Governance, Risk and Best Value Committee

10:00am, Tuesday, 13 August 2019

Internal Audit Update for the period 23 October 2018 to 6 May 2019 – referral from the Edinburgh Integration Joint Board Audit and Risk Committee

Executive/routine
Wards
Council Commitments

1. For Decision/Action

1.1 The Governance, Risk and Best Value Committee is requested to note and scrutinise the Internal Audit Update, as a number of the open Edinburgh Integration Joint Board Internal Audit findings relate to operational service delivery for the Health and Social Care Partnership by the City of Edinburgh Council.

Andrew Kerr

Chief Executive

Contact: Jamie Macrae, Committee Officer

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

Referral Report

Internal Audit Update for the period 23 October 2018 to 6 May 2019 – referral from the Edinburgh Integration Joint Board Audit and Risk Committee

2. Terms of Referral

2.1 On 31 May 2019, the Edinburgh Integration Joint Board (EIJB) Audit and Risk Committee considered a report by the Chief Internal Auditor which detailed the progress of Internal Audit (IA) assurance activity on behalf of the EIJB performed by the EIJB's partners (the City of Edinburgh Council and NHS Lothian) IA teams.

2.2 The EIJB Audit and Risk Committee agreed:

2.2.1 To note progress with delivery of the EIJB 2018/19 IA plan.

2.2.2 To note the outcomes of the three completed Council reviews that had been referred following scrutiny by the Council's Governance Risk and Best Value committee.

2.2.3 To note progress with the implementation of agreed management actions to support closure of IA findings raised.

2.2.4 To note the actions proposed by management to address overdue EIJB Internal Audit findings.

2.2.5 To note that discussions with NHSL in relation to the IA assurance approach were ongoing.

2.2.6 To refer this report to the City of Edinburgh Council's Governance, Risk, and Best Value Committee for their information and further scrutiny, as a number of the open EIJB IA findings relate to operational service delivery for the Health and Social Care Partnership by the Council.

3. Background Reading/ External References

None.

4. Appendices

Internal Audit Update for the period 23 October 2018 to 6 May 2019 – report by the Chief Internal Auditor

Report

Internal Audit Update for the period 23 October 2018 to 6 May 2019

IJB Audit and Risk Committee

31 May 2019

Executive Summary

1. This report provides details of progress of Internal Audit (IA) assurance activity on behalf of the Edinburgh Integration Joint Board (EIJB) performed by the EIJB's partners (the City of Edinburgh Council (the Council) and NHS Lothian (NHSL)) IA teams.
2. All four of the EIJB Internal Audits included in the Internal Audit plan approved by the Committee in July 2018 have commenced, and are expected to be completed in sufficient time to support presentation of the annual EIJB Internal Audit opinion at the August Audit and Risk Committee.
3. Three reports completed by Council's IA team have been referred to the EIJB for information following scrutiny by the Council's Governance, Risk, and Best Valued Committee (GRBV).
4. As at 6 May 2019, the EIJB had a total of 14 open Internal Audit findings (10 High; and 4 Medium). This reflects a decrease of two from the position reported as at 15 February 2019, with two Medium rated overdue findings now closed.
5. Of the 14 open findings, 10 (6 High; and 4 Medium) are currently overdue. Consequently, the EIJB continues to be exposed to the risks associated with these findings, as detailed in the original IA reports.
6. Discussions in relation to revised proposals for a more consolidated and effective IA assurance approach between the Council and NHSL teams are ongoing.

Recommendations

7. The Audit and Risk Committee is requested to:
    I. Note progress with delivery of the EIJB 2018/19 IA plan;
    II. Note the outcomes of the three completed Council reviews that have been referred following scrutiny by the Council's GRBV committee;
    III. Note progress with implementation of agreed management actions to support closure of IA findings raised;

IV. Note the actions proposed by management to address overdue EIJB Internal Audit findings;

V. Note that discussions with NHSL in relation to the IA assurance approach are ongoing; and

VI. Refer this report to the City of Edinburgh Council's Governance, Risk, and Best Value Committee for their information and further scrutiny, as a number of the open EIJB IA findings relate to operational service delivery for the Health and Social Care Partnership by the Council.

Background

8. The EIJB IA plan is risk based and is developed from review of the EIJB risk register with the objective of providing assurance over all Very High and High rated risks.

9. The outcomes of the audits included in the plan will support the 2018/19 EIJB Internal Audit annual opinion, and inform the annual Governance Statement included in the financial statements.

10. The Plan is delivered by the Internal Audit teams of the EIJB's partners, the City of Edinburgh Council (The Council) and NHS Lothian.

11. All EIJB IA reports prepared by the Council are presented to the EIJB Audit and Risk Committee for scrutiny, and then referred to the Council's GRBV Committee for information and further scrutiny.

12. All EIJB Reviews completed by the NHSL are presented initially to the NHSL Audit and Risk Committee for review and scrutiny, and subsequently referred to the EIJB Audit and Risk Committee.

13. Where relevant, audits completed by both the Council and NHSL IA teams will be referred to the EIJB Audit and Risk committee for information, following initial scrutiny by the respective Council GRBV Committee and the NHSL Audit and Risk Committee.

14. Whilst the Partnership is dependent on both the Council and NHSL to support closure of some EIJB IA findings, the Chief Operating Officer will own all EIJB findings, and obtain assurance (via the established Health and Social Care Assurance Oversight Group) that the Council and NHSL are satisfactorily progressing towards closure for the areas where they provide support to the EIJB.

Main report

Progress with delivery of the EIJB annual plan

15. All four EIJB Internal Audits included in the 2018/19 Internal Audit plan approved by the Committee in July 2018 have commenced. The fourth review is currently in planning.

    A progress update on each of the individual reviews is provided below:

    15.1 **Financial and Budget Management (NHSL)** – review has been completed and the draft report discussed with management. Management is in the process of drafting their agreed management actions and implementation dates by the end of May for presentation at the June 2019 NHSL Audit and Risk Committee.

    15.2 **Governance Structures (Council)** - review has been completed and the draft report discussed with management. Management is in the process of drafting their agreed management actions and implementation dates by the end of May 2019.

    15.3 **Partnership Infrastructure and Support – Integration Scheme (Council**) – the scope of this review has been subject to ongoing discussion since January 2019. Final agreement on the terms of reference was reached between the Chief Operating Offer; the Council; and NHSL on 7 May 2019. The review has now commenced and is scheduled to complete by June 2019.

    15.4 **Strategic Planning** – review is in progress, but has been impacted by delays in the provision of information by management in relation to the processes applied to support preparation of the revised strategic plan. Engagement with management is ongoing, however, if the information required to support our review is not provided, IA will conclude that it does not exist and will prepare our findings and conclusions on that basis.

City of Edinburgh Council IA Reviews to be referred to the EIJB Audit and Risk Committee

16. At the November 2018, the EIJB Audit and Risk Committee reviewed both the Council's and NHSL 2018/19 IA plans and selected the reports to be referred following initial scrutiny by the respective Council Governance, Risk, and Best Value Committee and the NHSL Audit and Risk Committee.

17. No reports have yet been referred by the NHSL Audit and Risk Committee.

18. Three Council reports that include findings that could potentially impact Partnership service delivery have been referred. These are:

- Public Sector Cyber Action Plan for Cyber Resilience Review (Appendix 2);
- Compliance with IR35 and Right to Work Requirements (Appendix 3); and
- Validation of Internal Audit Implemented and Sustained Management Actions (Appendix 4)

The Committee did not originally request this report, however, it has been referred as it includes findings relevant to service delivery by the Partnership.

19. The Committee had also requested referral of the final Developer Contributions report. This review has now been concluded, with the report provided to the Council's GRBV Committee in May for scrutiny. As the report does not include any findings relevant to the Partnership, it has not been referred to the EIJB Audit and Risk Committee.

20. Further detail on progress with the reviews to be referred by the Council to the EIJB Audit and Risk Committee are included at Appendix 1.

Health and Social Care Commissioning Review (July 2018) – agreed management actions

21. Following completion of the Health and Social Care Commissioning review in July 2018, it was agreed that when the new Commissioning Lead Officer for the Partnership joined, a Partnership working group would be established (including Partnership senior management and representation from the relevant Council teams), to ensure that the findings raised were incorporated into an overarching plan that focuses on delivery of strategic and operational commissioning solutions, and review and redesign (where required) of the established commissioning process.

22. Following appointment of the new Interim Head of Strategic Planning for the Partnership in January 2019, an initial workshop was held on 25 February 2019.

23. Management subsequently provided IA with a draft plan to deliver the strategic and operational commissioning solutions. This was reviewed by IA with feedback provided.

24. IA's feedback on the draft plan was then discussed at the Assurance Oversight Group on 16 April 2019, and management agreed to provide a revised draft of the plan for IA review. This had not been received as at 6 May 2019.

25. Consequently, management cannot provide assurance that appropriate action is being taken to address the risks associated with health and social care commissioning highlighted in the two findings (one High and one Medium) raised in this review.

Progress with implementation of agreed management actions to support closure of IA findings raised

26. As at 6 May 2019, the EIJB had a total of 14 open Internal Audit findings (10 High; and 4 Medium). This reflects a decrease of two from the position reported as at 15 February 2019, with two Medium rated overdue findings closed in March.

27. Of the 14 open findings,10 (6 High; and 4 Medium) are currently overdue, and 4 are not yet due for closure.

28. Three of the overdue findings (2 High and 1 Medium) are historic findings that had previously been closed, but were reopened in June 2018 and are recorded as overdue (based on originally agreed implementation dates) as the agreed management actions had not been effectively implemented and sustained, exposing the EIJB to unnecessary risk. Of the three historic findings:

    28.1 One High rated finding has been proposed for closure by management and is currently with IA for review.

    28.2 Management updates are required for the remaining two findings.

29. Of the 10 overdue findings:

    29.1 2 (Highs) are 3 - 6 months overdue;

    29.2 5 (3 Highs and 2 Medium) are 1 – 2 years overdue; and

    29.3 3 (1 High; and 2 Medium) are more than two years overdue.

30. A graphic illustrating the open and overdue findings position is included at Appendix 5, with details of the findings included at Appendix 6.

31. The 10 overdue findings are supported by a total of 24 agreed management actions. Of these:

    31.1 Five agreed management actions are currently with IA for review to confirm whether it can be closed.

    31.2 A total of 9 agreed management actions (4 High; and 5 Medium) have had their agreed implementation dates revised more than once since the inception of the new IA follow up system in July 2018.

32. The Partnership management team has provided an update on progress with the 10 overdue EIJB IA findings. This is included at Appendix 7.

IA Assurance approach – ongoing discussions with NHSL

33. The EIJB 2019/20 EIJB annual Internal Audit plan and supporting Charter were approved at the March EIJB Audit and Risk Committee. It was also agreed at that meeting that the plan and charter would be sent to the NHSL Audit and Risk Committee with a request to recognise both the plan and charter, and support

the EIJB Chief Internal Auditor with access to NHSL employees and records (as required) to support delivery of the 2019/20 plan. These documents have been forwarded to NHSL for consideration at their June Audit and Risk Committee.

Key risks

34. The IA plan is not sufficiently comprehensive to provide the level of assurance that the Integration Board requires in all the areas that it needs.

Financial implications

35. There will be no financial impact to the Integration Joint Board should the four currently planned audits take place. Any requirement to increase assurance provision as a result of new and emerging risks may result in the need to fund additional IA resource.

Implications for Directions

36. There are no specific implications for directions arising from this report.

Equalities implications

37. There are no equalities impacts.

Sustainability implications

38. No direct sustainability implications.

Involving people

39. The IA plan is based in the EIJB's draft risk register. In preparing the risk register, the EIJB's Risk team consulted widely with senior management from the Integration Joint Board; the Council and NHSL.

Impact on plans of other parties

40. The four IA reviews currently expected to be undertaken by the Integration Joint Board's partners IA functions (3 by the City of Edinburgh Council & 1 by NHS Lothian), have been incorporated into the internal audit plans of those organisations.

Background reading/references

None

Report author

Lesley Newdall

Chief internal Auditor

Contact: lesley.newdall@edinburgh.gov.uk

E-mail: | Tel: 0131 469 3216

Appendices

Appendix 1	**Progress with City of Edinburgh Council IA Reviews to be referred to the EIJB Audit and Risk Committee**
Appendix 2	**Public Sector Cyber Action Plan for Cyber Resilience Review**
Appendix 3	**Compliance with IR35 and Right to Work Requirements**
Appendix 4	**Validation of Internal Audit Implemented and Sustained Management Actions**
Appendix 5	**Graphic of Open and Overdue IA Findings**
Appendix 6	**Overdue Management Actions Detailed Analysis**
Appendix 7	**Partnership Management Update on Overdue EIJB Findings**

Appendix 1 - Progress with City of Edinburgh Council IA Reviews to be referred to the EIJB Audit and Risk Committee

Ref	Report	Status	Comments
1.	Payments and Charges	In progress	Scheduled to complete by end of June
2.	Transformation	In progress	Scheduled to complete by end of June
3.	Emergency Prioritisation and Complaints	In progress	Scheduled to complete by end of June
4.	ICT Systems Access Controls	In progress	Scheduled to complete by end of June
5.	Portfolio Governance Framework	In progress	Scheduled to complete by end of May
6.	Localities Operating Model	In progress	Scheduled to complete by end of June
7.	Developer Contributions	Complete	Scrutinised by GRBV May 2019 and not referred to EIJB Audit and Risk Committee There were no findings in this report that were relevant to the Health and Social Care Partnership.
8.	Quality, Governance and Regulation	In Progress	Scheduled to complete by end May
9.	Public Sector Cyber Action Plan for Cyber Resilience Review	Complete	Scrutinised by GRBV May 2019 and referred to the May 2019 EIJB Audit and Risk Committee
10.	Compliance with IR35 and Right to Work Requirements	Complete	Scrutinised by GRBV May 2019 and referred to the May 2019 EIJB Audit and Risk Committee
11.	Validation of Internal Audit Implemented and Sustained Management Actions	Complete	Added by the Chief Internal Auditor as this includes findings relevant to Partnership Service Delivery Scrutinised by GRBV May 2019 and referred to the May 2019 EIJB Audit and Risk Committee

The City of Edinburgh Council

Internal Audit

Public Sector Cyber Action Plan for Cyber Resilience Review

Final Report

9 April 2019

Overall report rating:

Significant enhancements required	Significant areas of weakness and non-compliance in the control environment and governance and risk management framework that puts the achievement of organisational objectives at risk

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk, and Best Value Committee in March 2018. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation there to.

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

Digital technologies bring enormous opportunities for Scottish Public Services, but with them new threats and vulnerabilities that the Public Sector must effectively manage. The WannaCry ransomware attack in May 2017 that impacted areas of the NHS in Scotland and England, highlighted the seriousness of cyber threat to public sector organisations. The National Cyber Security Centre (NCSC) has also reported that the severity of cyber incidents affecting public (and private) sector organisations is likely to increase.

The Scottish Government has noted the importance of cyber resilience in Scotland's public bodies and has set forth a cyber resilience strategy which includes an action plan (the Public Sector Action Plan for Cyber Resilience (the Plan) to promote a consistent risk-based approach to cyber resilience across Scottish public bodies.

The Plan is a set of actions designed to strengthen cyber resilience, and has not been formalised as either legislative or regulatory requirements. However, implementation of the actions included in the Plan is strongly recommended by the Deputy First Minister.

The Scottish Government has requested that public sector organisations and their key partners confirm that assurance has been provided on their critical technical cyber controls by the end of October 2018, and can demonstrate progress toward implementation of the Plan actions by December 2018. Confirmation that these actions have been implemented will provide the Scottish Government with assurance that cyber resilience risks are managed consistently and effectively across the public sector.

The Council's Cyber Security framework and key cyber controls are managed and operated on behalf of the Council by their technology partner CGI.

Public bodies were encouraged by the Government to conduct a Cyber Essentials pre-assessment by end of March 2018. Completion of the pre-assessment enables organisations to identify whether their existing cyber security controls require remediation before applying for the cyber essentials certifications included in the Plan. There are two types of certification included in the Plan:

- Cyber Essentials - a self-assessment questionnaire covering 5 key controls: firewalls; secure configuration; access controls; malware protection; and patch management, and an external vulnerability scan to independently assess the adequacy of security, which is reviewed by an external certifying body; and
- Cyber Essentials Plus - this includes the same cyber security controls as Cyber Essentials, with additional verification performed by the external body to confirm the effectiveness of the controls through testing.

The Cyber Essentials Plus certification is the Scottish Government's preferred option where organisations cannot provide other alternative evidence of existing independent assurance on the effectiveness of their cyber security controls. Where independent assurance has been obtained on the effectiveness of the five critical cyber controls, Cyber Essentials is an acceptable alternative option.

Whilst the Plan focuses on cyber resilience, implementation of the actions will also support ongoing compliance with the requirements of the European Union's Directive on Security of Network and Information Systems (the Directive).

The Directive became effective in August 2016 and aims to increase cybersecurity resilience across Europe. EU member states had until 9th May 2018 to transpose the Directive into their national laws.

The Directive provides legal measures to enhance cybersecurity, particularly for industries and organisations that provide services essential to everyday life and the security of a nation. Specifically, the Directive aims to safeguard the supply of essential services that rely heavily on IT, such as energy, transportation, water, banking, financial market infrastructures, healthcare, and digital infrastructure.

Organisations in those sectors that are identified as operators of essential services (OESs) or digital service providers (DSPs) will be required to take appropriate security measures and comply with the incident notification requirements as set out by the Directive. These organisations will be required to report incidents to a regulatory authority and will face fines of up to £17m if breaches are due to failures in cybersecurity defences.

The NIS Directive will apply to all OESs and DSPs from 9th May 2018, with member states required to identify all OESs and DSPs in their country that are essential to the supply of electricity, water, digital infrastructure, healthcare, and transport by 9 November 2018. It has not yet been confirmed whether the requirements of the Directive will be extended to Scottish local authorities.

In addition to the Directive, implementation of Plan actions will also support ongoing compliance with new General Data Protection Regulations (GDPR) that became effective in May 2018,

Consequently, public sector organisations should also consider how their cyber resilience and technical cyber controls align with both Directive and GDPR requirements on an ongoing basis. Whilst the Council's Customer and Digital Services team will be responsible for confirming to the Scottish Government that Plan actions have been implemented, effective cyber Security resilience is priority for all Service Areas across the Council, as the Plan also includes governance; risk; and supply chain recommendations.

Failure to achieve at least Cyber Essentials accreditation by October 2018, and demonstrate progress with implementation of the actions included in the Plan by December 2018 could result in potential adverse reputational damage for the Council.

The Scottish Government has published the following 11 key actions for public sector organisations (https://www.gov.scot/Publications/2017/11/6231/2) to work towards alignment with their cyber resilience strategy. 8 of the 11 key actions had been issued by the government at the time of our review:

1. To adhere to the Public Sector Cyber Resilience Framework requirements (note that these requirements had not been at the time of our review);
2. To have minimum cyber security Governance arrangements in place by June 2018;
3. To promote awareness of cyber threats and intelligence;
4. To have appropriate independent assurance of critical technical controls and defences;
5. To make use of National Cyber Security Centre (NCSC) Active Cyber Defence Programme by June 2018;
6. To set up appropriate staff training and awareness and disciplinary procedures. Government Document and guidance to be provided by June 2018;
7. To adopt cyber incident response process and protocols;
8. To adopt a proportionate risk based security view of the supply chain (note that the SG supply chain cyber security policy has not yet been issued);

9. To ensure appropriate access to expertise in supporting public bodies on cyber resilience, the Scottish Government will put in place an Innovative Dynamic Purchasing System for Digital Services;
10. Participate in the creation of the Public Sector Cyber Catalyst Scheme; and
11. To apply the monitoring and evaluation framework designed by the SG to monitor progress against this action plan. This had not been issued at the time of our review.

Scope

The objective of this review was to assess the Council's progress towards Cyber Essentials accreditation by end of October 2018, and progress with delivery of the Plan actions (detailed above) by December 2018.

We also reviewed the independent assurance provided as part of the Cyber Essentials pre-assessment process to confirm whether appropriate actions are planned to address any significant control gaps identified.

Our work was performed during August 2018 and concluded by the end of August. Our opinion and the findings included in this report are based on the outcomes of our work as at **31 August 2018**.

Limitations of Scope

- This review focused only on the design of the Council's cyber security controls that are relevant for the Plan. No detailed testing was performed to determine their effectiveness;
- Only those processes and policies within the control of the Council and CGI were included in scope. Cyber security controls applied by third party organisations supporting Council services are excluded as the Plan is not yet clear on these requirements;
- Cyber security controls in relation to the Public Services Network (PSN) provided by the UK government were specifically excluded from the scope of this review. PSN compliance will be assessed within the scope of our planned review of 'Out of Support Technology and Public Services Network Accreditation'; and
- Our work does not guarantee that the organisation will be fully compliant with requirements of the Plan.

2. Executive summary

Summary of findings raised	
High	1. Critical Operational Cyber Security Controls
Medium	2. Key Cyber Security Controls Monitoring
Medium	3. Public Sector Cyber Action Plan Project Governance

Opinion

The City of Edinburgh Council ("the Council) recognises Cyber Security as high priority and acknowledges that the Scottish Government (SG) wants Scottish public sector bodies to become exemplars in cyber resilience. The Council confirmed in their covering letter to the Scottish Government in July 2018 (supporting submission of their baseline cyber security questionnaire) that

they will initially aim for Cyber Essentials (CE) accreditation, with CE plus accreditation post October 2018.

Areas for Improvement

Our review has confirmed that significant enhancements are required to ensure that the Council achieves Cyber Essentials (CE) accreditation by end of October 2018, and can demonstrate progress with delivery of expected Plan actions by December 2018.

This opinion reflects a number of known significant weaknesses in existing key cyber security operational controls; the need to establish and ensure ongoing monitoring of the effectiveness of the Council's full population of cyber security controls; and the need to confirm whether areas of the Council that operate standalone networks (for example, schools and the Lothian Pension Fund) and other standalone systems (such as the EDINDEX system used by citizens to submit applications for Council property) will be included in the scope of the Council's applications for accreditation.

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

Progress to Date

Whilst a number of significant control enhancements are required to achieve and support the implementation of the cyber actions detailed in the Plan, it is important to note that the Council has already met a number of expected Plan timeframes. These include:

- Completion of the independent Cyber Essentials Pre-Assessment test and receipt of the results by April (a prerequisite of action 4);
- Submission of the initial SG Public Sector Action Plan for Cyber Resilience baseline questionnaire in July 2018, confirming current progress against the Plan, and providing details of ongoing cyber remediation work;
- Establishing minimum cyber security governance arrangements by June 2018 (action 2), through formation of the Cyber Information Security Steering Group (CISSG);
- Progress on staff training and awareness through ongoing campaigns and phishing training (action 6); and
- Participation in the Public Sector Cyber Catalyst Scheme (action 9).

Areas of Good Practice

Whilst we identified a number of areas for improvement, the following areas of good practice were also noted during the review:

- Establishment of strong ongoing dialogue with both the SG and the SG Cyber Resilience Unit;
- Attendance at SG training and Public Sector Cyber Catalyst meetings designed to facilitate knowledge sharing and identification of practical cyber security solutions;
- Regular consideration of both cyber and information security risks by the Council's Corporate Leadership Team;
- Formation of the Cyber Information Security Steering Group (CISSG) in June 2018 with representation from all Council Directorates; Information Governance; and CGI;
- A proactive approach to GDPR has been adopted; and
- SG recognition that the Council's cyber security training is exemplary. and there is opportunity to replicate it across other public sector organisations.

3. Detailed findings

1. Critical Operational Cyber Security Controls — High

Our review confirmed that remediation work in relation to key cyber security controls is ongoing, with completion timeframes that currently extend past the planned Council's Cyber Essentials and Plan completion dates. We have outlined the following findings that relate to actions 4 and 5 from the Public Sector Action Plan for Cyber Resilience (see Background section for details of the of actions) as they relate to independent assurance over critical controls and the NCSC defence programme. Specifically:

- **Patch Management (action 4)** – Whilst the Council has implemented a monthly patch management regime for WINTEL and UNIX servers, the results of the Pre-Assessment conducted in March 2018 for Cyber Essentials confirmed that the Council would not qualify for Cyber Essentials Plus accreditation without appropriate, timely, and fully effective patch management remediation;
- **Legacy Operating Systems and Unsecure Software (action 4)** – The Council currently uses legacy operating systems and unsecure software that increases exposure to cyber attacks, and impacts patch management as patches are generally only available for current and most recent versions.

  A technology refresh programme has commenced and is expected to complete in June 2019. This programme will replace all of the Council's end user devices across the estate, ensuring that only fully supported software applications are used and supported with effective ongoing patch management controls. If the programme cannot be delivered in line with expected Plan timeframes, reliance could be placed on compensating vulnerability scanning controls, however, our review has confirmed that these controls are currently not effective.
- **Vulnerability Scanning (action 4)** - Manual vulnerability scanning is currently being performed by CGI, with the most complex aspects of the work to be completed in September 2018. CGI has advised that real-time vulnerability scanning tools will be in place by November 2018, however this implementation date has been consistently revised.

  Lack of ongoing vulnerability scanning was also noted as an outstanding item raised by Scott Moncrieff as part of their 2016/17 external audit technology controls work;
- **Shadow IT (action 4) –** Customer and Digital Services compiled a list of all shadow IT (bespoke systems or applications that are not supported by CGI) used across the Council based on information provided by Service Areas in October 2017. To prohibit future purchase of shadow IT, reliance is placed on existing procurement controls, however, procurement controls do not prevent the purchase of shadow IT where the cost is less than the £3K procurement threshold required for approval.

  Whilst technology controls exist to prohibit Council staff downloading software on to devices, and Web Check is used to scan for website vulnerabilities, cyber security risks associated with shadow IT cannot be effectively managed and will not be fully mitigated until completion of the technology refresh programme that will address the risks associated with legacy software, and implementation of ongoing real-time vulnerability scanning;
- **Network Segregation (action 4)** - The Council has confirmed that the schools network will be excluded from the Public Sector Action Plan for Cyber Resilience on the basis that this is a stand-alone network. The CGI contract includes specific Output Based Specifications (OBSs) relating to

network management, and includes responsibilities for monitoring the segregation of network traffic, which is achieved through Virtual Routing and Forwarding (a network router that enables network paths to be segmented without using multiple devices). Whilst CGI has provided written confirmation to confirm segregation between schools and the core council network, no evidence has been provided to support this view.

- **Domain Name System Controls (action 5)** – A Public DNS is one of the National Cyber Security Centre (NCSC) Active Cyber Defence Programme recommended tools. When connecting to networks or websites, a DNS directs users to the correct server location/IP address by accurately translating domain names.

  The Council's existing Domain Name System (DNS) is situated internally within the Council's network and is not designed to support an externally hosted DNS as recommended by NCSC (Plan action 5). The existing DNS requires manual intervention when there is a switch over to a secondary infrastructure.

  CGI has confirmed that the DNS cannot be enhanced without significant network redesign as the Council's network is not designed to access an externally hosted DNS such as the Public DNS recommended by NCSC. Whilst compensating controls have been established, these will only prevent redirection to known malicious sites

  No analysis has been performed to assess whether the current internal design is any less secure than the recommended Public DNS tool.

- **User Access Controls (action 4)** - Whilst significant progress is evident with improving user access controls (such as removal of desktops from the network after 30 days of inactivity), outstanding actions identified by Scott Moncrieff as part of their 2016/17 external audit technology controls review are only partially complete. These relate to privileged user accounts for Wintel and UNIX operating systems; and the requirement to update the UNIX password policy to align with the Council's policy.

Risks

- The Council may be unable to provide assurance over critical cyber security controls and may not achieve Cyber Essentials accreditation and by October 2018;
- The Council may be unable to demonstrate adequate progress towards implementation of the Public Sector Action Plan for Cyber Resilience actions by 31 December 2018; and

  If the DNS is not operating effectively or is comprised, this can result in changes to the IP address with users redirected to unknown malicious sites. Another risk is that anti-virus software can also be jeopardised, which means networks may not be adequately protected against malware.

1. Recommendation - Cyber Essentials Accreditation

1.1. A decision should be taken as to whether it is realistic to aim for CE plus accreditation in 2019, as the Technology Refresh Programme that will resolve known patch management issues is not scheduled to complete until June 2019; and

1.2. CE Plus accreditation may still be possible if reliance is placed on the effectiveness of compensating vulnerability scanning controls across the Council's networks, however, assurance should be obtained from CGI that the current manual vulnerability scanning will be completed on schedule by the end of September 2018, with automated scanning implemented and fully operational by November 2018, supported by an appropriate remediation process to ensure that all vulnerabilities identified are addressed in a timely manner.

Agreed Management Actions - Cyber Essentials Accreditation

1.1. CE Accreditation was achieved October 2018. Based on the advice received, we are therefore continuing with the current plan for Cyber Essentials Plus accreditation in 2019. We are dependent on some improvement plans and programmes by CGI that are tracked via the Public Services Network Board and Security Working Group.

1.2. CGI 's progress will be reviewed at the end of January 2019 and monthly afterwards.

1.3. A formal review to assess whether accreditation can be achieved will be completed by end March 2019 by the Enterprise Architect with support and oversight by the Chief Information Officer. A proposal to continue for submission will be then made by the CIO, to the Head of Customer and Digital Services, and the Executive Director of Resources.

1.4. CGI completed a complete manual vulnerability scan of the estate in November 2018 Vulnerabilities identified from this scan are being resolved as part of the Public Services Network remediation action plan. CGI have been formally requested to implement automated vulnerability scanning as a service. To ensure this is in place in time for Cyber Essentials Plus accreditation this automated vulnerability scanning is targeted to be implemented by end of June 2019.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: 30 September 2019

2. Recommendation – network segregation

2.1 Evidence should be requested from CGI to support their confirmation that the schools network remains effectively segregated from the main Council network. This should include details of the testing performed, and a summary of the outcomes; and

2.2 Ongoing confirmation of network segregation (based on testing) should also be either requested every six months, or in the event of any significant changes to the design of the network architecture.

Agreed Management Action – network segregation

2.1 CGI have confirmed in writing that our networks are segregated. We will also provide additional evidence of network segregation between the Corporate and Learning and Teaching networks. We will raise a change request to ask CGI to carry out PING tests from a selection of 20 representative schools to see if they can locate corporate network assets.

The PING test will confirm whether the content of one server can be viewed from another. If nothing can be viewed, this means that the servers cannot be accessed as they are appropriately segregated.

We will raise the appropriate request 28th February 2019 and ask CGI to complete the work by the end of June 2019.

If the PING tests prove that the networks are appropriately segregated, then no further action is required in relation to Cyber Essentials Plus accreditation. If the networks are not appropriately segregated, then a proposal will be made to the Corporate Leadership Team to either combine the networks, or include the schools and learning network within the scope of Cyber Essentials Plus accreditation.

2.2 A process will be agreed with the CGI Network team to repeat the PING tests in the event of significant change to network architecture. This will be managed through the Network Improvement Working Group, and will be included in the change request noted above.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: 30 September 2019

3. Recommendation - Domain Name System Controls

3.1 A gap analysis should be performed in conjunction with CGI to assess the gaps between the current internal DNS and the Public DNS solution;

3.2 The outcomes of the gap analysis should be used to determine whether the Public DNS solution should be fully or partially implemented;

3.3 The decision in relation to the DNS solution should be based on an assessment of the risks associated with each option, and a supporting cost and benefit analysis;

3.4 If the DNS approach is to be changed, a supporting implementation plan should be developed and applied; and

3.5 DNS controls should be tested to ensure that they are operating effectively prior to implementation.

Agreed Management Action – Domain name system controls

3.1 **Action 1** - We have requested that CGI provide a gap analysis by 28th February 2019. The output will be provided to audit.

3.1.1 On the basis of this, recommendations to consider PDNS implementation in part or completely, or whether we will continue the with current DNS solution will be provided to the Head of Customer and Digital Service; the Executive Director of Resources. With a recommendation by 14th March 2019. Evidence of the gap analysis, recommendation and decision will be provided to audit.

3.1.2 Risks will be considered as an integral part of the decision making process, with cost impacts to change included in determination. If the decision is take not to not implement the PDNS, the risk will be captured on the ICT risk register, and managed through the risk management framework.

3.2 **Action 2** - If the decision is taken to implement PDNS then the following agreed management actions will be raised and an implementation date agreed.

3.2.1 A supporting implementation plan will be developed and considered as part of the decision making process

3.2.2 A Change request (CR) will be raised as necessary with CGI to formulate an Implementation Plan in the event of a decision to change to PDNS. The CR will be raised following the conclusion of Action 1 directly above.

3.2.3 The tool will be fully tested prior to implementation to confirm that it is operating as expected prior to go live.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date for Action 1: 31 May 2019

Agreed Implementation Date for Action 2: to be determined when the decision is taken in relation to PDNS implementation.

4. Recommendation – User access controls

4.1	Formal confirmation and supporting evidence should be requested from CGI that external audit recommendations in relation to privileged user accounts for Wintel and UNIX operating systems; and the requirement to update the UNIX password policy to align with the Council's policy have been addressed prior to completing CE Plus accreditation.

Agreed Management Action – User Access Controls

4.1	CGI indicated that the full recommendations made by the external auditor could not be implemented without significant change to the contract and at a notable additional cost. CGI provided the Council and the External Auditors with details of the current oversight of the CGI Wintel and UNIX password policies. Current ongoing evidence of this oversight via the SWG will be provided to external audit, a statement confirming the risk acceptance by the Executive Director of Resources will be prepared, approved, signed, and provided to Scott Moncrieff.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: 31 May 2019

2. Cyber Security Controls Monitoring — Medium

The Scottish Government expects public sector organisations to ensure they have in place appropriate independent assurance over critical cyber security controls by the end of October 2018. The Council is dependent on their technology partner CGI for identification and confirmation of the ongoing operating effectiveness of these controls.

To date, the full population of the Council's critical cyber security controls has not been fully identified, and reporting on their ongoing effectiveness established. Monthly security reports detailing the operational performance of some key controls (for example, patch management which is a high risk area for the Council due to the volume of legacy IT estate) are received from CGI and reviewed by ICT.

Whilst management acknowledges that the content and quality of the security reports is improving, review of a sample of reports confirmed that their format is inconsistent; they include inaccurate data; and performance dashboards are not consistently populated.

Additionally, performance of recently implemented cyber controls is not being monitored due to delays in implementation and reporting. For example, a new Intrusion Prevention System (PIPS) was implemented between February and June 2018, however CGI have yet to provide any reporting on the effectiveness of its operation.

Risk

- The Council will be unable to monitor the ongoing effectiveness of cyber security controls; resulting in the inability to monitor trends; identify and prioritise remediation of control gaps; and report to findings to senior management;
- The Council may be unable to provide assurance over critical cyber security controls and may not achieve Cyber Essentials accreditation and by October 2018; and
- The Council may be unable to demonstrate adequate progress towards implementation of Plan actions by 31 December 2018.

1 Recommendations - Cyber Security Controls Performance Dashboard
1.1 Establish and implement a cyber security control performance dashboard (based on agreed key performance indicators) that includes the full population of preventative; detective; and compensating controls operating across the Council covering the SG five key critical Plan cyber security themes (firewall; secure configuration; patch management; access management; and malware) in conjunction with CGI, that measures the effectiveness of their ongoing operational performance.
Agreed Management Action - Cyber Security Controls Performance Dashboard
1.1 The council agreed a dashboard for reporting on key controls as part of previous internal and external audits. This forms part of the monthly SWG Service report. The Council has requested that a record of firewall rules reviews and intrusion prevention and detection controls (detailing all attempts made to gain access through internal and external firewalls) are included in the dashboard. As at December 2018, CGI has not been able to provide a consistent and complete report for a continuous period of 3 months. This was escalated within the established partnership escalation procedure, and now appears to have been resolved, however, Digital Services are monitoring for a period of 3 months from Jan to March 2019 to confirm that the reports are complete and accurate. There is one exception to this as CGI currently do not provide vulnerability scanning as a Service. This is covered in Finding 1.
Owner: Stephen Moir, Executive Director of Resources Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty
Agreed Implementation Date: 31 July 2019
2. Recommendations - Escalation and Resolution of Operational Performance Issues
2.1 Ensure that any significant weaknesses in the operational performance of these controls are escalated by the Security Working Group to the Partnership Board for resolution within specified timeframes; and 2.2 Weaknesses in the operation of key cyber security controls will be reflected in the CISSG risk register (refer finding 3 below)
Agreed Management Action - Escalation and Resolution of Operational Performance Issues
2.1 We believe escalations around operation matters are via the SWG and then the CEC/CGI escalation procedure to either the Partnership Board or the Executive Review Board. We have evidence this has happened. 2.2 Issues around vulnerability will continue to be recorded in the ICT Risk log (as is done now) and where appropriate will be recorded in the CISSG Risk Log as is proposed.
Owner: Stephen Moir, Executive Director of Resources Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty
Agreed Implementation Date: Now complete. 30 April 2019 (for IA validation).

3. Public Sector Action Plan for Cyber Resilience Project Governance	Medium

Whilst a Public Sector Action Plan for Cyber Resilience tracker and risk log has been established detailing the requirements to achieve CE; CE Plus; and implementation of Plan actions, detailed timeframes and the risks and dependencies associated with timely delivery have not yet been recorded and presented to the CISSG and the Corporate Leadership Team (CLT). These include:

- Lack of clarity regarding the scope of the Council's accreditation; subsequent CE plus accreditation and implementation of Plan actions will include areas of the Council that operate stand alone networks (for example, schools and the Lothian Pension Fund) and other stand alone systems (such as the EDINDEX system used by citizens to submit applications for Council property).
- Dependency on the Council's technology partner CGI for delivery of 2 strategic IT programme initiatives: the upgrade to Office 365 across the technology estate (scheduled to complete November 2018); the refresh of all technology devices and hardware (initially scheduled to complete June 2019, although will be likely extended given the volume of devices and hardware included in the Council's legacy technology estate); and remediation of known weaknesses in existing cyber security controls.

  Progress updates provided by CGI are not yet clear on completion timeframes for the technology refresh programme and remediation of known weaknesses in key cyber security controls;
- Lack of a consolidated thematic technology risk register that provides a holistic view of cyber security risks and the effectiveness of supporting controls across the Council, and no assurance (as yet) that Service Areas are effectively managing their own cyber security risks;

  Whilst plans have been developed to support delivery of a thematic risk register (for example, workshops facilitated by Risk Management for Heads of Service), no timeline for completion has been established;
- Timeframes for completion of the independent accreditation (Public Sector Action Plan for Cyber Resilience action 4) have been consistently revised, and no supplier has yet been engaged to perform the assessment.

  Management has confirmed that CGI has identified a preferred supplier, although arrangements for the independent accreditation review have not yet been confirmed given known and ongoing challenges with the technology refresh programme and remediation of known weaknesses in existing cyber security controls;
- Known difficulties in monitoring training completion rates due to incomplete and inaccurate employee data, which is restricting the analysis of training attendance; progress reporting to the CISSG; and provision of feedback to Service Areas. Additionally, as the Council does not apply a mandatory training approach, reliance is placed on managers and employees to take a proactive approach to complete the training.

  This issue has already been raised as a Medium rated finding in the Phishing Resilience Internal Audit review completed July 2018, and management is working to an agreed implementation date of 29 March 2019, which provides a significant challenge in relation to successful and timely delivery of Public Sector Action Plan for Cyber Resilience action 6.

Risks

- Until a thematic technology risk register is established, existing Council wide cyber security risks cannot be addressed;

- The Council may be unable to provide assurance over critical cyber security controls and may not achieve Cyber Essentials accreditation and by October 2018; and
- The Council may be unable to demonstrate adequate progress towards implementation of Plan actions by 31 December 2018.

1 Recommendations - Public Sector Action Plan for Cyber Resilience Project Scope

1.1 The scope of the Council's Public Sector Action Plan for Cyber Resilience project should be clearly defined, and agreement reached on whether this should include areas of the Council that operate standalone networks and systems.

Agreed Management Action - Recommendations - Public Sector Action Plan for Cyber Resilience Project Scope

1.1 The Council does not have 'standalone' networks. The Plan scope in general covers all services that are provided via the Council's Corporate and Learning and Teaching Networks. Cyber Essentials has been obtained on that basis. It is proposed that Cyber Essentials Plus will only be submitted for systems within the Corporate Network.

The Plan Council's Plan accreditation work does not include any systems that are hosted externally to the above networks.

This is being communicated to the Deputy First Minister in a response to be sent by the Council in December. Action complete and evidence to be provided

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: Completed - 30 April 2019 (for IA validation)

2 Recommendations - Public Sector Action Plan for Cyber Resilience Project Plan

2.1 The existing Plan project tracker and risk log should be enhanced to ensure that it reflects current timeframes for all CE Plus and Plan activities, including key dependencies on other projects / programmes and third party suppliers; and

2.2 CE plus and Plan action timeframe extensions should be discussed and approved by the CISSG, with the supporting rationale for the decision documented; approved by senior management and an explanation logged.

Agreed Management Action - Public Sector Action Plan for Cyber Resilience Project Plan

2.1 Complete - the existing Plan project tracker and risk has been enhanced to ensure that it reflects current timeframes for all CE Plus and Plan activities (including appointment of an independent accreditor once timeframes for CE Plus accreditation have been agreed), including key dependencies on other projects / programmes and third party suppliers.

2.2 As with Cyber Essentials, the Cyber Essentials Plus submission will be approved through the appropriate channels i.e. through the CIO; the Head of Service; the Director; the Security Working Group (SWG) and wit the CISSG kept informed. This will be further reviewed formally at end of March 2019

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey; Carolann Miller; Neil Dumbleton; Alison Roarty

Agreed Implementation Date: 30 April 2019

3 Recommendations - Thematic Cyber Security Risk Register

3.1	Timeframes for completion of planned risk workshops and design and implementation of a thematic technology / cyber security risk register should be finalised;
3.2	The risk register should reflect all known and significant potential Council wide cyber security risks; details of established cyber controls and an assessment of their effectiveness as advised by the relevant service risk owners; with ownership, actions, and timeframes to address the risks allocated and documented; and
3.3	Once created, the risk register should be regularly updated and the effectiveness of key controls regularly assessed by the relevant service risk owners on an ongoing basis (at least quarterly).

Agreed Management Action - Thematic Cyber Security Risk Register
The Internal Audit recommendations at 3.1 to 3.3 above will be implemented
Owner: Stephen Moir, Executive Director of Resources Contributors: Nick Smith, Head of Legal and Risk; Duncan Harwood, Chief Risk Officer; and Rebecca Tatar, Principal Risk Manager
Agreed Implementation Date: 30 September 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.

The City of Edinburgh Council

Internal Audit

Compliance with IR35 and Right to Work Requirements

Final Report

15 March 2019

RES1802

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2018. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

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

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

1. Background and Scope

Background

IR35

In April 2017, HMRC introduced changes to the IR35 working rules for temporary off payroll workers in public authorities. The objective of these changes was to prevent individuals from working as 'disguised employees' through their own limited company, personal service company or partnership whilst saving on income tax and National Insurance (NI). These individuals, though not employed by the Council, may be subject to income tax and NI if they perform work similar to that of a permanent employee. For example, where the worker is under the supervision, direction, and control of the Council.

As a result, the Council now has responsibility to:

- determine whether the off-payroll working rules should apply, both initially and when future engagements are made;
- monitor the duties performed by the worker to ensure they remain reflective of the initial assessment, and reperform the assessment should these change;
- confirm whether the off-payroll working rules should apply to workers supplied via an agency; and
- respond to any written requests from a worker or agency to set out the reasons for the IR35 assessment outcome within 31 days.

The Council has implemented processes to ensure compliance with IR35 working rules. Responsibility for completing the necessary checks and determining the IR35 status of the worker is devolved to Service Areas, with the engaging manager required to complete the assessment using HMRC's online IR35 assessment tool, prior to engaging the worker.

The outcome of the online assessment then determines the Council's responsibilities and how it subsequently makes payments to workers:

- If the assessment confirms that that the worker is 'Employed for Tax Purposes' then the Council, is responsible for deducting PAYE and NI contributions as if they were a Council employee through its payroll system; or
- If the assessment confirms that the worker is outwith IR35 and not Employed for Tax purposes then the Council would pay treat the worker as a supplier, making payment through the purchase ledger. This process is managed by the Commercial & Procurement Services (CPS) Vendor Team and Banking and Payment Services.

Alternatively, where a recruitment agency is used, payment is made via the agency who subsequently recharges the costs to the Council.

HMRC conducts Employer Compliance Reviews which consider the operation of IR35 rules within organisations. HMRC has confirmed that the will only stand by assessment results that are based on accurate source information.

Right to work

The Immigration, Asylum and Nationality Act 2006, places a duty on the Council to prevent illegal working by undertaking checks on all employees' right to work in the UK. The Council may be liable for a civil penalty if they employ someone who does not have a right to work. The penalty can be revoked if the Council can demonstrate that they have performed the prescribed documentation checks to confirm a legal right to work prior to employment.

In line with Home Office requirements, the Council has implemented processes to conduct right to work checks as part of recruitment and selection processes. Recruiting managers must obtain, check and copy original documents, recording the date the check was conducted. They must also carry out further checks for workers with a limited right to work in the UK. Copies of original documents must be retained for not less than two years after the employment has come to an end.

Scope

This review assessed the design and operating effectiveness of the Council's onboarding controls to ensure that all agency workers/contingent labour are IR35 compliant, and that all new employees have a right to work in the UK. The review also considered ongoing controls within Service Areas to ensure that IR35 compliance and right to work status is maintained.

Our audit work concluded on 24 September 2018 and our findings and opinion are based on the outcomes of our testing at that date.

2. Executive summary

Summary of findings raised	
High	IR35 Compliance and oversight framework
Medium	Inclusion of IR35 responsibilities in contracts for agency worker suppliers
Low	Compliance with right to work requirements

Opinion

Our review of controls established to ensure that the Council achieves ongoing compliance with both HMRC IR35 and Home Office Right to Work legislation confirmed that whilst generally adequate controls have been established to ensure Right to Work compliance, some enhancements are required to ensure ongoing compliance with IR35 requirements.

Consequently, 1 High; 1 Medium; and 1 Low rated findings have been raised.

Whilst some controls have been established that ensure compliance with aspects of IR35 legislation; including payroll procedures for deducting income tax and NI due, areas of weakness have been identified in both the design of the Council's IR35 control framework and operating effectiveness of the established controls. These weaknesses have resulted in instances of non-compliance with IR35 legislation, exposing the Council to potential penalties from HMRC, and repayment of historic employee income tax and NI liabilities.

The High rated finding highlights that processes require to be designed and implemented to ensure ongoing compliance with all aspects of IR35, including the requirement to respond to worker requests for assessment outcome details within prescribed timeframes; and initial and ongoing assessment of the employment status of worker groups (for example Daybreak Carers) and partnerships who provide services to the Council.

The High rated finding also reflects the need to ensure that training and guidance is provided to engaging managers to reflect their full range of IR35 responsibilities when engaging temporary workers.

Our Medium rated finding focuses on the need to ensure that contracts with third party recruitment agencies include details of the respective IR35 responsibilities for both the Council and the agencies, and details of the operational process that should be applied by both parties to ensure that the Council has discharged its duty to determine if IR35 working rules apply to temporary workers sourced from agencies.

We confirmed that controls to ensure compliance with Home Office Right to Work requirements are an integral part of the Councils recruitment and selection processes. Detailed procedures have been developed to ensure that appropriate checks are completed for all new employees, and re-performed where current employees have a limited right to work timeframe.

Review of documentation for a sample of employees identified some minor compliance issues relating to validation of documents confirming employee's right to work, and lack of Council wide monitoring to confirm the extent of ongoing compliance, and ensure that breaches are identified, addressed and reported to the Home Office where required. Consequently, a 'Low' rated finding has been raised.

3. Detailed findings

1. IR35 Compliance and Oversight Framework	High

IR35 Framework

Whilst the Council has established operational processes for assessing the employment status of temporary workers, no overall policy and supporting framework has been established that clearly defines IR35 roles and responsibilities across the Council.

Review of IR35 Operational Processes

Review of existing IR35 operational processes also established the following process and training gaps:

1. **Responding to worker requests** – currently no standard letters are issued to notify the worker or agency of the outcome of the initial IR35 assessment; and no process has been implemented to ensure that responses to worker or agency requests for details of IR35 assessment outcomes are issued within the 31 days specified in the legislation. Management has advised that they are not aware of receipt of any outcome requests to date;
2. **Partnerships** – Where a worker provides services through a partnership, an IR35 assessment should be completed should the partnership meet one of the conditions set out in section 61P of the Finance Act 2017. Management has confirmed that they were not aware of the requirement to assess the status of workers who provide services through partnerships. At the time of our audit, there were circa 300 live partnership vendor records, of which CPS has advised circa 107 are classed as small organisations providing services to the Council;
3. **Daybreak Carers** – At the time of our audit fieldwork, no IR35 assessments had been completed for a small group of approximately 40 workers (Daybreak Carers) provided through Shared Lives to the Health and Social Care Partnership (the Partnership) to provide short-term care to adults. These workers are self-employed and are paid as vendors through Oracle.

   Commercial and Procurement Services (CPS) requested copies of completed IR35 assessments, however were advised by the Partnership that Daybreak Carers may be entitled to HMRC's 'Qualifying Care Relief', and that IR35 requirements may not apply.

   CPS requested that the Partnership obtain a formal opinion from HMRC on the employment status of these workers. This had not been received by the conclusion of our audit fieldwork.

   Since the audit, Shared Lives have obtained an opinion from HMRC, however it is on a case specific basis, and for another local authority, therefore Shared Lives have advised they are unable to provide a copy of email from HMRC to evidence this. The position for City of Edinburgh Council therefore remains unconfirmed.

   Management also advised that Daybreak Carer arrangements are longstanding, and are supported by a 'Carer's Agreement' between the Partnership and the worker. Management advised no agreement was held on file for 2 workers sampled, and the 'Carer's Agreement' document had not been reviewed in some time.
4. **Training**– no training is currently provided to engaging managers to advise them of their initial and ongoing IR35 responsibilities.
5. **Orb content** - Locating the IR35 'off-payroll' process on the Orb assumes prior knowledge of IR35 legislation. The Orb content covers basic HMRC requirements for assessing the status of workers,

but does not provide all of the guidance required to ensure full compliance, including the requirement to:

- Monitor the duties, working arrangements, and integration of workers to ensure they remain reflective of the information which informed the assessment; and
- Reperform the IR35 assessment if the role, responsibilities or contract for a temporary worker changes during the period of engagement.

IR35 Compliance Oversight

Additionally, no oversight or monitoring processes have been established to confirm the extent of ongoing IR35 compliance across the Council, and ensure that breaches are identified; resolved and reported to HMRC (when required).

Instances of IR35 Non-Compliance

A total of 159 temporary workers were engaged across the Council between 1 October 2017 and 31 July 2018. We reviewed of a sample of 20 temporary workers engaged and identified the following areas of non-compliance with IR35 requirements:

1. 16 cases where, the HMRC assessment had been completed after the engagement commenced. Engaging managers sampled advised they had not been aware of this requirement until CPS requested a copy of the assessment to create/update the vendor record for payment. For each of these cases, the worker had been assessed as being outwith IR35;
2. 4 cases where a copy of the IR35 assessment and supporting evidence could not be provided by the Service Area; and
3. 1 case where the worker had completed the assessment themselves and forwarded it to the engaging manager

Risks

- Non-compliance with IR35 regulations;
- Lack of visibility of ongoing compliance with IR35 requirements across the Council, and inability to ensure that breaches are identified; escalated; addressed; and reported to HMRC where necessary;
- Inability to provide evidence to HMRC if required; and
- Potential non-compliance penalties and liability for payment of unpaid contributions to HMRC.

1.1 Documenting end to end IR35 processes

The Council should document and consider publishing via the Orb, the full end to end IR35 process, clearly setting out roles and responsibilities across Service Areas. (A process map was created by Internal Audit during the review which could be adapted and expanded for this purpose).

Agreed Management Action

The process map will be adopted, revised and maintained by Commercial and Procurement Services (CPS) with assistance from Human Resources and Payroll to ensure it clearly documents full end to end processes and sets out clear roles and responsibilities across all Service Areas. The process map will be made available on the Orb.

Owner: Stephen Moir, Executive Director of Resources. **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Colin Meikle, Senior Commercial Officer; Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant	**Implementation Date:** 30 September 2019

1.2 Responding to written requests within 31 days

A process for responding to written requests from workers regarding the outcome of their IR35 assessment (within 31 day legislative timeframe for response) should be designed and implemented. This could be achieved by requiring engaging managers to issue standard decision letters (sourced from the Orb) to workers following completion of IR35 assessments.

Agreed Management Action

The IR35 processes will be revised to require the engaging manager to issue a standard decision letter to all temporary workers following completion on an IR35 assessment. The revised process and template letters will be made available to engaging managers via the Orb.

Owner: Stephen Moir, Executive Director of Resources. **Contributors:** Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant; Steven Wright, Lead HR Consultant.	**Implementation Date:** 30 September 2019

1.3 Services provided by Partnerships

A process should be implemented to ensure IR35 assessments are complete all workers who provide services to the Council through a partnership.

In addition, a review of all current partnership records should be performed to identify where the engaging manager should be requested to complete a retrospective IR35 assessment for the worker.

Agreed Management Action

A new vendor form has been introduced which will trigger the requirement for an IR35 assessment to be complete for all small organisations with a headcount less than 10.

Circa 300 existing vendor records will be reviewed, and where required Commercial and Procurement Services (CPS) will request that the engaging manager complete a retrospective IR35 assessment for the worker.

Owner: Stephen Moir, Executive Director of Resources. **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Colin Meikle, Senior Commercial Officer.	**Implementation Date:** 30 September 2019

1.4 Employment status of Daybreak Carers

HMRC should be contacted to obtain a formal opinion whether the IR35 / intermediaries' legislation applies to Daybreak Carers providing services to the City of Edinburgh Council. A copy of the opinion confirmation letter should be provided to Commercial and Procurement Services (CPS) and Human Resources so they can update records as required.

Agreed Management Action	
The service has written to HMRC to obtain a formal opinion, this will be forwarded to both Commercial and Procurement Services (CPS) and Human Resources once received.	
Owner: Judith Proctor, Chief Officer Edinburgh Health and Social Care Partnership. **Contributors:** Tony Duncan, Interim Head of Strategic Planning; Mark Grierson, Disability Support & Strategy Manager; Anne-Marie Donaldson, Local Area Co-ordinator Manager; Craig Russell, Principal Solicitor – Employment.	**Implementation Date:** 31 July 2019

1.5 Daybreak Carer's Agreements
The current Carer's Agreement should be revised to ensure it clearly specifies the employment status of Daybreak Carers, and it complies with the requirements of General Data Protection Regulations (GDPR) in relation to confidentiality and record retention. All current Day Break Carers should be required to sign the revised agreement. The agreement should be reviewed on an annual basis and carers requested to resign where any revisions have been made.

Agreed Management Action	
The Carer's Agreement will be revised with assistance from the Council's Legal and Risk service to ensure it complies with all requirements. All current carers will be asked to sign a revised agreement. The agreement will be revised on an annual basis to take account of any relevant changes.	
Owner: Judith Proctor, Chief Officer Edinburgh Health and Social Care Partnership. **Contributors:** Tony Duncan, Interim Head of Strategic Planning; Mark Grierson, Disability Support & Strategy Manager; Anne-Marie Donaldson, Local Area Co-ordinator Manager; Craig Russell, Principal Solicitor – Employment.	**Implementation Date:** 30 September 2019

1.6 Review of all supplier groups
A review all current supplier groups paid via Oracle should be performed to ensure employment status has been confirmed, and appropriate action taken where retrospective IR35 assessments confirm that these workers should have been 'on payroll'.

Agreed Management Action	
All current supplier groups have been identified, however new groups may continue to arise as they are processed through feeder systems. A vendor form is required for all new vendors therefore effective controls are in place to manage this.	
Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Colin Meikle, Senior Commercial Officer.	**Implementation Date:** 29 March 2019

1.7 IR35 Training and awareness raising

Induction and refresher training for engaging managers should be designed and implemented to ensure that current and future engaging managers are fully aware of their IR35 responsibilities. This should include (but not be limited to) the requirement to consider and / or ensure:

- the employment status of temporary workers;
- services provided through partnerships;
- that assessments are performed and outcomes communicated prior to the start of the engagement; and
- that responses to queries received from workers and agencies regarding assessment outcomes should be provided within 31 days; and
- that all assessments are performed by the engaging manager and not the temporary employees.

Agreed Management Action

The current take-up of training across the Council is limited, therefore it is management's view that training would not be fully effective in addressing this risk. It is proposed that, in line with 1.8, the IR35 process and guidance available via the Orb will be revised to include all necessary requirements. Once revised, the revised guidance will be communicated across all the Council, with targeted communications for Service Areas who regularly use temporary workers.

Owner: Stephen Moir, Executive Director of Resources. **Contributors:** Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant; Steven Wright, Lead HR Consultant.	**Implementation Date:** 30 September 2019

1.8 IR35 Engaging Managers Guidance

In addition, IR35 'Off-payroll' content on the Orb should be revised to ensure it includes all points at recommendation 1.7, and instructions on the following:

- The requirement for the engaging manager to provide a copy of both the IR35 assessment and decision letter to either Commercial and Procurement Services (CPS) or Payroll when requesting payment to ensure evidence of assessments can be provided to HMRC if required;
- Additionally, to support this, the 'Off-payroll worker claim form' should be revised to include the requirement to attach the IR35 assessment and decision letter when requesting payment;
- The requirement for the engaging manager to manage the worker during engagement, including restrictions on the duties to be undertaken; and the requirement to reperform reassessments if the role or contract changes;
- Details of worker groups which are either IR35 exempt (for example, Foster Carers), or where a formal opinion on employment status has been obtained from HMRC (for example, Kinship Carers, Translators, and Curators Ad Litem). This should include the HMRC opinion for Daybreak Carers.

Agreed Management Action

As per 1.7, the IR35 process and guidance available via the Orb will be revised to include all necessary requirements. Once revised, the revised guidance will be communicated across all the Council, with targeted communications for Service Areas who regularly use temporary workers.

Owner: Stephen Moir, Executive Director of Resources. **Contributors:** Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant; Steven Wright, Lead HR Consultant.	**Implementation Date:** 30 September 2019

1.9 Monitoring and review of IR35 compliance

A risk based monitoring and review process should be designed and implemented to confirm the extent of ongoing compliance with IR35 requirements across the Council. Any breaches identified by either Commercial and Procurement Services (CPS) or Payroll should be reported to the relevant Heads of Service; Executive Directors; and the Corporate Leadership Team to ensure that appropriate remedial action is taken, and reported to HMRC where required.

Agreed Management Action

Commercial and Procurement Services (CPS) will, in collaboration with Payroll, monitor non-compliance with IR35 processes across the Council, and report on an exception basis to relevant Heads of Service to ensure remedial action is taken. Persistent breaches will be escalated to Executive Directors and the Corporate Leadership Team, and where required, reported to HMRC.

Owner: Stephen Moir, Executive Director of Resources. **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Colin Meikle, Senior Commercial Officer; Grant Craig, Employee Life Cycle Lead Consultant; Linda Rowe, Payroll Specialist.	**Implementation Date:** 30 September 2019

2. Inclusion of IR35 responsibilities in contracts for agency worker suppliers — **Medium**

Review of the contractual arrangements for the agencies who supply temporary workers to the Council established that:

1. Pertemps

Management advised, that by arrangement, Pertemps only supply workers who are either paid directly through Pertemps payroll or employed via an umbrella company. Therefore, no IR35 assessment is performed as it does not apply to the engagement. We note however, this arrangement, has not been agreed formally in writing, either within the original framework tender documents, or within the final contract issued.

In addition, Pertemps does not provide confirmation of the payment status for individual workers (whether paid via their payroll or an umbrella company) prior to the start of an engagement on a routine basis. Consequently, as the responsibility to decide if off-payroll rules apply lies with the Council, there is no assurance IR35 responsibility has been discharged.

Pertemps has confirmed that it will be possible to provide this information going forward.

2. Other Agencies

Other agencies are used when Pertemps cannot meet recruitment requirements for a specific role. We reviewed a sample of three out of eight agency contracts established that (as with Pertemps) whilst informal arrangements were in place, contractual arrangements did not specify the processes to be applied by the agency to ensure effective discharge of the Council's IR35 responsibilities.

Our review also noted the Council's Terms and Conditions for Services issued when a waiver is granted does not include any reference to compliance with IR35 or intermediaries' legislation.

Risks

- The Council cannot confirm that it has effectively discharged its IR35 responsibilities for workers engaged through recruitment agencies; and
- The Council could potentially be liable for penalties and payment of unpaid contributions to HMRC.

2.1 Formal Assurance from Pertemps

The Council should obtain formal written assurance from Pertemps that all current and future workers supplied to the Council will either be paid through Pertemps payroll or an umbrella company.

Agreed Management Action

A contract variation in relation to IR35 / intermediaries' legislation will be drafted and issued to Pertemps to ensure the Council receives assurance over the employment status of current and future workers supplied.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Katy Miller, Head of Human Resources; Steven Wright, Lead HR Consultant; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Craig Russell, Principal Solicitor – Employment	**Implementation Date:** 30 September 2019

2.2 Assurance for other recruitment agencies

The Council's Terms and Conditions for Services should be revised to include reference to IR35 / intermediaries' legislation. This should include the requirement for the provider to confirm how the worker will be paid (i.e. self-employed, agency payroll or umbrella company). In addition, the Terms and Conditions should advise that where the worker is not paid via the agency payroll or an umbrella company, the Council will need to complete an IR35 assessment prior to employment commencing. The revised Terms and Conditions should be issued with all waivers.

The Council should also seek confirmation on the payment status of all workers currently supplied by other recruitment agencies.

Agreed Management Action

The Council's Terms and Conditions for Services will be revised to include roles and responsibilities of both the Council and the recruitment agency in relation to IR35 / intermediaries' legislation. The revised Terms and Conditions will be issued for all future waivers.

The Commercial and Procurement Services (CPS) Waiver Team will produce a list of all workers currently provided by other recruitment agencies and request that the engaging manager seeks confirmation from the agency on how the worker is paid.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Ronnie Swain, Commercial Partner; Mark Crolla, Commercial Operations Officer; Craig Russell, Principal Solicitor – Employment	**Implementation Date:** 30 September 2019

3. Right to Work Compliance and Breach Reporting	Low

Right to Work Compliance

Review of a sample of 25 new employees and 10 employees with time limited right to work permission confirmed a high level of compliance with Home Office requirements. However, the following minor compliance issues were noted:

- For 1 worker, no documentation was held on file to demonstrate that the right to work check had been performed. Evidence was subsequently provided and added to the employee file;
- For 1 worker, while the date of the check was recorded within iTrent, it was not recorded on the validated copies of documents held within the employees file, in line with the Council's procedure; and
- Validated documents for 5 employees did not include the appropriate validation statement and signature of the manager completing the check in line with the Council's procedure.

Management have advised as the Home Office requirement is only to record the date of the check, they are considering removing the requirement to record the validation statement, date and signature on the copies of documents retained as this is now recorded electronically within iTrent.

Right to Work Breach Reporting

HR proactively monitors completion of right to work checks; issuing reminders to Service Areas to ensure follow-up checks are completed prior to expiry of time limited permission, and escalating instances of non-compliance to senior management for resolution. We note however, no Council wide reporting of overall compliance with right to work requirements has been produced since completion of the Employee Compliance project.

Management has advised that implementation of a suite of appropriate reports is currently being considered.

Risks

- The Council is unable to demonstrate full compliance with Home Office Right to Work legislative requirements;
- The Council cannot establish a 'statutory excuse' for employing an illegal worker; and
- The Council is liable to civil penalties, wider sanctions and reputational damage.

3.1 Recording the date of check in line with Home Office requirements

The Council is required to make a contemporaneous record of the date when the right to work check was conducted. Should the decision be made to remove the requirement for all recruiting managers to sign, date and record the validation statement, the Council will need to ensure the date recorded on iTrent is the *actual date* the check was conducted. Guidance on the Orb and within the Recruitment – manager guide should be updated and communicated to reflect this requirement.

Agreed Management Action

The Council will retain the requirement for recruiting mangers to sign, date and record the validation statement on the actual date the check was conducted. The Orb will be updated and communication sent to remind managers of this requirement.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant; Steven Wright, Lead HR Consultant; James Bertram, HR Consultant.	**Implementation Date:** 30 September 2019
3.2 Monitoring and review of right to work compliance	
Regular reporting should be developed to confirm the extent of ongoing compliance with right to work requirements across the Council. Any breaches identified should be reported to the relevant Heads of Service, and Executive Directors to ensure that appropriate remedial action is taken.	
Agreed Management Action	
We will implement regular reporting on right to work compliance, reporting six monthly on overall compliance across the Council and on an exception basis to relevant Heads of Service to ensure remedial action is taken to address any non-compliance. Persistent breaches will be escalated to Executive Directors.	
Owner: Stephen Moir, Executive Director of Resources **Contributors:** Katy Miller, Head of Human Resources; Grant Craig, Employee Life Cycle Lead Consultant; Steven Wright, Lead HR Consultant; James Bertram, HR Consultant.	**Implementation Date:** 30 September 2019

Appendix 1 - Basis of our classifications

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

The City of Edinburgh Council

Internal Audit

Validation of Internal Audit Implemented and Sustained Management Actions

Final Report

9 April 2019

CW1810

Overall report rating:

Significant enhancements required	Significant areas of weakness and non-compliance in the control environment and governance and risk management framework that puts the achievement of organisational objectives at risk

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2018/19 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2018. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

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

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

1. Background and Scope

Background

Internal Audit (IA) findings are raised where audit outcomes confirm that the controls established to mitigate the Council's most significant risks are either inadequately designed or are not operating effectively.

When finalising IA reports, management agree to implement agreed actions that will address the control weaknesses identified. Implementation of these agreed actions will ensure that the associated risks are effectively managed, reducing the Council's overall exposure to risk.

It is essential that (once implemented), the control improvements are effectively sustained. If not, the Council remains exposed to an unnecessary level of risk.

A 'validation' audit was introduced in the 2018/19 IA plan to assess whether management actions implemented to address historic findings raised by IA have been sustained and remain effective.

In March 2018, a 'self-attestation' exercise was completed across the Council. This involved Executive Directors attesting whether all 174 IA findings (48 High and 126 Medium) raised in the period 1 April 2015 to 31 March 2017 had been implemented and sustained; implemented but not sustained; or not implemented (see Appendix 2 for definitions).

The Executive Directors confirmed that a total of 114 (30 High and 84 Medium) IA findings raised had been implemented and sustained.

Scope

The objective of this review was to validate whether a representative sample (10%) of the 114 High and Medium rated IA findings have been effectively implemented and sustained as confirmed by completion of the 'self-attestation' exercise.

Of the 114 findings, a sample of 11 findings with 24 supporting management actions covering all Council Directorates was selected, and tested, to confirm their current status.

Our review concluded as at 7 December 2018, and our findings and opinion are based on the outcomes of our testing at that date.

Where the necessary control improvements have not been implemented and effectively sustained, the relevant findings and supporting management actions have been reopened; regraded (where appropriate based on residual risk) and reported as overdue, based on the originally agreed implementation dates.

2. Executive summary

Total number of findings: 3

Summary of findings reopened	
High	1. Communities and Families - Use of unsupported technology devices in schools
High	2. Health and Social Care – Management structure and business support arrangements – regraded from Medium
Low	3. Resources - One Time Payments Authorisation – regraded from Medium

Opinion

In our opinion, significant enhancements are required to ensure that management effectively implement and sustain the necessary control improvements to support closure of Internal Audit findings.

Our review confirmed that control improvements supporting 8 of the 11 original findings (4 High and 4 Medium) had had been effectively implemented and sustained, with three findings (1 High, and 2 Medium) where further action is required to fully address the risks.

Consequently, these findings and supporting management actions that have not been fully implemented and sustained have been regraded (where appropriate reflecting the associated residual risk); will be reopened; and reported as overdue based on originally agreed implementation dates.

One finding has been reopened as a High; one regraded from a Medium to a High; and one finding downgraded from Medium to Low.

Details of our ratings classifications and an explanation of the conclusions applied to our validation outcomes are included at Appendices 1 and 2.

Communities and Families - Use of unsupported technology devices in schools

The first reopened High rated finding relates to use of unsupported technology devices in schools. The original finding included three agreed management actions. Of these, one has been implemented but not sustained; one partially implemented; and one not implemented. The rating for this finding has not been reduced as the residual risk associated with lack of confirmation that non-centrally supported devices that could contain personal, sensitive information are appropriately secured is considered significant.

Health and Social Care – Management structure and business support arrangements

The second reopened High finding (regraded from Medium) relates to lack of clarity in relation to the Partnership' management structure, and the scope and oversight of business support arrangements provided by the Council to the Health and Social Care Partnership. The original finding included three management actions, and none of these have yet been implemented.

This is partially attributable to a significant number of senior management changes within the Partnership (the new Chief Officer was appointed in May 2018) and the Council (the new Head of Customer, with responsibility for Business Support functions, except in Schools, was appointed in March 2017). It is also important to note that the Business Support structure was only established in October 2016 as part of the Council's Transformation Programme, following a simplistic approach to the centralisation of the

majority of staff with Business Support job titles into a single function, with significant additional time required for its subsequent implementation.

As the full population of Partnership operational processes has not been documented (this is reflected in the High rated finding raised in the Health and Social Care Partnership Purchasing Budget Management review, completed July 2018), it has not been possible to reach formal agreement on the scope of the services provided by the Business Support and Transaction teams within Customer to support the Partnership, or establish appropriate service levels and supporting key performance indicators enabling effective oversight of service delivery.

The control gaps and residual risks associated with lack of clear definition and oversight of Partnership business support arrangements provided by the Council have been highlighted in the significant findings raised in relation to Business Support administrative support services provided to care homes (Care Homes Assurance review, February 2018); management of client funds (Social Work Centre Bank Account Reconciliations review, April 2018); and a number of financial and operational processes (Health and Social Care Partnership Purchasing Budget Management review, July 2018).

Resources - One Time Payments Authorisation

The final Low rated finding (regraded from Medium) relates to controls supporting authorisation of manually processed 'one time' payments. The original finding included three management actions. Of these, two have been implemented and sustained, and one partially implemented and sustained. The reduced rating reflects the residual risk associated with processing lower volumes of payments, without confirming that they have all been appropriately authorised by Directorates/Divisions.

Overall conclusion

Consequently, all three Findings have been reopened and will be reported as overdue based on originally agreed implementation dates.

Our detailed findings and new recommendations are detailed at Section 3 below.

3. Detailed findings

1. Communities and Families - use of unsupported technology devices in schools	High

Original finding

This High rated finding was originally raised in the Schools IT Systems review completed in February 2016. The original finding established that:

- Teaching staff commonly use personal and school-managed computers for work purposes, which may on occasion involve personal and sensitive data. These devices are not hosted on behalf of the Council by CGI, and may not have full security such as passwords and anti-virus and encryption software installed. We identified one instance where sensitive personnel data was held on an unencrypted memory stick;
- Office 365 has been introduced to all schools, enabling staff and pupils to work remotely on a secure web-based platform, eliminating the need for data to be stored on hard drives. However, use of Office 365 is still limited in some schools and there is evidence that data is still stored on personal and school-managed hard drives;
- Whilst staff are required to comply with the corporate Acceptable Use of IT policy, the policy does not specify security required when staff are using their own device for work purposes; and
- We further noted that staff at six of the14 schools visited had not completed mandatory training on information governance at time of our audit visits between September and November 2015.

Validation outcomes

The outcomes of our validation work confirmed that one of the three management actions associated with this finding has been implemented but not sustained; one partially implemented and sustained; and one not implemented.

Consequently, this finding will be reopened as a High rated finding (reflecting the residual risk) with supporting management actions tracked against the originally agreed implementation dates.

Our testing established that:

- Guidance for the use of non-hosted devices (now referred to as Personal Devices and Office 365) has been created, however there is a lack of clarity in the guidance in relation to physical security of personal devices containing Council information.

  Conclusion: Partially implemented and sustained.
- Evidence was provided confirming that guidance had been introduced to schools via head teachers' and ICT co-ordinators' forums, and that it had been circulated once to schools.

  Conclusion: Implemented but not sustained.
- An email was received confirming that annual confirmation that employees are applying the guidance is not obtained.

  Conclusion: Not implemented.

Risk

The original risk that personal and sensitive data may be held on unencrypted devices, increasing the risk of a data security breach if the device is lost or stolen has not been fully mitigated, as confirmation that employees are applying the guidance when using personal and school equipment is not obtained.

1. Recommendation – Guidance for use of non-hosted devices
The guidance for use of non-hosted devices in schools should be expanded to include physical security of devices (i.e. safe storage); and should be re-issued annually across all schools; special schools; and nurseries.
Agreed Management Action
A new protocol has been developed to accompany the Acceptable Use Policy This will be emailed to all school offices in May ready for the new school year.
Owner: Alistair Gaw, Executive Director of Children and Families **Contributors:** Andy Gray, Head of Schools and Lifelong Learning**,** Cheryl Buchanan, Operations Manager; Lorna Sweeney, Senior Manager Quality, Improvement & Curriculum; Richard Burgess, ICT Strategy Manager
Original Implementation Date: 31 March 2016 **Revised Implementation Date:** 30 August 2019
2. Recommendation – Application of guidance by employees
Employees should be requested to provide annual confirmation that they have read and understood the guidance, and consistently applying it to all devices used in schools.
Agreed Management Action
Staff will be asked to read and sign annually that they will adhere to the guidance, particularly the use of passwords and minimum operating requirements.
Owner: Alistair Gaw, Executive Director of Children and Families **Contributors:** Andy Gray, Head of Schools and Lifelong Learning, Cheryl Buchanan, Operations Manager; Lorna Sweeney, Senior Manager Quality, Improvement & Curriculum; Richard Burgess, ICT Strategy Manager
Original Implementation Date: 31 March 2016 **Revised Implementation Date:** 30 August 2019

2. Health and Social Care – Management structure and business support arrangements	High
Original finding This Medium rated finding was originally raised in the Integrated Health and Social Care review completed in August 2015 and established that: Although responsible officers had been assigned from both NHS Lothian and CEC to support several Partnership and EIJB processes, it is not clear how, roles and responsibilities will split between the two parties. This includes, but is not limited to, how the skills and resources of both partners will be used effectively to meet the demands for Health and Social care appropriately. Staff who support both delegated Partnership functions and the EIJB are employed either by CEC or NHS Lothian, and this will continue to be the case following delegation. An integrated partnership and EIJB management structure has not yet been agreed, and this may take a significant amount of time to implement once the structure has been agreed.	

Functions which are not delegated, for example business support roles, will be managed separately by the Council and NHSL. The operation of these functions will need to be agreed by both bodies, and the two must work co-operatively to agree how best to support the Partnership and IJB. This will be made more difficult by the changes in management as internal secondments finish, and as the new management structure begins, therefore potentially losing continuity between the pre- and post-delegation management structures.

Validation outcomes

The outcomes of our validation work confirmed that none of the three management actions associated with this finding have been implemented.

Consequently, this finding will be reopened as a High rated finding (reflecting the residual risk) with supporting management actions tracked against the originally agreed implementation dates.

Our testing established that:

- The originally agreed management action to implement an agreed Partnership organisational management structure has not been finalised, implemented, and embedded due to a number of Senior Management and Chief Officer changes within the Partnership and the Council.

  Conclusion: Not implemented

- The originally agreed management action to arrange focus groups to discuss partnership and EIJB business support arrangements and establish options has not been completed.

  Management has advised that the requirement for focus groups was superseded by meetings between the Interim Chief Officer and Head of Customer and Digital Services. Dates from two meetings in March and April 2018 were provided as evidence that these meetings took place, however no evidence of meeting outcomes; decisions in relation to the agreed structure of business support arrangements; and dates of subsequent meetings was provided.

  Conclusion: Not implemented

- The originally agreed management action to establish SLAs for business support outwith the organisational management structure has not been completed.

  Conclusion: Not implemented

Risk

- Partnership senior management structures are unclear and the Partnership may not be consistently and effectively managed; and
- The Partnership may not receive either the required scale or quality of operational business support required to ensure effective service delivery.

1. Recommendation – Partnership Management Structure

Review of the Partnership operational management structure should be completed by the Chief Officer, approved by the EIJB, and implemented.

Agreed Management Action

The Partnership's organisational management structure will be finalised, implemented, and embedded.

The revised structure does not need to be approved by the IJB because it is an operational matter. It will however be presented to the EIJB for information.

The revised implementation date of April 2020 will allow completion of Partnership budget and transformation Programmes.

Owner: Judith Proctor, Chief Officer HSCP

Contributors: Cathy Wilson, Health and Social Care Partnership Operations Manager

Original Implementation Date: 31 December 2015

Revised Implementation Date: 30 April 2020

2. Recommendation – Business Support Arrangements

Business support arrangements for both the Partnership and EIJB should be agreed, implemented, and consistently applied.

Agreed Management Action

- Focus Groups to review and discuss current Partnership and EIJB business support arrangements will be established.
- Senior Partnership Managers will nominate a Partnership Officer aligned to a business support service to provide insight on role expectations and key statutory and non-statutory functions for each business support function.
- Business Support Senior Managers will also nominate relevant officers to participate in Focus Groups.

Owner: Judith Proctor, Chief Officer HSCP

Contributors: Stephen Moir, Executive Director of Resources**;** Nicola Harvey, Head of Customer and Digital Services; John Arthur, Senior Manager, Business Support; Cathy Wilson, Health and Social Care Partnership Operations Manager

Original Implementation Date: 31 December 2015

Revised Implementation Date: 30 June 2019

3. Recommendation – Business Support Service Level Agreements

- A proportionate set of business support service level agreements and support key performance indicators that cover all aspects of business support and transaction services provided to the Partnership by the Council should be defined; approved by both Partnership and Council senior management; and implemented; and
- Ongoing meetings should be established between relevant senior managers in the Partnership and Business Support to ensure performance against SLAs is monitored on an ongoing basis, with any performance issues escalated to the Partnership senior management team for consideration and resolution.

Agreed Management Action

- The Partnership and Business Support Service will jointly establish SLAs for business support outwith the organisational management structure.
- Regular meetings between relevant senior managers in the Partnership and Business Support will be established to ensure performance against SLAs is monitored. Any performance issues will be escalated to the Partnership's Executive Team for consideration and resolution.

Owner: Judith Proctor, Chief Officer HSCP

Contributors: Stephen Moir, Executive Director of Resources**;** Nicola Harvey, Head of Customer and Digital Services; John Arthur, Senior Manager, Business Support; Cathy Wilson, Health and Social Care Partnership Operations Manager

Original Implementation Date: 31 December 2015

Revised Implementation Date: 31 October 2019

3. Resources - One Time Payments Authorisation	Low

Original finding

This finding was originally raised as a Medium in the Continuous Controls – One Time Payments review completed in January 2016, and established that:

- There were no effective controls around authorisation and approval of 'One Time Payment' (OTP) payments.
- The Oracle payment system did not record the name of the relevant Service Area manager who authorised the payment. Instead, a paper form, requiring two authorising signatures, was provided by the relevant service area to the Payments Services Team;
- Some payment request forms are 'pp'd' by a member of staff within the authorisation field.
- Some signatures authorising payment were illegible;
- Payments were processed by the Payments Services Team on the basis that they had been appropriately authorised by the service area. There was no authorised signatory list or delegated authority level available for reference by the for the Payments Services team to confirm that authorisation received from service areas is appropriate and authentic; and
- Segregation of duties controls supporting processing of OTPs were not effective.

Validation outcomes

The outcomes of our validation work confirmed that 2 of the 3 management actions associated with this finding have been implemented and sustained, and 1 has been partially implemented.

We also established that the volume of one time payments had reduced by approximately 2,000 and £1.3m in value between June 2016 and August 2017, reducing the risks associated with manual authorisation and processing.

Consequently, this finding will be reopened and downgraded to a Low rated finding (reflecting the residual risk) with supporting management action tracked against the originally agreed implementation dates.

Our testing established that:

- Payment Services agreed that any one time payment forms received with a 'pp' in the authorisation field would be rejected. Review of a sample of 25 one time payments established that only one payment request had been processed that included a 'pp' in the authorisation field, however Payments Services confirmed that the supporting documentation had been approved by the correct person in the service area; that the processing of this application had been an error and that the normal process is to reject these applications.

  Conclusion: Implemented and sustained.

- Payment Services had agreed that they would request one time payment authority lists from service areas; check all requests prior to processing to ensure that the appropriate authority had been obtained; and reject any requests that have not been correctly authorised. This management action has been partially completed.

  Review of a sample of 25 payments confirmed that 18 had been compared to an approved list of authorisers prior to payment, whilst 7 had not. Supporting evidence was provided for 6 of the 7 payments.

Management has confirmed that a list of authorisers is maintained for services areas who submit high volumes of one time payment requests (for example Council tax, PPSL, and Parking) and effective checks are performed to confirm that these have been appropriately authorised prior to processing the payment. Payments that have not been appropriately authorised are rejected.

Authorisation lists are not maintained for service areas that submit ad hoc one time payment requests, therefore no authorisation checks are performed prior to processing. If supporting evidence is not provided for a payment, the request will be rejected and returned.

Conclusion: Partially implemented and sustained

- Payment Services also agreed that manual signatures on payment authorisation forms would be replaced by requests received via e mail; processed where addresses were consistent with agreed departmental approval lists; and e mail requests retained in archive folders to enable confirmation of ongoing process compliance and audit review.

  Review of the payment authorisation process established that whilst paper payment requests continue to be accepted, the e mail confirmation process has been introduced. E mail payment requests retained for 12 months prior to automatic deletion by CGI, however all payment request forms are printed and archived at Iron Mountain in accordance with the Council's records retention policy.

  Conclusion: Implemented and sustained.

Risk

Potential risk of fraud and / or error associated with low volume high value payments where appropriateness of service area payment authorisation is not confirmed.

1. Recommendation – Authorisation of payment requests

- For ad hoc payment requests, a risk based approach should be adopted, where Divisions will be contacted to confirm that authority for all one time payments in excess of a specified threshold is appropriate; and
- Payments that have not been appropriately authorised should be rejected.

Agreed Management Action

- Services will be contacted and requested to confirm appropriateness of authority for all ad hoc payment requests received in excess of £500;
- Payments that have not been appropriately authorised will be rejected;
- A revised process note will be prepared and implemented within the Payments team, and signed confirmation obtained from team members that they understand the reviewed process; and
- A small sample of ad hoc payments will be reviewed by Payments managers on an ongoing basis to confirm that the process has been effectively embedded.

Owner: Stephen Moir, Executive Director of Resources

Contributors: Nicola Harvey, Head of Customer and Digital Services; Neil Jamieson, Senior Manager, Customer Contact and Transactions; Sheila Haig, Customer Manager.

Original Implementation Date: 29 February 2016

Revised Implementation Date: 30 April 2019

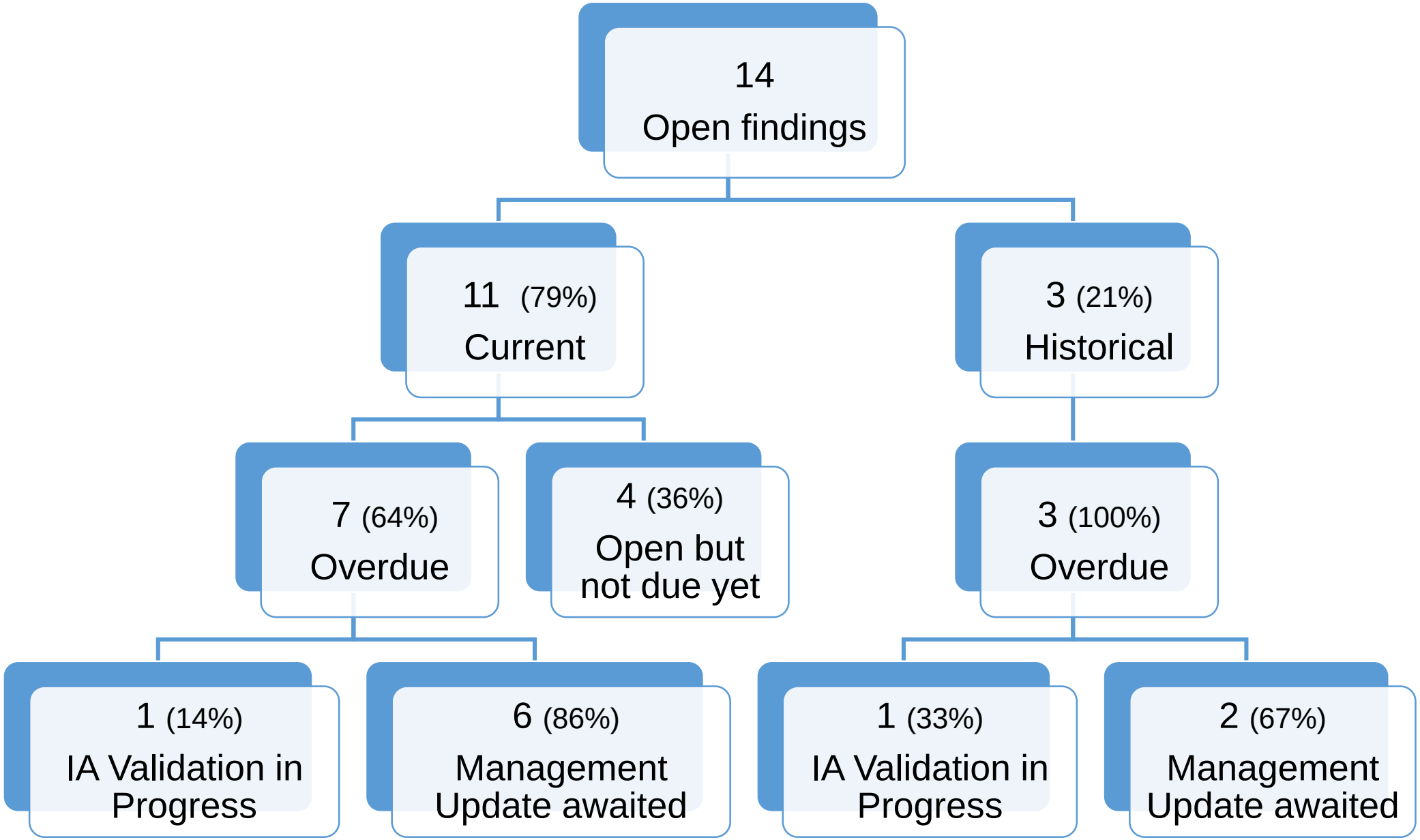
Appendix 1 - Basis of our classifications

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 – Conclusion definitions

Conclusion	Definition
Implemented and sustained	Controls have been fully implemented, and our testing confirmed that they have been sustained
Partially implemented and sustained	Controls have been partially implemented, and our testing confirmed that the elements implemented have been sustained
Implemented but not sustained	Controls were initially implemented, but have not been sustained
Not implemented	Controls have not been implemented

Appendix 5 – EIJB Internal Audit Open and Overdue findings position as at 6th May 2019



Internal Audit Overdue Management Actions Appendix 6

Glossary of terms
Project – This is the name of the audit report.
Owner – The Executive Director responsible for implementation of the action.
Issue Type – This is the priority of the audit finding, categorised as Critical, High, Medium, Low and Advisory.
Issue – This is the name of the finding.
Status – This is the current status of the management action. These are categorised as Pending (the action is open and there has been no progress towards implementation), Started (the action is open and work is ongoing to implement the management action), Implemented (the service area believe the action has been implemented and this is with Internal Audit for validation).
Agreed Management action – This is the action agreed between Internal Audit and Management to address the finding.
Estimated date – the original agreed implementation date.
Revised date – the current revised date. Red formatting in the dates field indicates that the action has missed the latest revised date.
Number of revisions – the number of times the date has been revised post implementation of TeamCentral. Amber formatting in the dates field indicates the date has been revised more than once.
Contributor – Officers involved in implementation of an agreed management action.

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates
1	Edinburgh IJB - Performance Data Performance objectives not stated for all Directions. Judith Proctor, Chief Officer	High	Rec 1.1 - Performance objectives not stated for all Directions. Started	Management Action: Current directions will be reviewed and revised to ensure that they state clear and effective performance objectives.	Estimated Date: 31/12/2018 Revised Date: 31/05/2019 No of Revisions 1
2	Edinburgh IJB - Performance Data Performance objectives not stated for all Directions. Judith Proctor, Chief Officer	High	Rec.2.1 - Reporting arrangements for directions Started	The Management Action: Reporting requirements for each direction will be explicitly stated, including which committee performance information will be reported to, who will report it, and how frequently it will be reported.	Estimated Date: 31/12/2018 Revised Date: 31/05/2019 No of Revisions 1

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates
3	Edinburgh IJB - Performance Data Performance objectives not stated for all Directions. Judith Proctor, Chief Officer	High	Rec.2.2 - Reporting frequency for directions Started	Performance reporting will now be done on the basis of the directions, and will be reported to relevant Integrated Joint Board committees on a regular basis to ensure that the implementation of the directions can be monitored effectively.	Estimated Date: 31/12/2018 Revised Date: 31/05/2019 No of Revisions 1
4	Historic Unimplemented Findings HSC1503 - issue 3 Quality Assurance Judith Proctor, Chief Officer	High	Recommendation 3a Implemented	There is an existing file audit process that will pick up on overall issues of both data quality and quality of recording. In order to address the specific issues identified through this audit the Quality Assurance Team will undertake a themed audit in respect of Personal Support Plans. This will involve engaging with key managers to establish the questions that need to be answered and will include consideration of the model used in the North West Team.	Estimated Date: 31/12/2016 Revised Date: 29/03/2019 No of Revisions 1

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates
5	Historic Unimplemented Findings HSC1603 - issue 1 Performance Management Framework in development Judith Proctor, Chief Officer	High	Recommendation 1a Started	We now monitor and have data against the 23 core indicators. However, the 2016/17 data will not be available by July 2017. This is a national issue and Scottish Government is aware of it. A Performance Board is being established as part of the overall governance framework for the Health and Social Care Partnership which will work closely with the Integrated Joint Board Performance and Quality Group. The main role of the Performance Board will be to agree the core set of performance indicators and monitor delivery against these. The Board will have its first meeting in February 2017.	Estimated Date: 28/02/2017 Revised Date: 28/02/2019 No of Revisions 1
6	Historic Unimplemented FindingsHSC1603 - issue 1 Performance Management Framework in development Judith Proctor, Chief Officer	High	Recommendation 1b Started	An initial meeting has taken place to discuss the content of the Annual Performance Report. A core group has been identified to take this forward and a series of meetings is being arranged for early in the New Year. The intention is for a draft report to go to the Integrated Joint Board Development session in April 2017.	Estimated Date: 31/07/2017 Revised Date: 28/02/2019 No of Revisions1

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates
7	Historic Unimplemented Findings HSC1603 - issue 1 Performance Management Framework in development Judith Proctor, Chief Officer	High	Recommendation 1c Started	A governance framework has been developed and documented setting out the roles remits and membership of the various committees and groups and the relationship between them.	Estimated Date: 28/02/2017 Revised Date: 28/02/2019 No of Revisions 1
8	Historic Unimplemented Findings HSC1603 - issue 2 Performance information does not meet the needs of users Judith Proctor, Chief Officer	Medium	Recommendation 2c Started	The existing Performance Improvement Meeting (PIM) will be replaced by a Performance Board, membership of which will include all members of the Integrated Joint Board Executive Team.	Estimated Date: 28/02/2017 Revised Date: 20/12/2019 No of Revisions 2
9	IJB Data Integration & Sharing Prioritisation process Judith Proctor, Chief Officer	High	Roadmap Started	Roadmap of Information Communication Technology requirements to be developed based upon priorities for delivery of the Integrated Joint Board Strategic Plan.	Estimated Date: 30/09/2017 Revised Date: 31/12/2019 No of Revisions 3
10	IJB Data Integration & Sharing Prioritisation process Judith Proctor, Chief Officer	High	Prioritisation process Started	Prioritisation of requirements to be agreed through the Edinburgh Health and Social Care Partnership Information Communication Technology and Information Governance Steering Group.	Estimated Date: 30/09/2017 Revised Date: 31/12/2019 No of Revisions 3

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates
11	IJB Data Integration & Sharing Prioritisation process Judith Proctor, Chief Officer	High	Communication Started	Vision and goals in respect of Information Communication Technology to be conveyed through the development and publication of an Information Communication Technology Strategy for the Edinburgh Health and Social Care Partnership.	Estimated Date: 31/10/2017 Revised Date: 31/12/2019 No of Revisions 3
12	IJB Data Integration & Sharing Robustness of access management & data protection processes Judith Proctor, Chief Officer	High	Access management Started	The existing processes within the Council and NHS Lothian for notifying system owners of staff changes will be communicated to all managers of integrated teams. Establishing an integrated system setting out the systems access requirements for all posts and the mechanism for gaining access for new staff and notifying system owners of leavers and changes in role will be a priority for the nominated officer to be identified in respect of Information Communication Technology and Information Governance.	Estimated Date: 30/09/2017 Revised Date: 31/12/2019 No of Revisions 2
13	IJB Data Integration & Sharing Hardware compatibility and connectivity in NHS and CEC locations Judith Proctor, Chief Officer	Medium	Connectivity and Hardware compatibility Started	The Information Communication Technology and Information Governance Steering Group will request a review of connectivity and hardware compatibility to be conducted across all sites housing integrated teams and consider any recommendations arising from that review.	Estimated Date: 30/06/2017 Revised Date: 31/12/2019 No of Revisions 2

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates
14	IJB Data Integration & Sharing Lack of available training, policies and guidance Judith Proctor, Chief Officer	Medium	Data Protection Training Started	The nominated officer with responsibility for Information Communication Technology and Information Governance will work with relevant colleagues in the Council and NHS Lothian to develop an integrated approach to data protection training taking account of the role and responsibilities of the Integrated Joint Board.	Estimated Date: 31/12/2017 Revised Date: 31/12/2019 No of Revisions 2
15	IJB Data Integration & Sharing Lack of available training, policies and guidance Judith Proctor, Chief Officer	Medium	Compliance with training plan Started	A training plan will be developed to ensure all existing staff who need to access systems belonging to both the Council and NHS Lothian receive the appropriate training to enable them to use the system appropriately with due regard to data protection. Training on all systems to be used by a postholder will become part of the mandatory training for new appointments. Compliance with this arrangement will be overseen by the nominated officer with responsibility for Information Communication Technology and Information Governance.	Estimated Date: 31/03/2018 Revised Date: 31/12/2019 No of Revisions 2

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates
16	Personalisation SDS - Option 3 Data Quality Judith Proctor, Chief Officer	Medium	Data Quality Implemented - Audit Approved	Original management action: A change management process will be established and overseen by the Self Directed Support Infrastructure Steering Group. The inconsistencies in data recording are as a result of numerous changes to processes and trying to reduce the recording burden of implementing these on frontline practitioners. The Research and Information Team are aware of all changes to recording practice and take these into account. A summary of all changes and the impact on data extraction has also been produced. Rebased management action: April 2019. Since the audit, the assessment tool has been revised. All assessments are now carried out using the same tool.	Estimated Date: 30/06/2016 Revised Date: 31/08/2019 No of Revisions 6
17	Purchasing Budget Management EIJB1701 - Issue 2 Financial Controls Judith Proctor, Chief Officer	High	EIJB1701 - Issue 2.5b Amendment of Personal Support Plan Implemented	The Personal Support Plan will be amended to enable multiple cost centres and multiple services to be used for relevant support packages. New authorisation field will also be set up and ready for alignment with current delegated authorities as part of the finance migration.	Estimated Date: 28/02/2019 Revised Date: No of Revisions 0

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates
18	Purchasing Budget Management EIJB1701 - Issue 2 Financial Controls Judith Proctor, Chief Officer	High	EIJB1701 - Issue 2.6b Authorisation for new care cost entries Implemented	A new entry will be made for each new care costs with appropriate authorisation providing an audit trail as part of the financial migration work.	Estimated Date: 28/02/2019 Revised Date: 30/04/2019 No of Revisions 1
19	Purchasing Budget Management EIJB1701 - Issue 3 Operational Structure Processes Judith Proctor, Chief Officer	High	EIJB1701 - Issue 3.3 Alternative generation of key client documents (ICT) Implemented	Information Communications Technology to resolve fault and successfully test asmall sample of users who had been rolled back to Office 2013 to Microsoft 2016 prior to the Computer Refresh Programme.	Estimated Date: 28/02/2019 Revised Date: No of Revisions 0
20	Purchasing Budget Management EIJB1701 - Issue 2 Financial Controls Judith Proctor, Chief Officer	High	EIJB1701 - Issue 2.3a Charging policy owner Started	The Chief Finance Officer is the member of the Partnership Executive Team with responsibility for charging.	Estimated Date: 31/01/2019 Revised Date: No of Revisions 0
21	Purchasing Budget Management EIJB1701 - Issue 2 Financial Controls Judith Proctor, Chief Officer	High	EIJB1701 - Issue 2.6a Prohibit Swift care cost override Started	The Swift system will be amended to prohibit any care costs override.	Estimated Date: 28/02/2019 Revised Date: 30/04/2019 No of Revisions 1

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates
22	Purchasing Budget Management EIJB1701 - Issue 2 Financial Controls Judith Proctor, Chief Officer	High	EIJB1701 - Issue 2.11 Recording of Direct Payments on Swift Started	Swift have updated Workflow descriptions which allows identification for a request if it is for a new service or an amendment to an existing one. Practitioners using the system are now compliant with the process. Communication to all users to reinforce the process will be sent early in the new year for maximum impact.	Estimated Date: 28/02/2019 Revised Date: No of Revisions 0
23	Purchasing Budget Management EIJB1701 - Issue 4 Supplier & Contract Manager Judith Proctor, Chief Officer	High	EIJB1701 - Issue 4.3 Former employee signatures Started	Information Communication Technology/SWIFT Development Team will find a solution to stop the use of electronic signature of former employees by June 2018 with verification by Internal Audit by February 2019.	Estimated Date: 29/03/2019 Revised Date: No of Revisions 0
24	Purchasing Budget Management EIJB1701 - Issue 4 Supplier & Contract Manager Judith Proctor, Chief Officer	High	EIJB1701 - Issue 4.6a Support of Partnership contracts team (short term) Started	The new contracts manager, who will be in post in January 2019, will review the existing processes and procedures and come up with a revised plan by March 2019. The new model will be based on best practice and implemented.	Estimated Date: 29/03/2019 Revised Date: No of Revisions 0

Appendix 7

Report

Overdue IJB and Partnership Internal Audit Findings

IJB Audit and Risk Committee

31 May 2019

Executive Summary

1. This report sets out affirmative actions that are underway to address internal audit assurance challenges and associated risks affecting health and social care services in Edinburgh.

Recommendations

2. The Integration Joint Board Audit and Risk Committee is asked to note:

   i. recent internal audit (IA) related activities across the Edinburgh Health and Social Partnership (the Partnership); and

   ii. status update for all overdue IA items for the Edinburgh Integration Joint Board (IJB) and Partnership.

Background

3. Internal audit (IA) overdue findings for the Edinburgh Health and Social Care Partnership (the Partnership) are regularly reviewed and monitored by the Partnership's Executive Team.

4. A large majority of the Partnership's IA overdue findings are not within the Partnership's sole gift to remediate. 41% (or 13 items) of the Partnership's overdue items rely on Council or NHS Lothian's services to take appropriate actions to mitigate risks and close IA findings.

5. Greater accountability is currently being achieved through the Chief Officer's Assurance Oversight Group (AOG). The Group is composed of the Partnership's Executive Team, the Chief Internal Audit Officer and relevant Council Head of Service whose officers are accountable for the delivery of IA actions. This approach will hopefully result in more IA findings being closed off in a timely manner.

6. An ownership protocol was agreed in January 2019 by the AOG for all IJB and Health and Social Care internal audits. The protocol enables the Partnership to retain overall ownership of risk findings, while holding to account contributing officers outside of the organisation through regular tracking and assurance from their respective Head of Service until completion.

7. Following this protocol arrangement, the IA team have reallocated several IA items which had previously sat in other Council Directorates to the Partnership in February 2019.

8. As part of the handover process, the Partnership is actively engaging with lead contributors to clarify what remains to be achieved to successfully close the items.

IA Closures

9. The Partnership is currently monitoring the performance of 179 IA recommendations (open and closed) identified from 47 IA risk findings.

10. In the last year, the Partnership has stabilised under a new management structure. With a new Chief Officer in post, followed by the appointments of a new Head of Operations and Head of Strategic Planning (January 2019), considerable progress has been made in closing IA items. The Partnership's IA Programme of regular catch ups with contributing officers, manager prompts, workshops (with IA team assistance) and senior manager oversight have resulted in the closure and sustainability of 80 IA items.

11. 26 items are currently marked as "implemented" and are currently awaiting IA validation prior to closure.

12. Once closed, the Partnership continues to monitor their progress to ensure that risk mitigating controls remain sustained.

Overdue IA items

13. Appendices 1 and 2 summarises all overdue IJB and Partnership IA items as of May 2019 and includes a current May update and/or action plan for each item. As of May 2019, there are 10 IJB items and 12 Partnership items that are currently overdue.

14. Overdue items have been reviewed and if appropriate, have been given a time extension which is then monitored through the Chief Officer's AOG. This is to ensure that a revised action plan has been considered at operational level and that the right level of accountability is in place to meet the new target date.

15. Various themed workshops have taken place between February and May 2019 to address long standing or historical IA items perceived to have stalled in progress. Usually chaired by one of the Partnership's Executive Team Officer, various contributing officers across multi-departmental services are asked to attend. With IA officers in attendance, each original risk finding and relevant management action are revisited. If deemed to be appropriate, the agreed management action may be altered to better reflect current organisational changes since the original IA report was published. It is also an opportunity to seek clarification from IA on what evidence will be needed to then close the finding.

16. Partnership staff continue to embed IA improvement actions as part of their core work functions. Thanks to a succession of internal audit training (delivered by the IA Team), new monitoring tool (Team Central), regular monitoring and a better understanding of 'quality' IA responses, general performance in this area is improving.

Key risks

17. If Internal Audit findings are not implemented, exposure to the risks detailed in the relevant detailed IA reports will remain. IA findings raised are based on control gaps identified during reviews and inherently impacts upon compliance and governance.

Financial implications

18. Although there are no direct financial implications arising from the consideration of this report, delivering the recommended audit actions will have a positive impact by strengthening financial control in audited Partnership service areas.

Implications for Directions

19. There are no specific implications for directions arising from this report.

Equalities implications

20. There are no equalities impacts.

Sustainability implications

21. No direct sustainability implications.

Involving people

22. IA risk findings status updates contained in appendix 1 were produced in consultation with individual IA risk owners.

Impact on plans of other parties

23. Not all of the Partnership's IA risk findings are within the Partnership's sole gift to remediate. The majority rely on Council or NHS Lothian services to take appropriate actions to mitigate risks. As such, continuous dialogue is necessary to ensure that any decision made in mitigating risk, which could have an impact on either parties plans, is done in consultation with the Partnership's business partners.

Background reading/references

24. N/A

Report author

Moira Pringle

Chief Finance Officer, Edinburgh Health and Social Care Partnership

Contact: Cathy Wilson, Operations Manager

E-mail: cathy.wilson@edinburgh.gov.uk | Tel: 0131 529 7153

Appendices

Appendix 1	Overdue IJB IA Findings – May 2019
Appendix 2	Overdue HSCP IA Findings – May 2019

Appendix 1 - Edinburgh Integration Joint Board – May Update

Overdue IA Items (IJB only) as of 21 May 2019

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates	EHSCP May Comments
1	IJB Management Information (Historic) Performance Management Framework in Development Judith Proctor, Chief Officer	High	Rec 1c Pending	A governance framework has been developed and documented setting out the roles remits and membership of the various committees and groups and the relationship between them.	Estimated Date: 28/02/2017 Revised Date: 31/12/2019	**Status:** Ongoing Governance Framework is being finalised by the Interim Head of Strategic Planning following the Good Governance Institute Report (IJB December 2018) through the transformation programme.
2	IJB Management Information (Historic) Performance information does not meet the needs of users Judith Proctor, Chief Officer	Medium	Rec 2 - Escalation Process Pending	The existing Performance Improvement Meeting (PIM) will be replaced by a Performance Board, membership of which will include all members of the IJB Executive Team.	Estimated Date: 28/02/2017 Revised Date: 20/12/2019	**Status:** Ongoing At the Assurance Oversight Group of 16/04 it was agreed that the agreed management actions would be revised to align itself with the Good Governance Institute's Review which provided recommendations to address performance management reporting arrangements.

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates	EHSCP May Comments
3	IJB Data Integration & Sharing Hardware compatibility and connectivity in NHS and CEC locations Judith Proctor, Chief Officer	Medium	Connectivity and Hardware Compatibility Pending	The ICT and Information Governance Steering Group will request a review of connectivity and hardware compatibility to be conducted across all sites housing integrated teams and consider any recommendations arising from that review. **New management action to follow**	Estimated Date: 31/01/2018 Revised Date: 30/06/2019	**Status:** Ongoing ***An IJB Data Integration & Sharing was recently held on 8 May 2019. New Management Actions to follow.***
4	IJB Data Integration & Sharing Lack of available training, policies and guidance Judith Proctor, Chief Officer	Medium	Compliance with training plan Pending	A training plan will be developed to ensure all existing staff who need to access systems belonging to both the Council and NHS Lothian receive the appropriate training to enable them to use the system appropriately with due regard to data protection. Training on all systems to be used by a postholder will become part of the mandatory training for new appointments. Compliance with this arrangement will be overseen by the nominated officer with responsibility for ICT and Information Governance. **New management action to follow**	Estimated Date: 31/03/2018 Revised Date: 31/12/2019	**Status:** Ongoing ***An IJB Data Integration & Sharing Workshop was recently held on 8 May 2019. New Management Actions to follow.***

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates	EHSCP May Comments
5	IJB Data Integration & Sharing Lack of available training, policies and guidance Judith Proctor, Chief Officer	Medium	Data Protection Pending	The nominated officer with responsibility for ICT and Information Governance will work with relevant colleagues in the Council and NHS Lothian to develop an integrated approach to data protection training taking account of the role and responsibilities of the IJB. *New management action to follow*	Estimated Date: 31/12/2017 Revised Date: 31/12/2019	**Status:** Ongoing ***An IJB Data Integration & Sharing Workshop was recently held on 8 May 2019. New Management Actions to follow***.
6	IJB Data Integration & Sharing Prioritisation Process Judith Proctor, Chief Officer	Medium	Prioritisation Process Pending	Prioritisation of requirements to be agreed through the EHSCP ICT and Information Governance Steering Group. *New management action to follow*	Estimated Date: 30/09/2019 Revised Date: 31/12/2019	**Status:** Ongoing ***An IJB Data Integration & Sharing Workshop was recently held on 8 May 2019. New Management Actions to follow***.

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates	EHSCP May Comments
7	IJB Data Integration & Sharing Prioritisation Process Judith Proctor, Chief Officer	Medium	Communication Pending	Vision and goals in respect of ICT to be conveyed through the development and publication of an ICT Strategy for the EHSCP. **New management action to follow**	Estimated Date: 31/10/2017 Revised Date: 31/12/2019	**Status:** Ongoing ***An IJB Data Integration & Sharing Workshop was recently held on 8 May 2019. New Management Actions to follow***
8	IJB Data Integration & Sharing Prioritisation Process Judith Proctor, Chief Officer	Medium	Roadmap Pending	Contingency plans will be developed, discussed with existing suppliers, and approved by the Core Group. **New management action to follow**	Estimated Date: 30/09/2019 Revised Date: 31/12/2019	**Status:** On Target ***An IJB Data Integration & Sharing Workshop was recently held on 8 May 2019. New Management Actions to follow***
9	IJB Data Integration & Sharing Robustness of access management & data protection processes Judith Proctor, Chief Officer	High	Access Management Pending	The existing processes within the Council and NHS Lothian for notifying system owners of staff changes will be communicated to all managers of integrated teams. Establishing an integrated system setting out the systems access requirements for all posts and the mechanism for gaining access for new staff and notifying system owners of leavers and changes in role will be a priority for the nominated officer to be identified in respect of ICT and Information Governance. **New management action to follow**	Estimated Date: 30/09/2019 Revised Date: 31/12/2019	**Status:** On Target ***An IJB Data Integration & Sharing Workshop was recently held on 8 May 2019. New Management Actions to follow***

10	Purchasing Budget Management EIJB1701 – Issue 4 Supplier & Contract Manager Judith Proctor, Chief Officer	High	EIJB1701 – Issue 4.6a Support of Partnership Contracts Team (short term) Started	The new contracts manager, who will be in post in January 2019, will review the existing processes and procedures and come up with a revised plan by March 2019. The new model will be based on best practice and implemented	Estimated date: 29/03/2019 Revised: 31/10/2019* *To be discussed at next AOG	**We had requested for this item to deleted as Management had never intended for this to be separate item. The agreed management response was meant to have been combined with item 4.6b (Item 4.6) for an original completion date of October 2019. There was no intention to have this split into two separate items.** **Issue to be raised at next AOG.**

Appendix 2 - Edinburgh Health and Social Care Partnership – May Update

Overdue IA Items (HSCP only) as of 21 May 2019

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates	EHSCP May Comments
1	Edinburgh Alcohol and Drug Partnership (EADP) – Contract Management Risk and Supplier Performance Management Judith Proctor, Chief Officer	High	Rec 1 - Risk Management Pending	A contracts management risk register will be developed describing, prioritising, and addressing risks to delivery. The risk register will be shared with and approved by the Core group by January 2018. The risk register will be refreshed quarterly and reviewed by the Core Group.	Estimated Date: 30/03/2018 Revised Date: 31/07/2019	**Status:** Ongoing Contract Management Framework Document has been completed and submitted to IA for Validation. However, in order to close this item, the next core group minutes will need to be submitted as evidence. The next meeting is scheduled to be in June 2019.
2	H&SC Care Homes - Corporate Report A3.5: Adequacy of Resources	Medium	A3.5(1) Pending	Unit managers submit monthly reports to Cluster manager and Locality management team. Locality management team responsible for ensuring resource meets the demand based on dependency scoring.	Estimated Date: 31/01/2019 Revised Date: 30/06/2019	**Status:** On Target Evidence is currently being gathered to support implementation/closure.

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates	EHSCP May Comment
3	H&SC Care Homes - Corporate Report A2.2: Purchasing Controls Judith Proctor, Chief Officer	Medium	A2.2(1) Started	All requisitioners / authorisers listed and limits will be reviewed, agreed, and formally documented. Discussions will be held with Finance and revised limits have agreed and implemented. Revised limits will be based on the highest invoice value expected in any one unit and applied consistently across all Care Homes Unit Managers.	Estimated Date: 28/03/2018 Revised Date: 31/05/2019	**Status:** Revised Date has been changed to 31/05/2019 There has been agreement to allow NHS access to the system, and senior managers have been asked to review there current users and approval limits / cost codes. A confirmed list has been agreed and in discussion with the systems team, all additional individuals have been asked to submit the relevant Oracle access forms to their line managers as per normal Council process. The revised implementation date is required to allow the systems team time to process the access requests as well as dealing with the impact of the financial year end.
4	H&SC Care Homes - Corporate Report A2.2: Purchasing Controls Judith Proctor, Chief Officer	Medium	A2.2(2) Started	Current approval guidelines and requisitioners / authorisers established to reflect new locality structure. Cluster Managers will approve any invoices that are outwith the authority limits for Unity Managers.	Estimated Date: 28/02/2018 Revised Date: 31/05/2019	**Status:** Revised Date has been changed to 31/05/2019 Same as above.

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates	EHSCP May Comments
5	H&SC Care Homes - Corporate Report A2.3: Welfare Fund and Outings Funds Judith Proctor, Chief Officer	Medium	A2.3(2) Started	A working group has been established that will focus on welfare. The remit of the group will focus on welfare committees; constitutions; accounts; criteria and donations. 2 officers from the working group have been assigned responsibility to write and implement welfare guidelines.	Estimated Date: 31/07/2018 Revised Date: 31/07/2019	**Status:** Revised Date has been changed to 31/07/2019 As picked up by Self-Assurance Framework - 2 Care Homes have not yet had their Welfare Committee this year. They aim to have this completed by the end of May.
6	H&SC Care Homes - Corporate Report A2.3: Welfare Fund and Outings Funds Judith Proctor, Chief Officer	Medium	A2.3(3) Started	A working group has been established that will focus on welfare. The remit of the group will focus on welfare committees; constitutions; accounts; criteria and donations. 2 officers from the working group have been assigned responsibility to write and implement welfare guidelines Task assigned to Business Officer for annual accounts and daily bookkeeping. Guidelines to be written for consistency.	Estimated Date: 31/07/2018 Revised Date: 31/07/2019	**Status:** Revised Date has been changed to 31/07/2019 As picked up by Self-Assurance Framework - 2 Care Homes have not yet had their Welfare Committee this year. They aim to have this completed by the end of May.
7	H&SC Care Homes - Corporate Report A3.3: Performance & Attendance Management Judith Proctor, Chief Officer	Medium	A3.3(2) Health & Social Care Teams Started	Health and Social Care Teams will ensure that annual performance conversations (once completed) are recorded on the iTrent system.	Estimated Date: 30/06/2018 Revised Date: 31/07/2019	**Status:** On Target Care Home Self-Assurance Framework is aiding Unit Managers to ensure that Performance Conversation/Annual Review are being completed.

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates	EHSCP May Comments
8	H&SC Care Homes - Corporate Report A3.3: Performance & Attendance Management Judith Proctor, Chief Officer	Medium	A3.3(3) Health & Social Care Teams Started	Health and Social Care Teams will ensure that managing attendance workshops have been attended by all H&SC line managers in Care Homes.	Estimated Date: 30/06/2018 Revised Date: 31/05/2019	**Status**: Revised due date 31/05/2019 Request for training completion records has been requested from HR Business Hub. Should be implemented by 24 May 2019.
9	Historic Unimplemented Findings HSC1502 - issue 1 lack of routine monitoring of users Judith Proctor, Chief Officer	Low	Recommendati on 1c Started	It is proposed that an online training module is developed to provide a mixture of operational guidance and system controls which would be mandatory for all Swift users to complete. Staff would be expected to undertake an annual refresher.	Estimated Date: 30/04/2016 Revised Date: 30/09/2019	**Status:** On Target SWIFT Development Team (ICT) are progressing on tis with Learning & Development (HR)

Ref	Project/Owner	Issue Type	Issue/Status	Agreed Management Action	Dates	EHSCP May Comments
10	Resilience BC Resilience responsibilities Judith Proctor, Chief Officer	High	Rec 3.3 H&SC - Resilience responsibilities Pending	Operational resilience responsibilities for completion and ongoing maintenance of Directorate and Service Area Business Impact Assessments; Resilience plans; and coordination of resilience tests in conjunction with the Resilience team will be clearly defined and allocated. The total number of employees with operational resilience responsibilities will be determined with reference to the volume of business impact assessments and resilience plans that require to be completed and maintained to support recovery of critical services.	Estimated Date: 20/12/2018 Revised Date: 30/04/2019	**Status:** Overdue Due to Brexit Planning and last Resilience Meeting cancellation, Group was unable to approve new Terms and Reference. Revised due date will need to be agreed at the next Resilience Meeting 29 May 2019.
11	Social Work Centre Bank Account Reconciliations Corporate Appointee Client Fund Management Judith Proctor, Chief Officer	High	Recommendati on 2 Started	2. New guidelines will be written to ensure clarity of responsibilities. Sections will be included detailing Social Work; Business Support; and Transactions team responsibilities. The objective is to create and implement an end to end process that includes eligibility criteria, Department of Work and Pensions processes and a full administrative process that will be applied centrally and across Locality offices; clusters; and hubs.	Estimated Date: 30/04/2018 Revised Date: 28/06/2019	**Status:** On Target
12	Social Work Centre Bank Account Reconciliations Corporate Appointee Client Fund Management Judith Proctor, Chief Officer	High	Recommendati on 8 Started	8. Refresher training will be offered as part of the implementation of the new guidelines to all staff involved in the process, and recorded on staff training records. The training will also be incorporated into the new staff induction process.	Estimated Date: 31/05/2018 Revised Date: 28/06/2019	**Status:** On Target – Due date was agreed as 28/06/2019 with IA following workshop.