Finance and Resources Committee

10.00am, Thursday 16 August 2018

Internal Audit Update Report: 1 January – 31 July 2018 – referral from the Governance, Risk and Best Value Committee

Item number	7.11
Report number	
Wards	All

Executive summary

The Governance, Risk and Best Value Committee on 31 July 2018 considered a report which detailed the Internal Audit progress for the period 1 January to 31 July 2018

The report has been referred to the Finance and Resources Committee on the recommendation that high and medium risk findings from audit reports be submitted to their parent Committee for information.

Terms of Referral

Internal Audit Update Report: 1 January – 31 July 2018

Terms of referral

1.1 On 31 July 2018, the Governance, Risk and Best Value Committee considered a summary of the findings and status of work from the Internal Audit plan of work. Additional reviews were to be added to the plan where considered necessary to address any emerging risks and issues identified during the year, subject to formal approval by the relevant committee.

1.2 The report by the Chief Internal Auditor indicated that Internal Audit recruitment had been successful and the team now expected to be at full complement by the beginning of October 2018.

1.3 Work had commenced on the 2018/19 annual plan, however, delivery had been impacted by the ongoing resourcing challenges. It had been agreed with PwC that resources would be provided in August to support delivery of three 2018/19 reviews.

1.4 The Governance, Risk and Best Value Committee agreed:

1.4.1 To note the risks associated with the 21 High rated findings raised in the 17 Council reports.

1.4.2 To note that the 2 Lothian Pension Fund reports had been presented to the Pensions Committee for scrutiny

1.4.3 To refer the 6 reports noted in Appendix 1 as potentially being of interest to the Audit and Risk Committee of the Edinburgh Integration Joint Board (EIJB), to that Committee.

1.4.4 To note that no reports were referred by the EIJB Audit and Risk Committee to the Governance Risk and Best Value Committee at their meetings in February, March and May 2018.

1.4.5 To note the current position with resources and successful recruitment.

1.4.6 To note the progress with the 2018/19 annual plan and recent IA priorities.

1.4.7 To ask for an update to the next meeting on the ability of the 18/19 Plan to deliver its outcomes.

1.4.8 To refer the audit report on CCTV noted in Appendix 1 to the CCTV Working Group for consideration.

1.4.9 To refer the high and medium risk findings to each executive committee as appropriate.

1.4.10 To ask for a further report on the processes involved for making changes to the 2017/18 Internal Audit Plan.

For Decision/Action

2.1 The Finance and Resources Committee is asked to note the attached audit reports with high and medium risk findings concerning Phishing Resilience, CGI Contract Management and Health and Social Care Purchasing Budget Management.

Background reading / external references

Webcast of Governance, Risk and Best Value Committee – 26 September 2017

Laurence Rockey

Head of Strategy and Insight

Contact: Louise Williamson, Assistant Committee Officer

Email: louise.p.williamson@hotmail.com | Tel: 0131 529 4264

Links

Appendices	Appendix 1 – Internal Audit Quarterly Update Report: 1 January 2017 – 31 June 2018 – report by the Executive Director of Resources

Governance, Risk and Best Value Committee

10.00am, Tuesday 31 July 2018

Internal Audit Update Report: 1 January – 31 July 2018

Item number	7.2
Report number	
Executive/routine	
Wards	
Council Commitments	

Executive Summary

This report provides details of Internal Audit (IA) reviews completed in the period; recent changes to the 2017/18 IA plan; and updates on resourcing; commencement of the 2018/19 Internal Audit plan; and IA priorities.

Internal Audit has now issued a total of 33 2017/18 audit reports to the City of Edinburgh Council (the Council) the Lothian Pension Fund (LPF) and the Edinburgh Integration Joint Board (EIJB), with 19 issued between 1 January and 31 July 2018. This included 15 reports for the Council; 2 for LPF; and 2 for the EIJB.

Of the 19 reports issued to the Council, two have been presented separately to the Committee for scrutiny. The remaining 17 reports include 65 findings (21 High; 34 Medium; and 10 Low).

A total of 6 reports are recommended for referral from the GRBV to the EIJB Audit and Risk Committee. No reports have been referred by the EIJB Audit and Risk Committee during the period.

IA recruitment has been successful and the team is now expected to be at full complement by the beginning of October 2018.

Work has commenced on the 2018/19 annual plan, however, delivery has been impacted by ongoing resourcing challenges. It has been agreed with PwC that resources will be provided in August to support delivery of three 2018/19 reviews.

·EDINBVRGH·
THE CITY OF EDINBURGH COUNCIL

Internal Audit Update Report: 1 January – 31 July 2018

1. Recommendations

1.1 Committee is recommended to:

1.1.1 Note the risks associated with the 21 High rated findings raised in the 17 Council reports and consider if further clarification or immediate follow-up is required with responsible officers for specific items;

1.1.2 Note that the 2 LPF reports have been presented to the Pensions Committee for scrutiny;

1.1.3 Refer the 6 reports noted in Appendix 1 as potentially being of interest to the EIJB Audit and Risk Committee;

1.1.4 Note that no reports were referred by the EIJB Audit and Risk Committee to GRBV at their meetings in February; March and May 2018.

1.1.5 Note the current position with resources and successful recruitment; and

1.1.6 Note progress with the 2018/19 annual plan and recent IA priorities.

2. Background

2.1 Internal Audit is required to deliver an annual plan of work, which is scoped using a risk-based assessment of Council activities. Additional reviews are added to the plan where considered necessary to address any emerging risks and issues identified during the year, subject to approval from the relevant Committees.

2.2 IA progress and a summary of findings raised in the reports issued are presented to the Governance, Risk, and Best Value Committee quarterly.

2.3 All audits performed for the Lothian Pension Fund (LPF) are subject to separate scrutiny by the Pension Audit Sub-Committee and the Pensions Committee, and are included in this report for completeness.

2.4 Audits performed for the Edinburgh Integration Joint Board (EIJB) are presented to the EIJB Audit and Risk Committee for scrutiny, with any reports that are relevant to the Council subsequently referred to the GRBV Committee.

2.5 Audits performed for the City of Edinburgh Council (the Council) that are relevant to the EIJB will be recommended for referral to the EIJB Audit and Risk Committee by the GRBV Committee.

3. Main report

Audit Findings for the period

3.1 A total of 33 2017/18 audit reports have now been issued to the to the Council (27); LPF (4); and the EIJB, with 23 issued between 1 January and 15 July 2018.

3.2 This included 19 reports for the Council; 2 for LPF; and 2 for the EIJB.

3.3 Of the 19 reports issued to the Council, the Building Standards, and Edinburgh Building Services (Housing Property Services) reports have been presented separately to the Committee for scrutiny.

3.4 The remaining 17 Council reports included a total of 65 findings (21 High; 33 Medium; and 10 Low). The majority of the findings raised (40%) were included in the Care Homes Assurance (4 High; 12 Medium; 4 Low) and Drivers Health and Safety (3 High and 6 Medium) audits. Details of completed reports are included at Appendix 1, with individual reports provided in Appendix 2 (following the order in Appendix 1).

3.5 The 2 LPF reports have been presented to the Pensions Audit Committee for scrutiny. These reports included a total of 11 findings (4 High; 3 Medium; and 4 Low).

3.6 The 2 EIJB reports were presented to the July EIJB Audit and Risk Committee, and it was agreed that these should be referred to the GRBV.

A total of 6 Council reports are recommended for referral from the GRBV to the EIJB Audit and Risk Committee (refer Appendix 1).

Changes to the 2017/18 IA Plan

3.7 The Health and Social Care Partnership Care Inspectorate Follow-up review that was included in the 2017/18 audit plan has been replaced with a review of the Edinburgh Mela Ltd at the request of management, given the significant reputational risks associated with the Council's decision to provide funding to support the Mela festival. Given resource constraints it was not possible in the timescales available to undertake both reviews.

3.8 It is expected that the Mela Ltd review will be completed in early July. This review has no impact on the Council's 2017/18 Internal Audit annual opinion.

Resourcing

3.9 Recruitment has been successful with offers now accepted for all vacant roles

3.10 It is expected that the IA team will be at full complement by the beginning of October, with new team members joining on a phased basis (aligned with notice periods) from July onwards.

Progress with 2018/19 Annual Plan

3.11 Work on the 2018/19 annual plan has commenced with one audit currently in progress.

3.12 Progress with the 2018/19 plan has been impacted by ongoing resourcing challenges, and the priorities noted below.

3.13 It has been agreed with PwC that resources will be provided in August to support delivery of three 2018/19 audits.

Internal Audit Priorities

3.14 Focus for the last quarter has been directed at finalising the audit reports for the 2017/18 annual plan; recruitment; and launching the new automated follow-up process.

3.15 The new system will be launched Council wide in early July, with training delivered during the weeks of 25 June and 2 July focusing on the role and importance of IA; rebranding IA as ‘your safety net’; sharing examples of best practice when finalising audit reports and providing updates and evidence to support closure of findings; and introducing the new system.

4. Measures of success

4.1 Once implemented, the recommendations contained within these reports will strengthen the Council’s control framework.

5. Financial impact

5.1 No direct financial impact.

6. Risk, policy, compliance and governance impact

6.1 Internal Audit findings are raised as a result of control gaps or deficiencies identified during audits. If agreed management actions are not implemented to support closure of Internal Audit findings, the Council will be exposed to the risks set out in the relevant Internal Audit reports.

7. Equalities impact

7.1 Not applicable.

8. Sustainability impact

8.1 Not applicable.

9. Consultation and engagement

9.1 Not applicable.

10. Background reading/external references

10.1 Building Standards Audit Report to GRBV 8 May 2018

10.2 Housing Property Audit Report to GRBV 5 June 2018

Lesley Newdall

Chief Internal Auditor

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

11. Appendices

Appendix 1	Summary of IA reports issued and findings raised during the period and recommendations for referral to the EIJB Audit and Risk Committee.
Appendix 2	Audit reports issued in period 1 January 2018 to 31 July 2018

Appendix 1 – Summary of IA reports issued and findings raised during the period and recommendations for referral to the EIJB Audit and Risk Committee.

		Findings Raised				
	Audit Review	**High**	**Medium**	**Low**	**Totals**	**Refer to EIJB**
	Council Wide					
1.	Drivers Health and Safety	3	6	0	9	Y
2.	Phishing Resilience	2	1	0	3	Y
	Safer and Stronger Communities					
3.	CCTV Infrastructure	2	0	0	2	N
	Resources					
4.	CGI Contract management	0	2	0	2	N
	Communities and Families					
5.	Foster Care Review	1	2	1	4	N
	Strategy and Insight					
6.	Resilience Assurance	2	2	1	5	Y
7.	Project Benefits Realisation	2	0	0	2	Y
	Health and Social Care – note that both reviews include management actions owned by Resources (Customer)					
8.	Care Homes	4	12	4	20	Y
9.	Social Work Centre Bank Account Reconciliations	2	0	0	2	Y
10.	Review of Social Care Commissioning	1	1	0	2	*
11.	Health and Social Care Purchasing Budget Management	4	0	0	4	*
	Place					
12.	Port Facility Security Plan	1	4	1	6	N
13.	H&S Waste and Recycling	0	4	2	6	N
	Lothian Pension Fund					
14.	Payroll Outsourcing	1	0	1	2	N
15.	Pensions Tax	1	1	0	2	N
	Totals	**26**	**35**	**10**	**71**	

* Reports referred to the Governance, Risk and Best Value Committee from the Edinburgh Integration Joint Boards Audit and Risk Committee

Appendix 2 – Audit reports issued in period 1 January 2018 to 31 July 2018

The City of Edinburgh Council

Internal Audit

Phishing Resilience

Final Report

12 July 2018

ICT1702

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

Phishing attacks are the most common form of cyber threat used against organisations. Phishing attacks involve an attacker sending emails designed to convince the recipient that they need to open an attachment or click on a spoof or hoax web page link. The attachments and links are often designed to either install malicious software (malware) which then infiltrates organisational networks, or trick the user into entering sensitive information (such as a username or password) providing the attacker with subsequent access to sensitive and confidential information.

In October 2017 Hamilton Academical Football Club was affected by a phishing attack and was ultimately defrauded of circa £1M.

Ransomware is a particularly destructive form of malware that catastrophically struck the NHS in May 2017 (the 'WannaCry' attack). The WannaCry malware encrypted data on infected computers and demanded a ransom roughly equivalent to £230 per computer to release the data. This prevented more than one third of English NHS trusts from accessing their systems, resulting in at cancellation of least 6,912 patient appointments, including operations.

The Scottish Government was also hit by two separate ransomware cyber attacks in 2016/17 at the Student Awards Agency Scotland and the National Records of Scotland, with hackers targeting official computers; encrypting sensitive data; and demanding money for the files to be unlocked.

"Whaling" is a unique form of phishing that specifically targets executives and senior management who hold power in organisations; with a significant public profile; and complete access to sensitive data. The term "whaling" refers to the seniority of the targets relative to targeted in typical phishing attacks. The objective of a whaling attack is to trick an executive into revealing personal or corporate data, often through email and website spoofing.

Whaling attacks are more difficult to detect than typical phishing attacks as they are highly personalised and sent to selected targets. Whaling attacks can rely solely on social engineering to fool their targets, and in some cases, will use hyperlinks or attachments to infect victims with malware or solicit sensitive information. Due to the high returns achievable from whaling, cyber criminals spend significant time and effort constructing attacks so that they appear legitimate. Attackers often source information from social media such as Facebook, Twitter, and LinkedIn, profiling targets' company information, job details, and names of co-workers or business partners. Whaling is becoming more successful, and as a result there has been an increase in its popularity.

There has also been a dramatic increase in the last two years in targeted fraud cases where cyber criminals send legitimate-looking emails imitating a real person known to the target. These attacks are known as business email compromise (BEC) fraud, and involve the attacker asking the victim to make bank transfers to accounts under the attacker's control. The sophisticated nature of the campaign highlights the investment that cyber attackers will make to successfully compromise their target.

Given the significant risks and impacts associated with phishing, it is essential that the Council operates effective cyber security technology controls, supported by a strong and effective cultural awareness of phishing to ensure that all employees can identify (or at least question) and report suspicious e mails.

Given the increasing sophistication of phishing and cyber security attacks, it is also important that the Council can analyse the volume and nature of attacks reported in order to ensure that cyber security controls can be appropriately enhanced to ensure that they remain effective.

Finally, it is essential that the Council has established adequately designed cyber security controls that operate effectively to meet the requirements of the Scottish Government Public Sector Action Plan for Cyber Resilience published in November 2017.

Scope

The objective of this review was to test the knowledge and awareness of phishing across a randomly selected sample of Council employees; Elected Members; and Member's Services teams using a mass phishing simulation technique, and assess the adequacy and effectiveness of established processes enabling employees to report receipt of suspicious e mails.

It should be noted that processes applied by CGI on behalf of the Council in relation to phishing e mails reported by employees were specifically exclude from the scope of this review.

PwC were engaged to perform this work under the terms of our Internal Audit co-source arrangements.

E mail design

Our approach involved designing and issuing three separate phishing scenarios across a random sample of employees. The e mails used in the exercise were tailored to differing degrees of sophistication. The first and second scenarios were limited in sophistication and were designed to test user susceptibility to phishing emails branded by 3rd party entities. These e mails were purportedly issued by:

- a fictitious company named G-Vouchers offering lucrative discounts on popular items; and
- A fictitious courier service named Secure Courier Co. who claimed they had failed to deliver the targeted users package.

The third scenario was specifically designed to simulate whale (also referred to as spear) phishing and targeted Council Executives; Heads of Service; Locality Managers and (importantly) Executive and Business Support Assistants who have access to and manage senior management e mail accounts.

The design of this e mail simulated a genuine internal Freedom of Information (FOI) request, with only a minor misspelling in the sender's e mail address (foi-requests@edinbrgh.org.uk) enabling recipients to identify it as a potential phishing request. Copies of all three e mails sent are included at Appendix 2 – Simulated Phishing e mails.

Sampling

A random sample of 6,017 employees (circa 45% of Council employees with e mail accounts) was selected using an extract from the Council's Global Address List. Further Details of the sample selected are included at Appendix 3 – Sample of Employees Targeted

The phishing e mails were sent to the employees included in the sample between 24 and 26 January 2018, and results as at 2 February 2018 recorded and analysed to determine:

- The total volume of clicks and responses across the sample of employees; and
- The total number of employees who took appropriate action to report receipt of a suspected phishing e mail.

Scope Limitations

As there is currently no single source of employee data that completely and accurately replicates the Council's organisational structure, it was not possible to perform detailed analysis of phishing responses across Directorates; Service Areas or employee groups (for example Elected Members and their business support teams; locality teams; or executive support teams).

Consequently, our results are split between learning and teaching employees (who have unique e mail addresses) and other Council employees, with some further manual analysis performed to identify any Corporate Leadership team members or Heads of Service and their executive support teams, and Locality managers who had actioned the phishing e mails.

It should be noted that phishing simulations usually target a smaller sample of employees (circa 500), in comparison to the Council's sample population of circa 6,000 employees given the potential risk employees become aware of larger scale exercises as they progress. This risk was addressed by issuing the e mails over a short time horizon.

2. Executive summary

Total number of findings

Critical	-
High	2
Medium	1
Low	-
Advisory	-
Total	**3**

Summary of findings

Phishing Responses

The results of the phishing simulation demonstrate that that the Council could potentially be exposed to cyber security risk with 9% (528) of the sample either clicking on the links or responding to the phishing e mails.

A significant weakness was identified in relation to knowledge and awareness of whale phishing amongst the Council's senior management and their support teams (who have access to and manage senior management's e mail accounts), with a 29% response rate to the sophisticated whale phishing simulation.

The outcomes of the remaining two scenarios (which were very limited in sophistication) are aligned with the average response rate of 10% when compared to similar organisations, and demonstrated a moderate degree of security awareness from targeted employees.

Learning and teaching staff accounted for 54% (282) of responses to the voucher and parcel delivery scenarios, with 46% (240) from the remaining employees sampled. A summary of the results per simulation is included at Table 1 below:

Table 1: Summary of phishing simulation outcomes

Scenario	Sample Population	Out of Office Responses	Final Sample	Clicked / Replied		Total Responses (%)
				Learning and Teaching	Other	
1) G Voucher Discounts	2,997	198	2,799	113 (4%)	117 (4%)	8%
2) Secure Courier – Failed Delivery	2,999	117	2.882	169 (6%)	123 (4%)	10%
3) Freedom of Information (whale phishing simulation)	21	-	21	6		29%
Totals	6,017			528		9%

Reporting Phishing

Employees who neglect to challenge suspicious emails also increase the Council's exposure to cyber crime as the Council cannot perform analysis on the volume and nature of e mails received, and implement appropriate measures to ensure that cyber security controls remain effective.

Our results demonstrated that only 1.4% of the 91% of employees who did not respond to the phishing e mails proactively reported receipt of a suspicious e mail. Review of historic reporting monthly reporting volumes established that these were lower than would normally be expected (an average of 17 incidents reported per month between January 2016 and January 2017) given the increasing volume and sophistication of phishing and cyber security attacks.

Additionally, review of the 'report phishing' guidance published on the Orb (the Council's Intranet) established that it cannot be easily located and that the process to report a suspicious e mail is unclear. This could potentially be the root cause of the low volume of suspicious e mails reported by employees.

Finally, there is currently no single source of employee data that completely and accurately replicates the Council's organisational structure, enabling analysis of employee e mail addresses to support future identification of employee groups for targeted ongoing cyber security training and future phishing simulation testing.

Consequently, 2 High and 1 Medium rated Findings have been raised. It is essential that these weaknesses are addressed in a time manner to ensure that the Council meets the requirements of the Scottish Government Public Sector Action Plan for Cyber Resilience.

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

3. Detailed findings

1. Targeted Training

Finding

The Council’s ICT team has been running a "Stop Think Connect" cyber security awareness programme across the Council which has clearly had a positive impact as 91% of employees did not respond to the simulated phishing e mails.

However, our testing identified a significant lack of knowledge and awareness of whale phishing across Council Executives; Heads of Service; Locality Managers and (importantly) Executive and Business Support Assistants (who have access to and manage senior management e mail accounts) with a 29% response rate to the Freedom of Information whale phishing simulation. These responses included:

- One Corporate Leadership Team member;
- One Head of Service and one Locality Manager;
- One Senior Executive Assistant and one Executive Assistant; and
- One Modern Apprentice

Whilst it is expected that Senior Management will delegate access to, and management of, e mail accounts to their Executive and Business Support Assistants, they must ensure that these employees have a strong knowledge and awareness of phishing enabling them to take appropriate action and prevent inappropriate responses that could expose the Council to risk of cyber attacks.

Additionally, there is currently no mandatory phishing and cyber security training in place for all Council employees who have e mail accounts.

Business Implication	Finding Rating
• Risk that the Council is exposed to malware or ransomware attacks that could infect technology networks; and • Risk that commercial or employee sensitive information is disclosed to cyber criminals by Senior Management.	**High**

Action plans

Recommendation	Responsible Officer
1. Targeted whale phishing training should be designed and provided to Council Executives; Heads of Service; Locality Managers and (importantly) Executive and Business Support Assistants on an ongoing basis; and 2. Generic phishing / cyber security training should be developed and included within induction and ongoing mandatory training for all employees with Council e mail accounts; 3. Phishing / cyber security training should be reviewed and updated annually to ensure that the training content remains aligned with the increasing sophistication of attacks experienced within the Council and across other public sector bodies; and	Neil Dumbleton, Enterprise Architect

4. Ongoing phishing simulation testing exercises should be designed and implemented across all employees and contractors with Council e mail addresses, with the results recorded and analysed to identify and address target training requirements.	
Agreed Management Action	**Estimated Implementation Date**
1. a) Accepted. A Members Briefing email was issued to Councillors and CLT members on 22/3/18. We have provided targeted training to the senior leaders group, using the term spear fishing as we feel this is most appropriate but explained how prominent people are at risk. The term whale phishing is described in our recent awareness poster. We would look to have this marked as completed. b) Targeted training in Cyber-Security for a wide range of staff roles is a Public Sector Action Plan for Cyber Resiliency (PScAP) requirement. ICT and Learning and Organisational Development (L&OD) attended at a workshop with Scottish Government in May 2018, and we believe that our training plans take account of all SG guidance. We subsequently demonstrated our training to then and they would like us to create guidance for Cyber Catalysts. We have a training and awareness plan for 2018. This has been issued to the new Cyber and Information Security Steering Group for further comment. 2. a) The Phishing Awareness Course developed in conjunction with Learning and Organisational Development has been released via an e mail that includes a link to the training course to: • All staff • Targeted version to senior leaders • Targeted version to ICT. We believe the training course is suitable for varied users, and have adopted an approach where we use the same course for all users but adapt / flavour the communications to bring it alive for the target groups. We would look to deliver this to (say) finance and legal next. Feedback on the course has been overwhelming positive and we would look to have this marked as completed. Until the fourth finding in this report is addressed which will provide a full population of employees; and their roles and position within the Council combined with their e mail addresses, we remain dependent on existing data such as manual lists and e mail distribution lists to ensure that the course is targeted at appropriate groups of employees. b) Ongoing training is also a requirement of the Public Sector cyber action plan. ICT now has a Training and awareness plan that exceeds the commitment here. We are on target to deliver this commitment. c) There is a requirement for the preparation of training courses. Completion of this audit action is subject to assistance from L&OD or a third party and identification of budget. Resources have so far been available from L&OD to support the Training & Awareness plan. If they are not we would look to escalate. The need for increased awareness is a key theme of the CISSG. We are on target	1. Completed 31 August 2018 for IA validation and closure 2. a) Completed 31 August 2018 for IA validation and closure 2b and c) 28 September 2019 2d) 28 September 2018 3. 28 September 2019 4. 31 October 2018

to deliver this commitment before 28th September so no extension is requested. d) Consideration will be given to the Council adopting this as mandatory training with output of discussions being provided to internal audit by ICT. The issue of making training mandatory has been raised with L&OD, and a meeting will be arranged to discuss. 3. Accepted. Once such courses are agreed ICT will ensure these are updated annually (or earlier depending on NSCS guidance changes or in response to incidents) in line with best practice advice and e.g. in-line with PScAP recommendations. The courses will be reviewed and updated by the first anniversary date of their release. 4. ICT will prepare costed proposals for ongoing phishing simulation tests. A change request has been raised with CGI to obtain the “utility” costs for an ongoing targeted simulation phishing service. The utility cost (e.g. cost per exercise per 1000 staff) will support implementation of flexible simulation exercises. We can aim for both a series of exercises e.g. one every 4 months OR carry out exercises on demand, say in response to a specific incident. If costed proposals are not feasible, alternative options will be explored.	

3. Reporting Phishing

Finding

Reporting Culture

Whilst our testing confirmed that 91% of employees in our sample did not respond to the simulated phishing emails, there was no corresponding increase in the volume of suspicious emails reported as only 1.4% of the 91% of employees proactively reported receipt of a suspicious e mail either via phone or e mail to the CGI helpdesk.

CGI has also confirmed that:

- an average of 17 suspected phishing e mails per month were reported to the Service Desk in the period January 2016 to November 2017;
- 10 suspected phishing e mails were reported in December 2017; and
- 7 were reported in January 2018

Phishing Guidance

A review of the ‘report phishing’ guidance published on the Orb (the Council’s Intranet) established that it cannot be easily located and that the process to report a suspicious e mail is unclear. Specifically:

- The process for reporting phishing is not included prominently on the Orb – the ‘report it’ box on the home page does not include any links to the report phishing process (refer Orb Home Page);
- The process to report phishing does not feature prominently on the ICT home page. Users must navigate their way to the ICT security link via a series of three clicks (from the main Orb home page) to find any references to e mail security; phishing and ransomware. This contrasts with only one click required on a phishing e mail link that could infect Council networks with malware;
- The process for reporting suspicious e mails in the e mail / security phishing page is unclear. Whilst the page includes a contact number and e mail address, it does not specify whether the e mails

should be forwarded or included as an attachment to enable further analysis and investigation (refer E mail Security / Phishing Guidance);

- There is no specific telephone number or e mail address dedicated to reporting suspected phishing e mails. The current telephone number included in the Orb directs employees to the Council's ICT Security Manager (who may not always be available to take calls) or to a generic ICT security e mail inbox. This is likely to cause confusion as the phishing and ransomware awareness images on laptop start up screens include a phone number and e mail address for the CGI service desk; and
- The final page of the phishing guidance page on the Orb includes a link to an online form (Related Items – Online Forms on Phishing Page) which is a form that should be used to report a data protection breach, and makes no specific reference to phishing.

Finally, whilst functionality is available to include a "report phishing" icon in the Microsoft Outlook e mail toolbar, enabling users to report receipt of suspicious e mails via one click directly from their inbox, this is not included in the version used by the Council.

Business Implication	Finding Rating
The Council has insufficient data to monitor the volume and nature of phishing attacks targeted specifically against the Council, and ensures that cyber security controls remain sufficiently effective to combat potential cyber security attacks.	High

Action plans

Recommendation	Responsible Officer
1. Phishing Guidance on the Orb should be reviewed and refreshed with the links to the revised guidance and 'report phishing' telephone numbers and e mail addresses featured prominently on the home page; 2. The revised report phishing process should include step by step guidance to support employees in reporting suspicious e mails and sending them to ICT for further investigation and analysis; 3. Analysis of the nature and volume of phishing attacks reported by employees should be performed and reported to the relevant ICT governance forum; and 4. ICT should investigate and implement (if feasible) the "report phishing" icon in the Microsoft Outlook e mail toolbar. Implementation should be supported by relevant guidance on the Orb.	Neil Dumbleton, Enterprise Architect for all actions.

Agreed Management Action	Estimated Implementation Date
1. and 2 - Accepted – these recommendations will both be fully implemented 3. a) Accepted in principle but there are practical constraints. Reports of phishing attempts are made to the CGI Service Desks. To provide analysis, CGI will need to extract data from the call centre records and provide data to the Council's Security Working Group (SWG). Delivery of such data for existing metrics is subject to an overdue audit already, and this additional analysis might be at a cost to the Council. We have a commitment from CGI that they will produce the figures. We did this through the Security Working Group and not the change request process as the latter has not been effective in the past.	1. and 2 Completed 31 August 2018 for IA validation and closure 3. a and b) 31 March 2019 4. 20 December 2019

b) If the proposal(s) are acceptable and are approved by the Council, we will aim for provision of phishing analysis to and review by the Security Working Group by March 2019. 4. CGI has agreed to add the icon as part of the EU/Office 365 roll out for both corporate and Learning and Teaching employees, and will amend the core functionality to report phishing attempts to their helpdesk. The risk is not that they don't accept doing it, but that the 0365 project is delayed. We understand this is a firm commitment with target completion date for June 2019.	

4. Employee Data

Finding

As part of the Public Sector Action Plan for Cyber Resiliency (published November 2017) The Scottish Government will seek assurances from Scottish public bodies that they have in place appropriate staff training, awareness-raising and disciplinary processes about cyber resilience for staff at all organisational levels (key action 6).

This, together with key action 4, which requires the Council to obtain appropriate independent assurance of critical cyber security controls by end October 2018, will require the Council to identify the full population of employees with e mail addresses and perform analysis of their roles, groups, and levels across the organisation (for example, Elected Members and their support teams; all executive support teams; heads of service; and locality employees).

There is currently no single source of employee data that accurately replicates the Council's organisational structure, enabling simple identification of groups of employees for targeted training or future phishing simulation exercises.

A data extract from the Council's global address list was used to select a random sample of employees for inclusion in the current phishing simulation, with the intention of selecting samples based on Directorates; Service Areas; and other groups so that results could be analysed in detail and provided to these groups for review and action (where appropriate).

This was not possible due to the quality of information recorded in the GAL which included a significant volume of both incomplete and factually inaccurate entries, and prevented accurate analysis.

Business Implication	Finding Rating
It may not be possible to meet the requirements of the Scottish Government's Public Sector Action Plan for Cyber Resiliency.	Medium

Action plans

Recommendation	Responsible Officer
1. An appropriate system solution (for example a database) that accurately reflects the Council's organisation structure and includes details of all employees with Council e mail addresses should be identified and implemented; 2. The content of the system should be structured to enable analysis of employees at Directorate; Service; and relevant group levels (for example Elected Members; localities; executive assistants) to support future identification of employee groups for targeted ongoing cyber security training and future phishing simulation testing;	1. to 4 Neil Dumbleton, Enterprise Architect with support from Katy Miller, Head of Human Resources.

3. An appropriate owner for the system will be established; and 4. Change management processes (linked to employee changes such as new starts; leavers; and movements within the Council) will be established and implemented to ensure that employee data is completely and accurately maintained.	
Agreed Management Action	**Estimated Implementation Date**
The iTrent system (owned by HR) holds details of the organisational structure and the location and reporting lines all for all permanent and fixed term employees. It also has the capacity to record e mail addresses, however this functionality is not consistently used at present. The iTrent system will therefore be used to provide employee data for future phishing simulations once the following actions have been completed. 1. An automated download of all permanent and fixed term employee e mail addresses will be extracted from active directory and uploaded into the iTrent system; 2. Appropriate reconciliations and checks will be performed to ensure that the data has transferred completely and accurately; 3. A process will be established to ensure that e mail addresses for all new employees is automatically uploaded into iTrent monthly, with appropriate reciliations and checks performed on the data; and 4. A process will be established and tested to confirm that e mail addresses for all agency employees can be provided to support future phishing simulations. As agency employee data is not recorded in the iTrent system, details of agency employees and contractors, their e mail addressed will be extracted from the active directory application which is used to populate the global address list (GAL). As line managers are responsible for ensuring that details provided to establish agency / contractor e mail accounts are complete and accurate, and updated to reflect any movement within the Council, there is a risk that the data used to support phishing simulations may not fully complete and accurate.	29 March 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 – Simulated Phishing e mails

1. G Vouchers

From: G-Vouchers Deals [mailto:deals@goupon-vouchers.co.uk]
Sent: 18 January 2018 10:36
To: City of Edinburgh Council Employee
Subject: Best Of This Week! Up to 60% Off Toys and Electronics!

G-VOUCHERS

OUR TOP 5 OFFERS YOU'VE MISSED THIS WEEK
SHOP NOW

Sphero Star Wars BB-8 with Droid Trainer

~~£130~~ £78 View Deal

Samsung Gear S2 Classic Smartwatch

~~£349~~ £140 View Deal

PS4 1TB Star Wars Battlefront 2 Deluxe Bundle

~~£280~~ £120 View Deal

Bose QuietComfort 35 Wireless Headphones 2

~~£330~~ £148 View Deal

Amazon Echo 2nd Generation

~~£70~~ £40 View Deal

Need help? Have feedback? Feel free to contact us.

You are receiving this email because The City of Edinburgh Council is signed up to receive exclusive dicounts from G-Vouchers.
If you prefer not to receive future G-Vouchers emails of this type, you can always unsubscribe with one click.
If you'd like to manage your other subscriptions, click here.

© 2017 G-Vouchers International Limited operation centre: Ocean House, 15 Moon Ln, London, EC4N 1TR

2. Secure Courier

From: Secure Courier Co. [mailto:yourdelivery@data-scout.co.uk]
Sent: 18 January 2018 10:34
To: City of Edinburgh Council Employee
Subject: ACTION REQUIRED: Package delivery failed

Dear XXXX,

Subject: Delivery Status Changed
Date: March 20, 2017

Your package could not be delivered by our courier service.

REASON: INVALID POSTCODE
PARCEL #: 541874072
SHIPPING SERVICE: PRIORITY MAIL
BOX SIZE: XL

To reschedule a delivery, please ***click here.***

Thank you for using our services.

Kind Regards,
The Secure Courier Co. team

This is an automated reply, so please do not reply to this mailing address.

This message may contain confidential information. If you are not the intended recipient please inform the sender that you have received the message in error before deleting it. Please do not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents, To do so is strictly prohibited and may be unlawful.Thank you for your co-operation.

Secure Courier Co. is the leading secure couriser service promoting sustainable solutions and independent edge delivery management solutions for the rapid despatch market. Secure Courier Co. is is approved for exchanging customer data within Secure Courier Co. to monitor parcel status. For more information and to find out how you can switch, visit http://www.secure-courier.co.uk

This email has been checked for viruses. However, Secure Courier Co. and its constituent companies cannot accept responsibility for loss or damages arising from the use of this email or attachments and we recommend that you subject these to your virus checking procedures prior to use.

3. Freedom of Information

From: FOI Admin [mailto:foi-requests@edinbrgh.org.uk]
Sent: 18 January 2018 11:13
To: City of Edinburgh Council Employee
Subject: [Action Required]: FOI Request

Request Assignment Form

The summary below provides details of an **FOISA** request for information that has been allocated to your service area for action. Please treat with high importance as statutory timescales apply.

Stage 1:- Please consider the requests and questions listed below and respond to the Information Rights Officer within 5 days of receipt of this request.

Stage 2:- Please respond by providing the requested information to the Information Rights Officer by no later than day 15.

Request summary

Cost, health and safety.

Please reply to this email with each section completed.

Please return authorised by DATE HERE
Finance team have advised this should be assigned to Health and Safety

Please can you provide me with the total number and total cost of equipment (furniture, computer and other aids) purchased in 2016, to make reasonable adjustments required by the Equality Act 2010.

Stage 1

Request assessment

Each request has to be initially assessed. This will help your service area deal with the request more effectively, and ensure that the Council can meet its statutory obligations under compliance legislation.

Please consider the points listed below and respond to the Information Rights Officer within 5 days of receipt of this request.

1. To ensure that statutory timescales can be met, it is important that information requests are assigned to the correct service area. Can you confirm that you hold the requested information in whole or in part? If in part or no, please suggest areas where the information may be held. If your response is that no information is held which would fulfil this request in whole or in part please record below.

2. Under FOI legislation we can seek clarification and further details if we are not clear about what is being asked for (e.g. date range). Please indicate if you require further clarification?

Stage 2

After responding, please continue to collate the requested information, unless instructed otherwise by the Information Rights Officer. **Please return requested information to the Information Rights Officer by no later than day 15.**

If you do not respond, we will assume that the requested information will be provided in full and returned to the Information Rights Officer by no later than day 15.

When providing the requested information, it would be helpful if you could provide an estimate of the total time taken to deal with the request. This will be used for performance and monitoring purposes.

Appendix 3 – Sample of Employees Targeted

Area	Sample Selected	Scenario
Corporate Leadership Team	4	FOI Request
CLT Support	5	FOI Request
Heads of Service / Locality Managers	7	FOI Request
Heads of Service Support	5	FOI Request
Teaching and Learning	1,198	G Vouchers
Teaching and Learning	1,199	Secure Courier – Failed Delivery
Other Employees	1,799	G Vouchers
Other Employees	1,800	Secure Courier – Failed Delivery
Totals	6,017	

The City of Edinburgh Council
Internal Audit

CGI Contract Management – Programme Management

Final Report

6 July 2018

ICT1702

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 are 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

CGI is the City of Edinburgh Council's (the Council's) strategic technology service provider to whom the Council has outsourced operational management and delivery of its key ICT systems and infrastructure.

The Council's ICT vision is to deliver technology solutions that are based on understanding and responding to customer needs. The ICT & Digital (ICT&D) transformation programme (the Programme) is therefore aligned with the Council's strategic objectives and comprises a number of significant transformational technology projects designed to deliver the vision, and circa 500 smaller projects and change requests. The Council is fully dependent on CGI as their technology partner to deliver the Programme.

Since the contract commenced in 2015, CGI has underperformed on agreed contractual commitments. Transformation projects have often missed the original delivery dates, and, in some cases, the revised delivery date. This has meant that the Council has been unable to realise the benefits and/or savings envisaged.

As a result of performance issues experienced, the Council has escalated the situation to CGI Senior Management, and the Council's Governance, Risk, and Best Value Committee and, in January 2018, the framework governing management of the CGI relationship and their delivery of the Programme was refreshed.

At the time that this review commenced (April 2018), the Council and CGI had been developing improved programme monitoring governance processes for 3 months and ICT management had advised that governance practices had improved.

A review of Project and Programme Management and Benefits Realisation was completed in January 2018, and raised a High rated finding in relation to programme management. The agreed management response included an action to implement and embed standard programme management standards and processes, including RAID management and reporting across the Council's Portfolio of Change.

Management has advised that Programme reporting (including the risks; issues; and dependencies or RAID log) is consolidated with progress reporting for each of the projects included in the Council's Portfolio of Change, and forms part of the ongoing reporting provided to the Council's Change Board.

Scope

Given the criticality of Programme delivery for the Council, this review was scoped to assess the adequacy of the design of the Council's refreshed governance model in place to oversee CGI Programme delivery during the period January – March 2018, during April 2018.

Scope Limitations

Note that scope was limited as follows:

1. only the governance processes in place to monitor CGIs delivery of the transformation programme were included, other aspects of CGIs project management and service delivery were excluded from scope; and
2. due to the short timeframe under review and the ongoing development of governance processes and controls in place, this review was limited to an assessment of the design of governance controls. It was not possible to test their operating effectiveness.

To the extent that documentation for individual projects was reviewed in relation to the governance processes described, this review targeted the following 2 projects selected based on their stage of completion and stakeholder group impacts:

- Customer Transformation; and
- End User Computing.

2. Executive summary

Total number of findings

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

Summary of findings

Our review confirmed that the Council's refreshed governance model established to enable oversight of CGI Programme delivery is generally well designed with some moderate control gaps. Consequently, two medium and one low rated finding has been raised.

This outcome reflects the governance improvements implemented in the first quarter of 2018; management's awareness of the gaps in the design of the governance framework, and the ongoing need for improvement; and the significant level of effort in early 2018 to improve the relationship between the Council and CGI. Specifically:

- Senior CGI staff assigned to the Programme have changed entirely in 2018 following escalations to the CGI CEO at the end of 2017;
- CGI performance issues have been escalated by senior management to the Council's Governance, Risk and Best Value Committee;
- a 3 day off-site Council and CGI working group was held at the end of April, resulting in a number of agreed collaborative actions for change;
- ICT has improved the escalation process with additional fortnightly programme status and fortnightly risk review meetings to focus on some of the detail that is causing delays and poor quality deliverables; and
- ICT have worked with CGI to improve the quality of governance documentation through improved templates and quality review activities.

The need to further improve the recently refreshed CGI governance model is reflected in our first Medium finding, which identifies the need to clearly define how the model will operate, and the requirement to set expectations regarding the quality and timeliness of documentation to be provided by CGI to governance forums. There is also opportunity to move towards a more effective partnership working model via co location (where possible).

Our second Medium finding highlights the need to ensure that all relevant Council employees have access to update the ICT and Digital programme (the Programme) risks, issues and dependencies (RAID) log maintained by CGI, and that CGI are clear on the Council's expectations regarding its completeness and quality.

The content of the RAID log should also be improved to provide a more holistic view of risks, issues and dependencies across the Programme, providing the Council's Change Board with a clearer view of their potential impact across the entire Portfolio of Change.

We also noted a general lack of reporting to governance on benefits realisation. As this has already been raised in our review of Project and Programme Management and Benefits Realisation, completed in January 2018, it has not been raised again.

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

3. Detailed findings

1. Joint governance model

Finding

Whilst the Programme governance reset has been beneficial and successful with a clear governance structure defined supported by good quality terms of reference, we have identified the following areas where further improvement is required:

Operating model definition and documentation

There is a written, mutual understanding of the combined CEC and CGI operating model (as documented in the Operational Framework Document), however, details in the governance section of the document are sparse.

During the review we noted the following ambiguities in the current governance process:

- lack of clarity on the process for collating and reporting Programme risks to governance committees;
- ICT staff performing quality review tasks that we would anticipate CGI would perform internally – e.g. relating to risk documentation, report preparation, dashboard template design; and
- a plan to bolster PMO capability within the ICT team where this is a service provided by CGI.

Quality of Governance Documentation *(note that these issues are self-identified by ICT)*

- papers are not always submitted by CGI on the agreed mailing date which undermines the effectiveness of the process as there is insufficient time for ICT to review the papers in advance of scheduled meeting dates;
- the Programme dashboard presented at the Programme Board is not a holistic view of the Programme, but a compilation of several project dashboards. This does not enable the Board to focus on the overall effectiveness and status of transformation including interdependencies between projects. Additionally, the quality of the RAID log taken to this Board should also be improved (as per finding 2 in this report)
- the Programme Board is a one hour meeting which does not provide sufficient time to review all of the transformation work in progress; and
- the Partnership Board reviews a report that is one month old i.e. the details discussed are not current but are statuses as at one month prior.

Business Implication	Finding Rating
• Potential duplication of effort; additional costs; and lack of clarity re roles and responsibilities; • effectiveness of programme delivery could be adversely impacted if governance processes do not operate effectively; and • the Council's ability to deliver transformation is not optimised.	Medium

Action plans

Recommendations	Responsible Officer
1. The revised governance operating model should be fully documented and agreed with CGI. The model should cover committee operating rhythms; roles and responsibilities of key staff; PMO responsibilities and	Derek Masson, Programme and Delivery Manager, ICT Solutions

deliverables; detailed governance processes; risk reporting and benefit monitoring; and the requirement to regularly review and refresh terms of reference and meeting schedules for the governance bodies; 2. A more relevant cut off date should be agreed for papers to be presented to governance committees; 3. Sufficient time should be afforded to Programme Board meetings to allow for full review, discussion, and challenge on the papers provided by CGI; and 4. Information should be presented at a Programme level in dashboard form, providing a holistic view across the Programme, to enable effective review, challenge and escalation where appropriate.	
Agreed Management Action	**Estimated Implementation Date**
1. Recommendation agreed. In partnership with CGI, the existing Governance Operational Framework document will be expanded to include detailed coverage of the areas highlighted above;	31 October 2018
2. Recommendation agreed. A governance papers receipt tracker will be created, with any issues arising reported to the Partnership Board. Reporting packs are produced as at relevant month end, however, an addendum will be created to cover any significant updates relevant to the interim period between month end and the required date of the governance papers submission;	31 October 2018 (Commencing as per September month end reporting pack.)
3. Recommendation agreed. The duration of the Programme Board meetings will be extended to two hours; and	31 August 2018
4. Recommendation agreed. Programme Governance reporting will be presented to the Programme Board in a dashboard format.	31 October 2018

2. Completeness and quality of Programme RAID log

Finding

Programme risks, issues, and dependencies are recorded in and reported from the CGI risk management system (RiskIT) by CGI project teams. Council staff do not have access to this system, and are secondary users of Excel excerpts generated from RiskIT provided by CGI. Consequently, Council employees are unable to contribute directly to a single source RAID log for the Programme

The RAID log provided by CGI, is a compilation of individual CGI project level technology RAID logs, with no clear evidence of programme level RAID entries or RAID entries which are non-technology items. The resulting output is, therefore, not a holistic CGI Transformation Programme RAID log.

The ICT team has identified a need to improve the quality of CGI RAID documentation to enable better understanding and communication between CGI; ICT; Council project teams and effective reporting to governance committees.

Our review of RAID logs dated March 2018, supports this view and identified the following issues with the RAID log content:

- poorly defined / ambiguous language;
- lack of explicit response - i.e. treat, accept, avoid or monitor;

- lack of clear actions with deadlines; and
- inconsistencies in the quality and type of information captured

CGI is the owner of the Programme RAID log and is responsible for quality of documentation. The Council does have a responsibility, however, to ensure that the content is of sufficient quality to enable effective reporting, monitoring and decision making.

ICT has implemented a fortnightly risk review meeting, providing a dedicated forum for ICT and CGI to review RAID logs together. However, improved quality at source is still something that CGI and CEC should work on.

Business Implication	Finding Rating
• The RAID log is incomplete; • No holistic view of risks; assumptions; issues and dependencies across the Programme, and lack of understanding of the content of the RAID log and any potential impact on project / Programme delivery; and • Risk of incomplete or inaccurate reporting to the Council's Change Board.	Medium

Action plans

Recommendation	Responsible Officer
1. All CGI and Council project and programme management employees should have access to and be able to contribute to one single consolidated Technology Transformation Programme RAID log; 2. An agreed format for the structure of the RAID log and quality of content should be agreed between the Council and CGI. If possible, the structure of the RAID log should be aligned with the RAID log produced for the Council's Portfolio of Change; 3. ICT should provide robust ongoing challenge re the quality of RAID documentation, and where this isn't of sufficient quality, should request review and revision by CGI; and 4. ICT should liaise with the Council's Strategic Change and Delivery Team to ensure that the refreshed ICT & Digital Programme RAID documentation is fully aligned with existing RAID reporting across the Council's Portfolio of Change, supporting ongoing consolidation of RAID reporting for presentation to the Council's Change Board.	Derek Masson, Programme and Delivery Manager, ICT Solutions
Agreed Management Action	**Estimated Implementation Date**
1. Recommendation agreed. The option for all CGI and Council project and programme management employees to be granted access to RiskIT, for the purposes of contributing to a single Programme RAID log will be explored. Failing this, an alternative means will be found to satisfy the requirements of the recommendation. 2. Recommendation agreed. Agreement will be reached between CGI and the Council on the structure and required content quality of the Programme RAID log. This will be recorded in a document which will also include risk parameter definitions and be approved by the Programme Board.	All actions to be completed by 31 October 2018.

3. Recommendation agreed. Ongoing challenge regarding the quality of the Programme RAID log will be facilitated at the bi-weekly Programme Risk meetings, with appropriate escalation to the Programme Board if required. 4. Recommendation agreed. ICT Solutions will liaise with the Council’s Strategic Change and Delivery Team with a view to ensuring the RAID reporting across the Technology Transformation Programme is fully aligned with existing RAID reporting across the Council’s Portfolio of Change.	

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

To: Stephen Moir, Executive Director, Resources
Bruce Strang, Chief Information Officer

From: Lesley Newdall, Chief Internal Auditor   Date: 19th March 2018

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

Background

CGI are the City of Edinburgh Council's (the Council's) strategic technology service provider and the Council have outsourced operational management and delivery of its key ICT systems and infrastructure to CGI.

The Council's ICT vision is to deliver technology solutions that are based on understanding and responding to customer needs. The ICT & Digital (ICT&D) transformation programme (the Programme) is therefore aligned with the Council's strategic objectives and comprises a number of significant transformational technology projects designed to deliver the vision, and circa 500 smaller projects and change requests. The Council is fully dependent on CGI as their technology partner to deliver the transformation programme.

Since the contract commenced, CGI have underperformed on agreed contractual commitments. Transformation projects have often missed the original delivery dates, and, in some cases, the revised delivery date and this has meant that the Council has been unable to realise the benefits and/or savings envisaged. As a result of performance issues experienced, the Council has escalated the situation to CGI Senior Management, and the Council's Governance, Risk, and Best Value Committee and, in January 2018, the framework governing management of the CGI relationship and their delivery of the Programme was refreshed.

Scope

Given the criticality of the Council's ability to deliver the Programme, this audit has been scoped to assess the effectiveness of the Council's approach to managing the contractual relationship with CGI, with specific focus on the Council's refreshed governance model and processes that facilitate oversight of the CGI Programme delivery.

To the extent that documentation for individual projects requires to be reviewed in relation to the governance processes described, this review will be targeted at the following 3 projects selected based on their stage of completion and stakeholder group impacts:

- Barclay Card;
- Customer Transformation; and
- End User Computing.

Limitations of Scope

- Interviews and follow up meetings with stakeholders will be limited to those we determine to be key or where we require further information to clarify processes and controls; and

- Only those processes, controls and activities within the control of the Council are included in scope. We will not review or comment on processes, controls or activities that are owned by CGI.

Approach

Our review will involve:

1. Desktop review of governance framework documents;
2. Discussion with the ICT management team and project stakeholders to understand the operation of the new governance framework across the Programme and individual projects; and
3. Review of Programme and project documentation that supports operation of the governance framework.

Sub-process	Focus Area
Programme governance	We will: • Review the new CGI governance framework applied by the Council and CGI with focus on oversight of CGI programme delivery; • Assess how the governance framework is designed to identify and escalate risks, issues, and dependencies in CGI's Programme delivery; • Determine that governance arrangements specify clear roles and responsibilities at all levels for both the Council and CGI and allows for effective and timely decision making throughout the duration of the Programme; and • Obtain and review a sample of key documents to confirm that the Programme governance framework is effectively and consistently applied.
Project Costs	We will: • Consider how the governance framework ensures that costs associated with change requests are either covered by the output based specification (OBS) aspect of the CGI contract, or should be separately costed on a commercial basis; • Confirm that the governance framework includes monitoring of CGI costs across the programme; • Sample test costs associated with the three technology projects in scope to confirm that all additional costs in relation to CGI deliverables have been reviewed and approved by the Council; and • Verify that there is an audit trail from the additional billed costs sampled (above) to approved change order or budget variance order.
Risks, Issues and Dependencies	We will: • Obtain and review the Programme risk, issues and dependencies register(s); • Assess how the Council confirms that Programme risks, issues and dependencies are effectively identified; assessed; escalated; managed and mitigated by CGI; • Review the Council's process for monitoring Programme risks, issues and dependencies to ensure they are actioned appropriately prior to closure; and • To validate understanding obtained above, obtain and review risk, issues and dependencies registers for three technology projects and sample test a subset of key risks, issues and dependencies to ensure that they are

	appropriately managed and escalated through both the project and Programme governance structure as required.
Resource planning	We will: • Determine how the Council ensures that CGI has allocated appropriate resources across the Programme and to individual projects; • Review how issues in resource planning and resource utilisation are escalated through governance; and • Test for three technology projects that resource issues have been escalated in line with the governance model.

Internal Audit Team

Name	Role	Contact Details
Lesley Newdall	Chief Internal Auditor	lesley.newdall@edinburgh.gov.uk
Susan Cummings	Senior Auditor Manager	susan.cummings@pwc.com

Key Contacts

Name	Role	Contact Details
Bruce Strang	Chief Information Officer	0131 529 5896 bruce.strang@edinburgh.gov.uk
Neil Dumbleton	Enterprise Architect	0131 529 7837 neil.dumbleton@edinburgh.gov.uk
Jackie Galloway	Commercial Manager	0131 529 7808 jackie.galloway@edinburgh.gov.uk
Derek Masson	Programme and Delivery Manager	07758 073 479 derek.masson@edinburgh.gov.uk
Carolann Miller	Service Manager	0131 469 2868 carolann.miller@edinburgh.gov.uk
Alison Roarty	Commercial Team Lead	0131 469 3476 alison.roarty@edinburgh.gov.uk

Timetable

Fieldwork Start	20th March 2018
Fieldwork Completed*	13th April 2018
Draft report to Auditee**	13th April 2018
Response from Auditee	27th April 2018
Final Report to Auditee	4th May 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 discussions during weeks commencing 3rd April and 9th April.

** Draft report will be in the form or draft findings on 13th April. Draft report will be available on 20th April.

The City of Edinburgh Council

Internal Audit

EIJB1701 – Health and Social Care Partnership Purchasing Budget Management

Final Report

20 July 2018

Contents

This internal audit review is conducted for the Edinburgh Integration Joint Board under the auspices of the rebased 2017/18 internal audit plan approved by the Audit and Risk Committee in December 2017. The review is designed to help the Edinburgh Integration Joint Board 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 Edinburgh Integration Joint Board 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 Edinburgh Integration Joint Board. 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

In April 2014, the Scottish Government enacted new legislation, the Public Bodies (Joint Working) (Scotland) Act 2014 (the Act) that required all Health Boards and Local Authorities in Scotland to integrate their health and social care services for adults.

This resulted in the creation of the Edinburgh Joint Integration Board (EIJB) which is responsible for commissioning; directing; and governing; the activities of the Edinburgh Health and Social Care Partnership (the Partnership). The Partnership comprises NHS Lothian, and the City of Edinburgh Council who work together to deliver health and social care services for adults across the City.

Four localities were established across Edinburgh in May 2017 to enable delivery of Partnership services, with emphasis on anticipatory planning for people's care needs and their long-term support in the community. Each locality is responsible for establishing and managing the resources required to support service delivery, including financial planning and management.

Directions

The Act places an obligation on Integration Joint Boards to issue directions to the Partnership to ensure effective implementation of health and social care strategic plans. To date, the EIJB has issued the following financial directions to the Partnership.

1. **EIJB Direction 2 – Integrated structure** - the City of Edinburgh Council and NHS Lothian are directed to complete the implementation of Phase 2 of the integrated structure; including final assessment of budgetary position and establishment of budgets held on a locality basis; and
2. **EIJB Direction 3 – Key processes**
   - (b) redesign the referral process including the integration of Social Care Direct; and
   - (f) review and simplify the Funding Allocation System used to calculate indicative budgets

Partnership Budget

The total Partnership budget for 2017/18 was £500M (2016/17 £676M). Of this, the total budget for social care services was £239M (2016/17 £190M), with the purchasing budget set at £148M (2016/17 £143M).

Social care services are predominantly delivered by the Council, with an approved purchasing budget for these services agreed at the start of each financial year. The main drivers of purchasing budget spend are:

- In house services – provision of in house services by the Partnership by CEC and NHS employees;
- Care at Home Contracts – provision of services with 3rd party suppliers to provide home care services;
- Block – provision of service via 3rd party suppliers with contracts based on pre-agreed volumes;
- Individual Service Funds (ISFs) – value of the care package is paid to a provider chosen by the client who then agrees with the provider how the care will be delivered;
- Direct Payments (DPs) – direct payment made to client who then arranges their own support; and
- Spot – spot purchasing of home care services from external 3rd parties when required.

Service Delivery and Technology Systems

The Partnership is supported in social care service delivery by a number of established Council teams, for example; Business Support; Transactions; ICT Solutions; and Strategy and Insight. A full list of the teams contacted during the course of our audit review is included at Appendix 3 – Partnership Support Teams.

The Partnership manages and records delivery of social care on Swift, an established Council care management database introduced in April 2006. All client information (for example assessment and personal support plans information) is recorded on Swift via the AIS (Adults Integrated Solutions) front end application. Swift also records financial data in relation to client financial assessments and external provider charges, and generates care payments and charges via an Oracle payment system interface. The system also supports service delivery planning and ongoing performance reporting.

Client assessment information is also maintained on the NHS 'TRAK' Patient Database, whilst the NHS 'Hospital Dashboard – Tableau' system is used to monitor hospital discharges where subsequent social care support may be required.

Scope

This review was added to the 2017/18 EIJB internal audit plan following identification of a forecast overspend on the Partnership's home care purchasing budget of £12m for the 2017/18 financial year as at 31 August 2017. Initial analysis performed by finance confirmed that this appeared to be driven by increased demand for services and failure to deliver approved savings under the Health and Social Care Transformation Programme.

Our review assessed the adequacy and effectiveness of controls established across the Partnership to support service delivery by the Localities and demand management in line with approved financial budgets. Our full terms of reference are included at Appendix 5.

A separate review of Social Care Commissioning has been completed as part of the EIJB 2017/18 Internal Audit plan.

2. Executive summary

Total number of findings

Critical	-
High	4
Medium	-
Low	-
Advisory	-
Total	**4**

Summary of findings

The forecast overspend on the Partnership's home care purchasing budget (£12M at 31 August 2017) has been addressed by obtaining £4.2M of recurring funding from the social care fund, and an additional one-off contribution of circa £7m from the Council.

Whilst this additional funding resolves the Partnership's 2017/18 budget position, it does not address the underlying root causes that contributed to the overspend. Council Finance senior management has advised that the Partnership has not achieved social care service delivery in line with agreed budgets since 2014/15, and attribute this to lack of strategic action to offset increasing ISF / DP growth (£16.6M in 2015/16 and £25.5M in 2017/18) and care at home demand; inability to deliver approved budget savings; and lack of implementation of both internal and external audit recommendations on both business and financial controls.

Our review has confirmed that Partnership management has not delivered against the financial directions (2 and 3) issued by the EIJB to the partnership organisations (the Council and NHSL), and identified four areas where significant and systemic operational and financial control weaknesses have adversely impacted upon purchasing budget spend. Consequently, four High rated findings have been raised.

Whilst noting that delivery against financial direction has not been achieved, it is acknowledged that the Partnership has been impacted by significant changes at senior management level, with three changes at Chief Officer level in the last year. A new senior management team has now been appointed and will focus on reviewing the current operational arrangements supporting service delivery.

The first High rated finding notes that as the Partnership's operating structure had not been finalised, financial budgets (including the locality purchasing budget) had not been devolved / allocated across the localities (as at December 2017), and that the client and cost data maintained in Swift was not aligned with the localities operating model. As a result, the Partnership has not yet met the requirements of the second EIJB direction (Integrated Structure), which required the establishment of locality budgets, and locality managers have been unable to effectively manage locality purchasing costs and budgets.

Management has advised that a 'purchasing realignment group' has been established and is working towards allocation of Partnership budgets across the localities.

Our second finding notes that there is currently no funding allocation model used across the Partnership as required by the third EIJB direction (Key Processes – part f). resulting in non-compliance with the requirements of the Social Care (Self-directed Support) (Scotland) Act 2013, as the range of care options prescribed by the Act cannot be accurately costed to support client choices. This issue was raised as a High rated finding in our Self-directed Support Option 3 review completed in August 2016, and has not yet been resolved.

This finding also reflects weaknesses in the design of financial controls that should be applied end to end processes to ensure that care packages are accurately and consistently costed with variances appropriately approved; care payments are stopped upon cessation of the service; and that all charges for additional services are completely and accurately applied. This finding also highlights a lack of controls within the Swift system enabling care costs to be overwritten, and a lack of segregation of duties when processing Individual Service fund and Direct Payment payments that should be immediately addressed.

The scale and complexity of the operational structure and lack of understanding of holistic processes, responsibilities, and accountabilities of the teams supporting delivery of social care is reflected in our third finding. This finding highlights that end to end procedures supporting service delivery have not been established; the significant number of hand offs between teams involved; and high volumes of manual workarounds applied.

The need to implement a framework to support contract and grant management across the Partnership, with focus on improving controls supporting ongoing supplier and contract management is reflected in our fourth finding. Our main concerns here are that there are no clearly established delegated authorities supporting issue of contracts; contracts are currently being issued in the name of a former employee; contracts are not consistently priced; there is no clearly defined operational guidance supporting use of spot contracts; and no monitoring performed to confirm that the volume and cost of spot contracts is reasonable. Management has advised that a new Partnership contracts manager has recently been appointed who will be responsible for progressing work in these areas.

Effective financial and budget management is also an important element of commissioning, as budgets generally constrain capacity to deliver services. A separate review of social care commissioning (EIJB1702) was completed in June 2018, and the outcomes reported separately. The findings raised in the commissioning review in relation to maturity of social care commissioning; management capacity; and the need for clarity on roles and responsibilities should be considered in the context of addressing the findings raised in this report.

Management Response

Whilst Partnership and Customer senior management recognise the need to address the financial control weaknesses identified, a wider review of both strategic (for example options in relation to Swift) and current operational service delivery arrangements is required, with appropriate project management resource and capacity to support this process.

In the interim, a Partnership working group will be established / existing working groups refreshed. This group will include Partnership senior management and representation from Finance; Customer; ICT; and Strategy and Insight. The group will ensure that these findings are included in the wider service delivery review, and incorporated into an overarching plan that focuses on delivery of strategic and operational service delivery solutions, with initial focus on addressing the supplier and contract management issued raised in Finding 4.

The Partnership working group will be established by the Chief Finance Officer by **28 September 2018** and the plan produced by **21 December 2018**. The plan will then be reviewed by IA to confirm that it addresses all findings raised in this report, and individual IA findings raised to support subsequent IA follow-up to ensure that the control gaps identified have been effectively addressed.

In the interim, control gaps that expose the Partnership to significant financial risk, or gaps that can be remediated in the short to medium term will be addressed. Management responses in relation to these and agreed implementation dates are included in the detailed findings at Section 3 below.

3. Detailed findings

1. Purchasing Budget Allocation

Findings

Whilst an overall Partnership purchasing budget has been established, the budget had not been appropriately devolved / allocated across the localities as at December 2017. Additionally, care package cost data maintained on the Swift system is not aligned with the localities operating model, and no locality financial management information is currently available.

Locality Management has advised that they are aware of these issues.

Finance senior management confirmed that a draft report was presented to the Partnership senior management team in April highlighting the need for alignment of financial budgets; income and cost centres with the localities operating model. The draft report notes that this exercise is a significant undertaking as it requires amendments to the general ledger; Swift; and other core financial systems.

We understand that a ‘purchasing realignment group’ has been established to resolve allocation of budgets across the localities.

Business Implication	Finding Rating
• Failure to deliver against EIJB direction 2, which requires that budgets should be established and maintained on a locality basis; and • Locality managers are unable to monitor actual in comparison to planned spend for their localities; and • Budget overspends are not identified in a timely manner.	High

Action plans

Recommendation	Responsible Officer
1. A detailed financial budget allocation delivery plan should be developed with defined timescales for each stage of the implementation of the locality operating model budgets. 2. A consistently applied budget monitoring process should be clearly defined, documented, implemented, and communicated to all budget managers within the Locality operating model; with training provided to budget managers on how budgets should be managed. 3. The budget monitoring process should include, but not be restricted to: • Agreement on how overspends should be managed against increasing demand for services; • Responsibility for ongoing oversight of locality budgets and upward reporting to relevant governance forums / committees; and 4. A detailed plan should be developed and implemented, to ensure that the Swift system is updated so that H&SC Swift system care costs and recharges are aligned with and set against the relevant locality budgets.	Chief Finance Officer

Agreed Management Action	Estimated Implementation Date
These recommendations will be addressed within scope of the strategic management action detailed in the Executive Summary at Section 2.	

2. Financial Controls

Findings

Our review identified a number of significant financial control gaps across the teams supporting delivery of social care by the Partnership, and the processes they apply:

1) Funding allocation model

There is currently no funding allocation model established within the Partnership to ensure that budgets for packages of care are established and monitored based on an ongoing assessment of client needs.

Additionally, there is no evidence to confirm that each of the self-directed support options have been fully discussed with clients, and that they are given the opportunity to choose from the available self-directed support options.

This issue was raised as a High rated finding in our Self-directed Support Option 3 ‘Communication of the budget’ review completed in August 2016, and has not yet been resolved.

2) Delegated financial authorities

No clear delegated financial authorities have been established for approval of the cost of care packages or spot purchase contracts.

Our review established that a number of interim financial guidance documents have been issued, and that there is a lack of clarity re the actual authorisation limits that should be applied. Further details of the guidance that has been issued is included at Appendix 2 .

Additionally, the Service Matching Unit (SMU) is processing packages of care initiated by hospital occupational therapists with no independent approval of costs by localities. It was not possible to identify the total volume and costs of these care packages, as it is understood that there is no unique identifier allocated to these cases to confirm their source.

Review of approval of personal support plans for a sample of 20 Individual Service Fund (ISF) and Direct Payment (DP) cases in comparison to the approval limits included within interim financial approval process and the national care home nursing care rate (included within the two documents provided by management as being the current authorisation limits applied as detailed within appendix 2) identified:

- at least five cases that were not appropriately approved within the specified limits; and
- a further four cases where the personal support plan was signed off by either a Hub or Cluster Manager where the cost of care exceeded the £2K per week limit specified. We were unable to confirm whether additional levels of authorisation were required for these costs, as this was not detailed in the interim procedures.

3) Charging Policy / Procedures

Charging policies to support consistent and accurate pricing and charging of social care services provided to clients in addition to their assessed needs have not been finalised. Whilst the Transaction Team confirmed draft charging procedures have been prepared, Partnership Senior Management has confirmed that there is currently no owner of charging policies and procedures,

Information regarding paying for care and the financial assessment process is available on the Council’s external website at Care and Support at Home, however we could not establish who owns this web content and whether the charges specified are accurate. The details provided are not aligned with the information published on the Orb (refer: receiving care and support at home guidance dated 2013-14 which specifies a rate for £12.50 per hour for any chargeable services.

We did confirm that client charges are being applied on Swift, however, the completeness and accuracy of charges applied could not be confirmed due to lack of an established charging policy detailing the costs to be applied for additional services.

In addition; the Transactions Team confirmed that if an 'allocated worker' has incorrectly indicated whether an element of the support (to be provided) is chargeable, this results in the client either being billed in error or not at all. The Transactions Team indicated that they are not able to assess the completeness and accuracy of the billing report which is produced from the Swift System.

4) Cessation of and reduction in service

Notification of cessation of and reduction in service is not provided by Social Workers to Business Support in a timely manner, resulting in reliance on external providers to advise of changes in service, and overpayments that must be reclaimed retrospectively from the relevant providers.

All changes should be advised to Business Support by Social Workers via updated case notes on Swift. Notification can also be provided by General Practitioners and hospitals via a share point portal.

This process is not operating effectively partly due to the backlog of locality client reviews and issues regarding the timely update of the SharePoint portal.

Our sample testing identified two overpayments to the value of £14k that had not been reclaimed from external providers.

5) Swift system controls

Standard care cost rates specified in the 'guide to price' owned by the Partnership's contracts team-are not hard coded into the Swift system to ensure consistent costing of care packages. Our review also confirmed that care costs can be manually entered into Swift.

Additionally, there are no established system approval controls to prevent unauthorised creation or cancellation of services; or changes to the nature or cost of existing services.

Review of a sample of 20 provider rates noted on Personal Support Plans (10 ISFs; and 10 DPs) by the allocated Social Worker and approved by their line managers identified a number of differences between rates detailed in the guide to price; the rates recorded in Swift; and the rates noted on the support plans
We have been unable to confirm whether pricing approval controls are available within Swift, and have not been activated.

6) Payment Controls

A number of significant control gaps were identified in relation to the payment processes applied by Business Support and the Social Care Finance Transactions Team that require to be addressed, most notably key person dependency and lack of segregation of duties within the Transactions Team.

Business Support - invoice processing and subsequent payment run

- Significant volumes of queries are raised by Business Support on invoices received from suppliers where they do not include client names or reference numbers, and often include unusual service rates;
- Business Support have only a one hour window to review and process Care at Home invoices on Swift (we understand that this is attributable to a unique one hour window in Swift when invoice headers for Neighbourhood Care at Home Contract Providers can be created - the 'AGEN' hour) impacting their ability to address all invoice queries prior to payment;

- Checks carried out on pre-payment reports are minimal due to transaction volumes and resource constraints; and
- Business support highlighted that a number of providers charged higher rates over the festive period, that were not subject to formal approval.

Individual Service Funds (ISFs) – Transactions Team

- There is lack of segregation of duties and key person dependency associated with ISF payment processing as one employee is solely responsible for updating service details (including payments) on Swift, and the processing; reviewing; and approving the ISF payment run;
- There is no one else within the team with the knowledge and skills to perform these tasks and the responsible (part time) employee currently manages their annual leave to avoid the timing of payment runs;
- The team confirmed that varying rates are being agreed with ISF providers that are not aligned with the 'guide to price' owned by the contracts team;
- Checks carried out on pre-payment reports are minimal due to transaction volumes and resource constraints and
- Retrospective adjustments are required where a change to the nature or cost of the service provided, or a change in level of client contribution is not advised and processed in a timely manner, resulting in inaccurate payments to providers that have to be subsequently adjusted.

Direct Payments – Transactions and Business Support Teams

Direct Payments can either be loaded on to a payment card or paid directly into the client's bank account. A review of client expenditure is performed to ensure that clients appropriately disburse funds to meet their assessed needs.   Review of this process confirmed that:

- the Transactions team experienced difficulty in identifying new DP cases from Swift workflows as social workers use inconsistent narrative to describe the package of care;
- Checks carried out on pre-payment reports by the Transactions team are minimal due to transaction volumes and resource constraints;
- Reviews of quarterly client paper returns by Business Support (for funds paid directly into client bank accounts) to confirm appropriateness of expenditure for clients not using loaded payment were delayed by a quarter;
- There is no clearly defined methodology supporting sample selection and review of client paper returns within Business Support; and
- The Direct Payment reclaim figure for 2017/18 (reclaim of inappropriate expenditure by clients) was £1.5M.

It is understood that the Business Support is in the process of transferring clients who receive funds directly into their bank accounts on to prepaid cards, enabling more effective real time monitoring of client expenditure, and that submission of paper returns for funds paid directly into client accounts are moving from quarterly to six-monthly.

Business Implication	Finding Rating
• Non-compliance with the requirements of the Social Care (Self-directed Support) (Scotland) Act 2013; • Financial decisions are made outwith approved authority levels; • Variations in cost of care are not appropriately authorised; • Income is not maximised • Clients are incorrectly charged for contributions to service provision;	**High**

• Ineffective supplier management and overpayments for services provided; • Inconsistent pricing applied to packages of care; • Packages of care are overpriced; • Potential risk of fraud; • Inaccurate payments; and • Direct Payment reclaims are not processed	
Action plans	
Recommendation	**Responsible Officer**
1) A funding allocation model or alternative solution should be designed and implemented to ensure that clients are provided with details of their budget when considering their options, (as per legislative requirements), with evidence of budget discussion recorded on Swift; 2) Delegated financial authorities should be established and implemented across the Partnership. These will include (but should not be restricted to) responsibility for approval of care package costs originated from all sources; and details of approval for spot purchase contracts. A process should also be established and implemented to ensure that evidence of approval in line with delegated authorities is recorded and retained. An appropriate owner of delegated authorities should be established and timeframes established for their ongoing review and refresh; 3) A charging policy for services provided should be established and implemented across the Partnership. This should specify the charges to be applied for additional services provided. A process should be established to confirm that these charges are consistently applied. Charges currently published on the Council's website and on the Orb should be updated to reflect the revised charging policy, and refreshed in line with ongoing review and refresh of the policy. An appropriate owner of the charging policy should be established and timeframes established for its ongoing review and refresh; 4) A process should be established to ensure that Business Support are advised re cessation of or reduction in services in a timely manner, either by social workers or third party providers; 5) Agreed provider rates should be automatically built into the Swift system. Where the 'alternative cost' field requires to be used, additional authorisation should be obtained in line with agreed delegated authorities. 6) Financial controls available within Swift System should be reviewed and implemented (where feasible) to ensure care costs either cannot be overwritten, or (where they are overwritten) a clear audit trail is available for review. 7) A communication should be sent to all providers specifying that invoices should include client names; reference numbers; and accurate hourly service rates charged;	4) 8 and 10 Neil Jamieson, Senior Manager, Customer 12) John Arthur, Senior Manager, Business Support

8) Appropriate sample based checks should be performed on pre-payment run reports to confirm the completeness and accuracy of invoices processed by all teams responsible for payments; 9) Business Support should escalate any rates applied by providers that are not aligned with agreed rates to management for approval in line with delegated authorities; 10) Key person dependency and segregation of duties issues within the Transactions team should be addressed immediately; 11) A standard process should be established to ensure that Direct Payment cases are clearly recorded on Swift with a unique identifier, enabling the Transactions team to easily identify them for inclusion in payment runs; and 12) A risk based approach should be designed; implemented; and consistently applied to support ongoing review of client paper based returns for Direct payments within the Business Support team, with all instances of inappropriate expenditure escalated for immediate reclaim.	
Agreed Management Action	**Estimated Implementation Date**
1. Management has advised that they will 'risk accept' this recommendation on the basis that the Partnership is compliant with the spirit of SDS legislation as funding is being allocated on the basis of the SDS legislation. There is recognition that the evidence of conversations in relation to allocation of funding should be recorded and this will be addressed as part of the review of the Swift system. 4. Process is in place for Care homes. Providers submit form with returns to identify changes of circumstances which would affect charging levels (e.g. hospitalisation). No further action required. Transactions would expect that service authorisation would be achieved prior to the activity for financial assessment, otherwise the calculation would be inaccurate. This is a requirement of social workers. Actions will be addressed as part of wider strategic recommendation for the Partnership. Early investigations are in place to determine the legitimacy of the charging team sitting within Business Support, and whether it would be more appropriate to bring this service within Transactions. Due to inappropriate data base use by services in the past, some areas (Transactions Community Alarm Team) make it difficult to ascertain eligibility to continued service. Whilst this risk is mitigated by checks and balances, confident adherence will not be in place until this service is processed within SWIFT and linked to all other social services. 8. A quality control framework for sample based checking that is aligned with the process applied to checking benefits payments will be developed (with support from the Quality Control team) and implemented. We will aim for the process to be implemented and operational by 21 December 2018, with a three month period to embed and final closure by 29 March 2019. 10. The Transactions team have recently decided to apply additional resource to support this function immediately. As well as this, the Team Manager and Customer Manager will be looking across the entire team structure to ensure that segregation of duties is addressed sufficient resilience exists by cross training individuals to participate in the process.	1. N/A 4. 31 January 2019 for decision re charging team; and 29 March 2019 for SWIFT replacement 8. 29 March 2019 10. 31 October 2018 12. 28 September 2018 for IA follow-up

12. The backlog has been addressed and the review process changed to review the full population of client returns every 6 months with effect from January 2018. Recommendations 2 – 3; 5 – 7; 9; and 11 will be addressed within scope of the strategic management action detailed in the Executive Summary at Section 2.	

3. Operational structure and processes

Findings

Our review confirmed that a significant number of Council teams are involved in supporting the Partnership with delivery of social care.

No holistic social care processes and supporting operational procedures have been established to ensure effective service delivery. The processes applied within individual teams are often complex, involving use of both Council and NHS systems; involve a significant number of hand offs between teams; and involve high volumes of manual workarounds.

A review of a sample of social care operational processes applied by the teams involved, confirmed that they are performed inconsistently and often without a full understanding of their overall purpose or objective, and that the volume of briefing emails issued detailing changes to procedures causes confusion for the teams performing the processes. Additionally, a number of links to procedural documentation on the Orb are broken, or documents have been removed and not replaced. Further detail is provided below:

1. Locality Processes and Procedures

Draft Hub Standard Operating Procedures were created in December 2017 and have not yet been finalised. These provide a high-level overview of locality service delivery and are not supported by current detailed operational procedures.

2. Service Matching Unit (SMU)

- End to end SMU procedures have not been fully reviewed and refreshed since 2012. The SMU Business manager did provide evidence of standalone procedures and process maps that had been reviewed and revised, however these were unclear, and have not been incorporated into end to end procedural documentation.
- Controls in relation to approval of packages of care by hospital Occupational Therapists (OTs) are unclear. The SMU Business Manager was unaware that there had been a ‘verbal instruction’ received from a locality manager which enabled SMU staff to process all service requests received from occupational therapists without approval. When this issue was identified, the SMU Business Manager issued an instruction to the SMU team limiting the number of hours that could be processed without approval to 18 hours, until the process is clarified.
- Additionally, an inconsistent approach was evident in relation to requests for care received from hospitals, and those received from Social Care Direct (SCD) or social workers, as hospital requests are not supported by a client assessment.

  For hospital requests, SMU issues a memo to the third-party care provider asking them to contact the allocated worker directly if they require further information on client needs. There was also no process documentation evident detailing the process to be applied when sharing personal, sensitive client information with third-party providers.

3. Social Care Direct (SCD)

- The need to review and update SCD processes supporting screening and allocation of care referrals to service areas was highlighted by Internal Audit in October 2015, as processes applied were inconsistent and did not include ‘trigger points’ to ensure that clients remained informed of progress with their cases.

SCD processes have not yet been updated, and an SCD options appraisal (being completed by Strategy and Insight); that would improve how referrals are received, recorded, and responded to across the localities is understood to be ‘ongoing’.

Additionally, existing SCD processes have been criticised by the Care Inspectorate and a number of issues were highlighted within the internal Partnership quality assurance report in December 2017.

- Our review also established instances where SCD are copying and pasting client information received from hospitals into the Swift system / Assessment of Needs Forms;

4. Client Review Process

There is currently a significant backlog of client reviews to be completed across the localities; and completed reviews are not recorded consistently on Swift to support a clear audit trail between the review and subsequent changes to the nature and cost of care. Specifically:

- The ‘Adult Care Service Reviews’ procedure was last updated in December 2015. The procedure notes that the outcomes of the reviews would recorded in the ‘My Steps to Support Review Tool’ on the Swift / AIS system or in a Case note titled ‘Review Outcome’ for ease of identification; and
- There was evidence supporting completion of client reviews in Swift, however, the outcomes and decisions are not always consistently recorded in the Outcomes’ and ‘Decisions’ tabs within the system. Some review outcomes were included within case notes; however, these outcomes /decisions were not always clear due to the volume of information included within the case notes.

5. Technology Issues

A number of the social care process require creation of documents such as the Assessment of Needs through a mail merge function within the Swift system. This functionality does not work with Microsoft 2016, resulting in employees reverting to Microsoft 2013 to generate these documents. CGI has advised that this is unsustainable as Microsoft 2013 will become unsupported. No detailed timeframes have been confirmed.

Business Implication	Finding Rating
• End to end processes supporting service delivery risks are not clearly understood and are not effectively managed; • Poor quality service for clients; • For care requests received from hospitals, providers may not fully understand the needs of the client and client needs may not be met; • Clients are not effectively matched with the most appropriate service provider; • Incorrect client data is copied into the Swift system and populated in Assessment of Needs Forms; • Potential breach of General Data Protection Requirements (effective 25 May 2018) if there is no established process supporting provision of client information to third parties in a secure and compliant manner; • Review outcomes are not identified and required changes in levels of care not communicated to care providers and associated costs revised; • There is no clear link from assessments through to revised personal support plans; changes in care provided; and the associated cost;	**High**

• Current processes supporting generation of key documents via the mail merge process are unsustainable.	
Action plans	
Recommendation	**Responsible Officer**
1) A review of holistic social care processes should be performed from point of origination / referral to ongoing review and payment processes; and new processes designed and implemented. These processes should include (but not be restricted to) responsibilities and accountabilities and hand offs between the teams involved. Key controls and checks to be performed to confirm that service delivery is consistently recorded in Swift, costed, and processed completely and accurately should also be included in process documents; 2) The process for recording client reviews in Swift should be specifically documented; implemented and consistently applied; and 3) ICT should be formally engaged to ensure that an alternative solution is found for the generation of key client documents via Swift; prior to support for Microsoft 2013 being removed.	
Agreed Management Action	**Estimated Implementation Date**
These recommendations will be addressed within scope of the strategic management action detailed in the Executive Summary at Section 2.	

4. Supplier and Contract Management

Findings

A number of significant and systemic control weaknesses have been identified in relation to supplier and contract management where third-party providers are used to provide social care services.

1. Contract Authorisation

The register of 'Proper Officers' held by the Council's Committee Services Team has not been updated to reflect the Partnerships delegated authority for signing contracts under the Council's Scheme of Delegation. A number of contracts continue to be issued with manual signatures, and it is unclear whether these signatories have the required authority.

Additionally, a significant number of contracts (mainly Care at Home Contracts) are being issued with the electronic signature of a former employee. This issue was immediately escalated to the Interim Chief Officer when identified (5 January 2018) and has not yet been fully resolved. Appendix 4 – Timeline – Electronic Signatures includes details of the issue and progress and actions implemented to date.

2. Contracts Team

The Partnership contracts team is responsible for procurement; agreeing rates with on contract and spot service providers; monitoring supplier performance; and also own the 'guide to price' which specifies the cost of services provided.

Review of the contracts team established that:

- they currently have no established operational processes and procedures;

- no clear approval and change management process has been established to support changes to the cost of services detailed in the guide to price. The rates included on the Orb are noted as April 2018 rates, however there is no clear audit trail supporting how these costs were established and approved;
- the 'guide to price' is not aligned with the service costs included in the Swift system;
- there is no defined ownership of and review of agreed third party supplier rates charged for cost of care, and no established maximum limits for off contract 'spot' purchases;
- no monitoring is performed on Individual Service Fund (ISF) care providers to ensure that clients are receiving the expected level of care. Effective monitoring of ISFs was raised as a High rated finding in the Personalisation and SDS (Self-Directed Support) – Stage 3 audit report issued in June 2015.
- Quarterly returns are received from ISF providers detailing how funds received have been disbursed on client care, but are not reviewed due to lack of resources. The Individual Service Fund Agreements request providers to submit quarterly returns, however, there are no detailed procedures specifying the checks to be performed; or when payments should be delayed (as specified in the Payment section of Provider agreements issued by the Contracts Team);

  Consequently, reliance is placed on client complaints or case reviews to identify instances where clients are not receiving the level of service specified within personal support plans. A review of 10 ISFs confirmed that six monthly case reviews had not been completed for 60% of our sample;

3. <u>Care at Home Contract</u>

No formal process has been established to ensure that 'on contract providers' contact the Partnership to advise when the client has been unable or unwilling to accept the service for four consecutive weeks.

The current Care at Home Contract enables 'on contract providers' to continue to receive automatic payments (90% of the client's personal budget) during any length of temporary client absence (section 4.3.5), but does not include a formal definition of 'temporary'.

The contract also specifies (section 4.5.2) that if a client is unable or unwilling to accept the Service for four consecutive weeks and / or the provider believes that they can no longer meet the client's needs, then the provider should contact Social Care Direct to request a review.

Business Support identified one client who was in hospital for more than 3 months, where the provider had been paid £9K. Due to the backlog of reviews, it was unclear whether a review had been requested by the provider and not completed. Business Support persuaded the provider to refund part of the payment, however, the provider was under no contractual obligation to do so.

4. <u>Spot Contracts</u>

Discussions with the teams involved in matching assessments to providers confirmed that a significant volume of spot contracts are issued to meet increasing demand for care. Review of processes supporting the issue of spot contracts confirmed that:

- review of a sample of Spot contracts issued on behalf of Partnership by the Service Matching Unit and Transactions team identified four different variations of the same contract that included different clauses. There is currently no established owner for the content of these contracts;
- there is no clear guidance available detailing when spot contracts should be used. Current practice is that where a package of care cannot be matched to an existing provider and no guide price is available for the service, then a spot contract should be used;
- no management information is available detailing the volume of spot contracts issued, as use of spot contracts and their associated costs are not recorded using a unique identifier in Swift;
- there is no established guidance on acceptable spot contract rates.

- review of a sample of spot contracts established that they do not consistently specify the rate applied for the cost of care. 60% of our sample of spot contracts simply included a weekly total;
- Electronically signed spot contracts are not consistently returned to business support by providers enabling subsequent validation of contract rates against invoices received prior to payment.

Business Implication	Finding Rating
• Contracts may not be legally enforceable; • The contracts team is not operating and supporting the Partnership effectively; • Inconsistent pricing applied to packages of care; • Inability to confirm that client care needs are being effectively met by ISF service providers; • Overpayment to ‘on contract’ where service has not been provided to clients for four consecutive weeks; • Excessive use of spot contracts that are not appropriately priced; • Inconsistent terms in spot contracts issued; and • Spot contract rates are not validated prior to invoice payment;	🟥 High

Action plans

Recommendation	Responsible Officer
A new framework to support management of contracts and grant across the partnership should be designed and implemented. This should include (but not be restricted to) the following areas: 1) Authorities for issuing contracts should be agreed across the Partnership and the register of proper officers updated to reflect the outcomes of this review; 2) Revised authorities for contract approval should be communicated and implemented across the Partnership; 3) A solution should be implemented to prevent issue of electronically signed contracts by former employees; 4) A process should be established to ensure that contract delegated authorities are revised to reflect all new starts and leavers; 5) A formal owner of contract authorities should be established and timeframes agreed for their ongoing review; 6) Procedures should be established to support the operation of the Partnership contracts team; 7) The ‘guide to price’ should be reviewed and updated to reflect current cost of care (including agreed third-party supplier and spot contract rates), with changes communicated across the Partnership. This document should be used as a single source of truth for pricing. Costs of care per the guide to price should be updated in the Swift system. An appropriate owner of delegated authorities should be established and timeframes established for their ongoing review and refresh.	

A change management process should be established to support all future guide to price changes in line with approved delegated authorities, ensuring that the changes are also updated on Swift in a timely manner; 8) A process should be established to ensure that quarterly provider ISF returns are reviewed to confirm that clients are receiving the expected level of care. The process should include a clear escalation procedure where it is identified that clients are not receiving the expected level of care. The review performed should be a risk based sampling approach, with all results and actions taken clearly documented and retained; 9) The process for delaying payments to ISF providers should be clearly documented, and should include effective engagement with providers specifying ISF payments have been withheld; 10) A process should be established to ensure that the Partnership is advised of all instances of client hospitalisation that lasts for more than four weeks, so that appropriate payment adjustments can be agreed with on contract providers; 11) The spot contract template should be reviewed and refreshed, with support from Legal, to ensure that the content of all contracts issued is consistent, and includes specification of rates applied for cost of care in line with the guide to price. A formal owner of the contract template should be established and timeframes agreed for ongoing review of the content; 12) Guidance should be established detailing when spot contracts can be used, and communicated across the partnership. This guidance should include the requirement to use a unique identifier or field (if possible) on Swift to ensure that spot contracts can be easily identified; 13) Management information detailing the volume and value of spot contracts issues should be produced (at least monthly) and provided to budget managers; and 14) A process for review and retention of spot contracts should be established, enabling rates applied to be agreed to invoices processed by Business Support prior to invoice payment.	
Agreed Management Action	**Estimated Implementation Date**
These recommendations will be addressed within scope of the strategic management action detailed in the Executive Summary at Section 2.	

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 – Financial approval guidance applied across the Partnership

- An interim financial approval process (Purchasing budget - financial approval process and budget monitoring) was established in February 2016 and has not been reviewed. This document details the authorisation levels required to approve specific service types;
- Interim guidance (Assessment and Support Planning Guide) was issued in May 2017 and specified that the authorisation levels for seniors/first line social work mangers was to be increased from £400 to £574 in line with the national care home residential home rate. A further change was implemented in June 2017; to £667 (the national care home nursing care rate);
- A briefing paper on the changes for social workers (New Hospital Processes and Standards 290517) was prepared by Cluster managers and issued via email in June 2017; and
- Whilst the June 2017 increase was reflected in Swift questionnaires, the May 2017 Interim guidance was not updated to reflect this change.

The Interim guidance was forward to Internal Audit by a number of managers as evidence of the current procedure applied across the Partnership. When IA queried the national care home rate used in April 2018 the "New Hospital Processes and Standards 290517" paper was provided.

Appendix 3 – Partnership Support Teams

The table below provides details of teams involved in supporting delivery of social care who were engaged as part of the audit. Please note that this list is not exhaustive and may not be fully complete.

Team	Service Area	Location	Role and Responsibilities
Locality Managers	HSCP	Locality Offices	Lead and manage all locality services delegated to the Edinburgh Health and Social Care Partnership.
Locality Hubs Managers	HSCP	Locality Offices	The Hub is a new operating model which assumes the role and remit of a number of different services, including Intermediate Care, Reablement and Sector Initial Intervention teams and what were previously hospital social workers. Hub teams work directly with the services detailed below to develop effective, person-centred care pathways, and are responsible for monitoring and reducing delayed discharge. • Early intervention, • < 6weeks (level of care required) • Reablement • Intermediate Care • Step up and Step down • Range of voluntary organisations
Locality Cluster Managers	HSCP	Locality Offices	Responsible for a range of community and hospital based services providing assessment and care management services; community and district nursing; AHP services; and homecare services including the following: • Complex and continuing care • > 6weeks (level of care required) • Care Homes, Care at Home, Social Work assessment and support • District Nursing, Therapies • Older People's Mental Health • Carer support, respite services • Hosted services, pharmacy
Locality Mental Health &	HSCP	Locality Offices	Responsible for the performance, efficiency and development of the locality integrated mental health and substance misuse service:

Team	**Service Area**	**Location**	**Role and Responsibilities**
Substance Misuse Manager			• Social work assessment and support, Mental Health Officer team, • Alcohol and drug prevention and rehabilitation services
Locality Development Manager	HSCP	Locality Offices	Developed Draft Hub Standard Operating Procedures.
Allocated Workers	HSCP	Locality Offices	Allocated workers include: • Senior Social Workers Responsible for the management of all social work teams; allocation of assessments; reviews; and other tasks across the community and hospital sites. • Social Workers • Occupational therapist • Community Care Assistant Responsible for assessments; support planning; and review of people in hospital and in the community. A number of allocated workers were contacted during the course of the audit review to clarify key stages of the end to end process.
Social Care Direct	Resources	Waverley Court	All service referrals are processed through the Social Care Direct team. SCD, who log all referrals onto data systems and progress new referrals to Locality Hub
Service Matching Unit	HSCP	Locality Offices	Matches requests for Care at Home Services to third party providers.
Contracts Team	HSCP	Waverley Court	Responsible for negotiating contracts; monitoring supplier performance; and management of agreed third party provider rates.
Business Support	Resources	Waverley Court / Locality Offices	Business Support provides a business partnering approach between Business Support and services promoting joint working to provide a strong and strategic centre supporting frontline services across the four localities. Responsibilities include: • Personal Support Plans • Spot Contracts • Payment of Invoices and • Direct Payments Quarterly Returns

Team	Service Area	Location	Role and Responsibilities
Customer Transactions Team	Resources	Waverley Court	The transaction team supports the partnership by processing, issuing, and reviewing: • Individual Service Funds • Direct Payments • Care Home Contracts • Spot Contracts • Payment of Invoices and • Individual Service Funds Quarterly Returns
Strategy and Insight	Chief Executive's	Waverley Court	Provide management information / performance reports.
Finance	Resources	Waverley Court	Provides Financial and Budgetary Support to HSCP
ICT Solutions	Resources	Waverley Court	Provides IT support for the Swift system
Financial Systems	Resources	Waverley Court	Maintain user access to the Council's Frontier System (used for budget monitoring) and user information in respect of budget monitoring reports.
Quality Assurance Service	Safer and Stronger Communities	Waverley Court / Locality Offices	Currently supporting Locality teams in completing quality assurance assessments on their key processes; (i.e. screening, allocation, workload management, assessment, service matching, review, etc) which had been graded as being unsatisfactory by the Care Inspectorate and Healthcare Improvement Scotland as part of their Older People's Inspection of 2016.

Appendix 4 – Electronic Signatures Timeline

Our review established that there were a number of third party contracts being issued on behalf of the Partnership that included the electronic signature of a Senior Manager who had left the organisation in December 2017.

The contract production process involves manually entering information into Swift which is then 'merged' into the standard contract documentation.

The electronic signature is embedded in the Swift system and is automatically applied via 'print' functionality. Contract documentation is then either printed or saved onto a local drive before being issued (either by post or through SharePoint) to the third-party provider.

A timeline of events from initial discovery of the issue to date is detailed below:

Date	Description of events
05 January 2018	Internal Audit site visit to the Service Matching Unit (SMU) identified that 'SMU Spot Contracts were being issued to third party providers with the signature of former Senior Manager.
09 January 2018	Internal Audit met with SMU Business Manager who noted that the required change to the spot contracts would need to be completed through the Contracts Team. SMU Business Manager also noted that there would be other documents which held the Electronic Signature of Senior Managers.
09 January 2018	Internal Audit contacts SMU Business Manager and Contracts Officer to advise of the issue and to request that the signatures be updated. Advised via email by Contracts Officer that: "… it is the responsibility of the team using the spot documentation to arrange for the signature updates and that this would not be undertaken by the Contract team who are not involved with Spot Contracts".
09 January 2018	Internal Audit wrote to Interim Chief Officer to highlight the issue and note that there may be other documents issued with historic electronic signatures.
10 January 2018	Interim Chief Officer issues instruction to all relevant staff regarding the use of the electronic signatures. Action to be taken The email noted that the use of the electronic signature should 'cease immediately' and that electronic signatures should only be used by a) current employees; and b) appropriately authorised individuals, i.e. consistent with standing orders.
10 January 2018	SMU Business Support Manager contacts ICT Solutions (Swift Team) with change request form to remove the electronic signature from relevant spot contracts. Action to be taken ICT Solutions (Swift Team) to remove signature from spot contracts.
10 January 2018	SMU Business Support Manager contacts each of the four 'Locality Managers' to request that they agree to the use of their 'electronic signature' for the Locality that they are responsible for.

Date	Description of events
10 January 2018	Locality Manager notes that a check is required to ensure that the use of Locality Managers signatures is compliant with Standing Orders. Action to be taken The Senior Accountant, (Finance) was copied in to advise.
10-12 January 2018	Correspondence between the ICT Solutions (Swift Team) and the SMU Business Manager which highlighted difficulties in changing the electronic signature; as the document had been created in a 'bespoke format' and requests that staff manually "delete" the electronic signature from the document until the "issue can be fixed". Action to be taken SMU staff to manually 'delete' the electronic signature of the member of staff who has left the organisation from the 'spot contract'.
17-23 January 2018	SMU Business Manager advises Internal Audit of the interim process within the NE Locality and provides email evidence of some of the difficulties in the 'signing off' of the spot contracts which is causing slight delays.
30 January 2018	Internal Audit met with SMU Business Manager to discuss the interim process and discuss some of the difficulties that the team are having. Advised that one Locality manager had a 'question over the legality of using electronic signatures on spot contracts' and that the Cluster Managers in a separate Locality were signing off the spot contracts in the interim.
01 February 2018	Internal Audit contacted the Locality Manager's to establish whether there has been a decision on the SMU spot contract process.
01 February 2018	Internal Audit contacted two Cluster Managers who had previously been identified as signing off SMU spot contracts in the absence of the Locality Manager in order to establish the process being followed.
02 February 2018	Hub Manager NW Locality provides confirmation (via email) of the checks undertaken prior to signing off the SMU Spot Contract.
07 February 2018	Update provided by IA to the Interim Chief Officer which notes that there are ongoing challenges re the authorisation and signature of the contracts which is resulting in delays in obtaining care services from third party providers.
07 February 2018 **07 February 2018 cont.**	Operations Manager (Risk and Compliance) noted that contact had been made with SMU who confirmed that there are no outstanding 'spot purchasing' delays and provided details of interim arrangements in NW. Also noted that the Locality Managers Forum for 8th February had been cancelled and that the process for 'spot contracts' would be added to the agenda for the following week. Action to be taken The four Locality Managers to agree a process for the signing of SMU spot contracts at Locality Forum of 15 February 2018.
07 February 2018	SMU Business Manager requests confirmation from the Operations Manager (Risk and Compliance) of the process to be followed within NE Locality.

Date	Description of events
	Also requests confirmation that the current process followed in SE & SW can continue, i.e. can the electronic signature (of the Senior Manager still in post) continue to be used. Operations Manager (Risk and Compliance) confirms that there is a requirement for all localities to agree on a consistent process and that the proposed process would be discussed at the Locality Managers Forum on 15 February 2018.
07 February 2018	Executive Assistant to Health and Social Care NW Locality Manager confirms that there are no delays in the signing of Spot Purchase Contracts in NW but that there are delays in NE and that the Locality Manager is addressing these.
07 February 2018	Cluster Manager NW confirms that the process noted by the Operations Manager (Risk and Compliance) is the process being followed.
07 February 2018	IA updated the Interim Chief Officer re lack of response from Locality Managers to previous audit correspondence of 01 February. Interim Chief Officer requested that Internal Audit contact the Operations Manager (Risk and Compliance) to take forward. This was completed and a meeting was held on 13 February 2018.
08 February 2018	IA established during site visit to Business Support area office that there are spot contracts issued via a completely different process from the spot purchase contracts which are processed by SMU although both sets of contracts are headed with the same form number / title. In terms of the signature; these spot contracts are printed in hard copy and signed by a Senior Manager and the third-party provider prior to the services being added to the Swift system; rather than being electronically signed by the Locality Manager.
09 February 2018	Three spot purchase contracts which were identified through a Business Support process walkthrough were queried with the SMU Business Manager as to why these spot contracts bypassed the SMU Team. The SMU Business Manager confirmed that one case was for a short-term emergency therefore the spot purchase was appropriate; but that she felt that the remaining two cases should have been processed by the SMU Team.
12 February 2018	The SMU Business Manager provides IA with a breakdown of the difference in the spot purchase contract process between SMU, the Assessors (i.e. Allocated Worker) and Business Support Staff.
13 February 2018	Meeting held between Internal Audit and Operations Manager (Risk and Compliance) to discuss the current position with the electronic signing of the SMU spot contracts. Internal Audit advised of the separate spot contract process established from Business Support site visit of 08 February 2018 (see note above). Operations Manager (Risk and Compliance) advised IA of the proposed interim spot contract process to be discussed at the Locality Managers Forum subject to Locality Managers agreement.
15 February 2018	IA attended the Locality Managers Forum with the Operations Manager (Risk and Compliance), Business Services Manager and each of the Locality Managers. Operations Manager (Risk and Compliance) discussed the proposed interim spot contract process. Locality Managers noted that they would require time to review the

Date	Description of events
	proposed process documentation presented at the meeting and that a decision would be made at the following weeks Locality Managers Forum. The SE Locality Manager noted that she was unaware that the electronic signature was being used for the signing of the SMU Spot Contracts. Email issued from Operations Manager (Risk and Compliance) to Locality Managers 16 February to confirm agreed actions from the meeting and request that a decision on the paper be made by 21 February 2018.
21 February 2018	Internal Audit identified during a walkthrough of the Individual Service Funds (ISFs) process within the Transactions Team (Resources) that the electronic signature for the former Senior Manager was still in use.
26 February 2018	Meeting held between Internal Audit and Operations Manager (Risk and Compliance) to discuss the current position with the electronic signing of the SMU spot contracts. The Operations Manager had advised that feedback had been received from three out of the four Locality Managers as one Manager was not available at the time. Operations Manager advised that she was meeting SMU Business Manager 27 February 2018 and Interim Chief Officer 28 February 2018 to discuss the new interim process.
27 February 2018	Internal Audit informs Operations Manager that ISFs are being electronically signed by former Senior Manager within the Transactions Team (Resources). Internal Audit met with the Transactions Team Manager to advise that Operations Manager had been informed and that the Operations Manager would be in contact regarding the proposed interim process.
27 February 2018	The Transactions Team Manager advised that there are thirteen Residential Care Home contracts and seven Financial Assessment documents and letters which are still using the electronic signature of the former Senior Manager.
27 February 2018	The Transactions Team Manager provides email evidence of correspondence issued to Locality Managers dated 19 January 2018 and 16 February 2018. A response was received to the email dated 16 February from the SE Locality Manager.
27 February 2018	Phone call from Operations Manager notes that ICT Solutions (Swift Team) have advised that a member of the team who has now left the Council had created the SQL signatures using Matrix Code. Replacement of the documents would be a complicated process as the ‘whole programme’ would need to be recreated. An acceptable work around is to be put in place. Locality Manager has noted that she is unaware that the electronic signatures were being used.
01 March 2018	The Transactions Team Manager confirmed that the list of Residential Care Home contracts and Financial Assessments had been passed to the Operations Manager and ICT Solutions (Swift Team) to be actioned (once process is agreed).
05 March 2018	Email correspondence between the Operations Manager and SE Locality Manager to obtain current position regarding the electronic signature on Care Home Contracts.

Date	Description of events
	SE Locality Manager advised that she is liaising with Transactions Team Manager regarding this issue.
16 April 2018	Transaction Team Manager contacted Internal Audit to advise that she had been in contact with the contracts Team and Legal regarding the use of electronic signatures. Legal have advised that the contracts can be produced with a named person who is a Designated Signatory printed on the contracts without the need to have a signature. However, the Transitions Team Manager noted that there is no current list of signatories in place. The Transactions Team Manager has noted that she is currently having to remove the former Senior Manager's Signature from the contracts and manually sign each one.
16 April 2018	IA met with Interim Chief Officer and Operations Manager as part of initial audit close out meeting and advised them of the email received from the Transactions Team Manager. The Operations Manager agreed to take this forward.
17 April 2018	IA met with Transactions Team Manager to discuss the closure of the audit review and the issue she had raised in respect of the electronic signatures. The Transactions Team Manager advised that she is not a Designated signatory but that there is no current list of Designated Signatories in place. It was established that ISFs were still being issued in the former Senior Manager's name. The Transactions Team Manager advised that this process would stop that day.
17 April 2018	Email from IA to the Interim Chief Officer (HSCP) and Head of Customer Services and IT to advise of current position. It was suggested that a meeting be held by all relevant parties to discuss and agree a way forward. Both the Interim Chief Officer (HSCP) and Head of Customer agreed that this was the correct approach.
20 April 2018	Operations manager has set up a 'Short Life Working Group' with the first meeting to be held on 23 April 2018 with the following members of the group required to attend: • SE Locality Manager (HSCP) • Operations Manager (HSCP) • ICT/Swift - Systems Development Team Lead (Resources) • Transaction Team Manager (Resources) • SMU Business Manager (HSCP) • Business Support – Business Services Manager and / or Business Support Manager. (Resources) Action to be taken Objective: to produce 'end to end' interim flow processes for Chief Officer and Head of Customer Services and IT approval.
23 April 2018	Short life working group meeting held.
26 April 2018	Operations Manager issued draft "Interim Purchase Budget Management Process for Localities" document to IA for comment. IA Comments were returned to the Operations Manager
02 May 2018	Operations Manager issues the "Interim Purchase Budget Management Process

Date	Description of events
	for Localities" to all Cluster and Hub Managers within H&SCP via email.
08-09 May 2018	ICT Solutions issue newly formatted draft contract documentation for consultation to Short Life Working Group. Action to be taken Short Life Working Group to provide confirmation that the newly formatted draft contract documentation can go 'Live' within the Swift system.
09 May 2018	IA contacted Legal Services to obtain confirmation of advice provided. Legal Services confirm that no written advice had been supplied to H&SCP IA met with Senior Solicitor who advised that "all contracts must be signed by 'Proper Officer's' who have the 'delegated authority' to sign contracts on behalf of H&SCP. A register of proper officers is held by the "Committee Services" team.
09-10 May 2018	IA contacted Committee Services and requested sight of "Proper Officers' register. Governance Manager confirmed that the Interim Chief Officer has delegated authority through the Council's Scheme of Delegation; however, the register required to be updated in terms of subsequent delegation of authority by the Interim Chief Officer.
10 May 2018	At an introductory meeting with the newly appointed Chief Officer; IA updated Interim Chief Officer of current issue regarding delegated authority.
14 May 2018	Interim Chief Officer requests clarification from IA of the detail of the current issue which was provided via email. Operations manager contacted IA to confirm the detail of the delegated authority issue and provided the Interim Chief Officer with a detailed note of the issue. Interim Chief Officer confirmed that new Chief Officer and Chief Finance Officer will determine a way forward with the process.
17 May 2018	Operations Manager has advised IA that Legal advice has now been obtained. A letter requires to be produced by the Chief Officer for each of the 'Proper Officers' to give them the appropriate delegated authority to sign contracts. Once issued the letters require to be forwarded to Committee Services to allow them to update the 'Proper Officers' register. At this stage only, the Spot Contracts; Care Home Contracts and Individual Service Funds will be updated with the Interim Process / Delegated authority. An analysis requires to be undertaken to identify any other contracts or documents that are electronically signed. The above process requires to be discussed and agreed with the Partnership's Chief Officer.
24 May 2018	Operations Manager issued email to Committee Services which includes Delegated Authority Letters for both Locality and Cluster Managers within the Partnership.

Appendix 5 – Terms of Reference

Health and Social Care – Purchasing Budget Management

To: Michelle Miller, Interim Chief Officer, Edinburgh Health and Social Care Partnership
Stephen Moir, Executive Director of Resources

From: Lesley Newdall, Chief Internal Auditor Date: 23rd October 2017

Cc: Wendy Dale, Strategic Commissioning Manager, Edinburgh Health and Social Care
Moira Pringle, Interim Chief Finance Officer, Edinburgh Integration Joint Board
Hugh Dunn, Head of Finance
Nicola Harvey, Head of Customer
Laurence Rockey, Head of Strategy and Insight
Health and Social Care Locality Managers.

This review has been added to the 2017/18 internal audit plan at the request of the Interim Chief Officer, Health and Social Care, and the Head of Finance.

Background

The Edinburgh Health and Social Care Partnership (City of Edinburgh Council in partnership with NHS Lothian) is responsible for delivering care and meeting support needs across the City through the recently established Localities model.

The Partnership is committed to reducing delays and waiting times for assessment, care, treatment, and support, and providing the right care at the right time in the right place. Consequently, treatment and support should (where possible) be delivered in homes or in homely settings in the community, and hospital admissions minimised. Where hospital admission is necessary, this should take place in a timely way.

Four localities have been established to deliver these services with emphasis on anticipatory planning for people's care needs and their long-term support in the community.

Locality services are delivered via Hubs and Clusters. Hubs respond to initial service requests, avoid the need for hospital admission, and support the return home of people who have been in hospital. Clusters provide longer term care services and focus on prevention and early intervention,

Each locality is responsible for establishing and managing the resources required to support service delivery, including financial planning and management.

At 31st August, the forecast overspend on Health and Social Care home care purchasing was £12m for the 2017/18 financial year. Supporting analysis confirms that this appears to be driven by increased demand for services and failure to deliver approved savings under the Health and Social Care Transformation Programme.

The main drivers of increased purchasing costs are:

- In House – provision of in house services by the Partnership via CEC and NHS employees,
- Block – provision of service via 3rd party suppliers with contracts based on pre-agreed volumes,
- Individual Service Funds (ISFs) - value of the care package is paid to a provider chosen by the client who then agrees with the provider how the care will be delivered,
- Direct Payments (DPs)– direct payment made to client who then arranges their own support, and
- Spot – spot purchasing of home care services from external 3rd parties when required.

Scope

Our review will assess the adequacy and effectiveness of controls established across Health and Social Care to support service delivery by the Localities and demand management in line with approved financial budgets, and will provide assurance over the following key Corporate Leadership Team (CLT) and Finance Risks:

- CLT (High): Health and Social Care - through either lack of CEC resource and/or provider capacity, the Council may be unable to secure appropriate contracts with its providers or deliver appropriate services as directed by the Integration Joint Board (IJB) As a result, we may be unable to deliver our own commitments as part of the Health and Social Care Partnership's strategic plan
- Finance (Medium): Approved savings, including procurement-related savings, are not delivered and/or risks and pressures not managed, resulting in service or Council-wide overspends

We will assess the design adequacy and operating effectiveness of the key controls supporting the processes detailed below:

1. Review and prioritisation of initial requests for assessment,
2. Management of waiting lists,
3. Completion, review, and approval of initial assessments, support plans, and future reviews, including costs,
4. Completeness and accuracy of care packages and costs recorded on Swift,
5. Cessation or reduction of service,
6. Completeness and accuracy of charging and payments made to clients and third-party suppliers, and
7. Ongoing budget management.

An early priority will be to review arrangements for assessment and authorisation of ISFs and DPs where increases in financial commitments are most material.

Approach

Our audit approach is as follows:

- Obtain an understanding of the processes detailed above through discussions with key personnel, review of systems documentation and walkthrough tests;
- Identify the key risks associated with these processes;
- Evaluate the design of the controls in place to address the key risks; and
- Test the operating effectiveness of the key controls.

Limitations of Scope

The following areas are specifically excluded from the scope of our review:

- Adequacy of the agreed 2017/18 Health and Social Care budget – this was subject to review by Internal Audit in May 2016.
- Compliance with the requirements of the (Self-directed Support) (Scotland) Act 2013 – whilst our scope will not assess full compliance with all requirements of the Act, any instances of non compliance identified from our testing will be raised.

The sub-processes and related control objectives included in the review are:

Sub - process	Control Objectives
1. Review and prioritisation of initial service requests	• There is a clearly defined process for recording, assessing, and responding to all requests for assessments received. • The process includes guidance on how requests should be prioritised and a clear escalation process for critical or emergency requests and use of ‘spot’ contracts. • The process has been communicated across all Localities and is consistently applied.

Sub - process	Control Objectives
	• All requests are correctly prioritised in line with applicable guidance. • Prioritisation of requests is subject to management review and approval. • Requests are then either added to the waiting list, or assessment progressed.
2. Management of waiting lists (including provision of Performance Management Information)	• Localities operate waiting lists within approved tolerance limits. • There is a clearly defined process supporting client transfers from the waiting list to service providers. • The process has been communicated across all Localities and is consistently applied. • Waiting list management information (MI) is provided to all Locality managers on an ongoing basis, and consolidated MI provided to H&SC Senior Management. • MI is reviewed and discussed at Locality and H&SC management meetings and appropriate action taken to address any concerns.
3. Completion, review, and approval of initial assessments, support plans, and future reviews, including costs,	• There is a clearly defined process for completion of initial assessments, support plans and future reviews, including calculation of the cost of care. • Initial and ongoing care assessments are consistently performed and the outcomes recorded. • Clear guidance on cost of care calculation is available and consistently applied. • Cost of care is accurately calculated. • All SDS options (arranged and manged by the Council; ISFs; and DPs) are discussed with the client, • Where clients have requested provision of chargeable services, the associated charges are communicated and included in the cost of care. • There are clearly defined delegation and authorisation controls which identify the financial thresholds at which commitments should be escalated to more senior managers for authorisation. • Assessments, proposed care packages, and costs of care are consistently and thoroughly reviewed and approved by the relevant manager, with evidence of review retained There is an established process for dealing with assessment backlogs. • Volumes of assessment backlogs are monitored by Locality managers and H&SC Senior Management.
4. Completeness and accuracy of care packages and costs recorded on Swift	• Details of the care package to be provided (including costs) are completely and accurately recorded on the Swift system. • Any subsequent changes made (and associated costs) are also recorded on Swift.

Sub - process	Control Objectives
	• There is a clear audit trail in Swift demonstrating that all care packages and costs have been reviewed and approved by managers.
5. Cessation of Service	• There is a clearly defined process supporting cessation or reduction of services on a temporary or permanent basis, • The process has been communicated across all Localities and is consistently applied. • Swift records are updated to record the change in service.
6. Completeness and accuracy of charging and payments made to clients and third-party suppliers	• All payments made (arranged and manged by the Council; ISFs; and DPs) have been checked to Swift prior to payment to confirm accuracy. • All charges to be applied to clients have been identified and completely and accurately invoiced, • All payments made to block 3rd party suppliers are in line with contractual terms and conditions. • Block payments are only authorised where service delivery volumes have been achieved. • Payments to spot 3rd party suppliers are only made when supported with payment requests that have been authorised in line with applicable authorities or standing orders.
7. Ongoing budget management	• Locality managers have clear visibility of their devolved care purchasing budgets. • Budgets are regularly monitored and reviewed and considered when making decisions in relation to demand and management of waiting lists. • Budget transfers are performed to address emerging overspends. • H&SC senior management have clear visibility of the total H&SC purchasing budget. • H&SC regularly review the purchasing budgets and develop appropriate strategies, and agree and implement actions to deal with any significant variances.

Internal Audit Team

Name	Role	Contact Details
Lesley Newdall	Chief Internal Auditor	lesley.newdall@edinburgh.gov.uk 0131 469 3216 (x 43216)
Karen Sutherland	Internal Auditor	karen.sutherland@edinburgh.gov.uk 0131 469 3451 (x 43451)

Key Contacts

Name	Title	Role	Contact Details
Michelle Miller	Interim Chief Officer, Health and Social Care	Review Sponsor	0131 553 8201
Wendy Dale	Strategic Commissioning Manager	Key Contact	0131 553 8322
Lyn McDonald	Health and Social Care Operations Manager	Key contact	07540 334 800
Patrick Jackson	Locality Manager, South West	Key contact	0131 453 9010
Angela Lindsay	Locality Manager, North East	Key Contact	0131 469 3927
Marna Green	Locality Manager, North West	Key Contact	0131 553 8318
Nikki Conway	Locality Manager, South East	Key Contact	0131 553 8364
John Connarty	Senior Manager – Business Partnering, Finance, Resources	Key Contact	0131 469 3188
Karen Dallas	Principal Accountant, (Health and Social Care), Finance, Resources	Key Contact	0131 529 7937
Eleanor Cunningham	Lead Officer Strategy and Insight Planning	Key Contact	0131 553 8220
Jo McStay	Corporate Manager, Strategy and Insight	Key Contact	0131 529 7950
Edel McManus	Data Services Manager, Strategy and Insight	Key Contact	0131 469 3285
Mary McIntosh	Business Services Manager, Customer, Resources	Key Contact	0131 529 2138
Jon Ferrer	Quality, Governance & Regulation Senior Manger	Key Contact	0131 553 8396
Katie McWilliam	Strategy Planning & Quality Manager, Older People	Key Contact	0131 553 8382
Liz Davern	Team Manager, Transactions Social Care Finance, Customer, Resources	Key Contact	0131 553 8232

Timetable

Fieldwork Start	6th November 2017
Fieldwork Completed	24th November 2017
Initial Discussion – Draft Observations	30th November 201
Submission of Draft Report	8th December 2017
Response from Auditee	15th December 2017
Final Report to Auditee	22nd December 2017

Follow Up Process

Where reportable audit findings are identified, the extent to which each recommendation has been implemented will be reviewed in accordance with estimated implementation dates outlined in the final report.

Evidence should be prepared and submitted to Audit in support of action taken to implement recommendations. Actions remain outstanding until suitable evidence is provided to close them down.

Appendix 1: Information Request

It would be helpful to have the following available prior to our audit or at the latest our first day of field work:

- Details of the following processes and procedures:
    - Review and prioritisation of service requests;
    - Completion of initial and ongoing care assessments;
    - Calculation of all service support care package costs;
    - Delegated authorisation limits for financial commitments arising from care assessments;
    - Recording care packages and costs on Swift;
    - Payments process for all support services (both invoiced and non-invoiced);
    - Charging process;
    - Cessation of service and removal from Swift
- Details of waiting lists tolerances (e.g. maximum length of waiting lists; maximum time spent on waiting lists).
- Management information on waiting lists across the last year

This list is not intended to be exhaustive; we may require additional information during the audit which we will bring to your attention at the earliest opportunity.