Governance, Risk and Best Value Committee

10.00am, Tuesday 3 November 2020

Internal Audit: Final Internal Audit reports supporting the 2019/20 Annual Opinion

Item number	
Executive/routine	**Executive**
Wards	
Council Commitments	

1. Recommendations

It is recommended that the Committee:

1.1 reviews and scrutinises the final Internal Audit reports supporting the 2019/20 Annual Opinion which are provided as appendices to this report.

Lesley Newdall

Chief Internal Auditor

Legal and Risk Division, Resources Directorate

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

Report

Internal Audit: Final Internal Audit reports supporting the 2019/20 Annual Opinion

2. Executive Summary

2.1 The purpose of this paper is to provide the Committee with copies of three final Internal Audit (IA) reports that formed part of the 2019/20 IA annual opinion for their review and scrutiny.

3. Background

3.1 At the June 2020 meeting, the Governance, Risk, and Best Value (GRBV) Committee requested that IA should provide copies of final IA reports that either have an overall red (Significant Improvement Required) outcome, or include any red (High) rated findings for review and scrutiny in advance of presenting the IA annual opinion in August 2020.

4. Main report

4.1 Final IA reports that that either have an overall red (Significant Improvement Required) outcome, or include any red (High) rated findings are provided to GRBV Committee members as they are finalised.

4.2 The three final 2019/20 reports to be formally presented meet the criteria noted at 4.1 above and are included as appendices to this report.

5. Next Steps

5.1 IA will continue to provide reports completed to support the 2020/21 annual opinion that either have an overall red (Significant Improvement Required) outcome, or include any red (High) rated findings to GRBV committee members as they are finalised.

6. Financial impact

6.1 None

7. Stakeholder/Community Impact

7.1 Effective review and scrutiny of IA assurance outcomes performed by the Committee with Directors and relevant Council officers.

8. Background reading/external references

8.1 None

9. Appendices

9.1 Appendix 1 – Unsupported Technology (Shadow IT) and End User Computing

9.2 Appendix 2 – Life Safety

9.3 Appendix 3 – Social Media Accounts

The City of Edinburgh Council

Internal Audit

Unsupported Technology (Shadow IT) and End User Computing

Final Report

9th October 2020

[CW1901]

Overall report rating:

Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2019/20 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2019. 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

Shadow IT

Shadow IT is a term that refers to Information Technology (IT) applications and infrastructure that is managed and used without the knowledge of an organisation's IT department. They are typically externally hosted by a third party supplier, and usually cloud based.

Shadow IT can also include software or hardware such as laptops, smartphones, and scanners that can be connected to an organisation's network.

Across the Council, Shadow IT includes technology systems used by directorates and divisions that are not hosted on either the Council's Corporate or Learning and Teaching networks, or not supported and maintained by Customer and Digital Services and CGI, the Council's technology partner.

Third party shadow IT assurance

The Council's externally hosted ICT services protocol also requires nominated business and asset information owners to ensure that shadow IT contracts are appropriate for the Council's needs both at inception and for the duration of the service or contract, and specifies a number of areas (section 5) where business owners should obtain assurance on the system.

An example of the assurance that can be obtained from third party system providers on the adequacy and effectiveness of their Shadow IT technology systems is an annual International Standard for Assurance Engagements (ISAE) 3402 service organisation control (SOC) report. This standard is designed to provide customers with assurance that suppliers operate adequate and effective technology and service delivery internal controls.

ISAE 3402 assurance work is commissioned annually by the service provider; is performed by an independent auditor (usually a professional services firm); is tailored to cover a range of controls; and the final report is provided free of charge to the organisation's customers. Further information is available at ISAE3402

End User Computing

End user computing is defined as bespoke systems or complex models using applications (for example Microsoft Excel or Access) that are hosted on, and can be accessed from, an organisation's network with no support from system developers. These models are developed by users to improve efficiency; automate tasks; and facilitate operational processing in contrast to typical use of these applications for data interrogation and analysis.

Given their significance and dependencies, appropriate security controls; ongoing information management; and resilience arrangements should also be applied to these end user computing models.

A good example of an end user computing model used in the Council is the Homelessness Information System access database that is used by Communities and Families to record and manage homeless applications and generate data to support quarterly and annual statutory reporting on homelessness to both the Scottish Government and Scottish Housing Regulator. Use of this model was included in our review of Homelessness Services completed in July 2019

Shadow IT and end user computing management across the Council

First line divisions and directorates are responsible for the procurement and ongoing management of shadow IT and end user computing applications in line with Contract Standing Orders and applicable Council policies.

The Council's June 2019 Contract Standing Orders included a change requested by the Executive Director of Resources to specify that that the purchase of or tender for any form of Information and Communications Technology (ICT) device or digital service, software or hardware must be approved by Digital Services at the Procurement Requirement Form stage, with any purchase for *any value* undertaken in collaboration with, and the approval of Digital Services.

The Council's Cloud or web-based shadow IT systems should also be managed in accordance with the Council's externally hosted ICT services protocol designed and owned by Digital Services also requires first line divisions and directorates to ensure that systems have appropriate security controls; are supported by appropriate resilience arrangements; and include appropriate information management controls to ensure ongoing compliance with applicable regulations.

When using cloud based systems, it is also important to ensure that users are managed in line with the licencing requirements specified by the system supplier.

Previous internal audit outcomes

External Security review (May 2017) - the risks associated with use of Shadow IT across the Council were first highlighted in the IA 'Review of External Security' completed in May 2017. This included a High rated finding that highlighted the limited control and oversight of shadow IT across the Council, with recommendations that a risk assessment should be performed to identify all shadow IT being used across the Council, and decisions made regarding whether the risks should be accepted (and shadow IT allowed to operate autonomously); or whether the systems should be 'on boarded' and managed centrally by Digital Services in conjunction with CGI.

The review of 'IT Disaster Recovery' completed in May 2017 also included a High rated finding highlighting the need to ensure that shadow IT is resilient and could be recovered following a major incident.

Following this review Digital Services completed a one off exercise in November 2017 (that was supplemented by additional information in March 2018) that attempted to identify shadow IT that is critical to service delivery.

This exercise was reliant on divisions understanding of their use of shadow IT and communicating this to Digital Services. The exercise identified 371 items of shadow IT. Of these 98 were identified as critical either due to the potential impact of their failure or data misuse.

No subsequent decision was made in relation to whether shadow IT systems should be on boarded and managed centrally by Digital Services and CGI, or whether the current approach where first line divisions and directors are responsible for the procurement and ongoing management of shadow IT in line with applicable policies should continue.

Financial Systems Access Controls (July 2019) – this review highlighted the need for the Council to establish a Council wide user access management framework to ensure that access to systems is effectively managed; toxic user profiles (where users have a combination of system access rights on either one system or a combination of systems that enables them to perform tasks that should never be completed by a single user) are either prevented or detected; and that adequate segregation of duties is maintained within and across systems.

Whilst this audit focused predominantly on financial systems hosted on the Council's corporate network, it is essential that appropriate user access controls are applied to shadow IT systems to ensure ongoing compliance with Audit Scotland system security requirements; applicable UK and EU data protection legislation; and the Council's records management policies.

To address the controls gaps highlighted in this report, Digital Services agreed to develop and implement a Council wide user access management framework, and this is currently in the process of being finalised and approved.

Scope and Approach

The objective of this review was to assess the adequacy of design and operating effectiveness of the key controls established across the Council to manage the security, information, and resilience risks associated with ongoing use of shadow IT and end user computing applications to support service delivery.

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

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

A survey was issued to Council divisions requiring Heads of Service to provide details of Shadow IT used in their areas. From the responses provided, a sample of eleven Shadow IT technologies (nine third party supported technologies and two end user computing applications) were selected to support the testing detailed in our terms of reference, with work performed across November and December 2019.

Limitations of Scope

Systems used exclusively for the Edinburgh Integrated Joint Board (EIJB); Lothian Pension Fund; and Arm's Length External Organisations (ALEOs) are specifically excluded from the scope of this review.

Reporting Date

Our audit work concluded on 6th January 2020, and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Total number of findings: 2

Summary of findings raised	
High	1. Digital strategy and governance
High	2. Ongoing shadow IT and end user computing management

Opinion

Significant control weaknesses were identified both the adequacy of design and operating effectiveness of the key controls established across the Council to manage the security, information, and resilience

risks associated with ongoing use of shadow IT and end user computing applications to support delivery of Council services.

Consequently, two High rated findings have been raised

The first finding highlights the need to refresh the Council's digital strategy for both the Corporate and Learning and Teaching networks to provide a clear strategic direction for future use and alignment of technology systems across the Council that includes consideration of use of both shadow IT and end user computing applications following assessment of their associated advantages and risks.

This finding also confirms that there is no current register of shadow IT and end computing user applications used across the Council and notes that Directorates and Divisions are currently procuring shadow IT applications on their own with limited oversight by or engagement with either Commercial and Procurement Services or Digital Services to confirm that all relevant risks have been considered either prior to purchase or in advance of contract extensions through a waiver of the Council's Contract Standing Orders.

Consequently, the established Digital Service and CGI enterprise architecture governance forum is limited in its ability to effectively ensure that the Council's current and future technology architecture is optimised; efficient; provides best value; and remains aligned with the Council's digital strategy and technology risk appetite.

The second finding notes the need to improve first line directorate and divisional controls supporting the ongoing management and use of shadow IT and end user computing applications across the Council, and highlights that the risks associated with use of shadow IT and end user computing applications are not well known, understood and recorded; roles and responsibilities of system owners have not been clearly defined; requirements detailed in the externally hosted ICT services protocol are not yet being consistently applied by system owners; and that there is currently no second line oversight provided and limited assurance obtained from suppliers to confirm that shadow IT and end user computing application risks are being effectively managed.

Areas of good practice

The following areas of good practice in relation to management of shadow IT and end user computing applications were identified:

- colleagues interviewed across divisions were knowledgeable of the shadow IT and end user computing applications used in their areas;
- good awareness of the externally hosted ICT services protocol across all survey respondents; and
- network controls operated by CGI were generally effective in controlling user permissions to install technology on the network.
- the draft user access management framework has been prepared and is currently being finalised and approved prior to implementation across the Council. The draft framework also includes specific requirements to ensure that access to shadow IT applications is effectively managed by first line divisions and directorates.

3. Detailed findings

1. Digital strategy and governance	High
Digital Strategy The Council's digital strategy was last updated in 2016, with no approved updates or amendments since, although management has advised that the digital strategy will be refreshed by Digital	

Services in 2020.

There were no references to the Council's existing digital strategy as part of the procurement of the nine third party supported shadow IT technology systems selected in our sample, with the systems procured and adopted as business need has arisen. Whilst our survey responses highlighted a generally good awareness of the security and information security compliance requirements that must be obtained when divisions are procuring Shadow IT solutions, there is currently no strategic guidance to support divisions in these procurement decisions.

Shadow IT and end user computing register

There is currently no register detailing the full population of shadow IT and end user computing solutions used across Council directorates and divisions, with no team currently responsible for collation and maintenance of this information.

A total of 88% (28 of 32) respondents to the Shadow IT survey confirmed that cloud based shadow IT and / or end user computing applications (such as Excel macros and Access databases) are used in their area, with the majority of respondents confirming multiple instances of shadow IT in use in their service area. There were generally recognised system owners for these applications within divisions.

Enterprise Architecture

Management has confirmed that an enterprise architecture governance forum has been established between the Council and CGI, however, in the absence of a current digital strategy and full list of shadow IT and end user computing applications used across the Council, the forum is currently unable to effectively perform enterprise analysis; design; plan; and successfully implement technology solutions (including shadow IT) in line with the Council's digital strategic direction.

Additionally, there is currently no established process to support identification and consolidation of common technology functional requirements and synergies across Council divisions. For example, the shadow IT system currently used to support the Internal Audit follow-up process could be used to support recording and follow up of other assurance activities performed across the Council.

Procurement

Divisional shadow IT survey results confirmed that 61% (17 of 28) of divisions had a Contract Standing Orders waiver in place to support ongoing use of Shadow IT and end user computing applications (where required), however, divisions advised that 5 of the 17 waivers had not been reviewed and approved by Digital Services as is now required in the Council's Contract Standing Orders (CSOs) waiver process.

It is acknowledged that until June 2019 the CSOs only required consultation with Digital Services for technology related purchases, and not actual approval, so some or all of these might have been compliant with the CSOs that applied at the date of purchase, however the necessary information has not been supplied to Commercial and Procurement Services (CPS) to verify this.

Additionally, whilst the current CSOs specify the need for Digital Services approval of technology devices or digital services of any value, they do not specify the requirement for Digital Services to approve any free technology related purchases or services provided.

Risks

The potential risks associated with our findings are:

- The enterprise architecture governance forum is limited in its ability to meet its responsibilities by ensuring that the Council's technology architecture and future direction remains aligned with its

digital strategy.

- Use of multiple fragmented systems, duplicate shadow IT, and end user computing solutions across the Council.
- No holistic view of historic purchases and ongoing support costs for shadow IT and end user computing solutions used across the Council. Consequently, costs associated with ongoing use of shadow IT may be unnecessarily high.
- No holistic view of any free / no cost digital services equipment and services used across the Council.
- Increased technical debt associated with use of Shadow IT (for example software bugs; legacy code; and missing functionality), and inability to fully realise expected system benefits.
- Increased security; information management; compliance; and regulatory risks where shadow IT systems are procured and implemented with no oversight from Digital Services.

1.1 Recommendation: Digital strategy development

1. The Council's digital strategy should be reviewed and refreshed. This should include (but not be limited to) a list of strategic technology objectives that includes consideration of future use of both networked and cloud-based systems solutions that are aligned with the Council's strategic and service delivery objectives and applicable security and compliance requirements.
2. The refreshed technology strategy should be developed following engagement and consultation with Council directorates and divisions and citizens (where required) to understand future technology system requirements to support efficient and effective service delivery and ongoing citizen engagement with the Council.

1.1 Agreed Management Action: Digital strategy development

1. The Council's digital strategy is currently being refreshed as part of the Adaptation and Renewal Programme, and will include consideration of use of both networked and cloud-based systems solutions that are aligned with the Council's strategic and service delivery objectives and applicable security and compliance requirements.

   A separate cloud strategy will also be prepared as part of the overarching digital strategy that outlines the opportunities and risks associated with ongoing and future use of cloud based shadow IT systems.
2. The digital strategy will be developed following engagement and consultation with Council directorates; divisions; citizens; and other organisations (where required).

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Nicola Harvey, Head of Customer and Digital Services; Heather Robb, Chief Digital Officer; Alison Roarty, Commercial Team Lead, Digital Services; Layla Smith, Operations Manager, Resources	**Implementation Date:** 31st December 2020

1.2 Recommendation: Shadow IT and end user computing application register

1. A Council wide register of shadow IT and end user computing applications should be developed and centrally maintained, with responsibility for ongoing maintenance of the register allocated to an appropriate Council division.
2. The register should include (but not be limited to):
   - all existing applications used across the Council;
   - an assessment of their criticality; and

- details of system owners

3. The register should be updated to reflect any new shadow IT and end user computing applications subsequently procured or developed.
4. The register should be published on the Orb as a point of reference for Council divisions and directorates.

1.2 Agreed Management Action: Shadow IT and end user computing application register

1. Commercial and Procurement Services (CPS) will assume responsibility for maintaining the Council's centralised shadow IT and end user computing register.
2. CPS will provide directorates and divisions with the list of shadow IT applications that was collated by Digital Services between November 2017 and March 2018; request them to confirm its completeness and accuracy; and instruct them to ensure that it is accurately maintained with the inclusion of all future shadow IT and end user computing applications procured or developed.
3. Divisions and directorates will also be requested to ensure that the shadow IT and end user computing applications that they currently use are recorded in their resilience business impact assessments, together with an assessment of their criticality, and communicated to Digital Services to ensure that they are restored in a timely manner in the event of a resilience incident
4. Details of the register will be published on the Orb as a point of reference

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Nicola Harvey, Head of Customer and Digital Services; Heather Robb, Chief Digital Officer; Kevin Wilbraham, Information Governance Manager and Data Protection Officer; Layla Smith, Operations Manager, Resources	**Implementation Date:** 18th December 2020

1.3 Recommendation: Architectural roadmap

1. A technology architectural roadmap should also be developed that is aligned with the refreshed digital strategy.
2. The roadmap should be used together with the register of shadow IT and end user computing applications (refer recommendation 1.2) by the enterprise architecture governance forum to review all new shadow IT technology and end user computing procurement and waiver requests to confirm their alignment with the Digital strategy, and that there is no duplication with existing systems.
3. The outcomes of the enterprise architecture governance forum review should be used to inform the final procurement / development decision.

1.3 Agreed Management Action: Architectural roadmap

1. The digital strategy will be supported by a digital roadmap.
2. The roadmap will be designed to understand both existing and future technology system requirements across Council directorates and divisions, including existing shadow IT systems and the potential future use of shadow IT to support ongoing service delivery. This road map will be prepared in consultation with divisions and directorates.
3. A process will be established to ensure that all new technology procurement requests are considered by the enterprise architecture governance forum together with the register of shadow IT to inform final procurement / system development decisions. This will include a RACI document

that clearly defines who should be responsible; accountable; consulted; and informed for all relevant aspects of enterprise architecture governance between the Council and its technology partners CGI.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Nicola Harvey, Head of Customer and Digital Services; Heather Robb, Chief Digital Officer; Mike Bell, Technical Architect, Digital Services; Alison Roarty, Commercial Team Lead, Digital Services; Layla Smith, Operations Manager, Resources	**Implementation Date:** 17th December 2021

1.4 Recommendation: Review of existing shadow IT application contracts

1. Following completion of the shadow IT register (refer recommendation 1.2), a review should be completed by directorates and divisions to confirm that all existing (or at least critical) shadow IT applications provided by third party suppliers are supported by appropriate contracts; that Contract Standing Orders waivers are in place where a compliant procurement process has not otherwise been applied; and that Digital Services has been involved in the procurement process or has approved the waivers.
2. Where recurring Contract Standing Orders waivers have been used to support ongoing use of shadow IT applications within the Council, divisions should review these to determine whether the systems can be subject to a compliant procurement process in advance of the next contract renewal date, assuming the systems are still required.
3. Where Digital Services has not reviewed Contract Standing Orders waivers, this should be noted, and their approval obtained prior to any subsequent Contract Standing Orders waiver extensions.

1.4a Agreed Management Action: Guidance for review of existing shadow IT contracts by divisions and directorates

1. Following completion of the shadow IT and end user computing register, Commercial and Procurement Services will prepare (with support from Legal Services as required) and provide guidance to all Council divisions and directorates that specifies the expected content of shadow IT / cloud based system provision contracts. This guidance will also be aligned with the requirements of the Council's externally hosted ICT services protocol, and should include (but not be limited to) the need to understand:
   - the security and information management arrangements supporting the system;
   - the full extent of the supply chain involved in the operation of the system, with specific focus on which suppliers are transferring, processing, and storing Council data;
   - business continuity and resilience arrangements, including the frequency of ongoing testing and actions taken to address any weaknesses identified;
   - the process for making changes to the system, including the how changes are tested prior to implementation in the live operating environment;
   - the ongoing assurance requirements to be provided by all suppliers involved in supporting the ongoing delivery of cloud based services; and
   - any unique supplier relationship management requirements that specifically relate to the ongoing use of shadow IT / cloud based technology applications.
2. divisions and directorates will be requested to assess the adequacy of their existing shadow IT / cloud based applications against these requirements; identify any gaps; and engage with CPS to

support negotiation of new contracts where required. 3. divisions and directorates will also be instructed to identify any shadow IT applications that are supported by Contract Standing Orders waivers; requested to review these to determine whether the systems can be subject to a compliant procurement process in advance of the next contract renewal date; and engage with CPS and Digital Services to support these procurement activities.	
Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Layla Smith, Operations Manager, Resources; Annette Smith, Executive Assistant.	**Implementation Date:** 30th April 2021
1.4b Agreed Management Action: Review of existing shadow IT contracts	
The following actions were discussed and agreed by the Council's Corporate Leadership Team and will be applied by all Directorates following receipt of guidance from Commercial and Procurement Services as per recommendation 1.4a above. 1. The Directorate will complete a review of all contracts supporting the ongoing use of shadow IT / cloud based applications used within divisions in comparison to the guidance provided by Commercial and Procurement Services (CPS) to ensure identify any contracts that need to be refreshed or procured, with support from CPS and Digital Services. 2. Where inadequate contracts are identified, and the supplier is unable to support an immediate contract refresh, the criticality of the system and the service it supports will be assessed to determine whether the system is required, or whether an alternative system solution can be procured. 3. Where inadequate contracts support critical systems that cannot be immediately re-procured, the risks associated with ongoing use of these systems and their contracts will be recorded in divisional and directorate risk registers, and the contract re-procured at the earliest possible date.	
Resources **Owner:** Stephen Moir, Executive Director of Resources **Contributors:** Nicola Harvey, Head of Customer and Digital Services; Hugh Dunn; Head of Finance; Katy Miller; Head of Human Resources; Peter Watton, Head of Property and Facilities Management; Nick Smith, Head of Legal and Risk; Layla Smith, Operations Manager, Resources	**Implementation Date:** 30th September 2021
Place **Owner:** Paul Laurence, Executive Director of Place **Contributors:** Michael Thain, Head of Place Development; Gareth Barwell, Head of Place Management; Lynne Halfpenny, Director of Culture; Alison Coburn, Operations Manager, Place	**Implementation Date:** 30th September 2021
Communities and Families **Owner:** Alistair Gaw, Executive Director of Communities and Families **Contributors:** Andy Gray, Head of Schools and Lifelong Learning; Jackie Irvine, Chief Social Work Officer and Head of Safer & Stronger Communities; Crawford McGhie, Senior Manager, Estates & Operational	**Implementation Date:** 30th September 2021

Support; Bernadette Oxley, Head of Children's Services; Nickey Boyle, Senior Executive Administrator; Michelle McMillan, Operations Manager, Learning and Teaching; Nichola Dadds, Senior Executive Assistant.	
Health and Social Care **Owner:** Judith Proctor, Chief Officer, Edinburgh Health and Social Care Partnership **Contributors:** Tom Cowan, Head of Operations; Tony Duncan, Head of Strategic Planning; Moir Pringle, Chief Finance Officer; Cathy Wilson, Operations Manager	**Implementation Date:** 30th September 2021
Strategy and Communications **Owner:** Laurence Rockey, Head of Strategy and Communications **Contributors:** Gavin King, Democracy, Governance & Resilience Senior Manager; Paula McLeay, Policy & Insight Senior Manager; Andy Nichol, Programme Manager (PMO) Edinburgh & South East Scotland City Region Deal / Edinburgh 2050 City Vision; Gillie Severin, Strategic Change & Delivery Senior Manager; Donna Rodger, Executive Assistant	**Implementation Date:** 30th September 2021
1.5 Recommendation: Procurement threshold for purchase of technology services and equipment	
The Council's Contract Standing Orders should be updated to include the requirement for Digital Services to approve any free technology related purchases or services provided.	
1.5 Agreed Management Action: Procurement threshold for purchase of technology services and equipment	
The Council's Contract Standing Orders will be updated to include the requirement for Digital Services to approve any free technology related purchases or services provided.	
Owner: Stephen Moir, Executive Director of Resources **Contributors:** Hugh Dunn, Head of Finance; Iain Strachan, Chief Procurement Officer; Layla Smith, Operations Manager; Resources.	**Implementation Date:** 31st March 2021

2. Ongoing shadow IT and end user computing management	**High**

Survey responses from Council divisions and the outcomes of testing performed across a sample of 9 shadow IT and 2 end user computing applications confirmed that:

1. The risks associated with the use of shadow IT and end user computing applications are not well known or understood across the Council, as most divisions (61% survey respondents) did not include ongoing use of shadow IT and end user computing applications as risks on their divisional and relevant directorate risk registers, and these are not recorded as specific risks on the Corporate Leadership Team risk register.
2. No third-party assurance is requested by divisions from shadow IT system providers (such as ISAE 3402 or SOC 2 independent assurance reports) to provide ongoing independent assurance on the design adequacy and operating effectiveness of the key technology system controls (for example security; information management; and resilience controls) as required by the Council's externally hosted ICT services protocol to ensure that these remain aligned with applicable Council standards

and requirements.

3. There is currently no established second line oversight performed to confirm that directorates and divisions are consistently meeting the requirements of the externally hosted ICT services protocol in relation to ongoing use of shadow IT applications.
4. Whilst there were generally recognised system owners for both shadow IT and end user computing applications within divisions, ownership roles and responsibilities were not consistently recorded or documented.
5. Third party supplier remote access is used for most shadow IT applications (67% of survey respondents confirmed that this was the case) to resolve system issues, with limited assurance provided by suppliers in relation to the security and information management controls supporting remote access. Instead, reliance is placed on contractual agreements and supporting service level agreements where these have been established.
6. Shadow IT system user access is informally managed by a small team of users within divisions, with reliance on the Council's network security controls to maintain the integrity of end user computing applications.
7. Sufficient numbers of user licences have been established to support shadow IT applications, however limited ongoing monitoring is performed to assess whether the volume of licences purchased is in excess of user requirements.

Risks

The potential risks associated with our findings are:

- The Council's total exposure to the risks associated with use of shadow IT and end user computing applications is not understood as these risks are not currently recorded in divisional and directorate risk register, and considered for inclusion in the Corporate Leadership Team risk register.
- The Council currently has no independent oversight or assurance in relation to the adequacy and effectiveness of controls established to mitigate security; information management (i.e. how data is transferred into, and processed and stored within cloud based systems); resilience; and other significant risks associated with ongoing use of shadow IT and end user computing applications.
- Non-compliance with the requirements of the Council's externally hosted ICT services protocol that requires system owners to confirm that shadow IT and cloud based systems controls remain aligned with established Council policies and procedures.
- In the event of significant service disruption or a disaster, it may be difficult or impossible to restore shadow IT and end user computing applications used to support delivery of critical services.
- Shadow IT and end user computing system owners lack clarity in relation to their ongoing responsibilities in relation to ongoing management of shadow IT and end user computing applications, including ongoing supplier and user access management responsibilities.
- Third parties may have inappropriate access to Council networks and systems and private sensitive data via remote access to externally hosted shadow IT applications that is not effectively managed or controlled.
- Council users may have inappropriate or 'toxic' access rights to shadow IT applications and the data and information that they hold.
- End user computing applications such as excel models or access databases may not be appropriately restricted and secured, resulting in inappropriate access to data maintained in these applications or unauthorised changes to their structure (for example formulae and macros).
- Financial impacts associated with purchasing more system licences than actually required by users.

2.1 Recommendation: Shadow IT and end user computing system owner responsibilities

A clear set of requirements should be established for, implemented, and consistently applied by all shadow IT and end user computing system / application owners in first line divisions and directorates to support their effective ongoing management. These should include, but not be limited to:

- completion of initial and ongoing risk assessments across all shadow IT and end user computing applications used, including the system security; resilience; and information risks associated with their ongoing use, with guidance requested from the Council's Risk Management; Digital Services; and Information Governance teams where required;
- obtaining ongoing (at least annual) independent assurance from system providers (for example independent International Standard on Assurance Engagements (ISAE) No. 3402 Service Organisation Controls (SOC2) reports) in relation to the controls in place to manage the risks associated with shadow IT systems as required by the Council's externally hosted ICT services protocol. This assurance should also include assurance on controls established to support remote access to systems by supplier employees.
- confirming (at least annually) that all critical end user computing applications developed within the Council (for example in Microsoft Excel or Access) are supported by adequate development documentation detailing their purpose, and how they have been developed and operate in practice; can be accessed only be relevant employees; include appropriate controls to prevent overwrite of key coding or formulae; and can be restored within appropriate timeframes in a resilience event.
- including details of any risks shadow IT and end user computing risks (where assurance has not been obtained or the supplier has confirmed that they do not have effective controls in place) in divisional and directorate risk registers and annual governance statements;
- ensuring that there is a clear understanding of system user profiles (i.e. what activities each profile within the system allows the user to perform);
- ensuring that user profiles are allocated to Council employees in line with their relevant roles and responsibilities with clearly defined processes established and consistently applied to support addition of new starts and removal of leavers and employees moving internally within the Council;
- ensuring that regular ongoing reviews are performed to confirm that user access remains appropriate and aligned with employee roles and responsibilities, and that any potentially inappropriate or toxic user combinations are identified and immediately resolved.
- Reviewing shadow IT licences and costs (at least annually) to ensure that they remain aligned with the required number of Council employees.

2.1 Agreed Management Action: Shadow IT and end user computing system owner responsibilities

1. A detailed cloud based / shadow IT framework will also be designed and implemented across the Council. This will consolidate and include links to procurement requirements; the new user access management framework; and the existing externally hosted ICT services protocol, ensuring that all existing requirements that apply to ongoing use of Shadow IT systems are consolidated and reflected in one place.
2. Where the points above are not included in the existing frameworks or protocols, they will be reflected in the new shadow IT framework document.
3. The new framework will be communicated across all divisions and directorates and published on the Orb.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Nicola Harvey, Head of Customer and Digital Services; Heather Robb, Chief Digital Officer; Mike Brown, Cybers Security Manager, Digital Services; Mike Bell, Technical Architect, Digital Services; Mike Brown, Alison Roarty, Commercial Team Lead, Digital Services; Layla Smith, Operations Manager, Resources	**Implementation Date:** 30th June 2021

2.2 Recommendation: Second line assurance and oversight

1. Management should consider whether ongoing independent second line assurance is required to confirm that relevant security, information, and resilience risks associated with ongoing use are of shadow IT and end user computing applications are being effectively managed by directorates and divisions.
2. If implemented, this assurance process should confirm the extent of compliance with the Council's externally hosted ICT services protocol in relation to ongoing use of shadow IT applications, and that system owner responsibilities in relation to both shadow IT and end user computing applications (refer recommendation 2.1) are being consistently applied
3. Where instances of non-compliance with the protocol or application of shadow IT and end user computing system owner responsibilities are evident, these should be communicated to divisional and directorate management with recommendations made to address the gaps identified.

2.2 Agreed Management Action: Shadow IT assurance and oversight

The following actions were discussed and agreed by the Council's Corporate Leadership Team and will be applied by all first line divisions and directorates.

1. divisions and directorates will confirm whether they are consistently applying shadow IT framework and meet the requirements of the Council's externally hosted ICT services protocol in their annual assurance statements, and with any gaps or instances of non-compliance disclosed;
2. reliance will be placed on third line oversight by Internal Audit (IA), acknowledging that the assurance provided in relation to the ongoing management of shadow IT technology applications across the Council will be considered as part of IA's ongoing risk based assurance proposals, with assurance unlikely to be provided on an ongoing basis.

Resources **Owner:** Stephen Moir, Executive Director of Resources **Contributors:** Nicola Harvey, Head of Customer and Digital Services; Hugh Dunn; Head of Finance; Katy Miller; Head of Human Resources; Peter Watton, Head of Property and Facilities Management; Nick Smith, Head of Legal and Risk; Layla Smith, Operations Manager, Resources	**Implementation Date:** 30th June 2021
Place **Owner:** Paul Laurence, Executive Director of Place **Contributors:** Michael Thain, Head of Place Development; Gareth Barwell, Head of Place Management; Lynne Halfpenny, Director of Culture; Alison Coburn, Operations Manager, Place	**Implementation Date:** 30th June 2021
Communities and Families **Owner:** Alistair Gaw, Executive Director of Communities and Families	**Implementation Date:** 30th June 2021

Contributors: Andy Gray, Head of Schools and Lifelong Learning; Jackie Irvine, Chief Social Work Officer and Head of Safer & Stronger Communities; Crawford McGhie, Senior Manager, Estates & Operational Support; Bernadette Oxley, Head of Children's Services; Nickey Boyle, Senior Executive Administrator; Michelle McMillan, Operations Manager, Learning and Teaching; Nichola Dadds, Senior Executive Assistant.	
Health and Social Care **Owner:** Judith Proctor, Chief Officer, Edinburgh Health and Social Care Partnership **Contributors:** Tom Cowan, Head of Operations; Tony Duncan, Head of Strategic Planning; Moir Pringle, Chief Finance Officer; Cathy Wilson, Operations Manager	**Implementation Date:** 30th June 2021
Strategy and Communications **Owner:** Laurence Rockey, Head of Strategy and Communications **Contributors:** Gavin King, Democracy, Governance & Resilience Senior Manager; Paula McLeay, Policy & Insight Senior Manager; Andy Nichol, Programme Manager (PMO) Edinburgh & South East Scotland City Region Deal / Edinburgh 2050 City Vision; Gillie Severin, Strategic Change & Delivery Senior Manager; Donna Rodger, Executive Assistant	**Implementation Date:** 30th June 2021

Appendix 1: Basis of our classifications

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

Please see the Internal Audit Charter for full details of opinion ratings and classifications.

Appendix 2: Areas of audit focus

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

Audit Area	Control Objectives
Shadow IT and end user computing guidance	• establish whether use of shadow IT systems and end user computing solutions are covered by Council guidance that has been communicated to all employees; and • Evaluate the extent to which Digital Services have been informed and are aware of shadow IT usage within the Council following the one off shadow IT exercise completed November 2017 and March 2018.
Service area assurance on shadow IT controls	For a sample of shadow IT systems used across the Council, establish: • whether a named owner has been established and recorded; • what assurance is obtained from third party system providers and whether this covers the areas specified in the externally hosted ICT services protocol.in relation to system security; ongoing GDPR compliance; and the ability of the system provider to restore the system (in the event of a disaster) within expected timeframes (recovery time objectives) and to the agreed restoration point (recovery point objectives), • whether an appropriate user access management process has been established by the service area; • whether third party access rights to the system are effectively managed; • whether a sufficient volume of user licences is available, and that these are renewed in sufficient time to ensure ongoing system access; • whether Digital Services / CGI have been made aware of the shadow IT system by the relevant service area; and • whether the risks associated with ongoing use of the of shadow IT system have been included in the relevant risk registers and reflected in the annual governance statement (where appropriate).
Service area end user computing controls	Where end user computing solutions (for example, Microsoft Access databases; Excel spreadsheets; or macros) have been established that are critical to support ongoing service delivery, confirm that: • they are adequately protected to ensure that the content cannot be overwritten; and • recovery time and point objectives have been communicated and agreed with Digital Services / CGI to recover end user computing files stored on the Council's network drives.
Procurement controls	Confirm that appropriate procurement controls have been established to:

	• identify potential purchases of new technology systems that meet the definition of shadow IT over £3,000; • identify procurement waivers that relate to shadow IT prior to approval; and • ensure that all procurement of shadow IT systems over £3,000 (including waivers) are subject to review and approval by Digital Services (following consultation with CGI) prior to procurement / waiver approval / renewal.
Corporate network controls	For the Council's Corporate network, confirm that: • the security designs agreed between the Council and CGI are appropriately designed. • user devices are appropriately secured by CGI in line with the agreed designs to prevent unauthorised installations. • third party network user access rights are appropriately allocated and effectively managed by CGI to support manual installations. This will not involve engagement with third parties. • only software that has been approved by the Council or is supported by an approved CGI change request is installed on the networks.
Learning and teaching network controls	For the Council's Learning and Teaching network, confirm that: • the established controls that enable completion of installations on the Learning and Teaching network have been adequately designed. • a clear policy has been established and communicated that details the nature of acceptable installations and the installation process applied to the Learning and Teaching network. • there is an established process to request and allocate user access rights that enable employees to perform installations on the Learning and Teaching network. • there is a comprehensive list of users who have the relevant access rights to make installations on the Learning and Teaching network. • the list of users who can complete installations is effectively maintained and regularly reviewed to ensure that it remains appropriate. • All network installations are completed in line with the established policy.

The City of Edinburgh Council

Internal Audit

Life Safety

Final Report

14th October 2020

CW1910

Overall report rating:

Significant Improvement Required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2020/21 internal audit plan approved by the Governance, Risk and Best Value Committee in [insert month] 2020. 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

Life safety within the City of Edinburgh Council (the Council) considers the health and safety risks associated with fire (including fires resulting from gas and electricity issues); asbestos (that could potentially result in risk of harm to maintenance workers and occupants); and water (legionella).

Asbestos is a material composed of naturally occurring silicate minerals that include microscopic 'fibrils' that can be released into the atmosphere by abrasion and other processes, causing significant harm when inhaled.

Legionella is a type of pneumonia typically caused by breathing in small droplets of water in the air that contain the bacteria, from water sources such as water tanks; cooling towers; showers; or swimming pools.

The Council owns a significant number of properties (including Council housing stock) that are either used by the Council to deliver services (for example crematoria; schools; and care homes) or leased to external third party organisations or citizens.

Consequently, it is essential that life safety risks are effectively identified and properly managed to ensure the ongoing health and safety of employees, citizens and third parties accessing and using these properties.

Legislation and regulations

Workplace health and safety across the UK is regulated by the Health and Safety Executive (HSE) who operate with the objective of preventing workplace death, injury or ill health. There are a large number of regulations organisations need to comply with to ensure that life safety risks are managed, including the Fire (Scotland) Act 2005; the Fire Safety (Scotland) Regulations 2006; the Control of Asbestos Regulations 2012; The Health and Safety at Work Act 1974; Management of Health and Safety at Work Regulations 1999; and the Control of Substances Hazardous to Health Regulations 2002 (as amended) (COSHH). Water safety is also managed in line with Managing legionella in hot and cold water systems and Health and Safety in Care Homes guidelines and publications.

The Council must be able to demonstrate that the established health and safety policies and governance framework are aligned with, and will support, ongoing compliance with all legislative and regulatory requirements and supporting guidance.

Lessons Learned from External Incidents

It is also essential that the Council responds appropriately to any external life safety incidents (for example the June 2017 Grenfell Tower Fire and Professor John Cole's February 2017 findings) and provides assurance that the associated root causes and lessons learned from relevant reviews and investigations (for example the 2018 Hackitt report on the adequacy of the regulatory system covering high rise and complex buildings) have been considered, assessed, and incorporated into the Council's established health and safety governance framework.

The Three Lines of Defence Model

The Three Lines of Defence model can be applied to the ongoing management of life safety across the Council where the 'first line' is the divisions and directorates who are responsible for ensuring that life safety risks and issues are identified, prioritised and addressed in line with applicable health and safety policy requirements.

'Second line' teams are typically responsible for developing and maintaining health and safety frameworks and supporting policies and guidance; ensuring these are effectively communicated; providing ongoing training and support; and delivering an audit programme to assess whether health and risk is effectively managed.

The 'third line' (for example Internal Audit) provides independent assurance on key controls established within the first and second lines to manage life safety risks.

The Council's Health and Safety Framework

The Council has an established health and safety governance framework designed with the objective of achieving effective ongoing management and oversight of health and safety risk across the Council, together with ongoing compliance with Council Health and Safety policy requirements established to protect the health, safety and welfare of Council employees and third parties including members of the public, contractors and service users.

The overarching Health and Safety policy is also further supported by the Water Safety, Fire Safety and Asbestos policies that specify the Council's approach to, and roles and responsibilities for, managing each of these distinct life safety risks.

This involves ensuring that;

- both management and Council employees have an appropriate level of awareness of life safety risks;
- there is a clearly established route to report any issues identified (for example, where a life safety risk is identified in a school);
- that property risk assessments are routinely performed to identify life safety risks;
- reported risks and survey outcomes are recorded and considered and the necessary repair work prioritised; and
- that immediate action is taken to address any significant risks (for example building closures).

Health and Safety Roles and Responsibilities for the Council's operational estate

Water Safety

The Property and Facilities Management (P&FM) division has overall responsibility for the management of water safety across the operational estate used by the Council to deliver services, with the exception of operational properties managed by third parties on behalf of the Council and leased properties.

Edinburgh Scientific Services (ESS) supports P&FM with their ongoing management of water safety by managing a programme of legionella risk assessments, and sampling and testing water systems to check for bacteria (including legionella) and chemicals across the Council's operational properties.

ESS also performs routine inspections and ongoing maintenance of water systems based on risk assessment outcomes, including monthly water temperature checks; quarterly showerhead disinfection; and 6 monthly water tank and calorifier inspections. Reports detailing the outcomes of the ESS risk assessments and inspections are then provided to P&FM.

P&FM water quality officers are responsible for compliance with water safety statutory requirements across the estate; maintaining water quality information; reviewing legionella risk assessments performed by ESS; arranging any urgent remedial works; and delivering an annual programme of routine remedial work across water systems to ensure that legionella risk is effectively managed.

'Duty holders' or responsible senior managers (for example Headteachers) in each property (circa 600 across the Council) and their relevant Heads of Divisions also have a responsibility for ensuring

that actions from legionella risk assessments are completed; infrequently used outlets are flushed at least weekly; log books are maintained; and that emergency procedures are applied where properties have tested positive for legionella or other bacteria and chemicals.

Fire Safety

The Council's current Fire Safety policy confirms that duty holders for each operational property are responsible for ensuring completion and review of fire risk assessments on an annual basis; completion of ongoing quarterly inspections; ensuring that an appropriate number of fire wardens are appointed and trained; ongoing completion of fire drills; maintenance of emergency evacuation plans (including personal and generic emergency evacuation plans, where required); and ongoing compliance with all other aspects of the Fire Safety policy, with support from external experts where required.

Heads of Divisions are accountable for the ongoing compliance of duty holders in their respective areas (for example, the Head of Schools and Lifelong Learning will be accountable for Fire Safety policy compliance across the school estate).

Any potential fire safety risks identified are escalated to the Property and Facilities Management division for inclusion in the fire safety improvement programme that they are responsible for delivering across the Council's operational estate, including completion of fire safety surveys; delivering a prioritised programme of fire safety remediation and improvement activities; performing fire safety audits and investigations; and ongoing testing, maintenance and reporting.

Asbestos

The P&FM division is currently responsible for the management of asbestos across the operational estate, with the exception of properties managed by third parties on behalf of the Council and leased properties. Asbestos management services are commissioned from specialist external providers and include maintenance of asbestos registers and management plans; completion of asbestos surveys and sample testing; completion of air testing; preparation of reports detailing the outcomes; and the safe removal of asbestos.

Health and Safety Roles and Responsibilities for housing revenue account (Council housing stock) properties.

The Housing Property Team (HPT) is responsible for the ongoing inspection, repair, and maintenance of the Council's housing stock and comprises a number of teams responsible for responsive repairs; planned maintenance; mechanical and electrical and gas repairs and maintenance (fire safety); the ongoing management of asbestos in common areas of domestic properties; and a capital maintenance programme.

Ongoing repair and maintenance of Council housing stock is completed with support from external third-party contractors, with specialists engaged (where required) for any high risk or technically complex repairs and removal of asbestos.

HPT is also currently responsible for ongoing asbestos inspection and resolution, and management of water safety across the housing stock estate. Asbestos inspection and resolution activities are currently being performed with support from external specialists, whilst ESS supports HPT with water safety management by completing ongoing legionella inspections and resolving any potential legionella risks identified across these properties.

Second Line Corporate Health and Safety

The second line Corporate Health and Safety team is responsible for the design and ownership of the Council's health and safety framework and supporting policies and guidance; ensuring that these are appropriately communicated across the Council; providing ongoing health and safety training; and

delivering a programme of audits to assess policy compliance and the effectiveness of processes supporting identification and resolution of health and safety risks and issues.

Leased Council Properties

Whilst the Council retains full responsibility for all repairs and maintenance associated with housing stock that is leased to citizens, third party organisations are responsible (per the requirements of lease agreements) for all repairs and maintenance of investment portfolio properties leased to them by the Council, including health and safety and life safety risks. Where new tenants are entering a vacant property, the new tenant is required to ensure that the property is fully compliant with applicable health and safety regulations prior to opening for trading.

Scope

The objective of this review was to assess the design adequacy of the key controls established to ensure that the Council is effectively identifying, managing and addressing life safety risks across its property portfolio in line with the requirements of the Council's overarching health and safety and associated life safety policies.

The review specifically considered the key life safety controls applied across schools; care homes; crematoria; council housing stock; and owned and leased Council properties

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

Health and Safety*: As a result of potential gaps in training, management or understanding, deliberate or accidental actions, there is a risk of non-compliance with legislative requirements and/or the Council's health and safety policies or operational procedures. This could lead to an incident resulting in regulatory breaches, harm to staff, service users or members of the public, subsequent liability claims, fines and associated reputational damage.*

Our areas of audit focus as detailed in our terms of reference are included at Appendix 2.

Our review considered the design of the life safety processes applied across the period February to May 2020. These processes were governed by Life Safety policies covering the period 2017 to 2020.

Limitations of Scope

This review focused only on the design adequacy of the Council's established health and safety framework in relation to life safety risks and did not test its operating effectiveness.

The following areas were also specifically excluded from scope:

- asbestos risk identification and remediation as the Council has recently performed an extensive review of this area with support from external consultants.
- second line assurance oversight provided by the Corporate Health and Safety team as which is a known issue given a number of existing vacancies has impacted on team capacity.

Approach

The following approach was applied:

- Development of a framework to test the design of the Council's controls to mitigate key life safety risks;
- Workshops and interviews with key management individuals from P&FM, HPS, ESS and Corporate Health & Safety to enable completion of the framework
- Review of key life safety policies and any supporting guidance;
- Evaluation of the design of the key controls in place to address the key risks;
- Preparation of a draft report detailing the findings raised and Internal Audit recommendations;

- Discussion on control gaps identified and agreeing management actions with key stakeholders; and
- Preparing a final report that includes agreed management actions and implementation dates.

Reporting Date

Our audit work concluded on 19 May 2020, and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Total number of findings: 5

Summary of findings raised	
High	1. Life safety systems and reporting
High	2. Operational estate – fire, gas, electricity, and water risk management
High	3. Life safety – training, competence and assurance
Low	4. Housing Property Services – fire and water safety processes
Low	5. Corporate Health and Safety

Opinion

Significant Improvement Required

Our review identified significant and numerous control weaknesses in the design of the control environment and governance and risk management frameworks established to support the ongoing identification, management, and resolution of the Council's fire and water life safety risks. Consequently, only limited assurance can be provided that life safety risks are being managed and that the Council's objectives to protect employees; service users; and members of the public by ongoing compliance with applicable legislative and regulatory requirements will be achieved.

Three High and two Low rated findings have been raised, with the majority of the High rated findings demonstrating the need to improve the design of control and assurance frameworks supporting ongoing fire safety management across the Council's operational property estate.

Responsibility for completion of fire risk assessments.

The current Council Fire Safety Policy directs that first line divisional and directorate building or site health and safety responsible person (duty holders) are responsible for ensuring completion of fire risk assessments (FRAs) (as required by Scottish fire regulations) and their annual review. It is important to note that the Council's policy is more stringent than current Scottish fire legislation which requires that a review of FRAs should be performed at regular intervals an and does not specify an FRA review timeframe. The Council currently requires either an annual review, or a review when circumstances change, rendering existing FRAs out of date.

The policy also states that duty holders are responsible for prioritisation and actioning of fire safety discrepancies identified from the FRAs, but does not specify any requirement for first line management to confirm that these have been completed to an appropriate level of quality

Currently, with the exception of Property and Facilities Management (P&FM), first line Council divisions and directorates have no established processes to confirm that duty holders have completed FRAs; that they are of an appropriate quality; and that they are reviewed annually. Instead reliance is placed on assurance reviews performed by Property and Facilities Management. .

Our review confirmed that the policy is not being consistently applied in practice as, whilst there is now a plan in place for rolling inspections by P&FM, there remain circa 400 properties across the operational estate where existence and quality of FRAs has not yet been confirmed.

Operational property estate

Significant progress is evident in relation to management of life safety risks across the operational property estate since completion of the last full estate property condition survey performed by an external consultant in September 2017, with asset condition surveys now completed across the full estate; fire safety reviews (168 audits in 2019/20) completed for circa one third of the estate; and daily property checks performed by onsite Facility Technicians.

Additional assurance is also obtained from audits performed by the second line Corporate Health and Safety team (although completion has recently been impacted by availability of resources due to ongoing vacancies); independent fire safety audits performed by the Scottish Fire and Rescue Service (33 audits completed in 2019/20); and a rolling programme of property risk improvement surveys (with specific focus on fire risk) performed by the Council's external property insurers with 13 reviews completed since their appointment in October 2018. Additionally, the Scottish Fire and Rescue Service randomly conducted 32 audits across the school estate in 2019 – 20 and in every case an FRA was in place.

However, further immediate action is required to confirm whether FRAs have been completed across the remaining (circa 400) properties; whether completed assessments are of an appropriate quality; and whether there are any new significant life safety risks associated with these properties that should be urgently addressed. Additionally, as the extent and significance of potential life safety risks and associated repairs has not been assessed across the full estate, it is not possible to confirm the adequacy of current budgets to address and manage these risks on an ongoing basis.

It is important to note that concerns in relation to completion and quality of fire risk assessments across the operational property estate have been escalated by both P&FM and Corporate Health and Safety through relevant risk committees and to the Corporate Leadership Team

Housing property services

We also established that (whilst some improvements are required), fire and water life safety controls supporting ongoing management of the Council's housing property portfolio are generally adequately designed (refer finding 4).

Thematic findings

A number of thematic findings have also been raised that apply across both the operational and housing property portfolios and to the second line Corporate Health and Safety team. These reflect the need to:

- establish effective systems and reporting processes to support the ongoing completeness and accuracy of life safety data across the Council and provide management with consolidated holistic reporting on ongoing life safety risk management and incident reporting (finding 1);
- identify all employees with life safety responsibilities; assess their training needs; and ensure that they attend relevant training on an ongoing basis to confirm that their life safety knowledge remains aligned with current Council policies and procedures and any relevant legislative of regulatory changes (finding 3);
- confirm first line (divisional – including P&FM) and second line (Corporate Health and Safety) life safety assurance responsibilities; agree relevant requirements for ongoing proportionate risk based assurance; and implement and maintain effective life safety assurance frameworks (finding 3);

- review and refresh existing life safety policies and confirm responsibilities for development and ongoing maintenance of first line life safety procedures; review and assess capacity for provision of second line technical life safety support to first line operational teams; and ensure that all relevant Council employees have access to the Safety Heath and Environment (SHE) incident reporting portal that is also used to monitor resolution if second line assurance findings (finding 5).

Further detail on each of the findings raised is included at Section 3.

Areas of good practice

Properties and Facilities Management – operational estate

- A monthly fire safety dashboard is produced and shared with Head of P&FM that includes data on fire incidents and Unwanted Fire Alarm systems (UFAS); fire authority audits; fire safety inspections performed by P&FM; and insurer surveys.
- A monthly fire safety group has also been established that is attended by Property and Facilities Management; Housing Property Services and Corporate Health and Safety.
- P&FM have established procedures for escalating any fire related H&S issues identified from ongoing condition surveys across the operational estate; competent contractors have also been established to support ongoing fire safety maintenance and equipment compliance testing and planned preventative maintenance programmes, with the objective of ensuring that operational properties are safe and dry through completion of quarterly visits; ;
- The ZetaSafe system is used to manage and monitor completion of water safety checks, sampling, testing and maintenance. The system holds information on all water assets; risk assessments; management plans; and maintenance and testing.

  All water assets have a barcode that can be scanned using a tablet following completion of any type of inspection or works, with the information then uploaded to the system. ZetaSafe also provides auto notifications when tasks are due/overdue or when issues have been identified during monitoring and testing and allows various reports to be generated.

  A status report is generated for every building on a monthly basis and this is reported to P&FM senior management and the Water Safety Steering committee (chaired by the Head of Property and Facilities Management). The report highlights any significant instances of non-compliance, for example gaps in regular flushing which should be completed on site by Facilities Technicians (see finding 5). Any water related issues are escalated via the various council Health and Safety governance forums.
- Whilst there is no legal or regulatory requirement for organisations to maintain a standalone fire investigation process, P&FM has developed their own fire safety incident investigation procedure, and there would be significant benefit to the Council if this was shared with and used by Housing Property Services.

Housing Property Services

- Senior Officers meet quarterly with Scottish Fire and Rescue Service (SFRS) to discuss and review the approach to capital and responsive works. SFRS also completes annual Fire Inspections on each of the 44 multi blocks in the City that are owned by the Council, with outcomes provided to Housing Property. Appropriate actions to address any weaknesses identified are recorded on the Northgate system, and closed actions are reported back to SFRS.
- A well designed quality assurance process has been established in relation to fire and water safety testing and ongoing repairs and maintenance activities. This includes oversight of capital works; team leader review of work performed by internal teams, supported by upward reporting to management; and use of a team of trained quality control experts who review 10% of all completed work on an annual basis.

- Contracts for external assurance on the quality of gas life safety testing and maintenance have been established with CORGI, and similar contracts are being established for fire and electrical works and asbestos.
- Whilst there is no requirement under Scottish Law to conduct fire risk assessments (FRA's) for the council's housing stock, including high rises, following Grenfell, new independent FRAs on high rise blocks were completed.

  Recommended actions to address the risks identified from these FRAs are now being implemented for some blocks, with a programme and supporting budget of circa £4.5M to complete the work required in the remaining blocks planned or completion in the 2020/21 financial year.

3. Detailed findings

1. Life safety systems and reporting	High

Review of the systems and processes established to record and manage life safety risks across both the Council's operational and housing revenue properties established that:

1. **Completeness and accuracy of life safety data** - whilst systems have been established to support recording and ongoing maintenance of the Council's operational properties (the Computer Aided Facilities Management (CAFM) system); housing revenue properties (the Northgate system); Edinburgh Scientific Services (ESS) ZetaSafe system for water management across operational properties; and ESS's own system for housing revenue properties, these systems do not currently include the full population of life safety asset registers, risk assessments and testing (planned and completed), and testing outcomes.

   Instead, reliance is placed on a number of manual systems and processes and, in some instances, information is lacking. Specifically:

   Operational Properties

   - fire safety equipment asset register - currently maintained on an Excel spreadsheet. Management has advised that this was in the process of being transferred into the CAFM system during the audit.
   - fire safety and gas and electrical inspections; testing; ongoing maintenance; and repairs - a large proportion are currently recorded and monitored on various Excel spreadsheets that are also in the process of being transferred into CAFM.
   - there is currently no gas and electrical equipment asset register - management has advised that this has now been completed prior to completion of our audit fieldwork and is included in the CAFM system. Additionally, details of electrical and gas testing and maintenance are retained in circa 300 separate building files that are reviewed individually to confirm that maintenance and testing has been completed by external contractors across all equipment.
   - Unwanted Fire Alarm Signals (UFAS) **–** UFAS are currently reported using a form on the Council's Intranet (the Orb) and not through the established Safety Health and Environment (SHE) incident reporting system. There is also a lack of understanding in relation to the UFAS reporting process that is resulting in significant under reporting of the actual position.

     It is acknowledged that Properties and Facilities Management (P&FM) has implemented some actions to address this issue with reporting on UFAS to management; creation of an interim UFAS procedure and diagnostic report; visits to the top 5 offenders; and design of a change process that has still to be implemented.

- Remediation of water risks **–** Whilst the Zetasafe water management system is used to record completion of actions implemented in response to planned ESS inspections, actions implemented to address water risk assessment outcomes are not centrally recorded. Instead, these actions are centrally recorded in onsite log books that are manually reviewed by ESS as part of the next scheduled inspection.

Housing Property Services

- five year electrical testing programme and electrical upgrade works - the outcomes of testing and upgrade works performed by external contractors are currently retained on a contract by contract basis, requiring manual consolidation of testing outcomes for each contractor to confirm progress across the estate.
- asset registers, testing, maintenance, and repairs – are managed and recorded outwith the Northgate system where work is performed by external contractors.
- testing, maintenance, and repairs - where recorded on Northgate, the process applied to update and maintain these records is manually intensive.

2. **Life safety key performance measures and reporting** - there are currently no established Council-wide life safety key performance measures and no holistic management reporting on Council-wide life safety risks in the following areas:
   - operational estate – completion or review of fire risk assessments; fire safety equipment testing and maintenance; and gas and electrical equipment testing and maintenance.
   - housing property services – fire incidents (currently only reported informally on an ad hoc basis); fire safety audits and inspections; fire safety equipment testing and maintenance; gas and electrical equipment testing and maintenance (currently gas safety check outcomes are reported annually to the Head of Place Development prior to submission to the Scottish Housing Regulator); gas and electrical and water safety incidents (currently only reported informally on an ad hoc basis) and completion of water safety testing and maintenance.
3. **Life safety incident identification and escalation** - there is no established criteria to determine the significance of life safety incidents, and no established escalation process to ensure that P&FM and HPS management are immediately advised, with incidents subsequently reported through the Council's established health and safety governance framework.

   Currently, P&FM and HPS teams use their professional judgement to determine which life safety incidents should be escalated and who they should be reported to.
4. **Incident and near miss reporting** – there is a general issue across the Council in relation to completeness of reporting of life safety incidents and near misses by onsite duty holders via the Safety, Health and Environment (SHE) incident reporting system, with fire related incidents often advised to management by the Fire and Rescue Service following their attendance at incidents.

Risks

The potential risks associated with our findings are:

- failure to complete key life safety risk assessments and inspections, testing and maintenance with an increased risk of incident occurrence.
- limited assurance that appropriate remedial actions have been implemented in a timely manner to address the outcomes of fire and water risk assessments.
- non-compliance with applicable legislation and regulations.
- potential improvement/prohibition notices from Fire and Rescue Service where faulty fire alarm equipment results in increased number of call outs where there is no fire, resulting in potential

fines.

- inadequate management oversight resulting in failure to identify instances where checks have not been completed and non-compliance with legislation and regulations.
- Directors are unable to fulfil their responsibilities as detailed in the Council's Health and Safety policy in relation to effective governance and oversight of health and safety, and ensuring that incident escalation procedures have been established and communicated.
- Incomplete reporting of fire related incidents and near misses resulting in inability of operational teams to identify trends and root causes and make any necessary changes to prevent recurrence.

1.1 Recommendation: Consolidated life safety management and reporting systems

1. Management should consider the feasibility of incorporating and consolidating all stand-alone life safety date into one existing system that covers both the operational and housing property portfolios or (alternatively) recording all operational property data (including water safety data) in the CAFM system and housing property data in the Northgate system.
2. In the interim, management should assess whether it is feasible to incorporate stand-alone life safety data into the following existing systems
   - Computer Aided Facilities Management (CAFM) for operational properties;
   - Northgate for housing properties;
   - Zetasafe for water management; and
   - Safety, Health and Environment (SHE) portal for incident reporting and ongoing management of second line health and safety assurance findings.

   Where this is possible, stand-alone life safety data should be uploaded into these systems and regularly maintained.

1.1.1 Agreed Management Action: Consolidated life safety management and reporting systems

1. The Head of Property and Facilities Management and the Head of Place Development have confirmed that their preference is to maintain separate systems for the operational property (the CAFM system) and housing property estates (the Northgate system).

   Housing Property Services has advised that all housing property estate asset and tenant data is maintained on Northgate and its supporting feeder systems, ensuring effective risk management and ongoing compliance with Scottish Housing Regulator requirements – no further action required.

   Management is currently investigating the feasibility of consolidating the second line teams and resources that have life safety responsibilities across the housing and operational property estates. The feasibility of consolidating stand alone systems and data will be considered as part of this assessment.

   If a decision is made to consolidate the stand alone systems and data into either a new or existing system, a business case will be developed and (if approved) a new project established or the scope of an existing project (for example the CAFM system project) extended to support this process.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Peter Watton, Head of Property and Facilities Management; Layla Smith, Operations Manager, Resources; Audrey Dutton, Executive Assistant	**Implementation Date:** 31 January 2022

1.1.2 Agreed Management Action: Property and Facilities Management - consolidated life safety management and reporting systems

2. In the interim, the feasibility of incorporating stand-alone life safety data in relation to the operational property estate (as noted in finding 1 above), including any relevant associated costs into the following existing systems will be considered
   - Computer Aided Facilities Management (CAFM) for operational properties;
   - Zetasafe for water management; and
   - Safety, Health and Environment (SHE) portal for incident reporting and ongoing management of second line health and safety assurance findings.

Where this is possible, stand-alone life safety data will be uploaded into these systems and regularly maintained.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Peter Watton, Head of Property and Facilities Management; Andrew Field, Senior Manager, Property and Facilities Management; Brendan Tate, Property and Facilities Management; Brenda; Mark Stenhouse, Senior Manager, Facilities Management; Gohar Khan, Performance and Audit Officer, Facilities Management; Layla Smith, Resources Operations Manager; Audrey Dutton, Executive Assistant	**Implementation Date:** 29 January 2021

1.1.3 Agreed Management Action: Housing Property Services - consolidated life safety management and reporting systems

The issue with the asset register, testing, maintenance and repairs is part of the ongoing Housing Service Improvement Plan, and will be addressed by implementation of the Total Mobile technology solution.

The Council is now in phase two of a three phase Total Mobile programme that includes workstreams relating to responsive repairs, gas safety checks, and voids. Total Mobile has also been successfully implemented to support completion and recording of annual Gas Safety Checks

Phase 3 will include an automated solution for the current Mechanical and Electrical regime plus routine Legionella maintenance and testing, and will also be used to support programmed works completed by external contractors.

Housing Property are also implementing an Asset Management register which will sit within the Northgate system. This is being delivered as part of the Northgate system upgrade by the Council's Digital Services team working in partnership with our CGI and Northgate.

Owner: Paul Lawrence, Executive Director, Place **Contributors:** Michael Thain, Head of Place Development; Willie Gilhooly, Housing Property Manager; Patricia Blore, Housing Property Operations Manager; Alison Coburn, Place Operations Manager.	**Implementation Date:** 30th June 2023

1.2 Recommendation: Life safety key performance measures and reporting

1. Until comprehensive life safety systems are implemented, a mapping should be performed across both the operational and housing property portfolios to identify all current sources of life safety and other relevant health and safety data held, and assess its prioritisation and importance in relation to confirming ongoing regulatory compliance and supporting management reporting.
2. Following completion of the data mapping exercise, management should determine relevant risk based and proportionate life safety key performance measures designed to support reporting to management and governance forums (including risk committees and Council executive committees)

and confirm ongoing compliance with applicable legislation and regulations. These performance measures should be agreed by the Council Health and Safety Group and the Corporate Leadership Team (CLT).

3. Existing management reporting processes should be refreshed across both portfolios to incorporate an assessment of performance in comparison to agreed life safety key performance measures, and the extent of ongoing compliance with applicable legislative, regulatory, and Council policy requirements. This should include supporting rationale where performance measures have not been achieved or instances of non-compliance have occurred, together with details of remedial actions.
4. Appropriate quality checks should be performed to confirm the completeness and accuracy of management information, especially where the preparation process involves manual consolidation of data from a wide range of sources.

1.2 Agreed Management Action: Life safety key performance measures and reporting

A holistic life safety performance framework will be established following consolidation of the second line teams and resources that have life safety responsibilities across the housing and operational property estate, and implementation of comprehensive life safety systems that include all relevant life safety data.

This framework will incorporate all existing performance frameworks (for example the Housing Property Services performance framework that is current being reviewed) and will include a new set of standard risk based and proportionate life safety key performance measures designed to support reporting to management and governance forums (including risk committees and Council executive committees) and confirm ongoing compliance with applicable legislation and regulations

The revised performance framework will be reviewed and approved by the Corporate Leadership Team (CLT) prior to implementation.

Life safety performance management information will include supporting rationale where performance measures have not been achieved or instances of non-compliance have occurred, together with details of remedial actions.

The process applied to produce relevant life safety management information for reporting purposes will also include completion of quality checks to confirm its ongoing completeness and accuracy, especially where the preparation process involves manual consolidation of data from a wide range of sources.

In the interim, there will be no changes made to the existing performance frameworks and the processes supporting production of existing life safety management information by divisions and directorates.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Nick Smith, Head of Corporate Health and Safety; Peter Watton, Head of Property and Facilities Management; Gohar Khan, Performance and Audit Officer, Property and Facilities Management; Layla Smith, Operations Manager, Resources; Michelle Vanhegan, Executive Assistant; Audrey Dutton, Executive Assistant	**Implementation Date:** 29th April 2022

1.3 Recommendation: Life safety incident identification, escalation, and reporting

The second line Corporate Health and Safety Team should:

1. Set relevant criteria to determine the significance of life safety incidents. The criteria should be agreed by the Council Health and Safety group and the Corporate Leadership Team (CLT); included within relevant life safety policies; and communicated across the Council.

2. Design an appropriate and proportionate risk based near miss and incident escalation process to be applied by managers in first line divisions and directorates (including duty holders) across both the council operational and housing property estates. The escalation process should also detail the significance of near misses and incidents to be reported to the Council's Health and Safety Group; the Corporate Leadership Team; and relevant Council executive committees as appropriate.
3. Communicate and reinforce the importance of recording incident, diseases, and near miss reporting across the Council with particular focus on onsite duty holders at operational properties across the Council through the Safety, Heath, and Environment (SHE) reporting portal.
4. Consider whether incidents and near misses are being consistently recorded and escalated as part of their ongoing health and safety assurance programme.

1.3 Agreed Management Action: Life safety incident identification, escalation, and reporting

Corporate Health and Safety will:

1. issue guidance to establish relevant criteria to determine the significance of life safety incidents, for approval by the Council Health and Safety Group.
2. send out a communication to all Council employees about the importance of reporting all incident types on the SHE system and the statutory nature of RIDDOR. This will be highlighted when opening SHE and the forthcoming HS policy review and will include a procedure for reporting incidents through management in addition to SHE.
3. send out a communication to all staff about the importance of reporting and the statutory nature of RIDDOR. This will be highlighted when opening SHE and the forthcoming HS policy review.
4. consider whether incidents and near misses are being consistently recorded and escalated in line with policy as part of the ongoing health and safety assurance programme.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Nick Smith, Head of Legal and Risk; Robert Allan, Senior Health and Safety Manager; Layla Smith, Operations Manager, Resources; Michelle Vanhegan, Executive Assistant.	**Implementation Date:** 30th June 2021

2. Operational estate – fire, gas, electricity, and water risk management **High**

Review of the processes applied across the Council's operational estate in relation to the ongoing management of fire, gas, electricity, and water life safety risks confirmed that:

1. **fire risk assessments (FRA) population** – there is currently no register of all Council buildings where an FRA is required and their completion status. Whilst the full population of Council properties is included in the CAFM system, fire risk assessment requirement and completion details have not yet been populated. Instead, FRAs (where completed) are retained locally at each property, with no copies provided centrally for review by management to assess completion and quality.
2. **FRA completion and review** - the Council's Fire Safety Policy confirms that the building or site health and safety responsible person (duty holder) is responsible for ensuring FRA completion and annual review, and prioritisation and actioning of fire safety discrepancies identified from FRAs. Currently, first line Council divisions and directorates have no established processes to confirm that duty holders have completed FRAs and that they are reviewed annually. Instead reliance is placed on assurance reviews performed by Property and Facilities Management (P&FM) to confirm FRA completion and assess their quality (refer finding 3).

3. **investment property FRAs and equipment safety testing** – there is no established system to support ongoing monitoring of completion of fire risk assessments (FRAs) and gas and electrical testing and maintenance for multi-let buildings with common parts leased by the Council. Currently, progress is monitored using spreadsheets for the three separate portfolios of buildings.
4. **Fire Safety Policy –** review of the Council's fire safety policy confirmed that it requires FRAs to be reviewed at least once per year, which is not aligned with Scottish fire regulation requirements that require review of FRAs where a significant change been made to the premises or processes or operations within the premises.
5. **adequacy of life safety financial budget** – whilst there has been a substantial increase on life safety related repairs and maintenance following completion of the last full operational property estate property condition survey performed by an external consultant in September 2017, there is still no clear linkage evident between the outcomes of life safety risk assessments; the work required to address any significant risks identified; the prioritisation process applied; and available budget. P&FM management has confirmed that budget would be allocated to address any life safety risks identified regardless of current budget availability.
6. **oversight of FRA remedial actions** – some minor FRA remedial actions are immediately completed onsite at the time of P&FM reviews or following completion of a FRA, however, completion of these actions is not recorded. Additionally, no follow-up is performed by P&FM where FRA remedial actions are not implemented on the date of the site visit.
7. **Facility Technician (FT) fire safety equipment checks** – whilst the volume of regular (daily and weekly) legally required fire safety equipment checks of fire alarms; fire panels; and visual fire safety checks performed by P&FM FTs has substantially increased to a circa 85% completion rate, further action is required to address instances where these checks are not consistently completed by onsite FTs and increase this completion rate.
8. **FT water maintenance checks** – essential onsite water maintenance checks (for example running taps and flushing systems) are either not being completed by P&FM FTs, or are being completed, but not recorded in the Zetasafe water management system, which is currently showing only a 6% completion rate across the operational estate. Further action is required to address instances where these checks are not consistently completed by onsite FTs and increase this completion rate.
9. **electrical and gas contractor risk assessments** – there is no established process for ongoing review of contractor employee risk assessments that should be performed in advance of completing electrical and gas testing and maintenance activities. Currently, risk assessments are reviewed at the start of each contract (contract tenure can be 3 – 7 years) with informal reviews performed as part of ongoing supplier relationship management meetings. Management has confirmed that they are aware of this issue and that it will be addressed as part of the current wider retender process that includes delivery of these services

Risk

The potential risks associated with our findings are:

- Non-compliance with applicable legislation and regulations in relation to FRA and life safety checks, testing and maintenance.
- Life safety risks are not identified and addressed.
- Actions required to address FRA outcomes are not implemented.
- Incomplete or poor-quality risk assessments performed by third party contractors are not identified in advance of their employees completing gas and electrical equipment safety testing and maintenance.

- Increased risk of significant life safety incidents.

2.1 Recommendation: Responsibility for completion and ongoing review of fire risk assessments

The Council's Corporate Leadership team should:

1. consider the appropriateness of current support arrangements for duty holders who are responsible for completion and ongoing review of Fire Risk Assessments (FRAs) across the operational and investment property estates, and multi-let buildings with common parts leased by the Council, as specified in the Council's current Fire Policy.

   The feasibility of the following alternative options should be considered together with their associated risks and benefits:

   a. adequacy of the current process where responsibility for ensuring completion and ongoing review of FRAs is allocated to first line operational property duty holders. Actions required to address known gaps with the current process should also be considered.

   b. procurement of an external third party contractor to complete the remaining population of FRAs, with ongoing oversight and assurance provided by Properties and Facilities Management (P&FM). This is the recommended approach in the P&FM draft fire strategy document.

   c. transfer of responsibility for completion, ongoing review and assurance on the quality of completed FRAs to P&FM. Note that adopting this approach will require allocation of responsibilities to two separate P&FM teams to ensure effective segregation of duties between employees responsible for completion and ongoing review of FRAs, and those responsible for assessing their quality. Management estimates that this approach will require circa 3 years to complete review of the remainder of the operational property estate based on current resources and budget.

      When reviewing this option, management should also consider adequacy of resources and budget to support this process and, if necessary and in recognition of change of responsibility, approve budget transfers from individual service areas to P&FM.

2. Obtain advice and input from the Council's Health and Safety Group in relation to the available options.
3. Present the final recommendation to the Finance and Resources Committee for approval together with any required financial and budget implications. The final recommendation should include (but not be limited to) a process for ensuring that all FRA remedial actions are centrally recorded with follow-up performed to confirm that they have been implemented.
4. Implement and communicate the revised process across the Council, ensuring that duty holders in operational properties are clear on their respective roles and responsibilities.
5. Review the Council's Fire Safety Policy to align with the new process and obtain approval for any changes from the Policy and Sustainability Committee.

2.1.1 Agreed Management Action: Responsibility for completion and ongoing review of fire risk assessments

The appropriateness of current support arrangements for duty holders who are responsible for completion and ongoing review of Fire Risk Assessments (FRAs) across the operational and investment property estates, and multi-let buildings with common parts leased by the Council was considered by the Corporate Leadership Team (CLT) and the following actions agreed:

1. External resources will be procured by Property and Facilities Management (P&FM) on behalf of Council divisions to assess the completeness and adequacy of fire risk assessments (FRAs) across the remainder of the Council's operational property estate; refresh FRAs where required; and enhance the current baseline position. The costs associated with this exercise will be advised to divisions for inclusion in relevant divisional / directorate budgets.
2. First line duty holders will remain responsible for ensuring that FRAs are reviewed and updated as required in line with the Council's fire policy.
3. Property and Facilities Management will ensure that duty holders update their FRAs (where required) as part of their ongoing capital works programme across the operational property estate.
4. Following consolidation of the second line Housing and Operational Property teams and resources that have life safety responsibilities, the compliance team responsible for assessing the completeness and quality of FRAs will be strengthened, to ensure adequate ongoing coverage across the operational estate.
5. the revised processes supporting completion and review of FRAs will be implemented and communicated across the Council, ensuring that duty holders in operational properties, and property and facilities management teams responsible for completion of capital works and oversight of fire risk compliance are clear on their respective roles and responsibilities.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Peter Watton, Head of Property and Facilities Management; Andrew Field, Senior Manager, Property and Facilities Management; Brendan Tate, Property and Facilities Management; Brenda; Mark Stenhouse, Senior Manager, Facilities Management; Gohar Khan, Performance and Audit Officer, Facilities Management; Layla Smith, Resources Operations Manager; Audrey Dutton, Executive Assistant; Nick Smith, Head of Legal and Risk; and Robert Allan, Corporate Health and Safety Manager	**Implementation Date**: 30 September 2021

2.1.2 Agreed Management Action: Review of the Council's Fire policy in relation to Fire Risk Assessments

3. The Council's current fire policy will be reviewed to ensure alignment with the requirements of Scottish fire regulations in relation to Fire Risk Assessments (FRAs). This will include the need to review FRAs where a significant change been made to the premises or processes or operations within the premises.

   The requirement for completion of an annual review of FRAs will be removed and an appropriate review timeframe considered recognising the fire risk profile of the property.

   The policy will also be updated to reflect the revised approach adopted by the Council in relation to discharge of duty holder responsibilities for completion and ongoing review of FRAs.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Nick Smith, Head of Legal and Risk; Robert Allan, Council Health and Safety Manager; Layla Smith, Resources Operations Manager; Michelle Vanhegan, Executive Assistant.	**Implementation Date:** 30 September 2021

2.2 Recommendation: Adequacy of budget to address life safety risks

Following completion of the review of the status and quality of Fire Risk Assessments across the operational estate (refer recommendations 2.1.1) Properties and Facilities Management (P&FM) should:

1. Confirm that there is sufficient budget available to address all significant life safety risks identified from completed Fire Risk Assessments (FRAs).
2. Establish a process to confirm the ongoing adequacy of available budgets based on the outcomes of completed P&FM and Corporate Health and Safety assurance reviews, and ongoing annual reviews of FRAs.

2.2 Agreed Management Action: Adequacy of budget to address life safety risks

1. To ensure that all significant fire and other immediate safety risks are addressed as soon as they are identified, a process will be established to ensure that they are prioritised for allocation of funding within available budget.
2. A process will be established that considers the costs associated with fire risk remediation work identified from completed FRAs and ongoing fire safety audits. These costs will be recorded and compared against available budgets to ensure the ongoing adequacy of available budget for fire remediation works.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Peter Watton, Head of Property and Facilities Management; Andrew Field, Senior Manager, Property and Facilities Management; Brendan Tate, Property and Facilities Management; Brenda; Mark Stenhouse, Senior Manager, Facilities Management; Gohar Khan, Performance and Audit Officer, Facilities Management; Layla Smith, Resources Operations Manager; Audrey Dutton, Executive Assistant	**Implementation Date:** 1 January 2023

2.3 Recommendation: Completion of ongoing fire maintenance and water safety checks by Facilities Technicians.

The Property and Facilities Management (P&FM) team should:

1. Implement a process to identify instances where facilities technicians (FTs) do not consistently complete and provide the outcomes of daily and weekly fire safety equipment and water safety checks, and take appropriate action to ensure that this is addressed.
2. Design and maintain a process (using CAFM if possible) to ensure that appropriate follow-up of actions required to address the outcomes of facilities technician (FT) fire safety equipment and water safety checks is performed, that includes evidence of completion.

   The outcomes of this follow-up process should also include upward reporting to management on the volume and age of outstanding actions, and their significance.

2.3 Agreed Management Action: Completion of ongoing fire maintenance and water safety checks by Facilities Technicians.

1. Completion of ongoing daily and weekly fire safety equipment and water safety checks by Facilities Technicians (FTs) should be carried out by all FTs. A process will be implemented to identify FTs who do not consistently complete these checks and provide details of the outcomes, and appropriate action will be taken to ensure that this issue is addressed.
2. A follow-up process will be designed and implemented to ensure that the outcomes of FT fire and water safety checks have been addressed, with evidence provided to confirm completion. This

process will include reporting to first line management; duty holders; and relevant health and safety governance forums on the significance and age of outstanding items to be addressed.

3. A process will be designed and implemented that records all outstanding fire risk assessment (FRA) and fire safety and water safety actions together with agreed completion dates; reminds duty holders in advance that the work is due to be completed; and requests evidence of completion.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Peter Watton, Head of Property and Facilities Management; Andrew Field, Senior Manager, Property and Facilities Management; Brendan Tate, Property and Facilities Management; Brenda; Mark Stenhouse, Senior Manager, Facilities Management; Gohar Khan, Performance and Audit Officer, Facilities Management; Layla Smith, Resources Operations Manager; Audrey Dutton, Executive Assistant	**Implementation Date** 1 January 2023

2.4 Recommendation: Third party contractor gas and electrical risk assessments

Properties and Facilities Management (P&FM) should:

- perform an annual review of all third party risk assessments for electrical and gas works to confirm that they are appropriate.
- Confirm through established ongoing supplier management arrangements that these continue to be completed in advance of their employees completing gas and electrical testing and maintenance activities.

2.4 Agreed Management Action: Gas and electrical risk assessments and testing

Agreed, these actions will be implemented as recommended by Internal Audit and are already included in the scope for retendered hard FM contract

Owner: Stephen Moir, Executive Director of Resources **Contributors**: Peter Watton, Head of Property and Facilities Management; Andrew Field, Senior Manager, Property and Facilities Management; Brendan Tate, Property and Facilities Management; Brenda; Mark Stenhouse, Senior Manager, Facilities Management; Gohar Khan, Performance and Audit Officer, Facilities Management; Layla Smith, Resources Operations Manager; Audrey Dutton, Executive Assistant	**Implementation Date**:1 April 2023

3. Life safety – training, competence and assurance **High**

Review of both first (divisional and directorate) and second line (Corporate Health and Safety) responsibilities in relation to ongoing life safety management responsibilities highlighted that there is a lack of clarity in relation to first and second line responsibilities for training, competence and ongoing assurance. Specifically:

Training and competence

1. **Duty holder competence to complete fire risk assessment (FRA) and personal and generic emergency evacuation plans (P/GEEPs)** - there is a lack of clarity over the level of duty holder competence required to complete FRAs and P/GEEPs. No training needs assessments have been performed to identify whether duty holders have an appropriate level of competence, or whether completion of these activities should be outsourced. Additionally, the Council's fire policy

does not specify responsibility for ensuring the competence of duty holders, nor does it state how this should be assessed .

2. **FRA and PEEP training** – currently no mandatory training is provided for duty holders responsible for completion of FRAs and P/GEEPs.
3. **Fire warden training** – generic training is provided by the Corporate Health and Safety team, however, there is no on-site follow-up training cascaded or provided by the relevant on-site fire coordinator or duty holder.
4. **Facilities technician fire and water safety** checks – there is a strong likelihood that failure to complete ongoing fire and water safety checks by Property and Facilities Management (P&FM) facilities technicians (FTs) (refer finding 2) is attributable to a lack of training and competence in this area.
5. **Safety Health and Environment (SHE)** – whilst the Corporate Health and Safety team offers non-mandatory training on the use of the SHE portal that is used to manage incident reporting and implementation of agreed management actions to address health and safety audit outcomes, there is limited attendance across the Council, and feedback at the workshops indicated a lack of awareness of the importance and use of the SHE portal at management level. There is currently no established training needs assessment process to determine which employees across the Council should attend SHE training.

Assurance

6. **FRA assurance requirements** - the Council's Health and Safety policy and supporting procedures do not specify the required level of management assurance to be obtained on the quality of completed FRAs.
7. **FRA Assurance framework** – there is currently a lack of clarity on the design of the FRA assurance framework between the first (divisional and directorate) and second (Corporate Health and Safety) lines of defence in relation to confirming the completion and quality of FRAs. Currently, limited assurance is provided by both P&FM and Corporate Health and Safety given limited capacity in both teams.
8. **P&FM fire related assurance reviews** - whilst the volume of fire related assurance reviews performed by P&FM across the operational estate as part of their fire safety improvement programme has substantially increased, there remains circa two-thirds of the operational property estate that has not been reviewed since the last full operational estate property condition survey was completed by an external contractor in September 2017.

   Additionally, there is currently no established process to ensure that the P&FM asset condition survey and fire safety reviews, and reviews performed by the Council's insurers across the operational estate are appropriately prioritised in terms of life safety risks identified from completed risk assessments, and that no duplicate reviews are performed.
9. **Quality assurance of fire safety equipment testing** – previously, 10% sample quality checks were performed by P&FM on fire safety equipment testing and maintenance performed internally and by external contractors, however this process has now stopped in response to capacity constraints. Instead, reliance is placed on contractors who should report completion of work through the P&FM helpdesk, and on onsite FTs to complete a limited walk round inspection and report any issues to the helpdesk. FTs have not received training to support completion of these inspections.
10. **Quality assurance of third-party gas and electrical maintenance and repairs –** P&FM technical officers should quality assure a 10% sample of gas and electrical maintenance and repair work completed by external third-party contractors. These checks are no longer performed

due to capacity constraints, and management has advised that they are reliant on receipt of contractor completion reports. The current process does not provide an assessment of the quality of the work completed.

Risk

The potential risks associated with our findings are:

- Employees are unable to identify significant fire life safety risks for escalation and resolution and instances of non-compliance with applicable legislation and regulations.
- Inconsistent completion and quality of FRAs and PEEPs across the Council that is not identified and resolved.
- Issues with completion and quality of fire safety equipment testing and gas and electrical maintenance and repairs are not identified and resolved, resulting in increased risk of a potential fire related life safety incident.
- Potential risk of fraud where third-party contractors are either paid for work that has not been completed, or poor quality work that is not subsequently identified.

3.1 Recommendation: Training and competence – Corporate Health and Safety

The Corporate Health and Safety team should:

1. Review and refresh relevant Council policies to clarify and include first line (divisional and directorate) and second line (Corporate Health and Safety) responsibilities for assessing and confirming the ongoing competence of duty holders; facility technicians; and third party external contractors (where these activities are outsourced) in relation to completion of their life safety responsibilities.
2. Develop competency and training needs assessment criteria for operational property duty holders and facilities technicians in relation to their responsibilities for completion of fire risk assessments (FRAs) where this process is not outsourced; personal emergency evacuation plans (PEEPS); and completion of ongoing fire safety and water safety checks.

   The training needs assessment should also include confirmation re whether duty holders and facilities technicians have access to the Safety Health and Environment (SHE) portal, and whether training on use of the system is required to support incident reporting and recording completion of agreed management actions to address health and safety audit outcomes.
3. Issue training needs assessment forms to first line divisions and directorates with a request that these are completed for all duty holders and facilities technicians within an agreed timeframe.
4. Review the completed assessment forms to confirm whether any changes are required to existing training programmes. This should include the potential introduction of training to support completion of FRAs (where completion is not outsourced) and personal emergency evacuation plans (PEEPs), and completion of ongoing fire and water safety checks.
5. Ensure that all duty holders and facilities technicians requiring training on the SHE portal are registered for a training session.

3.1 Agreed Management Action: Training and competence – Corporate Health and Safety

1. Relevant Council policies will be revised to include first line (divisional and directorate) and second line (Corporate Health and Safety) responsibilities for assessing and confirming the ongoing competence of duty holders; facility technicians; and third party external contractors (where these activities are outsourced) in relation to completion of their life safety responsibilities.
2. Corporate Health and Safety will provide guidance to support completion of a training needs

analysis by first line managers for all relevant staff that will reflect the direct role responsibilities of duty holders in the context of Property and Facilities Management support

3. Following the training needs analysis being completed for relevant roles, consideration will be given to whether any changes are required to existing training programmes.
4. all duty holders and facilities technicians requiring training on the SHE portal will be required to register and attend a training session.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Nick Smith, Head of Legal and Risk; Robert Allan, Corporate Health and Safety; Robert Anderson, Lead Trainer, Corporate Health and Safety; Layla Smith, Operations Manager, Resources; Michelle Vanhegan, Executive Assistant	**Implementation Date:** 17th December 2021

3.2 Recommendation: On site fire warden training

Corporate Health and Safety should:

1. Consider whether onsite fire warden training is required across operational properties at an appropriate frequency (e.g. annually or six monthly). The requirement for training should be based on an assessment of the size and structure of individual buildings.
2. Consider whether support for delivery of onsite fire warden training is required from Corporate Health and Safety, or whether this can be performed by duty holders and facilities technicians.
3. Where considered necessary fire warden training should be implemented.

3.2 Agreed Management Action: On site fire warden training

1. Training needs analysis will identify the frequency of Fire Warden training (fire evacuation training on site will be conducted by duty holders not less than twice per year).
2. and 3. The best method of on-site fire training will be determined and entered into the training needs analysis and training event schedules.

Owner: Stephen Moir, Executive Director of Resources **Contributors**: Nick Smith, Head of Legal and Risk; Robert Allan, Corporate Health and Safety; Layla Smith, Operations Manager, Resources; Michelle Vanhegan, Executive Assistant	**Implementation Date:** 29th Oct 2021

3.3 Recommendation: First and second line assurance responsibilities

Corporate Health and Safety should:

1. Review and refresh the Council's existing Health and Safety policy and supporting procedures (where relevant) to ensure that they specify the required level of first line (divisional and directorate) and second line (Corporate Health and Safety) assurance on the quality of completed fire risk assessments; fire safety and water checks and ongoing gas and electrical testing and repairs and maintenance performed either internally by Council employees or external contractors.
2. Design a proportionate risk based H&S assurance framework that supports delivery of assurance responsibilities for implementation across divisions and directorates. This framework should consider:
    - outcomes of completed fire and water risk assessments;

- availability of resources;
- how outcomes will be reported and escalated to management; governance forums and Council executive committees where significant thematic findings are identified.
- the level of follow-up required to ensure that actions have been implemented and sustained to address outcomes of quality assurance reviews.

3. Ensure that any new Corporate Health and Safety assurance responsibilities as detailed in the framework are incorporated into the established second line Corporate Health and Safety assurance programme.

3.3 Agreed Management Action: Clarification of first and second line assurance responsibilities – Corporate Health and Safety

The relevant revised Health and Policies will outline first and second responsibilities and an assurance framework will be designed and implemented, including details of metrics to confirm assurance issues.

Owner: Stephen Moir, Executive Director of Resources **Contributors**: Nick Smith, Head of Legal and Risk; Robert Allan, Corporate Health and Safety; Layla Smith, Operations Manager, Resources; Michelle Vanhegan, Executive Assistant	**Implementation Date:** 30th Dec 2021

3.4 Recommendation: Assurance framework implementation – Properties and Facilities Management

Properties and Facilities Management (P&FM) should:

1. Develop a proportionate risk based assurance process that assesses the ongoing completion and quality of fire risk assessments (FRAs) and fire safety equipment and water safety checks performed by duty holders and FTs across the operational estate that is based on:
   - most effective use of established internal asset condition survey and fire safety review processes, and reviews performed by the Council's insurers to cover the entire operational estate on a rolling basis.
   - Identification of high risk properties in terms of their the age and structure, and quality of existing FRAs;
   - skills and experience of the individual or external organisation who completed the most recent FRA;
   - the geographical spread of the portfolio; and
   - capacity and availability of P&FM resources
2. Confirm that the review objectives will be to identify any significant life safety risks that need to be immediately addressed and confirm that all remedial FRA; water risk assessments; and safety check actions have been implemented, with review outcomes (including details of any remedial actions implemented at the site visit and any other actions required) recorded in CAFM.
3. Instruct immediate prioritisation and resolution of any significant life safety risks identified.
4. Advise duty holders and the Corporate Health and Safety team of any significant thematic risks identified from the reviews.

5. Agree a timeframe for completion of remedial actions that cannot be implemented on the date of the site visit with the duty holder, and record the action and expected completion date in CAFM for subsequent future review.

3.4 Agreed Management Action: Assurance framework implementation – Properties and Facilities Management

An appropriate risk based assurance programme will be implemented with resourcing requirements determined as part of the proposed consolidation of second line teams and resources that have life safety responsibilities across the housing and operational property estates (refer agreed management action 1.1.1 in this report).

The assurance programme will consider all of the Internal Audit recommendations noted above and also the recommendations resulting from the recent external asbestos review completed in 2019/20.

Owner: Stephen Moir, Executive Director of Resources **Contributors:** Peter Watton, Head of Property and Facilities Management; Layla Smith, Operations Manager, Resources; Audrey Dutton, Executive Assistant	**Implementation Date:** 30th April 2022

4. Housing Property Services – water and fire safety processes — **Low**

Our review of Housing Property Services established fire and water safety processes highlighted that:

1. Water risk assessments (RAs) – some water RAs have not been reviewed for more than two years in line with Council Health and Safety water policy requirements. A rolling programme to review water RAs commenced in 2019 covering all 20,000 properties, and it is anticipated that this will take circa five years to complete. Management has advised that all high risk buildings (high rise and sheltered accommodation) RAs are complete, and that the current frequency of testing is in excess of Health and Safety Executive minimum standards.
2. Visual fire safety inspections in low rise properties – the outcomes of daily visual fire safety checks performed to identify potential fire hazards (for example, fire exit blockages or significant waste build up) at low rise properties performed by housing patch officers are not recorded. In contrast, for high rise properties, the outcomes of daily inspections are recorded in onsite log books by concierges.

Risk

The potential risks associated with our findings are:

- Non-compliance with the Council's Health and Safety Water policy requirements.
- Issues identified from updated RAs could result in the need for more frequent inspections by Edinburgh Scientific Services (ESS) on high and medium risk properties, impacting their ability to complete ongoing water inspections across both the operational and housing property estate in line with applicable Health and Safety Executive requirements.
- Potential fire safety risks in low rise buildings are not recorded, escalated and addressed.

4.1 Recommendation: Housing Property Services – water risk assessments

Housing Property Services should:

1. Consider whether the rolling programme to review and refresh historic water risk assessments can be completed within two years.

2. Where this is not possible, record this as a risk in relevant divisional and directorate risk registers.
3. Ensure that the outcomes of fire safety inspections in low risk buildings together with details of any remedial action taken to address gaps identified are centrally recorded and maintained – preferably in the Northgate system if possible.

4.1 Agreed Management Action: Housing Property Services – water risk assessments

1. The Scientific Services team have reviewed the comment above against current legislation and will implement the following refreshed approach:

   Rather than a rolling programme covering all 20,000 Housing Property Services (HPS) properties equally, different types of property are classed in different priority risk categories.

   The Council has responsibility for 44 multi storey blocks and 33 Sheltered Housing complexes. These properties are all classed as high risk and assessments will be carried out within the stated two year period currently specified in the Council's water policy, and then every two years going forward.

   The remaining properties on the Housing estate are considered low level priority and legislation states that these surveys should be undertaken over a five year period. Risk assessments will be carried out on sample properties for these low risk properties. For example, in a street of 100 homes with 20 different house types, only 20 surveys would be required.
2. Providing that Housing Property Services as the risk owner allocate sufficient budget resource, Scientific Services are comfortable that this work will not put a strain on their current resources and as the approach adopted is in line with the Council's Water Safety Policy and applicable regulations, there is no need to record completion in relevant divisional and directorate risk registers.

Owner: Paul Lawrence, Executive Director of Resources **Contributors:** Gareth Barwell; Head of Place Management; Robbie Beattie, Scientific, Bereavement, and Registration Senior Manager; Jemma Tennant, Operational Manager, Scientific Services; Alison Coburn, Operations Manager, Place	**Implementation Date:** 31 December 2020 for implementation of the rolling programme.

4.1 Agreed Management Action: Housing Property Services – fire safety inspections in low risk properties

3. Housing Property Services will investigate the feasibility of implementing a technology solution to enable recording of the outcomes of fire inspections in low rise buildings where the Council has responsibility with Digital Services.

   If a solution is feasible, a change request for implementation of the new system will be prepared and submitted to CGI, the Council's technology partner.

Owner: Paul Lawrence, Executive Director of Resources **Contributors:** Michael Thain, Head of Place Development; Willie Gilhooly, Housing Property Manager; Patricia Blore, Housing Property Operations Manager; Alison Coburn, Place Operations Manager.	**Implementation Date:** 18th December 2020

5. Corporate Health and Safety	**Low**
Review of the Corporate Health and Safety (second line) policies and processes designed to provide assurance and support to first line Properties and Facilities Management (P&FM) and Housing	

Property Services (HPS) teams, and discussion with the Corporate Health and Safety team established that:

1. Gas and electrical safety procedures – there are currently no established Council- wide gas and electrical safety procedures, although these present significant fire life safety risks. Ongoing testing of electrical equipment is noted in the Council-wide fire safety guidance for responsible persons
2. The Council's fire safety policy states that 'heads of service are responsible for ensuring that a fire safety management system and fire safety arrangements are implemented', however, this does not include specific reference to the need for directorate level policies and procedures such as gas and electrical safety procedures.
3. Capacity to provide ongoing technical guidance and support – the current capacity of Corporate Health and Safety team and its operational focus on health and safety policy; governance; frameworks; and audits is impacting its ability to provide ongoing technical guidance and support to first line P&FM and HPS teams. Consequently, first line teams use consultants to provide this expertise whilst the Corporate Health and Safety team have the relevant skills and experience but not the capacity to currently provide support.
4. Access to the Safety Health and Environment (SHE) incident reporting portal – there is currently limited Council-wide access to the SHE incident reporting portal due to availability of current licences, and no clearly established licence management process, first line teams have been requested to provide Corporate Health and Safety with details of any relevant licence holder changes.

Risk

The potential risks associated with our findings are:

- Procedures are unclear or unavailable which results in variations and inconsistencies, or key actions related to electrical and gas safety not being completed.
- The council incurs additional costs through procuring external life safety specialists instead of using technical experts within the council.
- Operational teams are unaware of incidents and therefore unable to identify trends and root causes and make any necessary changes to prevent recurrence

5.1 Recommendation: Review of life safety policies and procedures

1. The Council's existing life safety policies and procedures should be reviewed to consider whether there is a requirement for specific gas and electrical safety procedures that include the requirement for ongoing first line divisional and directorate gas and electrical equipment testing
2. Review of the policies should also incorporate recommendations in relation to training and competence and assurance included at recommendations 3.1 and 3.3 above.

5.1 Agreed Management Action: Review of life safety policies and procedures

Corporate Health and Safety will consider the need for additional policies (including any requirement for recommendations in relation to competence and assurance re gas and electricity compliance) covering Gas and Electricity or whether this should continue to reside as procedures within the appropriate directorate. CHS will ensure that H&S audits cover these areas.

Owner: Stephen Moir, Executive Director of Resources **Contributors**: Nick Smith, Head of Legal and Risk; Robert Allan, Corporate Health and Safety; Layla Smith, Operations Manager, Resources; Michelle	**Implementation Date:** 30th July 2021

Vanhegan, Executive Assistant	

5.2 Recommendation: Technical guidance and support

Corporate Health and Safety should:

1. Complete a skills matrix that details the existing skills and experience of their team members.
2. Based on the outcomes of the skills matrix, consider their capacity to provide technical guidance and support across first line divisions and directorates where they have relevant skills and experience.
3. Where the team has capacity to provide technical support, this should be published on the Council's intranet (the Orb) together with relevant contact details.
4. Where technical support requirements are significant and cannot be supported by the Corporate Health and Safety team, first line management should be advised to engage external consultants.

5.2 Agreed Management Action: Technical guidance and support

1. The preparation of the skills matrix is currently underway and will be finalised.
2. The issue of capacity will be considered as recruitment increases the size of the team and, recognising that capacity will change from time to time within the team, will plan in capacity for providing technical advice to services.
3. CHS will endeavour to provide support where requested by services.
4. Where this is not possible, CHS will advise teams to engage external consultants.

Owner: Stephen Moir, Executive Director of Resources **Contributors**: Nick Smith, Head of Legal and Risk; Robert Allan, Corporate Health and Safety; Layla Smith, Operations Manager, Resources; Michelle Vanhegan, Executive Assistant	**Implementation Date:** 30th June 2021

5.3 Recommendation: Safety Health and Environment (SHE) portal user and licence management

Corporate Health and Safety should establish a process to support ongoing and licence management to the Safety Health and Environment (SHE) incident reporting portal that should include:

1. Requesting monthly details of Council leavers from Human resources and ensuring that their SHE access is revoked, and user licence released for us by other Council employees.
2. Allocating licences and access rights to new users based on requests received from first line teams through training needs assessment forms (refer recommendation 4.1) or any other means.
3. Maintenance of a list of all Council employees with SHE licences and access.
4. Confirming that the volume of current licences remains appropriate to meet demand for access to the system and requesting additional licences from the supplier when required.

5.3 Agreed Management Action: Safety Health and Environment (SHE) portal user and licence management

The processes supporting ongoing use of the Safety Health and Environment (SHE) system will be reviewed and the issues noted above addressed as part of this process.

Owner: Stephen Moir, Executive Director of Resources **Contributors**: Nick Smith, Head of Legal and Risk; Robert Allan, Corporate Health and Safety; Layla Smith, Operations Manager, Resources; Michelle Vanhegan, Executive Assistant	**Implementation Date:** 29th Oct 2021

Appendix 1: Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on the 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 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.

Appendix 2: Areas of audit focus

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

Audit Area	Control Objectives
Risk assessments	1. The Council has established and maintains registers detailing: ● all Council owned and leased properties (including properties used by the Council; Council housing stock leased to citizens; and dormant properties); ● all communal areas owned and managed by the Council; ● all electrical and gas appliances used across the Council; and ● fire safety and fire fighting equipment (for example fire alarm panels and fire extinguishers); ● details of potential sources of ignition and flammable and / or dangerous substances that could cause fire or explosion; 2. A process has been established to ensure that risk assessments are routinely performed on all Council properties (including dormant properties) that includes: ● details of the frequency of risk assessments to be performed based on consideration of the age and structure of buildings, and the nature of Council services provided from them; ● provision of training or guidance on completion of risk assessments; ● the requirement to include photographs to support risk assessments; ● the requirement to provide details of recommended actions to address the risk and / or issue; ● guidance on how to apply an overall risk assessment outcome (for example red; amber; green; or high; medium; and low); and ● an effective quality assurance process to confirm the adequacy of completed risk assessments. 3. Action is taken following any significant external life safety incidents to assess whether the associated root causes could apply across Council properties, with remediation action taken (where required) and the risks / issues incorporated into the established health and safety governance framework through completion of ongoing risk assessments and repairs.
Reporting	1. there is an established process (for example via customer contact centres or the Council's social media accounts) that enables Council employees; Council tenants; and members of the public to report life safety risks and issues to the Council; 2. where life safety risks and / or issues are identified, details are immediately provided to the relevant Council divisions.
Recording and prioritisation	1. Reported life safety risks and / or issues and the outcomes of completed risk assessments are accurately recorded on relevant systems. 2. Life safety risks and issues are reviewed and appropriately prioritised for repair or action. This process involves: ● provision of guidance and training on how to prioritise life safety risks and issues for repair;

	● application of an established prioritisation process (e.g. red, amber, green or high, medium, and low) with supporting rationale provided in relation to the significance of the life safety risk or issue; ● details of the recommended action to be completed (for example repair or close down the building) and an estimate of the associated costs and impacts; ● a quality assurance process to confirm that all life safety risks and / or issues have been considered and accurately prioritised.
Testing and repairs	1. Details of all completed repairs are recorded on relevant systems to confirm that all significant life safety risks have been resolved. 2. Completed repairs are subject to risk based quality assurance reviews to confirm that life safety risks have been effectively addressed. 3. Outcomes in relation to reported life safety risks / issues are provided to the employee; organisation; or citizen who reported the incident. 4. All Council buildings and properties have established evacuation plans that are maintained and routinely tested so that they can be effectively applied in the event that a significant life safety risk is identified. 5. Electrical appliance testing is routinely performed across all Council electrical appliances and appropriate action taken to remove and / or replace any faulty equipment identified. 6. Fire safety equipment testing is routinely performed across all Council fire safety equipment and appropriate action taken to remove and / or replace any faulty equipment identified. 7. The outcomes of annual fire and rescue inspection testing are reviewed and all recommendations prioritised and addressed.
Leased properties	1. A risk assessment is performed on all leased properties prior to commencement of or changes in lease arrangements to confirm that there are no significant life safety risks. 2. All significant life safety risks identified are addressed in advance of commencement of the lease, or the decision taken that the building cannot be leased. 3. Lease agreements clearly specify tenant responsibilities in relation to ongoing health and safety regulatory compliance for the duration of the lease.
Third party contractors	Where third party contractors have been procured and are used to support completion of life safety risk assessments; prioritisation and / or repair processes, appropriate supplier management arrangements have been established that include: ● ensuring that third party contractors are clear on their roles and responsibilities and the processes to be applied; ● ongoing risk based quality assurance reviews to confirm the adequacy of work performed; ● regular supplier management meetings to provide feedback on performance and address any emerging issues.
Governance and oversight	The Council's health and safety governance framework is appropriately designed to ensure that: ● significant and systemic life safety risks and issues across all Council properties are identified and reported to relevant health and safety governance forums, with escalation to the Council Health and Safety

	Group; Corporate Leadership Team; Health and Safety Consultative Forum; and Council Executive Committees as required; and • appropriate action is taken to address significant new and emerging life safety risks and known life safety issues, including ensuring there either sufficient budget to address the issues or taking decisions to vacate impacted properties.

The City of Edinburgh Council

Internal Audit

Social Media Accounts

Final Report

14th October 2020

CE1901

Overall report rating:

Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.

Contents

This internal audit review is conducted for the City of Edinburgh Council under the auspices of the 2019/20internal audit plan approved by the Governance, Risk and Best Value Committee in March 2019. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

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

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

1. Background and Scope

Background

Use of social media across the Council

The Council has been using Social Media since 2006 as a method of communication with citizens to deal with their requests for services and complaints. Social media is also used to broadcast Council official communications (linked to the Council website); strategic information (for example updates on major projects and requests for feedback on Edinburgh 2050 City vision); emergency alerts (such as amber weather warnings); general travel and weather updates; and (more recently) to advertise employment opportunities.

The list of social media accounts maintained by the Social Media team, last updated in January 2020 , includes 199 different social media accounts used across Council. The Council uses a range of different social media platforms such as Facebook, Twitter, Instagram, LinkedIn, Flickr, Google Plus, Pinterest.

The most prominent 'Corporate' accounts and the number of followers on those accounts, as at 7th July 2020 were:

- Twitter - The City of Edinburgh Council(@Edinburgh_CC): 122k followers
- Twitter – 'Edinburgh Travel News' (@edintravel): 54.6k followers
- Facebook - 'The City of Edinburgh Council': Liked by approx. 24k users
- LinkedIn - 'The City of Edinburgh Council': 16.5k followers
- Twitter – 'Invest Edinburgh' (@investedinburgh): 9k followers
- Twitter – 'Edinburgh Council Help' (@edinhelp): 6k followers [operated on a 24/7 basis by Customer Contact Center]

Use of the remaining 193 social media accounts is spread across Council divisions.

There is currently no established social media performance reporting provided to governance forums or Council Executive committees that details use of the full population of social media accounts, however, the latest quarterly customer contact centre performance report provided to the Policy and Sustainability Committee in February 2020 noted that 37,054 tweets were received by the Contact Centre between October and December 2019, reflecting an increase of 35% during the same period in 2018.

Regulatory Requirements

The General Data Protection Regulation (GDPR), together with the UK Data Protection Act 2018, updated data protection legislation on 25 May 2018. Each of the social media platforms used by organisations should have established privacy notices with associated terms and conditions in relation to consent and data use. The Council needs to ensure that interactions with citizens and personal data is managed effectively on social media in accordance with data protection legislation.

It is also essential to ensure that social media providers and management tools can confirm compliance with the data legislation requirements related to international transfer of data e.g. the EU-U.S. Privacy Shield Framework designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States.

Governance

The Council's use of social media is governed by the Council's Social Media Acceptable Use Policy that outlines the expected standards for employees accessing social media platforms. The Policy

covers employee conduct; use of social media during pre-election periods; use in relation to complaint handling; and endorsement and removal of information on social media platforms.

Social Media Account Management

Social media account requests from Council divisions are submitted (via an account request form) to the Social Media team within Strategy and Communications for review and approval. Line management authorisation is then required by CGI (the Council's technology partner) to confirm that employees detailed in the account request form require social media access as part of their role, and that the established technology controls applied to the Council devices that restrict access to social media accounts should be removed for these employees.

The Council uses the 'Sprout Social' social media management system to manage its corporate social media accounts, providing individual users with unique user accounts. The platform also supports unique user access levels that enables employees to post updates and tweet or respond to messages.

Social media management systems are typically used to consolidate access to all social media accounts to one single login; ensure that important notifications are not missed; keep track of all conversations as all conversation data is located in one place; schedule social media posts in advance; monitor key words to identify key themes or trends using a dedicated search functionality; analyse data (for example number of retweets or website hits); demonstrate return on investment from effective use of social media; and ensure consistent messaging in social media posts.

'Facebook for Business' is also used to manage the Council's Facebook accounts and this platform also provides additional security measures for business users. Both, Sprout Social and Facebook for Business platforms are managed by the Social Media team.

The Social Media team engages with services areas on an ongoing basis to ensure that that published social media content is genuine; official; professional; helpful and non-offensive. They also perform annual reviews of the Council's social media accounts to ensure they continue to be actively and appropriately used.

Training and guidance

All new Council employees are required to complete mandatory ICT Acceptable Use training, which includes details of the Council's ICT Acceptable Use Policy and guidelines for appropriate use of technology and social media.

Social Media e-learning modules are also available for completion by employees on the Council's essential learning platform, CECiL.

The Social Media team also delivers dedicated training sessions to Council social media users that includes specific guidance on the strategic and operational aspects of using social media as a communication tool.

Scope

The objective of this review was to assess the adequacy of design and operating effectiveness of the key controls established to ensure the Council's social media accounts are securely operated and can only be accessed by authorised individuals.

Our areas of audit focus as detailed in our terms of reference are included at Appendix 2.

Testing was performed across the period 1st April 2018 to 15th June 2020.

Limitations of Scope

This review was limited to Council's official social media platforms and excludes personal use by elected members and employees.

Reporting Date

Our audit work concluded on 15th June 2020, and our findings and opinion are based on the conclusion of our work as at that date.

2. Executive summary

Total number of findings: 3

Summary of findings raised	
High	1. Social media (second line) operational framework
Medium	2. Social media security and privacy issues
Medium	3. Social media training

Opinion

Significant Improvement Required

Our review identified significant weaknesses in the design and effectiveness of the control environment and governance and risk management frameworks required to support the ongoing management and operation of social media accounts across the Council. Consequently, only limited assurance can be provided that social media risks are being managed, and that the Council's objectives in relation to the secure management and operation of social media accounts should be achieved.

Our review confirmed that whilst the Council's engagement and communication approach and objectives have been clearly defined and communicated to support the content, narrative and tone of the Council's social media content, there is currently no clearly defined Council-wide social media operational framework and supporting guidance available to ensure that the Council's circa 199 known social media accounts are securely, effectively, and consistently managed in line with applicable legislation and regulations by all first line divisional and directorate social media account owners and users.

We also established that that the full population of social media accounts is not currently managed through the Council's existing social media management system, and identified a number of current security management and privacy operational issues that should be addressed.

The most notable operational issues relate to lack of an established social media account deletion process that focuses on ensuring deactivation of leaver accounts on relevant social media platforms in addition to removal of Council network access rights; and limited capacity to perform regular social media 'sweeps' to identify and remove any unauthorised accounts that have been opened in the Council's name. Additionally, these risks have not been identified; assessed and recorded in relevant divisional and directorate risk registers.

We also identified the need to review and refresh existing social media training arrangements and the content of the social media e learning module; and highlighted the importance of assessing training needs for all social media account owners and operators across the Council, and ensuring that social media training is included in the essential learning requirements for their roles.

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

Further information is included at Section 3.

Areas of good practice

The following areas of good practice were identified during our review:

- A social media management system is used to operate the Council's 10 corporate social media accounts, and administrator rights to this system are restricted to users in the Social Media team.
- Bespoke Social media training sessions have been developed by the Social Media team and are delivered to divisions and directorates upon request.
- Data related to ongoing citizen engagement on Council's three key corporate social media accounts is recorded and monitored monthly.
- The Council's intranet (the Orb) includes strategic and operational social media tips that should be considered prior to creating new social media accounts.

Management response

Social media is a channel that is used alongside many others (print, outdoor, broadcast, online, etc), and its use is dictated by our overarching communications approach and the expertise of communications team in their roles.

'Goals' are set at a communications approach level, and within individual project communication plans. Currently, as part of the new social media account opening process, account owners must outline goals at an account level in the new account business case, ensuring they are meeting their own communication needs, and matching those to the objectives of their department and the Council as a whole. Additionally, as part of the new account opening process, Communications provides guidance to new account owners on their approach and platform choice to meet their unique communications objectives.

In 2015, the Communications Team began a more deliberate and structured approach to social media, with a particular focus on how the Council engages with and helps residents through social media, to build the size of our online audiences and, latterly, to optimise the quality and effectiveness of our social media content.

Since introducing this new approach, the Council has:

- Developed and launched @edinhelp, a 24/7 'help account', that is a model for many council and public sector organisations in the UK, and is now handling in excess of 10,000 messages a month, with an average reply time of 38 minutes.
- Through a renewed focus on strategically improving the quality of our content, and optimising our use across platforms, the Council has grown the Council Twitter account, our primary social channel, from 54,000 followers in 2016 to 122,125 in 2020 (+126%), and our impressions (times our posts are seen) in a year from 3.6 million to 25.6 million (+596%).
- Helped develop a range of smaller social media accounts providing for smaller audiences across a diverse range of areas within the Council.

This approach has evolved, and continues to evolve, to meet the changing needs of our residents and businesses, and the evolution of the social media platforms themselves. As a result, the Council now has social media channels that can help manage crises, offer efficient and convenient customer service, communicate messages quickly and at scale, and has channels that can form a central element of city-wide communication campaigns.

More recently, in late 2018, on assuming responsibility for Communications, the Head of Strategy and Communications highlighted areas for development that included improving the planning, quality and tone of (corporate) social media content.

Following his recommendations, an action plan was agreed and progressed across these activities, with the following specifically relating to social media:

- Develop social media activity/ content to be more in tune with strategic narrative and conveners' priorities
- Improve quality and visibility of content plans
- Expand 'ambition' across all channels with emphasis on richer, more engaging and accessible content
- Make best use of available design resources to produce high-quality, more consistent content
- Introduce tools (e.g. Typito) and skills to allow quicker turnaround

These areas of work (and progress against them) formed the basis of the presentations taken to the Council's Wider Leadership Team (in November 2019) to ensure that the key messages were shared across all Council teams. This had the dual purpose of highlighting progress while also helping to manage Communications risks highlighted in the Strategy and Communications risk register.

We agree there's a mixed landscape across the council in the quality of social media use and that this is primarily due to being unable to deliver training at suitable scale, as well as having appropriate council-wide policies in place that are integrated with established Human Resources and Digital Services policies and procedures, and that implementation of a social media framework to be applied across the Council should help to improve the controls supporting use of social media accounts and the consistency and quality of social media content.

3. Detailed findings

1. Social media operational framework	High

Review of the strategy, policies and procedures supporting ongoing use social media across the Council established that:

1. **Social media operational framework –** there is currently no defined Council-wide social media second line (Strategy and Communications) operational framework that details the security and records management / data protection requirements to be applied by first line divisional and directorate owners and users of social media accounts across the Council.
2. **Social media guidance -**. Review of existing social media tips on Orb; the social media e-learning module; and the ICT acceptable use policy established that their content is high level and generic, with no comprehensive operational guidance available for employees to ensure that the Council's social media accounts are managed and operated effectively and securely.
3. **Communications emergency plan –** the current Council communications emergency plan was last updated in 2014 and does not include any reference to use of social media in the event of an emergency.
4. **Performance reporting –** whilst performance reporting has been established for the Council's main Twitter and Facebook corporate social media accounts, there is currently no consolidated Council wide social media performance reporting prepared and provided to management that details the extent of use of social media accounts by citizens to engage with the Council; the ongoing effectiveness of engagement via social media; and the themes identified from social media content.

   Strategy and Communications management has confirmed that they are currently considering extending the existing social media performance dashboard to include performance reporting on all ten corporate social media accounts currently in use.

   It is acknowledged that social media usage is also included in Customer performance reports

presented to the Finance and Resources Committee, and that performance reporting is also provided in relation to specific campaigns.

5. **Social media risks –** the security and operational risks associated with ongoing use of social media accounts have not been recorded in divisional and directorate risk registers (where appropriate).

   It is acknowledged that a risk in relation to the inability to defend the Council against emerging threats such as social media attacks is included in the Cyber Information Security Steering Group (CISSG) risk register, and that the reputational risks associated with ongoing social media use are recorded in the Strategy and Communications risk register, however, these do not reflect all relevant social media security and privacy risks that could potentially impact the Council.

Risks

The potential risks associated with our findings are:

- lack of operationally aligned security controls and content management across the total population of social media accounts used by the Council
- limited assurance that social media accounts are being used securely; consistently; and in line with applicable regulatory requirements and Council policies.
- lack of clarity as to how social media should be used to share important messages with citizens in the event of an emergency.
- management has limited awareness of the effectiveness of social media as a communication and engagement channel, and the key themes emerging from engagement through these channels.
- risks associated with the ongoing use of social media are not identified; assessed; and recorded, with appropriate controls implemented to ensure that they are affectively managed.

1.1 Recommendation: Social media operational framework

1. A social media operational framework should be designed and implemented to ensure that all social media accounts are securely and consistently managed across first line divisions and directorates. The framework should include, but should not be limited to:
   - the need for the full population of social media accounts to be managed through the Sprout Social' social media management system currently used by the Council, or an appropriate alternative system;
   - the need to have an established account owner for all social media accounts, together with details of their responsibilities for ongoing (first line) management and oversight of the accounts;
   - the review and approval processes to be applied when social media accounts are either opened or closed, including the requirement to ensure that leavers access is removed from social media platforms in addition to Council networks;
   - the requirement for use of unique user IDs and passwords for all employees accessing the social media account management system and individual social media accounts, and confirmation that user IDs and passwords should not be shared;
   - privacy requirements including the requirement to ensure that all accounts include links to the Council's current privacy notice, and the importance of encouraging citizens to use private messaging functionality where they are sharing personal sensitive information with the Council;
   - the requirement to ensure that all social media accounts are validated with the platform provider as soon as possible;
   - training requirements for social media account owners and users; and

- responsibility for completion of ongoing sweeps (including their frequency) of social media platforms to identify any unauthorised accounts opened in the Council's name, and the need to ensure that they are closed.

2. Second line ownership of the framework should be defined and agreed, together with responsibilities for confirming that framework requirements are consistently applied on an ongoing basis.
3. The second line social media operational framework (including first and second line ownership and ongoing oversight responsibilities) should be reviewed and approved by the Corporate Leadership Team (CLT).
4. Once approved, the framework should be communicated across all Council divisions and directorates confirming that it has been approved by the CLT and should be consistently applied. The framework should also be published on the Council's intranet (the Orb).

1.1 Agreed Management Action: Social media operational framework

1. A social media operational framework will be developed to be used and followed be service areas across the Council. The content of the framework will cover all of the points noted at 1 above with the following exceptions:
   - whilst an enterprise social media tool would be the optimal solution to manage and report on ongoing use of social media across the council, implementation of Sprout Social for every social media account across the council would be prohibitive from a cost perspective. Instead, an appropriate risk based threshold will be applied to determine the Council's most significant social media accounts (for example, number of followers and / or usage volumes), and account owners will be requested to manage these accounts through the Sprout Social platform.
   - it is not always possible to obtain validation from platform providers; however social media account owners will be encouraged to achieve this where possible.
2. Second line ownership of the framework together with any cross Council support requirements (for example support required from Digital Services and / or Human Resources) will be defined and agreed, and first line divisions and directorates will be requested to confirm their ongoing compliance with framework requirements within their annual governance statement responses.
3. Once designed, the framework will be reviewed and approved by the Corporate Leadership Team (CLT) to ensure that all directorates are aware of and agree with the framework content.
4. Once approved by the CLT, the framework will be communicated across all Council divisions and directorates and published on the Orb.

Owner: Laurence Rockey, Head of Strategy and Communications **Contributors:** Michael Pinkerton, Senior Communications Manager; David Ure, Communications Officer; Donna Rodger, Executive Assistant	**Implementation Date:** 31st May 2021

1.2 Recommendation: Social media guidance

1. Where required, detailed guidance should be prepared to support the social media operational framework (refer finding 1.1). As a minimum, the following guidance should be prepared to address the following areas:

   1.1. opening and closing new social media accounts This guidance should include
   - allocation of unique user profiles and passwords;
   - the requirement to remove leavers access to the account on the social media platform;
   - the requirement to ensure that new accounts include a link to the Council's current privacy notice;

- the need to engage with the Council's Information Governance Unit to determine whether a data privacy impact assessment should be performed to support use of new social media accounts;
- the requirement to ensure that the Communications team is advised of all new social media accounts opened and closed; and
- the requirement to verify accounts as soon as possible.

1.2. completion of ongoing social media sweeps, and the process to be applied to ensure that any unauthorised accounts identified are disabled.

1.3. completion of ongoing reviews by account owners to confirm the appropriateness of content of social media feeds and identify any significant themes or trends that potentially highlight areas where further action is required by Council divisions and directorates.

1.4. privacy steps to be covered as part of social media engagement with citizens to ensure that the risk of sharing private sensitive information publicly is effectively mitigated. This should include the requirement to include links in posts that will direct citizens to the platforms private messaging functionality.

2. The guidance should also include details of management oversight required to confirm that the guidance is being consistently applied.
3. The guidance should be shared across divisions and directorates with a request that any existing local procedures should no longer be applied. The guidance should also be published on the Orb and linked to the social media operational framework (refer finding 1).

1.2 Agreed Management Action: Social media guidance

1. The operational framework will include a section on social media guidance and will seek to cover all the issues set out above. Further detailed guidance will be produced and circulated if required
2. The guidance will include details of the recommended management oversight to confirm that the guidance is being consistently applied.
3. The operational framework and guidance will be shared across divisions and directorates with a request that any existing local procedures should no longer be applied. The guidance will also be published on the Orb and linked to the social media operational framework.

Owner: Laurence Rockey, Head of Strategy and Communications **Contributors:** Michael Pinkerton, Senior Communications Manager; David Ure, Communications Officer; Donna Rodger, Executive Assistant	**Implementation Date:** 31st May 2021

1.3 Recommendation: Communications emergency plan

The communications emergency plan should be updated to include details of how the Council will use social media in the event of an emergency to share key messages with citizens.

1.3 Agreed Management Action: Communications emergency plan

The communications emergency plan has been updated to include details of how the Council will use social media in the event of an emergency to share key messages with citizens, and submitted to the Corporate Resilience Team for inclusion in the revised Corporate Emergency Plan.

Owner: Laurence Rockey, Head of Strategy and Communications **Contributors:** Michael Pinkerton, Senior Communications Manager; David Ure, Communications Officer; Donna Rodger, Executive Assistant	**Implementation Date:** Completed.

1.4 Recommendation: Social media performance reporting

1. Following the transfer of relevant social media accounts on to the 'Sprout Social' (Sprout) social media or alternative social media management system, a social media performance dashboard should be designed and implemented, and reported to management, the Corporate Leadership Team (CLT) and any relevant Council executive committees on an ongoing basis (for example quarterly).
2. The dashboard should be produced using available Sprout Social functionality (where possible) and should include, but not be limited to:
   - the total number of social media accounts used by the Council and their purpose;
   - usage information in terms of subscriptions; hits; or volume of messages; and details of repeat users;
   - the nature and themes associated with queries received through social media, and an assessment of the quality of engagement between the Council and citizens via social media channels, including details of any offensive or negative messages received;
   - the ongoing costs and benefits associated with use of social media channels;
   - details of the outcomes of sweeps performed and any unauthorised accounts identified and addressed.

1.4 Agreed Management Action: Social media performance reporting

Our aim to develop a communications dashboard that presents our ten current key social media accounts performance to senior management, twice yearly, would help with raising visibility on the most impactful elements of social media performance, whilst being deliverable. The report will focus on attributing social media performance to campaign and wider communication goals, together with ongoing reporting provided on the outcomes of individual campaigns.

The dashboard will also be updated to reflect any significant accounts that are added to the Sprout Social social media tool.

Owner: Mike Pinkerton **Contributors:** David Ure	**Implementation Date:** 29th August 2021

1.5 Recommendation: Social media risks

The risks associated with the ongoing use of social media should be identified, assessed and recorded in relevant divisional and directorate risk registers.

1.5 Agreed Management Action: Social media risks

The risks associated with the ongoing use of social media that are highlighted in this report will be assessed and recorded in the Strategy and Communications risk register together with details of mitigating actions to ensure that they are addressed.

Owner: Laurence Rockey, Head of Strategy and Communications **Contributors:** Michael Pinkerton, Senior Communications Manager; David Ure, Communications Officer; Donna Rodger, Executive Assistant	**Implementation Date:** 30th October 2020
2. Social media operational security and privacy issues	**Medium**

Review of the security and privacy arrangements established to support ongoing management and use of the Council's social media accounts identified the following social media operational issues that require to be addressed as they are currently exposing the Council to risk:

Security

1. **Shared user profiles and passwords** – the Customer and Communications teams have shared Sprout user access profiles and passwords. These generic user IDs and passwords are also recorded in a spreadsheet maintained by the Communications team.

   Management has advised that licencing requirements ensure that the Customer accounts managed through Sprout cannot be accessed simultaneously, however, use of generic user IDs and passwords means that individual users cannot be matched to account activities.

2. **Enforced password changes** – There are no established controls to ensure that social media account passwords are not shared amongst employees; are sufficiently complex; and changed frequently.

   Additionally, the Sprout system and social media platforms do not enforce regular password changes for users. The Social Media team has proactively implemented a manual workaround where manual password change reminders are scheduled into team members calendars, however this process does not extend to other Sprout users out with the Social Media team, and social media accounts managed that are not currently managed through the Sprout application.

   We also noted that this Social Media team's reminder process had lapsed during the period covered by our review, although management has confirmed that the process has now been reinstated.

3. **Account creation and deletion** - there are no established procedures and controls that prevent employees from creating new or deleting existing Council social media accounts where these are not managed through the Sprout system. Whilst the Social Media team maintains a list of all social media accounts that they are advised of, this was last updated in 2018.

   Review of a sample of 20 schools and libraries social media accounts identified by Internal Audit that are registered in the Council's name established 11 that were not included in the central list maintained by the Social Media team.

   Additionally, review of a sample of 20 accounts included in the central log highlighted that:

   - 7 included an inaccurate link to the relevant social media account;
   - 7 accounts had no details provided in terms of the key contact / account owner.

4. **Removal of leavers** - there are no established Council wide procedures to ensure that leavers access to Council social media accounts is removed.

5. **Unauthorised account identification** – the Social Media team performs an annual social media 'sweep' of existing accounts to assess the levels of account activity and engagement with citizens by monitoring the annual increase in followers. This exercise also enables the Social Media team to identify any unauthorised accounts created in the Council's name, and accounts created/closed by the Council's divisions/directorates without consulting with the Social media team.

   The last annual sweep exercise was performed in February 2020, and prior to that in 2017. Management has confirmed that completion is dependent on the availability of trainee/intern staff, and may not be complete if this additional resource is not available. Additionally, no reports are prepared detailing the conclusions of these exercises and any remedial action implemented.

6. **Account verification** - five of the six social media platforms used by the Council offer free verification programmes that provide assurance to users that these are genuine accounts, with the

only exception being LinkedIn. It is acknowledged that YouTube requires 100K subscribers before the accounts can be validated, and that the Council has not yet achieved this subscription level.

Of the remaining four platforms, the Council's Facebook and Twitter accounts had been verified, whilst the Instagram and Pinterest accounts had not.

Privacy

7. **Privacy notices** – review of a sample of 24 social media accounts used by the Council confirmed that 19 included a link to either the Council's main website or an associated school's website that include the Council's current privacy notice. However, 1 account did not include a link to either a privacy notice or Council website, and a further 4 included either broken links or links to a historic Council website.
8. **Security of citizen information** - review of all tweets from the @edinhelp twitter account for the period 13 to 20 August 2019 established that 34 of these tweets included a request for additional information that could have been personal / sensitive in nature. Review of the subsequent conversations confirmed that:
    - whilst citizens were not explicitly requested to share private information publicly, 4 tweets for the Council did not explicitly direct the customer to provide information via a private message. Our review of the social media training delivered to the Customer team confirmed that it highlights the need to ensure that citizens are requested to personal sensitive data via direct messaging.
    - 2 customers advised that they were unsure how to use direct message functionality, and contact centre teams were unable to respond via twitter. We confirmed that whilst some Contact centre team members embed the link to direct messaging in their response, this process was not applied consistently by all the contact centre team members.
9. **Publication of internal vlog** - the Chief Executive's weekly vlog for 1st June that is designed specifically for Council employees was made available to the general public. Management has confirmed that this was due to a technical anomaly, but had no significant concerns as the weekly vlog is designed to ensure that it does not include any sensitive or confidential content.

Risk

The Council is currently exposed to the following risks associated with our findings:

- Inappropriate social media content posted by the Council cannot be traced to employees where accounts are shared using generic user IDs and passwords.
- Where social media accounts are not updated to remove former employees, they can continue to post content using the Council's registered accounts directly via the relevant external social media platforms.
- Unauthorised social media accounts created in the Council's name or linked to the Council are not identified, reported to the social media platform and disabled (where there has been a breach of provider terms of service) in a timely manner.
- External social media users are unable to confirm whether social media accounts are genuinely owned by or linked to the Council where these have not been verified.
- External social media users do not understand the Council's processes for ensuring privacy where accounts are not linked to the Council's current privacy notice.
- Citizens may share private sensitive information publicly via social media platforms if they are not consistently advised to use private messaging as part of the social media engagement process.

2.1 Recommendation: Social media operational security and privacy issues

1. Unique user IDs and passwords should be provided to all Sprout users.
2. All Sprout users should be requested to change their passwords on an ongoing basis (for example quarterly) via an e mail request from Strategy and Communications.
3. The Social Media team's list of all social media accounts used across the Council should be updated to reflect the current population and maintained on an ongoing basis with the addition of new accounts and removal of deleted accounts as advised by directorates and divisions.
4. Divisions and directorates should be contacted and requested to perform a review of employees who have access to the Council's social media accounts and ensure that access rights for employees who have left the organisation are removed.
5. An annual sweep should be performed to identify any unauthorised accounts created in the Council's name, and accounts created/closed by the Council's divisions/directorates without consulting with the Social media tea, with details of action taken to address any unauthorised accounts recorded.
6. The Council's most significant social media accounts should be verified with platform providers where possible.
7. Council divisions and directorates should be contacted and requested to confirm to the Social Media team whether Data Privacy Impact Assessments (DPIAs) have been completed to support use of the social media accounts. Where these have not been completed, account owners should be requested to engage with the Information Governance Unit to ensure that DPIAs are completed and reviewed. Links to the Council's current privacy notice should also be provided to divisions and directorates with a request that they ensure this is linked to their relevant social media accounts.
8. The requirement to ensure that private citizen information is provided securely through social media private messages should be reinforced across all Council divisions and directorates.
9. Internal vlogs created via social media will not be made available to the general public, with checks implemented prior to publication to ensure that they are only made available to Council employees.

2.1 Agreed Management Action: Social media guidance on operational security and privacy issues

To prevent potential recurrence, these points will also be included in the operational framework and supporting guidance to be developed (refer finding 1).

Owner: Laurence Rockey, Head of Strategy and Communications **Contributors:** Michael Pinkerton, Senior Communications Manager; David Ure, Communications Officer; Donna Rodger, Executive Assistant	**Implementation Date:** 28th May 2021

2.2 Agreed Management Action: Social media operational security and privacy issues

The outcomes detailed in this finding will be shared with all social media account users across the Council with a request that they action points 4; 6; 7; and 8 above immediately (where possible) and advising that these areas will be a future ongoing requirement of the social media operational framework that is currently being designed.

Owner: Laurence Rockey, Head of Strategy and Communications	**Implementation Date:** 30th October 2020

Contributors: Michael Pinkerton, Senior Communications Manager; David Ure, Communications Officer; Donna Rodger, Executive Assistant	

2.3 Agreed Management Action: Social media operational security and privacy issues

The Communications team will address points 1; 2; 3; 5; and 9 in advance of finalising the social media operational framework.

It is important to note that the recommendation to provide unique user profiles and passwords for all Sprout social users could potentially be cost prohibitive, however the feasibility of this option will be assessed, and the risks associated with sharing user profiles and passwords reduced as far as possible.

Owner: Laurence Rockey, Head of Strategy and Communications **Contributors:** Michael Pinkerton, Senior Communications Manager; David Ure, Communications Officer; Donna Rodger, Executive Assistant	**Implementation Date:** 29th January 2021

3. Social media training	**Medium**

Review of established social media training arrangements established that:

1. **availability of training** – bespoke social media training is provided by the Communications team to social media users across the Council, however this is not included in the programme of available courses that can be booked through the Council's Learning and Teaching Orb page or the Council's electronic learning system (CECil), and is only available on request from the Communications team.
2. **e learning module** – ownership and responsibility for ongoing review and refresh of the Council's social media e learning module has not been clearly defined. Management has advised that the Communications team was involved in the initial development of the module, but that it has not been recently reviewed or refreshed.
3. **e learning module** – the social media e learning module is optional and has not been classified as essential learning for all social media account owners and users. It is acknowledged that the Council's Learning and Development team are in the process of collating essential learning requirements for employees across the Council.
4. **e learning module** –review of the module content confirmed that the module:
    - does not provide adequate explanations in relation to data protection and information compliance requirements prior to testing knowledge
    - doesn't provide correct answers where the user has responded incorrectly
    - includes historic links to the Data Protection Act and Council's social media intranet pages on the Orb that no longer work.
5. **e learning completion –** there is currently no central review performed to confirm that all social media account owners and users have completed the e learning module.

Risk

The potential risks associated with our findings are:

- social media account owners and users do not fully understand the risks (including data protection and privacy requirements) associated with the ongoing operation of social media accounts, and

the controls and mitigating actions required to ensure that these risks are effectively managed and mitigated

3.1 Recommendation: Social media training needs assessment

1. A training needs assessment should be completed to determine training needs for social media account managers and operators.
2. Social media training should be classified as an essential learning requirement for all social media account owners and users.

3.1 Agreed Management Action: Social media training needs assessment

1. A training needs assessment for social media account owners and users will be developed as part of the social media operational framework and supporting guidance with support (where required) from Human Resources. The training needs assessment will be provided to all Council directorates and divisions with a request that it is completed for all new social media account owners and users.
2. Directorates and divisions will be requested to ensure that social media training is classified as an essential learning activity within their essential learning programmes for those roles that include a social media remit / responsibilities.

Owner: Laurence Rockey, Head of Strategy and Communications **Contributors:** Michael Pinkerton, Senior Communications Manager; David Ure, Communications Officer; Donna Rodger, Executive Assistant	**Implementation Date:** 16 April 2021

3.2 Recommendation: Refresh of social media training materials

1. Existing training materials (including the social media e learning module) should be reviewed and refreshed to ensure that their content is aligned with applicable legislation and regulations and identified training needs.
2. The e learning module content should be refreshed to ensure that sufficient information is provided prior to testing user understanding; and that the correct answers are provided to incorrect responses.
3. Ownership of the content of the social media e learning module should be agreed between Human Resources and Strategy and Communications.

3.2 Agreed Management Action: Refresh of social media training materials

1. Existing training materials and the e learning module content will be reviewed and refreshed with support from Human Resources (where required) to ensure that it is aligned with applicable legislation and regulations.
2. The e learning module will be updated to ensure that sufficient information is provided prior to testing and that correct answers are provided to incorrect responses.
3. Ownership of the content of the social media e learning model will be agreed between Strategy and Communications and Human Resources.

Owner: Laurence Rockey, Head of Strategy and Communications **Contributors:** Michael Pinkerton, Senior Communications Manager; David Ure, Communications Officer; Donna Rodger, Executive Assistant	**Implementation Date:** 25 June 2021

3.2 Recommendation: Ongoing delivery of social media training	
Ongoing delivery of face to face by social media training by Strategy and Communications should be advertised through the Council's e learning (CECil) programme, with courses made available at an appropriate frequency (for example quarterly) enabling first line social media account managers and operators to ensure that the fulfil the essential learning requirements associated with their roles.	
3.2 Agreed Management Action: Ongoing delivery of social media training	
Strategy and Communications will engage with Human Resources to ask that face to face social media training is advertised through the Council's e learning (CECil) programme with courses made available at an appropriate frequency, and confirm whether there is scope for courses within the available budget.	
Owner: Laurence Rockey, Head of Strategy and Communications **Contributors:** Michael Pinkerton, Senior Communications Manager; David Ure, Communications Officer; Donna Rodger, Executive Assistant	**Implementation Date:** 29th January 2021

Appendix 1: Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on the 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 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.

Appendix 2: Areas of audit focus

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

Audit Area	Control Objectives
Strategy, Policy and Guidance	The Council has established the following documents to support ongoing use of social media accounts: • a Social Media Strategy that clearly states the objectives of using social media; its target audience; agreed social media channels; and key service area users • social media policies and supporting guidance that clearly define the roles and responsibilities of the Media team and employees using Council social media accounts; • social media policies and guidance are clear on what is required to ensure ongoing compliance to GDPR and Data Protection Act requirements in relation to the legal grounds for processing and storing data; • privacy notices, easily accessible to customers detailing how their personal data (exchanged during communication on social media) will be used, retained, shared, including the purpose to process personal data and its legal basis. The privacy notice also highlights the relevant risks associated with data protection arrangements of the social media platform. • policies and procedures stating requirement, frequency and responsibilities for using social media accounts to issue emergency communications and warnings in the event of any significant incident.
Security	The following security controls have been established to support ongoing use of social media accounts: • administrator access rights to Sprout Social and Facebook for Business are appropriately restricted and managed within the Social Media team; • Sprout Social and Facebook for business access is supported with strong technology controls such as unique user logon IDs and passwords that require to be changed at an appropriate frequency, and user logon details and passwords are not shared; • only authorised users / administrators can create new, and amend or delete existing Council social media accounts, and allocate new and remove existing users; • changes to social media accounts are only made when authorisation and supporting rationale is provided by service area management and Digital Services; and • user access to individual social media accounts is supported with strong technology controls such as unique user logon IDs and passwords that require to be changed at an appropriate frequency,

	and user logon details and passwords are not shared; regular user access reviews are conducted to ensure that user access rights remain aligned their roles and responsibilities; and • Confirmation has been obtained that all social media sites and management tools used by the Council are compliant with the requirements of the EU-U.S. Privacy Shield Framework
Ongoing management and monitoring	The following controls have been established to support ongoing management and monitoring of social media accounts: • details of the full population of the Council's social media accounts are maintained, with each account assigned a nominated service owner who is responsible for its secure operation and quality of published content; • clear guidelines have been established that details when management and Media team approval is required prior to publication of proposed social media content, and these are consistently applied; • social media account audit trails are available and regularly reviewed to identify any potentially unusual user activity, with appropriate action taken where this is noted; • processes to close and reinstate social media accounts in the event of password theft or account hacking, have been documented and communicated to all users; • ongoing monitoring of Council social media accounts to identify any potentially significant incidents across the City reported by citizens, and urgent citizen requests for assistance; and • regular reviews are performed to identify any 'fake' accounts created in the Council's name and these are reported to the relevant platform provider with a request for their removal. • a clear action plan has been developed based on the results of social media reviews undertaken by social media team and actions are regularly monitored. • where consent is required to publish any personal data on social media, the service areas have taken relevant consent from the customer(s), in accordance with the data protection legislation.
Training/ Support, Performance Reporting & Risk Management	• Regular training, support and guidance is provided to new and existing users to ensure that their social media activities are secure and aligned with Council security and information management procedures, and GDPR / Data Protection Act requirements; • Social media performance indicators have been established and performance is monitored by management and reported to relevant Council executive committees; and • All the risks relating to Council's social media operations (for example, legal; operational; reputational; information security; and technology) have been adequately considered, recorded in the Media team risk registers and there are controls in place to manage these risks.