of the programme had been delayed due to IGU resourcing challenges that could also potentially impact the IGU's ability to validate effective implementation of GDPR findings raised, and their capacity to support ongoing and increasing volumes of operational IGU activities and other general enquiries generated as a result of the new regulations.

Gap analysis outcomes

Prior to commencement of the gap analysis, an initial information risk priority assessment was performed by IGU across all service areas. This was based on an assessment of the privacy impact and processing risks associated with the information being processed and retained. The outcomes were then combined, and a priority ranking of High; Medium; or Low allocated to each service area.

Following completion of the gap analysis in April 2018, a total of 94 GDPR action plans with 715 supporting recommendations were issued by the programme across Council Service areas. These included 4 service areas with an overall 'red' report rating assessment; 78 with 'amber'; and 12 with green. Of the 715 supporting recommendations 118 were assessed as 'high' priority; 473 'medium'; and 124 as low, with the following definitions applied:

- High - address as quickly as possible and before 25th May 2018 if at all possible
- Medium - address when possible, if not prior to 25th May 2018 then as quickly as possible thereafter.
- Low - address within usual business practices.

A number of holistic Council wide GDPR related risks were also identified by the programme (for example third party; contracts; and shadow (non-centrally hosted) IT) and communicated to the Council's Corporate Leadership Team (CLT) and Directorate risk committees. The IGU also proposed that a Council working group should be established to ensure that these risks are effectively managed though Directorate risk committees, with local plans developed and implemented to ensure that they are addressed.

IGU GDPR readiness follow-up

Given their limited resources; increasing workload; and the volume of GDPR action plans and recommendations, the IGU adopted a self-attestation process to confirm with service areas that their GDPR actions had been addressed, and progress has been reported to individual Directors. In some instances, evidence of implementation was provided to IGU, however, for the reasons outlined above, no assurance testing was performed to confirm that the actions had been effectively implemented and sustained.

Information governance maturity model

IGU has also developed a GDPR maturity model (an assessment tool) that has been designed to enable services to assess the maturity of their established information governance processes in comparison to GDPR regulations and information governance more widely, to identify any potential risks and areas of non-compliance. The maturity assessment was issued across the Council in March 2019.

The model is based on the Generally Accepted Record Keeping Principles (GARP) developed by the Association of Records Managers and Administrators (ARMA). The eight GARP principles 8 include accountability; transparency; integrity; protection; compliance; availability; retention; and disposal.

Within the model, each principle has a set of questions with 5 answers attributed to each question. The responses are then matched to a graded maturity assessment that determines the maturity of information governance across the Council.

Information Board

A new Information Board has been established (the inaugural meeting was March 2019) with the objective of providing dedicated oversight of GDPR implementation; providing assurance to the Council's Corporate Leadership Team that appropriate frameworks have been established to support Directorates and service areas in effective management of information governance risk; and driving and supporting information management across the Council.

IGU management has advised that they now plan to close the Programme based on the self - attestation responses received from service areas, with ongoing assurance provided through a combination of reliance on the Council's established risk management framework to record and manage any remaining GDPR gap analysis actions that have not yet been addressed, and ongoing business as usual activity of the IGU which includes training and awareness, data protection impact assessments, records management assessments, the information maturity model, handling of information requests and breach management. All of which support the identification of information risks across the Council and reinforces the IGU's role as a second line of defence.

Scope

As the GDPR readiness programme was reviewed in 2017/18, the scope of our current review was limited to an assessment of the design adequacy of the IGU validation process to confirm that services had either closed their actions, or were making adequate progress towards completion

The review was also designed to provide assurance in relation to the following Corporate Leadership Team (CLT) risk:

Information Governance - A major loss of data from the Council's control could result in fines, claims, loss of public trust and reputational damage. This includes both physical records (papers, files, folders etc) and data lost as a result of cyberattacks. This risk takes into account new requirements under the new General Data Protection Regulation.

Approach

Sample testing of completed GDPR actions and recommendations

A total of nine GDPR reports and their 98 supporting recommendations (25 High; 66 Medium; and 7 low) were selected by Internal Audit for testing. This represents 10% of the 94 GDPR action plans issued by the IGU across the Council. All red rated reports were included in the sample, and five (6%) of the amber reports.

We reviewed service area action plans to confirm that they were aligned with GDPR recommendations; interviewed service area representatives; and requested evidence to determine whether actions had been effectively implemented and sustained.

Our sample covered the following Directorates and service areas:

Directorate	Service	IGU Initial Risk Ranking	GDPR Report Priority Rating
Communities and Families	Early Years and Childcare	**Medium**	**Red**
	Residential Care	**High**	**Red**
	Community Safety	**Medium**	**Amber**
Place	Parks, Greenspaces, and Cemeteries	**Low**	**Red**
Resources	Facilities Management	**Medium**	**Red**
	Human Resources	**Medium**	**Amber**
	Legal Services	**Medium**	**Amber**
	Transactions: Assessment & Finance	**Medium**	**Amber**
	Lothian Pension Fund	**Medium**	**Amber**

Review of risk registers

We also reviewed risk registers for each of the services and Directorates noted above to establish whether any GDPR actions that had not been completed were recorded on the risk registers; and that the holistic risks identified by IGU had also been recorded (where relevant).

Discussions were also held with the Chief Risk Officer to understand how Programme outcomes had been reflected in, and were being managed through, the Council's established risk management framework.

We also reviewed the IGU Maturity Model to assess whether it is adequately designed to support ongoing identification and management of information governance risks.

Further details on the scope of our review are included at Appendix 2 – Areas of Audit Focus

A summary of the testing outcomes for each service area reviewed are included at Appendix 3.

2. Executive summary

Total number of findings: 3

Summary of findings raised	
High	1. Implementation of GDPR gap analysis actions
Medium	2. Ongoing management of information governance risks
Low	3. Information Governance maturity model – design and implementation

Further detail on the basis of the classifications applied to our findings is included at Appendix 1.

Opinion

Our review established that there is currently insufficient evidence available to confirm effective implementation and sustainment by service areas of General Data Protection Regulations (GDPR) gap analysis actions raised by the GDPR readiness Programme (the Programme) to address gaps identified between current Council information governance processes and the new GDPR regulations

Additionally, the Council's risk management framework cannot be relied upon to confirm that the information risks associated with all remaining GDPR gaps (including holistic Council wide risks) have been recorded and are being effectively managed. It is therefore likely that the gaps identified that need to be addressed across the Council to progress towards GDPR compliance and meet the expectations of the Information Commissioner's Office have not been addressed, and could potentially result in loss of data and significant breach of applicable regulations.

Whilst the Council could have explored alternative options to confirm that GDPR actions had been effectively implemented and would be sustained across Service Areas, reliance was placed on the Information Governance Unit (IGU) to complete this exercise. Given the limited resources and capacity of the IGU (as highlighted in the High rated finding raised in the GDPR Readiness Programme report issued in August 2017) IGU adopted a self attestation approach that was not designed to obtain and review evidence from services confirming effective implementation.

IGU intend to close the GDPR Programme and obtain ongoing assurance on information governance risk management by first line service areas via the risk management framework and newly launched information governance maturity model, with oversight provided by the recently established Information Board. The proposed information governance assurance framework is well designed and could potentially be a leading approach across the public sector. As with the gap analysis, it is, however, dependent on service areas providing factual responses to the maturity model assessment, and identifying; managing; and addressing their information governance risks effectively.

It is Internal Audit's opinion that the Programme should not be closed until further assurance has been obtained to confirm that all significant GDPR actions have been implemented and will be sustained by services; remaining and holistic information governance risks effectively managed through the risk management framework; the maturity model effectively embedded and used as a tool to assess information maturity and identify any significant risk and control gaps; and the Information Board's authority and oversight responsibilities clearly established.

Consequently, three findings, one High; one Medium; and one Low have been raised.

Our detailed findings and recommendations are laid out at Section 3 below.

3. Detailed findings

1. Implementation of GDPR gap analysis actions — High

Implementation of GDPR actions

Our review of a sample of nine GDPR reports and their 98 supporting recommendations confirmed that:

1. Services have not attested to IGU that all recommendations have been addressed. Of the 98 recommendations included in our sample (25 High; 66 Medium; and 7 low), only 38% (38) have been self attested as closed; and
2. Supporting evidence of implementation was available for only 50% of the 38 actions where services had confirmed closure;

The recommendations where no evidence could be provided to support implementation covered the following GDPR themes highlighted by the IGU in their reports:

- *Storage limitation* – teams should be consistently applying Council record retention policies and schedules to both hard copy and electronic records. A disposal record should be created and maintained for records that have been destroyed in line with the Council Records Management Policy requirements;
- *Security, Integrity, and Confidentiality* – employees should be aware of and consistently applying Clear Desk and Acceptable Use Policies designed to support effective information governance and GDPR compliance;
- *Collection and Purpose limitation* - ensuring that online privacy notices are updated with links included on hard copy forms. Additionally, where privacy notices have been published online, they are not consistently linked to the customer's online journey. This was a consistent theme across all services with the notable exception of Human Resources.
- *Lawfulness, fairness, and transparency* – information sharing with third parties.

Further details on our sample testing outcomes and associated themes are included at Appendix 2.

Discussions with service area representatives highlighted a number of reasons for implementation delays and their inability to provide evidence to support closure. Whilst Internal Audit has not performed testing to validate these reasons, they have been included at Appendix 4 for information.

Risks

The potential risks associated with our findings are:

- The Council is unable to demonstrate that all High and Medium rated service priority actions identified by the Information Governance Unit (IGU) GDPR readiness programme have been effectively implemented and will be sustained as per the Information Commissioner's Office (ICO) expectations, and is unable to close the GDPR readiness programme;
- Potential risk of non-compliance with applicable legislation and internal information governance policies; resulting in potentially breaches; loss of data and potential penalties.

1.1 Recommendation – Implementation of GDPR gap analysis actions

An appropriate risk based approach to confirm satisfactory implementation of all actions identified by the gap analysis should be designed and implemented.

The approach should consider the limited resources within the Information Governance Unit (IGU), and should include, but not be restricted to obtaining independent assurance and supporting evidence from services and Directorates that the all high and medium rated actions included in GDPR action plans have been effectively implemented and sustained.

1.1 Agreed Management Action - Implementation of GDPR gap analysis actions

The Information Governance Unit will adopt an evidence-based methodology and meet with service area representatives to assess and update (when appropriate) that current recommendations have been met and progressed. Progress and on-going risks will be monitored by the Information Board.

Owner

Laurence Rockey, Head of Strategy and Communications

Contributors

Kevin Wilbraham, Information Governance Manager

Sarah Hughes-Jones, Information Compliance Manager

Donna Rodger, Executive Assistant

Agreed Implementation Date

31 December 2019

2. Ongoing management of information risks — Medium

Our review of the risk management framework established to support ongoing management of information risk across the Council confirmed that:

1. The Corporate Leadership Team (CLT) risk register refers to controls such as the information Security and Information Governance policies; laptop and media encryption; Internal Audit testing of phishing; GDPR implementation tracked by IGU; and cyber essentials accreditation.

   These do not reflect the necessary controls required to effectively manage information risk across the Council by either preventing data breaches and losses or detecting them once they have occurred;
2. There is no clear link between the IGU GDPR gap analysis reports and the risks included in Directorate and service area risks registers;
3. Where risks are recorded and scored on the Pentana system, there is insufficient detail supporting the risk and describing the relevant controls;
4. Not all teams that own GDPR actions have established risk registers. It is acknowledged that Risk Management team is working proactively with service areas to establish risk registers where gaps have been identified;
5. The inaugural meeting of the Information Board was March 2019. At the time of our review, the Board terms of reference was in draft. Review of the draft terms of reference highlighted the opportunity to improve the scope of the Board in relation to the following areas:
   - Inclusion of Risk Management;
   - Inclusion of arm's organisations such as the Lothian Pension Fund; and
   - Ensuring that the service areas roles and responsibilities for managing and providing assurance on their management of information governance risk is clearly articulated.

Risk

The potential risks associated with our findings are:

Information governance risks are not being effectively managed through the established risk management process, and holistically across the Council within agreed and accepted risk tolerance parameters.

2.1 Recommendation – roles, responsibilities, and membership of the Information Board

1. Risk management should be invited to attend the new Information Board;
2. The Information Board should review and agree the appropriate wording and rating of all Council wide information risks, and supporting controls to be included in the Corporate CLT risk register in conjunction with risk management, and present this for consideration at the CLT risk committee;
3. The roles, responsibilities, and expectations of first line services; the second line Information Governance Unit (IGU) and the Information Board in relation to managing information governance and risks across the organisation should be clearly articulated in the Information Board's terms of reference.

   This should include (be not be restricted to) responsibility for providing ongoing assurance to the Board that services are compliant with applicable both applicable legislation and internal Council policies;
4. The Board should consider whether arm's length organisations should be included within membership (for example, the Lothian Pension Fund and the Lothian Valuation Joint Board);
5. The Board terms of reference should include responsibility for ongoing monitoring of service progress with implementation of GDPR gap analysis actions, enabling the Board to make a risk based recommendation to the CLT as to when the GDPR gap analysis validation process should be closed; and ongoing monitoring of the information governance maturity assessment model completion rates and outcomes to identify services who have not completed the questionnaire ensure that that failure to complete and any significant risk areas are communicated to services, with any significant themes or trends reported to the CLT.

2.1 Agreed Management Action – roles, responsibilities, and membership of the Information Board

1. Risk and assurance representation are already included within the Information Board's Terms of Reference.
2. The Information Board will review identified Council-wide information risks (and controls) from existing sources for presentation to the Corporate Leadership Team (CLT);
3. The Information Board's Terms of Reference will be reviewed to provide clarity around respective responsibilities and roles in relation to risk management, assurance and reporting.
4. Existing governance arrangements between the Council and its arm's length companies will be used to provide assurance that information legislation is compiled with.
5. The Information Board's Terms of Reference already provides for work stream monitoring and assurance. Specific projects and progress will be referenced through board documentation and papers.

Owner

Laurence Rockey, Head of Strategy and Communications

Contributors

Kevin Wilbraham, Information Governance Manager

Sarah Hughes-Jones, Information Compliance Manager

Donna Rodger, Executive Assistant

Agreed Implementation Date

30 June 2020

2.2 Recommendation – communication of requirements to implement outstanding GDPR actions and ongoing management of information risk

1. The Information Governance Unit (IGU) should issue a communication to all Directorates and service areas highlighting the need to:
   - Ensure that all GDPR agreed actions are progressed and implemented;
   - Retain appropriate evidence to confirm implementation of agreed actions (providing examples of evidence requirements), and ensure that the actions (once implemented) are sustained;
   - Record any unimplemented actions and any relevant holistic GDPR risks on their risk registers, and ensure that supporting implementation action plans have been developed with responsibility allocated to appropriate owners within their service;
   - Proactively advise the IGU when actions have been implemented; and
2. Information Governance should continue to maintain a tracker of all completed GDPR actions (as advised by services) and present this to the Information Board for their review and consideration of which actions should be included in the independent risk based assurance process recommended in Finding 1 in this report.

a. Agreed Management Action - communication of requirements to implement outstanding GDPR actions and ongoing management of information risk

Further communications will be incorporated into the current Information Governance annual communications plan to take account of the above recommendations.

The Information Governance Unit will continue to track completed GDPR actions and report to the Information Board.

Owner

Laurence Rockey, Head of Strategy and Communications

Contributors

Kevin Wilbraham, Information Governance Manager

Sarah Hughes-Jones, Information Compliance Manager

Donna Rodger, Executive Assistant

Agreed Implementation Date

30 December 2019

2.3 Recommendation – ongoing information risk management

To ensure effective ongoing management of information risks across the Council, Risk Management should obtain copies of the General Data Protection Regulation (GDPR) gap analysis action plans issued by the Information Governance Unit (IGU) and:

1. Review them in comparison to Directorate and service area risk registers to identify any risks that have not been included, and ensure that these are raised and discussed at risk committees; and
2. Identify any services with information governance risks and GDPR readiness gaps that do not currently have an established risk register, and ensure that their development is either prioritised, or the risks reflected in the risk register at the next level.

2.3 Agreed management action - ongoing information governance risk management

Through the quarterly risk committees and risk management group cycles, the Corporate Risk Management Team will ensure that Service Areas are advised, with specific reference to their GDPR gap analysis action plans, to identify and consider inclusion and escalation as appropriate, of any information risks that are not yet included in their risk registers.

Owner

Stephen Moir, Executive Director of Resources

Contributors

Nick Smith, Head of Legal and Risk; Rebecca Tatar, Principal Risk Manager; Michelle Vanhegan, Business Support Executive; Layla Smith, Business Manager

Agreed Implementation Date

31 December 2019

3. Information Governance maturity model – design and implementation

Low

Whilst the Generally Accepted Record Keeping Principles (GARP) that form the basis of the maturity model questionnaire have been adapted for relevance to the Council, our review of the launch and content of the model established that:

1. Limited guidance was provided to support the users expected to complete the questionnaire. Prior to launch, senior management teams were briefed and advised that the questionnaire would be sent to information asset owners (generally tier 4 managers) on a phased basis from December 2018;
2. The questions are technical and may not be easily understood by all asset information owners across the Council. Whilst some guidance was provided with the distribution e mail, individuals would need to have a strong knowledge and understanding of information governance principles to support completion; and
3. The questionnaire does not include a 'non applicable' response to questions and forces selection from a range of pre determined responses. A good example is the question on whether services have created and published privacy notices, which may not be relevant for teams who do not deal directly with customers (for example second and third line assurance teams) and instead place reliance on the overarching Council privacy notice in relation to the data that the process and retain.

Risk

The potential risks associated with our findings are:

Responses received may not accurately represent the effectiveness of information governance maturity across the Council.

3.1 Recommendation - Information Governance maturity model – design and implementation

The information Governance Unit (IGU) should

1. Produce guidance to support completion of the model, explaining why the model has been developed and launched; frequency of completion; and how the responses will be analysed and used / reported to governance forums.
2. Review and simplify the questions included in the assessment (where possible) and consider inclusions of examples for the answer options and 'non applicable' responses. Where non applicable responses are included, the survey should force respondents to provide supporting rationale; and
3. Include a question to determine whether services are including information risks on their risk registers and managing them effectively.

3.2 Agreed management action - Information Governance maturity model – design and implementation

1. The Information Governance Unit will revise the model guidance and provide further details to support services in completing the survey.
2. The Information Governance Unit will review the assessment form and give consideration to the use of ‘non-applicable’ responses.
3. Questions on risk and risk management will be included in the next version of the maturity model.

Owner

Laurence Rockey, Head of Strategy and Communications

Contributors

Kevin Wilbraham, Information Governance Manager
Henry Sullivan, Information Asset Manager
Donna Rodger, Executive Assistant

Agreed Implementation Date

31 December 2019

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 – Areas of Audit Focus

The audit areas and related control objectives that were tested in detail were:

Audit Area	Control Objectives
IGU Validation Process and Maturity Model	Review the IGU validation process and maturity model and confirm that: • a clear methodology has been developed to support the validation and maturity assessment process, and is consistently applied; • arms length external organisations associated with the Council (for example, Lothian Pension Fund) are included in scope of the validation and maturity assessment process; • where validation or maturity assessment outcomes identify areas where further action is required, these are communicated to service areas; and • GDPR action plan implementation progress (including areas where lack of progress is evident) is monitored and regularly reported to the CLT and relevant executive committees.
Management of GDPR risks	• Confirm whether a Council working group was established to address key generic GDPR corporate risks; • Obtain a copy of the terms of reference for the working group and confirm that the roles and responsibilities of the committee have been clearly defined; • Confirm that ownership of these risks has been appropriately allocated; • Confirm that the full population of risks has been discussed at Directorate risk committees and reflected in Directorate and Corporate Leadership Team risk registers, where applicable; • For a sample of risks, establish progress with defining and implementing key controls, and confirm that (where implemented) effectiveness of the controls has been assessed and recorded in risk registers; and • Review the CLT risk register and confirm whether appropriate controls have been established to manage information governance / GDP risks, and their effectiveness appropriately assessed.

Appendix 3 – Testing Outcomes

The following table summarises our testing outcomes across the 9 service areas included in our sample.

				Recommendations					
Sample	Area	IGU Initial Risk Ranking*	IGU GDPR Readiness Report Priority Rating	Total in report	High address pre 28/5/18	Medium address as soon as possible post 28/5/18	Low address as part of business as usual processes	Recs completed per self-attestation to IGU	Recs completed with supporting evidence
1	Residential Care	**High**	**Red**	10	8	2	0	6	1
2	Early Years and Childcare	**Medium**	**Red**	15	7	8	0	8	0
3	Parks, Greenspaces and Cemeteries	**Low**	**Red**	19	5	14	0	0	0
4	Facilities Management	**Medium**	**Red**	15	4	9	2	8	3
5	HR	**Medium**	**Amber**	9	1	6	2	3	2
6	Legal Services	**Medium**	**Amber**	4	0	3	1	1	2
7	Community Safety	**Medium**	**Amber**	8	0	8	0	6	0
8	Transactions: Assessment & Finance	**Medium**	**Amber**	11	0	10	1	6	10
9	Lothian Pension Fund	**Medium**	**Amber**	7	0	6	1	During our audit this was currently being assessed by IGU as a wider review.	1
Totals				**98**	**25**	**66**	**7**	**38**	**19**

Appendix 3 – Testing Outcomes (cont.)

The following table summarises the themes (based on IGU classifications used in original GDPR reports) associated with recommendations where evidence was not provided to support actions that had been closed.

Sample	Area	IGU Initial Risk Ranking	IGU Report Rating	Themes associated with medium and high recommendations of recs where no evidence of closure could be provided
1	Residential Care	**High**	**Red**	Record retention and disposal **(Storage Limitation**) Clear desk policy, DP training on breaches **(Security, Integrity, and Confidentiality)** Record of updating personal data, privacy notices **(Collection and Purpose limitation)**
2	Early Years and Childcare	**Medium**	**Red**	Information sharing. (**Lawfulness, fairness and transparency)** Privacy notices **(Collection and Purpose limitation)** Record retention and disposal **(Storage Limitation**)
3	Parks, Greenspaces, and Cemeteries	**Low**	**Red**	Security of laptops used, risk assessments of premises, staff training **(Security, Integrity, and Confidentiality.** Privacy notices (**Collection and Purpose limitation)** A process for ensuring that access control data **(Accuracy)** Record retention **(Storage limitation)** Transferring data **(Security, Integrity, and Confidentiality)**
4	Facilities Management	**Medium**	**Red**	**Collection and Purpose limitation.** (**Data Minimisation)** A process for ensuring that access control data **(Accuracy)** Suitable controls for the transmission of personal data electronically, removable media **(Security, Integrity, and Confidentiality)**
5	HR	**Medium**	**Amber**	Record retention **(Storage limitation)** Alternative use to personal data used in training **(Data Minimisation)**
6	Legal Services	**Medium**	**Amber**	Process used by team members for retention of data (**(Storage Limitation**)
7	Community Safety	**Medium**	**Amber**	Privacy notices; CCTV signage **(Collection and Purpose limitation)** A regular review of the siting and range of CCTV cameras **(Data Minimisation)** A process for ensuring that access control data **(Accuracy**

Sample	Area	IGU Initial Risk Ranking	IGU Report Rating	Themes associated with medium and high recommendations of recs where no evidence of closure could be provided
8	Transactions: Assessment & Finance	**Medium**	**Amber**	Privacy notices **(Collection and Purpose limitation)**
9	Lothian Pension Fund	**Medium**	**Amber**	Privacy notices **(Collection and Purpose limitation)** A process for ensuring that access control data **(Accuracy)** Disposal record **(Storage limitation)** Security of papers in transit **(Security, Integrity, and Confidentiality)**

Appendix 4 - Reasons provided by Service Areas for implementation delays and lack of evidence to support closure of GDPR actions

Discussions with service area representatives highlighted the following reasons for implementation delays and inability to provide evidence to support closure:

1. IGU did not provide guidance on the evidence required to support completion of actions. A number of services confirmed that this was discussed verbally by IGU when GDPR reports were issued;
2. Where services did provide evidence to IGU, there was limited response to confirm that the evidence provided was adequate. It is understood that this was attributable to the limited resources available within IGU;
3. Lack of clarity regarding team member completion rates of CECil online GDPR and information governance learning modules, as completion is not proactively tracked. Whilst completion reports are available from the system, these are not consistently used.

   Additionally, there is also no single source of employee data that accurately replicates the current Council organisational structure making completion difficult to track within Service Areas (this was also identified in the Phishing Resilience Internal Audit report finalised in July 2018. Management are currently implementing agreed actions to ensure that this is resolved).

Changes in team members responsible for implementation of GDPR actions with insufficient handover performed. Examples provided included changes in Business Support, or new Managers starting after GDPR action plans had been agreed.

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

The City of Edinburgh Council
Internal Audit

Quality, Governance, and Regulation

Final Report

5 July 2019

CW1802

Generally adequate but with enhancements required	Areas of weakness and non-compliance in the control environment and governance and risk management framework that that may put the achievement of organisational objectives at risk

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2018. 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

Provision of social work services by local authorities is regulated by the Care Inspectorate who performs annual inspections to confirm ongoing compliance with applicable regulations and assess the quality of the services provided.

The City of Edinburgh Council (the Council) and the Edinburgh Health and Social Care Partnership (the Partnership) provides a total of 173 regulated social work services to adults, children and young people across the following areas:

- Communities and Families - children's social work (e.g. care homes and young people’s centres);
- Safer and Stronger Communities - community justice social work, homelessness services and family and household support); and
- The Partnership - adult social work (e.g. care homes and care at home).

Local authorities are required to appoint a Chief Social Work Officer (CSWO) in line with section 3 of the Social Work (Scotland) Act 1968 requirements, and further supported by section 45 of the Local Government etc (Scotland) Act 1994. The CSWO is responsible for provision of appropriate strategic and professional leadership and advice; supporting overall performance improvement; and management of corporate risk in relation to statutory social work services delivered by both the Council and the Partnership.

This is achieved by providing the Chief Executive of the Council; the Council’s Corporate Leadership Team (CLT); the Edinburgh Integration Joint Board (EIJB) that is responsible for direction and scrutiny of the Partnership; and elected members with updates on risks and issues that could impact upon the safety of vulnerable people and / or social work services and sharing the outcomes of relevant service quality and performance reports.

The CSWO is also required to publish an annual report for both the Council and the EIJB on the functions of the CSWO role, and an evaluation of the quality of delivery of the Council and HSCP’s social work services. In Edinburgh, the Quality, Governance and Regulation (QGR) team is responsible for supporting the CSWO in performing their statutory role by providing ongoing review, support, and challenge in relation to delivery of adult and children social work services. QGR cover the following services: quality and compliance, regulation; public protection; family & household support; and the Syrian Refugee and Migration Programme.

QGR is also responsible for monitoring implementation of Care Inspectorate Improvement plans (issued following completion of annual inspections) to ensure that the weaknesses they have identified are addressed

Included within QGR, is the Quality Assurance and Compliance team (QAC). The remit of the QAC is to support services - highlighting strengths; areas for improvement; identifying and analysing trends and themes; and developing action plans (where required) to ensure that barriers preventing delivery of effective social work services in line with applicable regulatory requirements are removed.

QGR works closely with both Council and Partnership teams; in collaboration with external partner agencies; and also works with external regulatory bodies such as the Scottish Social Services Council; the Care Inspectorate; and the Healthcare Improvement Service.

The Three Lines of Defence model can be applied to delivery of social work services across the Council and Partnership, where the ‘first line’ is the teams responsible for delivery of social work services; the ‘second line’ the CSWO supported by QGR and QAC who provide assurance on delivery and quality of social work services, and report to senior management and relevant Committees and Board through delivery of the CSWO annual report. The ‘third line’ provides independent assurance (for example, Internal Audit or the Care Inspectorate) on key controls established to manage social work risks.

An Audit Scotland coordinated governance forum, the Local Area Network (LAN) that includes the Care Inspectorate; Education Scotland; the Housing Regulator; Audit Scotland; and external audit (Scott Moncrieff); meets quarterly to discuss their scrutiny activities across the Council and Partnership, and areas of concern, in line with the Audit Scotland Code of Audit Practice 2016.

These quarterly discussions include focus on the quality of delivery of social work services.

Scope

This review assessed the design and operating effectiveness of the QAC assurance framework to confirm that it enables the CSWO to effectively discharge their statutory responsibilities across the Council and Partnership, and adequately supports the CSWO annual reports provided to the Council and the EIJB.

Sample testing was performed for the period 1 October 2017 to 31 October 2018. Our audit work concluded on 28 February 2019 and our findings and opinion are based on the outcomes of our testing at that date.

Limitations of Scope

There were no limitations of scope.

2. Executive summary

Total number of findings: 3

Summary of findings raised	
High	1. Quality Assurance and Compliance Assurance Framework
Medium	2. Quality Assurance and Compliance Methodology and Operational Processes
Low	3. Data Protection Impact Assessment

Opinion

Generally adequate but with enhancements required

The Council's Quality Assurance and Compliance (QAC) team is a highly skilled and experienced team that provides invaluable second line assurance in relation to the Council and Partnership's key social work risks; supports the CSWO's evaluation of the quality of delivery of social work services in their annual report; and also, the effective delivery of CSWO statutory obligations.

Our review confirmed that the design and operating effectiveness of the QAC is generally adequate with enhancements required, as we identified some areas of weakness in the QAC assurance framework that could have a potentially significant impact upon the quality of assurance delivered, and the content of the CSWO's annual report.

Consequently, one High; one Medium; and one Low rated findings have been raised.

Our High rated finding reflects the need for QAC to establish a Terms of Engagement that clearly defines how they will engage with both the Council and the Partnership, and the levels of access required to employees, systems, records and files to support delivery of their assurance reviews.

This finding also highlights that there are currently no established protocols to ensure that QAC assurance review outcomes are reported to, and subject to scrutiny by, appropriate Council; Partnership; and EIJB governance forums; and the importance of ensuring that QAC are engaged to review and where involved provide feedback on the quality of service improvement plans designed by service areas and submitted to external assurance providers prior to their submission.

Whilst QAC applies an established methodology to support delivery of their reviews that is subject to ongoing review to improve the quality of their review process, our Medium rated finding reflects a number of areas where the methodology should be further enhanced.

These include the need to develop and implement a risk based annual plan to confirm appropriate coverage of all high risk social work services; apply ratings to findings raised to reflect the risks associated with the weaknesses identified in the quality of social work practices; document the escalation process applied to significant findings identified prior to completion of reviews or where immediate concerns relating to practice or conduct are highlighted; and implement a risk based follow up process to ensure that agreed management actions have been effectively implemented and sustained.

The Medium rated finding also reflects the need for QAC to develop and maintain a risk register that captures the potential risks that could impact upon their assurance delivery, and the key controls established to ensure that these risks are effectively managed.

Our Low rated finding highlights that there is currently no Data Protection Impact Assessment covering the processes applied by QAC in relation to the personal data they obtain; review; process; and retain to support completion of their assurance reviews, to ensure that they are compliant with applicable data protection legislation and principles.

3. Detailed findings

1. Quality Assurance and Compliance Assurance Framework	High

Quality Assurance and Compliance (QAC)Terms of Engagement

QAC Service level agreements (SLAs) have been recently drafted and are supported by revised template scoping and procedural documents covering the key types of assurance review undertaken. Our review noted, that while the SLAs provide an overview of the team's assurance responsibilities & engagement approach, they are not supported by an overarching Terms of Engagement to support their ongoing engagement with, and rights of access to, employees and records of the Council; the Health and Social Care Partnership (the Partnership); and the Edinburgh Integration Joint Board (EIJB), enabling them to deliver their ongoing assurance, and discharge their responsibility to provide professional advice in relation to any planned significant social work service changes.

Management has confirmed that their direct reporting line to the CSWO and existing (informal) escalation processes would be applied if required in the event of any access issues that could potentially impact upon assurance delivery.

Review and scrutiny of QAC assurance outcomes

There are currently no established protocols to ensure that QAC planned assurance activities and outcomes (with the exception of public protection) are reviewed and scrutinised by appropriate governance forums on an ongoing basis, to confirm that appropriate coverage of all significant social work risks is planned, and enable early identification and resolution of significant issues and / or recurring themes in advance of receiving the Chief Social Work Officer's (CSWO's) annual report.

Review of the 2016/17 CSWO annual report found only limited reference to specific QAC reviews and links to EIJB; Children's Services; and Community Justice annual performance reports. In addition, the 2017/18 CSWO annual report did not include any detail on QAC assurance reviews. Management advised that this was the result of an oversight.

Ongoing CSWO engagement with senior management and external assurance providers

Whilst the CSWO has regular meetings with the Chief Executive of the Council; reports directly to the Executive Director of Communities and Families (CF); and attends quarterly CF Risk and Assurance Committee meetings, ongoing engagement with Partnership senior management Team is currently limited to invitation from the Chief Officer to attend Partnership senior management meetings.

We also confirmed that the CSWO does not attend and is not represented at Local Area Network (LAN) meetings.

Review of quality improvement plans to address external assurance actions

There is currently no requirement for QAC to perform an independent second line review of the quality of improvement plans designed by service areas and submitted to external assurance providers (for example the Care Inspectorate). Our review noted that improvement actions submitted by Service Managers generally included short term solutions rather than the longer term strategic improvements required to address the root causes of the concerns raised.

The Regulation Service is currently piloting a programme of continuous improvement with three Care Homes to track progress with implementation of Care Inspectorate improvement plans, using Pentana, the Council's performance and risk management system. The processes being set up, aim to encourage managers to consider the root causes of quality issues identified, and each action will have to be validated before being signed off as completed in Pentana. Responsibility for validation is still to be determined.

Risks

- Insufficient second line assurance coverage of all Council and Partnership significant social work risks.
- Inability to provide assurance to the Council; the Partnership and the EIJB on significant social work risks.
- Significant issues and holistic themes are not identified and addressed in a timely manner.
- The Chief Social Work Officer annual report could potentially be incomplete and / or inaccurate.
- The Chief Social Work Officer is unable to fulfil their statutory obligations in relation to providing professional advice on planned significant social work service changes.

1.1 Recommendation - Terms of Engagement

A Terms of Engagement, should be developed and agreed with Council and Health and Social Care Partnership (Partnership) senior management and where appropriate, relevant Council Executive and Edinburgh Integration Joint Board (EIJB) committees to support ongoing delivery of second line social work services assurance activities, and discharge of Chief Social Work Officer (CSWO) responsibilities to provide professional advice. The Terms of Engagement should include, but should not be limited to:

1. CSWO statutory obligations;
2. Roles and responsibilities of the second line Quality Governance and Regulation teams and how the team supports the CSWO in discharging their statutory obligations and the CSWO annual report;
3. The requirement for Quality Assurance and Compliance (QAC) to prepare and deliver an annual, risk-based assurance plan that provides coverage of all significant Council and Partnership social work risks on an ongoing basis;
4. Right of access to all relevant Council; Partnership; and EIJB employees and records (including ongoing engagement with senior management and external assurance providers), and a supporting escalation process where potential blockages arise;
5. Details of relevant governance forums responsible for approving the proposed QAC annual plan and reviewing and scrutinising assurance review outcomes, as agreed in consultation with key stakeholders;
6. Involvement in any planned significant changes to delivery or registration requirements of social work services across the Council and Partnership to provide professional advice; and
7. Responsibility for review of service improvement plans prior to submission to external assurance providers.

Agreed Management Action

The service has prepared a Service Charter, which sets out the role and wider function of the service devolved under the Chief Social Work Officer. This will act as a vehicle to deliver audit activity and a framework which will be supported by a Service Level Agreement to ensure the focus, scope and frequency of audit activity is agreed with key stakeholders and customers on a rolling annual basis.

These documents are now available for internal audit to review, with a launch planned for August 2019.

Owner: Alistair Gaw, Executive Director Communities and Families **Contributors:** Jackie Irvine, Chief Social Work Officer, Jon Ferrer Senior Manager Quality, Governance and Regulation, Keith Dyer Manager, Quality and Compliance	**Implementation Date:** Service Charter – 31 August 2019 Directorate level SLAs – 31 October 2019

1.2 Recommendation - Review of service improvement plans

Quality Assurance & Compliance (QAC) should develop a process to support review and challenge of service improvement plans to address external social work services assurance finding raised across the Council and the Health and Social Care Partnership (the Partnership) prior to their submission.

The process should include, but not be limited to:

1. Confirming that the root causes of external assurance recommendations have been identified by service areas;
2. Confirming that improvement plans will address the root causes identified and satisfy the relevant external assurance provider
3. Confirming that ownership is appropriate and that implementation dates are realistic and achievable; and
4. Detailing the expected evidence to be retained and any follow up work to be performed by QAC to confirm satisfactory implementation advance of the next planned visit from the external assurance provider.

This could be achieved through formalising the approach used for the Care Homes pilot project currently underway.

The process should be agreed with relevant service areas; the Corporate Leadership Team (CLT) and Council Executive and Edinburgh Integration Joint Board (EIJB) Committees prior to implementation.

Agreed Management Action

The Quality Assurance and Compliance (QAC) Service would not have sufficient capacity or coverage to actively support, review and challenge all improvement plans generated from external assurance activity due to the overall size of the service compared with the volume and scale associated with many of the plans and improvement actions generated from activity.

Some areas of development may require several phases of work over a number of years. It is also the case that improvement plans become the responsibility of a recognised governance forum, such as the Integration Joint Board, Public Protection Committee's and Senior Management Teams who are responsible and accountable for oversight. The Service Managers and Chief Social Work Officer (CSWO) hold membership at these forums.

The following processes will however be developed where QAC is overseeing progress of assurance actions from self-evaluation/audit activity:

- Where service improvements and/or recommendations have been generated as part of self-evaluation and/or audit activity, tracking of progress and/or monitoring against agreed implementation dates/targets will be undertaken by a nominated officer at 3, 6 and 12-month intervals.

- The process for recording and reporting progress will be agreed at the point in which the Terms of Engagement are signed. Any change or deviation from this agreement will require agreement by both parties.
- Each improvement action will be assigned a lead officer or nominated point of contact and completion or target end date.
- Where tracking and monitoring reveal limited progress, or in cases where concerns have been raised by the lead officer and no discernible action taken, the matter will be escalated by the CSWO to the Director, Chief Officer or in some cases directly to the Chief Executive.
- These processes will be set out in the Directorate Level Service Level Agreements.

Owner: Alistair Gaw, Executive Director Communities and Families **Contributors:** Jackie Irvine, Chief Social Work Officer, Jon Ferrer Senior Manager Quality, Governance and Regulation, Keith Dyer Manager, Quality and Compliance	**Implementation Date:** 31 October 2019

2. Quality Assurance and Compliance methodology and operational processes	Medium

Annual Planning Process

Our review established that Quality Assurance and Compliance (QAC) do not have an established risk based annual plan to determine their coverage of both the Council's and Health and Social Care Partnership's most significant social work risks.

Currently, QAC annual work plans are determined by Quality Governance and Regulation (QGR) and approved by the Chief Social Work Officer (CSWO).

Quality Assurance and Compliance (QAC) review methodology

Review of a sample of four QAC assurance reports completed between 1 October 2017 to 31 October 2018 highlighted the need to improve the QAC methodology in the following areas:

1. Findings raised in reports are not currently rated to reflect the risks associated with the weaknesses identified in the quality of social work practices;
2. Significant issues identified during an assurance review that could adversely impact the quality of services delivered or result in a regulatory breach are immediately highlighted to Quality Assurance management; the CSWO; and senior management. However, this escalation process is not documented. Concerns were also noted that outcomes and actions taken by management are not always fed back to QAC to evidence satisfactory resolution;
3. Service areas are not required to provide management responses detailing the actions that they will take to address findings raised or provide dates for implementation of these action. Management has advised that QAC methodology is currently being refreshed and will include implementation of terms of reference detailing the work to be performed in individual reviews; and the requirement for management to develop and deliver improvement plans that will be reviewed by a Quality Assurance Officer at 3, 6 and 12 monthly intervals, with the CSWO kept informed of progress.

   This approach was noted for one of the reviews tested: Management actions to address findings raised in the review of Community Justice Services Practice Evaluation completed in September 2018 have been recorded in an improvement plan and the service has committed to providing regular progress updates. It was noted however, that some of the QAC report recommendations outlined in the plan are in the format of statements rather than actions;

4. No consistent follow up approach was applied to confirm that agreed management actions have been implemented and effectively sustained.

In, addition, the QAC Manager provided details of seven assurance reports issued between October 2017 and April 2018 where there was either no action or limited action taken by Service Areas in response to findings raised. Four of these reports covered 69 recommendations or proposals. Three further reports were in respect of extensive quality improvement work undertaken in Locality Offices. This feedback was in line with the results of the IA review of four reports.

It is recognised that not all recommendations or proposed actions will be prioritised and/or taken forward by the service area, however, in such cases, a record of the decision should be noted and held.

Risk Register

QAC does not currently maintain a risk register that captures the potential risks in relation to the quality of assurance provided, and availability of resources required to ensure appropriate coverage of social work risks across the Council and Partnership to support the CSWO's annual report.

Skills and Experience

Whilst QAC roles, responsibilities, and reporting lines are clearly defined and recorded in job descriptions and role specifications, they are not currently used as the basis for setting employee performance objectives as part of their annual 'looking forward' conversations.

Management advised that the requirement for Quality Assurance Officer to hold a social work qualification and have relevant social work experience was revised in 2017, however the revised job description could not be located, and the original job description was used for recruitment in Autumn 2018.

Risks

- Assurance outcomes do not cover all significant social work risks and do not fully support the Chief Social Work Officer's annual report;
- Findings raised do not include a rating indicating the significance of the associated risks;
- A risk-based approach checking that a sample of management actions have been effectively implemented cannot be applied if findings are not rated;
- There is no assurance that gaps identified in social work services have been addressed by both Council and Partnership management;
- Quality Assurance and Compliance (QAC) assurance risks have not been identified and recorded, and management cannot demonstrate that they are being effectively managed; and
- QAC team objectives do not reflect roles and responsibilities as detailed in job descriptions and role specifications.

2.1 Recommendation - Risk based annual planning

A risk based annual plan should be developed and implemented to support delivery of Quality Assurance and Compliance (QAC) assurance across both the Council's and Health and Social Care Partnership's (the Partnership's) key social work service delivery risks. This should include, but not be restricted to:

1. Establishing an ‘assurance universe’ of the full population of social work services delivered by the Council and the Partnership;
2. Performing an annual risk assessment of Council and Partnership social work services to ensure that all high-risk services are reviewed on an ongoing basis (for example, once every three years); and
3. A process supporting changes to the plan in response to new risks, or changes in existing risk profiles.

Annual Programmes of Activity should be generated in consultation with customers and partners and reviewed by the Corporate Leadership Team (CLT) and the relevant Council executive and Edinburgh Integration Joint Board (EIJB) committees.

Agreed Management Action

Each Directorate will in partnership with the Quality Assurance and Compliance (QAC) Service generate a Programme of Work or Activity Plan for the forthcoming 12 months. This Programme of Work will detail areas of interest and scrutiny, the approach, model and methodology to be used, timescale for completion, reporting arrangements and agreed frequency of monitoring/tracking.

This expectation will also be set out in the Service Level Agreements (SLAs) between QAC and Communities and Families; the Health and Social Care Partnership (the Partnership) and Community Justice. It is not envisaged that programmes of work will be reviewed by the Corporate Leadership Team (CLT) or the relevant Council executive/Edinburgh Integration Joint Board (EIJB) committees.

Governance for reporting and escalation processes will reside with the Chief Social Worker Officer (CSWO) and Head of Service/Director, and will be delivered through the Senior Management Teams, Public Protection committee’s and Health and Social Care Partnership (the Partnership).

QAC will ensure high risk services and areas of social work delivery, particularly Public Protection and the focus of decision making with regard removal of liberty are prioritised within each plan and are subject to scrutiny at least once every two years. The Programme will also consider and absorb activity as generated and commissioned by each relevant Public Protection Committee or Partnership.

Activity commissioned by or generated from Public Protection and Safeguarding Partnerships will corelate directly to the capacity available to the respective service areas (i.e. Child Protection Committee commissioned child protection audit linked to Communities and Families Annual Programme of Activity.)

The QAC Manager will be responsible for ensuing there is sufficient time, capacity and resource allocation available and where/if necessary remove or delay other areas of work detailed on the programme to this end. If required medium/low risk work will be carried over to the following year or at a point in time where capacity becomes available.

Activity generated from unplanned/unpredictable events, episodes or incidents, such as death and serious harm, findings from SCR’s or LSI’s, outcomes following SSSC investigation or recommendations following external scrutiny/inspection may where appropriate replace pre-agreed activity/work where required. Where additionality is not possible due to lack of capacity, the Department/Chief Officer will be notified of the need for planned work to be cancelled, scaled back or rescheduled. The CSWO reserves the right to commission activity in response to any of the above scenarios as required to ensure they are able to dispense their statutory duties accordingly.

Owner: Alistair Gaw, Executive Director Communities and Families	**Implementation Date:** 31 October 2019

Contributors: Jackie Irvine, Chief Social Work Officer, Jon Ferrer Senior Manager Quality, Governance and Regulation, Keith Dyer Manager, Quality and Compliance

2.2 Recommendation - QAC methodology

Existing QAC methodology should be reviewed and refreshed to include:

1. Application of ratings to findings raised that reflect the significance of the control gaps identified and the associated risks;
2. The requirement to record the process applied where significant issues have been escalated to senior management prior to completion of a review; and
3. Implementation of a risk based follow up process to confirm that management has implemented and sustained their agreed actions to address the findings raised.

Agreed Management Action

1. Quality Assurance and Compliance (QAC) does not propose to apply ratings to findings. The rationale for this is, that the QAC methodology and the presentation and interpretation of the findings generated is often subject to a number of variables. Evaluation can comprise of and include the use of both qualitative and quantitative evidence that can offer insight of patterns, trend and trajectory. Other methods of intelligence/evidence gathering, such as the use of testimonials and people's stories provide a user experience that may not necessarily reflect prescribed changes or improvements to policy, procedure, process or practice. The impact of change to service provision, practice approaches and legislation can shift the balance of care and focus within the social work and public protection sphere, impacting on data and performance that can potentially present artificial and/or flawed interpretation.

   It is important that each service area has a degree of autonomy and independence to prioritise work/activity and in certain situations reject proposed activity in favour of an alternative yet equally effective approach. Such decisions are important for social work services to retain a degree of control.

   However, where proposed areas of improvement are identified and subsequently rejected, the decision, rationale and alternative approach, if any, will be recorded and held by the commissioning service and QAC.
2. The following escalation processes will be developed:

   <u>During Activity</u>

   Should concerns be raised that relate to an individual's immediate safety or protection or where the service becomes aware of evidence of (gross) misconduct whilst undertaking any commissioned work, the matter will be immediately escalated in writing to the Quality Assurance and Compliance Manager or Senior Manager Quality, Governance and Regulation or the Chief Social Work Officer (CSWO). The matter will be raised/escalated to the Director or Commissioning Manager for immediate action as required. This escalation process is detailed in the Service Level Agreement.

   <u>Post Activity</u>

   For escalation post activity (concerned with monitoring and tracking of service improvements and recommendations) we will follow this process outlined at management action 1.2.
3. For recommendation 3 – we will apply the follow-up process for monitoring progress with actions, as set out in the management action for 1.2.

Owner: Alistair Gaw, Executive Director Communities and Families	**Implementation Date:** 31 October 2019

Contributors: Jackie Irvine, Chief Social Work Officer, Jon Ferrer Senior Manager Quality, Governance and Regulation, Keith Dyer Manager, Quality and Compliance	

2.3 Recommendation - QAC Risk register

A Quality Assurance & Compliance (QAC) risk register should be established and maintained in the Pentana risk management system that includes all relevant QAC assurance risks and supporting controls,

The risks and controls should be allocated to appropriate owners who will be responsible for ensuring that the risks are regularly re assessed and the controls remain effective.

The register should be regularly reviewed to establish if any risks require to be escalated to the Quality, Governance and Regulation risk register.

Agreed Management Action

Quality Assurance and Compliance (QAC) recognise the need for a service Risk Register. Version 1 of the register was generated on 16 April 2019 and will be monitored through QAC Management within Safer and Stronger and reported to Communities and Families Wider Management Team in accordance with current reporting requirements.

Owner: Alistair Gaw, Executive Director Communities and Families **Contributors:** Jackie Irvine, Chief Social Work Officer, Jon Ferrer Senior Manager Quality, Governance and Regulation, Keith Dyer Manager, Quality and Compliance	**Implementation Date:** 31 August 2019

2.4 Recommendation - Skills and experience

Job descriptions and role specifications should be used as the basis for setting Quality Assurance and Compliance (QAC) employee performance objectives as part of their annual ‘looking forward’ conversations.

In addition, the qualifications and experience required for the Quality Assurance Officer role should be clarified; the role description updated to reflect the requirements; and the revised role description used to support all future recruitment activity

Agreed Management Action

The ‘essential requirements’ and qualifications deemed necessary for the role of Quality Assurance Officer (QAO) and Regulation Officer will be reviewed and amended as required within the existing job descriptions and Job Specification.

Whilst the Service acknowledges the need to reflect and align the work of the QAO role with the existing job description, skills, experience and knowledge are gained through ongoing professional development, training and directed learning opportunities.

QAO’s are required to work across a range of disciplines ands areas of social work practice and legislation, this requires a broad knowledge, yet successful delivery of activity is subject to competency-based project management, time management, clarity of role and function and a predetermined set of parameters. The QAC service adopts a variety of approaches which include quality improvement, quality assurance, evaluation and scrutiny, each deployed to meet the needs of the approach, identified model or the questions generated by the service.

Owner: Alistair Gaw, Executive Director Communities and Families	**Implementation Date:** 31 October 2019

Contributors: Jackie Irvine, Chief Social Work Officer, Jon Ferrer Senior Manager Quality, Governance and Regulation, Keith Dyer Manager, Quality and Compliance	

3. Data Protection Impact Assessment — Low

There is currently no Data Protection Impact Assessment (DPIA) covering the processes applied by Quality Assurance and Compliance (QAC) in relation to the personal data they obtain; review; process; and retain to support completion of their assurance reviews.

A DPIA must be completed to confirm that appropriate controls have been established to ensure ongoing compliance with General Data Protection Regulation (GDPR) legislation; Data Protection principles; and the Council and Partnership's records management policies.

Risks

- Non-compliance with the data protection principles set out in the Data Protection Act 1998, General Data Protection Regulation, and the new Data Protection Act 2018.
- Failure to safeguard personal data, resulting in reputational, and potentially financial, damage to the Council.

3.1 Recommendation - QAC Data Protection Impact Assessment

1. A Data Protection Impact Assessment (DPIA) should be prepared to cover the processes applied to all data obtained; reviewed; processed; and retained by Quality Assurance and Compliance (QAC).
2. The completed document should be submitted to the Information Governance Unit (IGU) for review and assessment.
3. Following receipt of a DPIA assessment report from the Information Governance Unit (IGU), QAC should implement the recommended improvement actions then submit the assessment report, and evidence of completed improvement actions to their Information Asset Owner for the processing to be authorised.

Agreed Management Action

The Quality Assurance and Compliance Manager has completed a Data Protection Impact Assessment which was signed off by the Information Governance Unit on 9 April 2019. This is now available for Internal Audit to review.

Owner: Alistair Gaw, Executive Director Communities and Families **Contributors:** Jackie Irvine, Chief Social Work Officer, Jon Ferrer Senior Manager Quality, Governance and Regulation, Keith Dyer Manager, Quality and Compliance	**Implementation Date:** 31 August 2019

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 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 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 of the organisation.
Low	A finding that could have a: • ***Minor*** impact on 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: Areas of audit focus

The areas of audit focus and related control objectives included in the review are:

Roles and responsibilities

- The roles and responsibilities and reporting lines for the QG&R team have been clearly defined, and are reflected in the team's 'looking forward' performance objectives;
- An appropriate independent reporting line through to the CSWO and elected members has been established;
- There is clear alignment between team objectives; the Chief Social Work Officer's responsibilities; and applicable regulatory requirements;
- Terms of reference detailing the team's assurance responsibilities and engagement approach has been prepared; agreed with; and approved by the Executive Director of Communities and Families; the Chief Officer for the H&SCP; the Corporate Leadership Team; and relevant Council and EIJB Executive Committees;
- The scope of work provides QG&R with right of access to all relevant personnel and documentation in relation to delivery of social work services by the Council and the H&SCP; and
- The scope of work includes the requirement to engage the CSWO and QG&R for professional advice in relation to any planned significant changes to delivery of social work services across the Council and the H&SCP.

Skills and experience

- Skills and experience required for all roles within the QG&R team have been clearly defined and included in team role specifications; and
- The current team is suitably qualified and are required to ensure that continuing professional development (CPD) requirements for their relevant professional bodies are maintained.

Methodology

- A QG&R methodology has been defined and is consistently applied across all reviews performed;
- The methodology includes guidance on understanding key social work risks and controls; preparing the annual plan; planning, performing and reporting on individual assurance reviews; follow-up; and reporting to governance committees; and
- Key performance indicators have been established to manage both QG&R team delivery and ensure effective engagement with relevant Council and H&SCP teams.

Planning

- A risk based annual assurance plan detailing QG&R focus for the financial year is prepared and approved by the CLT; the H&SCP and the relevant Council and EIJB Executive committees;
- The annual assurance plan is based on an assessment of the key risks that could impact delivery of social work services across the Council and the H&SCP;
- The annual plan considers whether available team resources are sufficient to provide assurance on all key social work service delivery risks;

- The plan provides an appropriate level of coverage across all social work services provided by the Council and the H&SCP, and includes an appropriate balance between service delivery and thematic reviews;
- Planning for reviews includes sufficient time to understand social work services processes applied;
- Any process design issues that could impact the quality of services delivered are immediately highlighted and escalated; and
- An appropriate sample selection methodology is applied to ensure that representative samples are selected and tested for assurance reviews.

Fieldwork

- Any significant issues that could result in a regulatory breach or adversely impact quality of social care services is immediately escalated to the CSWO and senior management within the Council and the H&SCP;
- The outcomes of sample based testing performed is recorded, with any testing and emerging themes identified and recorded; and

Further testing is performed (where required) to identify the extent of any significant or system issues.

Reporting and follow-up

- Reports are prepared detailing the outcomes of all QG&R reviews, raising issues / findings where issues have been identified;
- Management responses detailing the actions that will be taken to address findings raised are obtained, together with agreed implementation dates;
- An appropriate risk based follow-up approach is applied by QG&R to confirm that all agreed management actions have been implemented and effectively sustained; and

The follow-up process includes an assessment of progress with implementation of findings raised by external regulatory / scrutiny bodies.

Governance and reporting

- There is a clearly established independent reporting line for reporting QG&R assurance outcomes to appropriate H&SCP governance forums; the CLT and relevant Council and EIJB executive committees;
- Governance and Committee reporting include progress with delivery of the QG&R plan; assurance review outcomes; and progress with implementation of agreed management actions to address the findings raised;
- QG&R reports are shared with the Care Inspectorate and other regulatory bodies upon request;
- Either the CSWO or QG&R are represented at relevant Council and H&SCP risk committees to ensure that any risks relating to quality and delivery of social work services are highlighted and included in risk registers (where appropriate); and

Either the CSWO or QG&R are represented at the Local Area Network meeting hosted by the Council and attended by all assurance providers (including the Care Inspectorate) to ensure that plans and outcomes are shared and discussed (where appropriate).