The City of Edinburgh Council

Internal Audit

CW1702 - Resilience

7 September 2018

Contents

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

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

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

1. Background and Scope

Background

In September 2017, the Council published its strategic business plan ("Programme for the Capital") to build upon Edinburgh's successes, and demonstrate a commitment to improve services and amenities across the City.

The business plan includes five strategic aims, and one notable aim is to have 'a resilient city, where citizens are protected and supported with access to sustainable and well-maintained facilities'.

Delivery of certain services are necessary to meet statutory requirements or are critical for citizens. Ensuring that both statutory and critical services can be effectively recovered in the event of a disaster, is a key priority for the Council. Additionally, there is a legislative requirement for the Council to establish Business Continuity Management (BCM) arrangements under the Civil Contingencies Act (CCA) 2004.

Consequently, it is vital that the Council has identified and prioritised recovery of critical services by completion of business impact assessments (BIAs), and can demonstrate that adequate and effective resilience plans have been established for these services; are regularly tested; with lessons learned incorporated into ongoing resilience activities.

It is also essential to ensure that third party suppliers involved in delivery of critical services (including third party technology system suppliers) can demonstrate their ability to recover. Consequently, BIAs and resilience plans should include details of supplier recovery arrangements, with (at least) annual assurance provided by third parties that they remain effective.

Third party assurance can be obtained through provision of International Standard for Assurance Engagements (ISAE) 30402 service organisation control (SOC) reports from suppliers. This standard is designed to provide customers with assurance that suppliers operate adequate and effective service delivery or technology provision 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 covers a range of controls (including resilience); and the final report is provided free of charge to the organisation's customers. Further information is available at ISAE3402:

Effective citizen and employee communications are also critical elements of Resilience arrangements, and it is essential that customer communication plans and employee emergency call trees are maintained and tested.

The Council's Resilience Management System document (RMSD) outlines the current resilience risk management framework, including responsibility and accountability for management of resilience risks and activities, and the established resilience governance framework.

The Three Lines of Defence model can be applied to management of resilience risks and activities, and is aligned with the roles and responsibilities specified in the Council's RMSD. The 'first line' comprises service areas that own and manage service delivery resilience risks; the 'second line' includes specialist centralised teams (i.e. the Resilience team within Strategy and Insight) who establish and oversee compliance with relevant policies and frameworks and challenge the effectiveness of resilience risk management by service areas; with the third line (for example, Internal Audit) providing independent assurance on the operation of key resilience controls.

In the past 18months the council has faced a number of significant incidents that has required an emergency response from the Resilience team. The elevation of the UK terrorist Threat Level to 'Move to Critical' on two occasions; the Council's detailed response to Grenfell Tower fire; and a serious Severe Weather Incident in February / March 2018).

Additionally, the Council was a lead agent in a UK wide counter-terrorism exercise in 2017, which required extensive multi-agency planning.

The Council's Resilience team has also achieved and maintained ISO22301 International Standard for Business Continuity accreditation.

Scope

Our review was performed as at February 2018 and assessed the adequacy of the design and operating effectiveness of the key resilience controls established to ensure that the Council can continue to provide an appropriate level of service in the event of a major incident that renders Council buildings; employees and / or systems non-operational.

Our review focused on the adequacy and effectiveness of controls in the following areas:

- The Council's Resilience Management System (RMS);
- Emergency response plans;
- Oversight and governance of the RMS and emergency response plans; and
- Completion of resilience plans and BIAs for critical service areas.

Our full terms of reference are included at Appendix 2.

2. Executive summary

Total number of findings

Critical	-
High	2
Medium	2
Low	1
Advisory	-
Total	**5**

Summary of findings

Management has advised that none of the recent resilience incidents have resulted in any unavoidable loss of service, however, our review identified some significant control weaknesses that could adversely impact the Council's ability to recover in the event of a future major incident, as the full population statutory and critical services provided by the Council have not been identified, and are not supported by adequate and effective resilience plans (including resilience arrangements of third party service and technology providers) that are regularly reviewed and tested.

The Health and Social Care Partnership (H&SCP) is responsible for delivery of a number of statutory and critical services, and ensuring that effective resilience arrangements have been established across the entirety of these services, and by the Council; NHS Lothian; and partner providers. Currently, partnership services provided by the Council are not included within the Council's Resilience framework. Resilience management has advised that they provide advice and support on an ongoing basis as agreed with Partnership senior management.

Management has advised that (following completion of our review) the H&SCP has developed a resilience plan in consultation with both the Council and NHS Lothian that was approved by the Edinburgh Integration Joint Board (EIJB) in May 2018, and will be tested later in the year.

There is also a lack of clarity in relation to service area (first line) and Resilience team (second line) resilience responsibilities across the Council, with no clearly defined responsibilities and accountabilities in Directorates and Service Areas for completion and maintenance (with the support of the Resilience team) of the full population of BIAs and Resilience plans considered necessary (a total of 158 excluding the Health and Social Care Partnership). As a result, the Resilience team have become involved in delivery of first line service area resilience planning activities. Consequently, resilience activities are not being performed in line with the resilience framework detailed in the RMSD.

This is supported by the fact that that BIAs across the Council have not been fully completed (only 31% of the full population of BIAs was complete as at 28 February) and only a limited number of service area resilience plans (which are predominantly out of date) have been established.

Additionally, BIAs do not capture details of critical services and technology systems (shadow IT) provided by third party suppliers, or consider the adequacy of their resilience arrangements and their potential impact on the Council's ability to recover.

Whilst management has advised that communication in the recent severe winter weather worked effectively, we also confirmed that there is no established Council wide emergency call tree to ensure that all employees can be contacted in the event of a major incident. Instead, reliance is place on service areas to ensure that they maintain contact details for their employees. The resilience team do maintain contact details for employees with resilience responsibilities, and have advised that that plans are being progressed to upload all employee details into the resilience management system, however there is currently no completion date for this activity.

We also identified some moderate control gaps in relation to the ongoing maintenance of Council wide resilience plans; delivery of resilience training; and lessons learned from completion of resilience exercises.

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

Further information on the findings raised is included at Section 3: Detailed findings.

3. Detailed findings

1. Resilience responsibilities

Findings

The Council's Resilience team do not provide oversight and challenge on Health and Social Care Partnership resilience arrangements in relation to Partnership services delivered by the Council, but provide advice and support on an ongoing basis. Resilience management has advised that this approach was agreed with Partnership senior management.

Our review also established that service areas (first line) and the Resilience team (second line) are not delivering their respective resilience responsibilities effectively. These responsibilities are detailed in the current resilience management system document (RMSD) and include the requirement for Directorates and Service Areas to effectively manage their resilience risks; and prepare and maintain the total population of 158 (excluding the Health and Social Care Partnership) business impact assessments (BIAs), and resilience plans considered necessary across the Council. Additionally, where resilience responsibilities have been allocated, they are not consistently reflected in performance objectives and conversations. Currently, the Resilience team is performing the majority of these first line service area resilience activities.

Our testing also confirmed that there is an insufficient number of resilience coordinators and deputy coordinators established across the Council to support resilience incidents. The RMSD notes that there are currently:

- 3 locality resilience coordinators
- 4 service area coordinators; and
- 5 cross council resilience specialists

Finally, we noted that the Resilience Manager is also chair of the Council's Resilience Group (CRG) that is responsible for review and approval work delivered by the Resilience team (for example the RMSD and the annual resilience test programme), and that the roles and responsibilities of this group have not been formally defined.

Business Implication	Finding Rating
• Potential gaps in Health and Social care business impact assessments and resilience plans for services delivered by the Council are not identified and addressed; • Service area resilience responsibilities (for example completion of business impact assessments and preparation and maintenance of resilience plans) are not effectively performed; • Potential lack of clarity in relation to responsibility for implementing service areas resilience plans in the event of a major incident); • Employees with resilience responsibilities are not assessed on how effectively these are discharged; • Lack of segregation of duties when the CRG reviews and approves work delivered by the Resilience team; and • CRG members are not clear on their roles and responsibilities.	**High**

Action plans	
Recommendation	**Responsible Officer**
1. The Council's Resilience team responsibilities in relation to resilience support provided to the Health and Social Care Partnership for Partnership services delivered by the Council should be reconsidered and clearly defined; 2. A review of voluntary resilience coordinators will be performed in each Directorate to ensure that numbers are sufficient to provide support in the event of a resilience incident. Where numbers fall short, Directorates will endeavour to recruit additional volunteers; 3. Operational resilience responsibilities for completion and ongoing maintenance of Directorate and Service Area Business Impact Assessments; Resilience plans; and coordination of resilience tests in conjunction with the Resilience team will be clearly defined and allocated. The total number of employees with operational resilience responsibilities will be determined with reference to the volume of business impact assessments and resilience plans that require to be completed and maintained to support recovery of critical services; 4. Corporate; management; and team member objectives for operational resilience responsibilities (for example completion of Service Area Business Impact Assessments; Resilience Plans; and coordination of Resilience tests) will be established, with ongoing oversight performed by Directors and Heads of Service to confirm that these are being effectively delivered to support the resilience responses included in both the Directorate and Council's annual governance statements; 5. An alternative chair of the CRG should be considered to ensure effective segregation of duties; and 6. Formal terms of reference should be established and approved for the CRG.	1. Resilience Team and H&SC 2. to 4 All service areas 5. Resilience management 6. Resilience team
Agreed Management Action	**Estimated Implementation Date**

1. Strategy and Insight Head of Service to meet with the Chief Officer EHSCP, as the responsible officer, to agree appropriate, clear resilience support arrangements. 2. to 4 – IA recommendations agreed by all Directorates; 5. Governance arrangements for the Council Resilience Group and its subgroups will be considered as part of the regular resilience management review; and 6. Formal terms of reference for the CRG will be developed by Resilience and submitted for approval at the September CRG meeting.	1. 5 and 6 – 30 November 2018 2. and 3 - 20 December 2018 4. 31 July 2019 5. and 6 - 28 September 2018

2. Completion and adequacy of service area business impact assessments and resilience arrangements

Findings

Business impact assessments

The Council's Resilience team are heavily involved in completion of service area business impact assessments (BIAs). Service area BIAs are categorised as complete only when all underlying lower level BIAs have been completed and approved.

Completion of BIAs has not been prioritised on the basis of statutory and critical services. Instead, the Resilience team are facilitating completion of BIAs once service area restructures are complete. Management has advised that this has been agreed with the Corporate Leadership Team.

The Resilience team monitors completion of the 158 BIAs to be completed across the Council (excluding Health and Social Care) using a tracker. Review of the tracker as at 28 February 2018 established that:

- 35 (22%) BIAs have not been started. Of the 123 (78%) BIAs in progress, only 49 (31%) have been fully completed; and
- 27 of the 49 completed BIAs (55%) are more than one year old and past the annual review date specified on the front of BIA document.

Review of a sample of 20 completed BIAs also confirmed that:

- they do not consistently include reference to critical third party supplier resilience arrangements and agreed recovery objectives;
- they do not include resilience arrangements for all technology systems, notably critical shadow technology systems that are externally hosted. Of the 95 technology systems detailed in the 20 BIAs reviewed, only 12 were classified as either internal or externally hosted systems;
- the Artifax system used by Culture within the Place Directorate is recorded on the Culture BIA as internally hosted by the Council, but is also included in the shadow IT return completed by Place and provided to the Council's ICT team;
- whilst BIAs include recovery time objectives, they do not include recovery point objectives - the maximum targeted period in which data might be lost from a technology system following a major incident;

Resilience plans and emergency call trees

There is only a limited number of established resilience plans across service areas detailing the process to be followed in the event of an incident, however these are predominantly out of date.

Resilience management has advised that resilience plans will be created across the Council once all BIAs have been completed, as agreed by the Corporate Leadership Team.

Additionally, there is no established Council wide emergency call tree to ensure that all employees can be contacted in the event of a major incident.

The Resilience team maintains a directory that includes contact details for all Council employees with resilience responsibilities (there are currently 12 employees included in the resilience management system document who have resilience responsibilities) that is regularly tested.

Resilience management has advised that plans are being progressed to upload all employee details into the resilience management system, however there is currently no completion date for this activity.

Business Implication	Finding Rating
• The Council may be unable to recover critical services in the event of a significant or major incident and • The Council may be unable to contact employees in the event of a significant or major incident.	High

Action plans

Recommendation	Responsible Officer
1. Existing BIA templates should be reviewed and refreshed to include details of third parties involved in service delivery; shadow technology systems; recovery time objectives for services; and both recovery time (RTOs) and recovery point objectives (RPOs) for all both CGI hosted and shadow technology systems used by the service; RTOs and RPOs for CGI hosted systems should either be aligned with established CGI contractual recovery arrangements, or change requests initiated where shorter RTO timeframes are required by Service Areas. 2. Completion of BIAs and emergency call trees should be prioritised by service areas (with guidance provided by the Resilience team) and provided to Resilience for review, oversight and challenge, and a target date set for completion; 3. Processes should be established within service areas to ensure emergency call trees are updated to reflect employee changes; 4. Once BIAs have been completed, they should be reviewed and a list of statutory and critical services established and presented to CLT for agreement; 5. Following CLT agreement on the Council's population of statutory and critical services, development of resilience plans for these areas should be prioritised by services areas, with support provided by the Resilience team; 6. Existing third party contracts supporting critical services should be reviewed by Directorates in consultation with contract managers / owners to confirm that they include appropriate resilience arrangements. Where gaps are identified, Procurement Services should be engaged to support discussions with suppliers regarding inclusion of appropriate resilience clauses requiring third parties to establish adequate resilience arrangements for both services and	1. 4; 8; 9 - Resilience Team 2. and 3 Resilience Team 5. 10 and 11 - All service areas and Resilience Team 6. All service areas / procurement 7. Procurement 12. Service Areas

systems that are tested (at least annually) with the outcomes shared with / provided to the Council. Where these changes cannot be incorporated into existing contracts, they should be included when the contracts are re tendered. ; 7. When procuring critical services, procurement specification requirements should be considered at the design stage and enhanced to require third party confirmation that they have established adequate resilience arrangements for both services and systems that are tested at least annually; with the requirement to maintain and test resilience plans and provide assurance on the outcomes to the Council included in final supplier contracts; 8. Resilience plan templates should be revised to ensure that they include details of critical third party service and technology provider resilience arrangements in relation to the service, with appropriate recovery time and recovery point objectives; 9. All statutory and critical service resilience plans and emergency call tress should be reviewed at least annually by the Resilience team, with specific focus on ensuring that third party recovery time objectives for services, and recovery time and point objectives for shadow IT systems are aligned with the Council's recovery objectives for re-establishing the service; 10. Once established, all statutory and critical service BIAs; resilience plans; and emergency call trees should be reviewed and refreshed annually, and provided to resilience for review; 11. All statutory and critical service plans should be tested at least annually (this could either be an independent test or could form part of a council wide resilience test), with outcomes recorded and lessons learned factored into resilience plans; and 12. Assurance should be obtained annually for statutory and critical services from third party service providers that their resilience plans remain adequate and effective; and have been tested to confirm that the recovery time objectives for systems and recovery time and point objectives for technology systems agreed with the Council were achieved. Where this assurance cannot be provided, this should be recorded in Service Area and Directorate risk registers. Note that the requirement for provision of annual assurance by suppliers could be satisfied by provision of their annual ISAE 3402 service organisation controls reports; sharing the outcomes of internal audit reviews of resilience; and sharing the outcomes of resilience testing performed.	
Agreed Management Action	**Estimated Implementation Date**
1. The BIA template will be reviewed by Resilience, including recovery objectives, in conjunction with key internal stakeholders (dependent on Procurement's action 2.7); 2. And 3 Resilience to develop and provide appropriate methodology,	1. 31 July 2019 2. and 3 – 29 March 2019 4. 31 January 2019

protocols and templates for BIAs, call trees and resilience plans. Resilience will oversee and coordinate the completion and maintenance of all BIAs and emergency call trees, providing support, review and challenge to service areas and ensuring consistency of approach; 4. A list of Council essential activities will be submitted to CLT for final approval; 5. Following CLT agreement on the Council's list of essential activities, resilience plans for these areas will be prioritised on a risk-assessed basis, as far as practicable, with support provided by Resilience. The development of resilience plans will include capacity workshops, training on the Resilience Management Information System and scenario planning about key potential resilience incidents and their impact for each essential activity business areas. The development of resilience plans will prioritise high-risk essential activities (approximately 70) and these will be completed first; Following this, resilience plans for the remaining essential activities (approximately 105) will also be prioritised for completion on a risk basis; 6. and 7 – IA recommendations agreed by all Directorates; 8. Resilience plan templates, including recovery objectives, will be reviewed by Resilience, in conjunction with key internal stakeholders; 9. Resilience will, on the basis of risk assessment and in conjunction with key internal stakeholders, document which statutory and service resilience plans required to be reviewed annually in particular ensuring alignment of third party and shadow IT recovery time objectives with service re-establishment; these will be aligned with the revised BIA template (see management action 2.1), government and Resilience Partnership set priorities and confirmed annually as part of the CRG management review programme. 10. Once the new BIA template and initial resilience plans for essential activities are completed and established, Resilience will continue to support service areas to annually review their BIAs, essential activity resilience plans and call trees; 11. Resilience will, on the basis of risk assessment and in conjunction with key internal stakeholders, document which statutory and service resilience plans required to be tested annually. Relevant exercise actions for Resilience will be recorded and significant lessons learned incorporated into resilience plans, pending approval by multi-agency partners and the CRG, as appropriate; and 12. Agreed by all Directorates.	5. 30 June 2020 for first group and December 2021 for second 6. 20 December 2019 7. 21 December 2018 8. 29 March 2019 9. 21 December 2018 10. 21 December 2021 11. And 12 – 28 June 2019

3. Adequacy, maintenance, and approval of Council wide resilience plans

Findings

Review of the Resilience team plan review schedule that details the timeframes for review of Council wide resilience plans, protocols, and procedures confirmed that there is currently no cyber security Council wide resilience plan, and no Council wide significant incident framework to ensure that the

appropriate people are contacted and a critical response team established in the event of a serious incident (e.g. fatality or dangerous incident).

Additionally, 15 documents had been archived. Of these, 6 were noted as having been archived as there were insufficient resources to maintain them, with no further rationale provided.

Of the 36 remaining documents:

- 20 were reviewed in 2017
- 4 are in currently being reviewed
- 12 were not reviewed in 2017, but had been allocated 2018 review dates

The Edinburgh Major Incident Evacuation Plan was last published in July 2016 and is scheduled for review in December 2018, whilst the Corporate Bomb Threat and Suspicious Item Procedure was published in March 2016 and is scheduled for review in November 2018.

Finally, review of a sample of five council wide resilience plans confirmed that:

- they included references to the business continuity plan which has not been reviewed and updated since 2015; and
- As at 28 February 2018, the emergency response plan on Council's intranet (the Orb) was dated 2014. Resilience management has advised that this has now been addressed and the December 2017 version is now available.

Business Implication	**Finding Rating**
• The Council may be unable to recover critical services in the event of a cyber security attack and employees may not be aware of their responsibilities; • The Council may be unable to respond appropriately in the event of a critical occurrence; • Archived plans may include relevant resilience risks that could potentially crystallise and impact the Council; and • If a major incident or corporate bomb threat occurs, plans and procedures to be applied could be out of date and no longer relevant.	**Medium**

Action plans	
Recommendation	**Responsible Officer**
1. A Council wide significant incident escalation framework should be developed, communicated, and maintained together with the current population of council wide resilience plans; 2. A clear process should be established for archiving plans, and the rationale for archiving clearly documented; 3. The 6 plans archived on the basis of insufficient resources should be reviewed to confirm that they can be archived as the risks are no longer relevant; and 4. Review of the major incident evacuation plan; the corporate bomb threat and suspicious item procedure; and the business continuity plan should be prioritised.	1. to 5 Resilience team
Agreed Management Action	**Estimated Implementation Date**

1. a) Resilience will prepare a paper for CLT highlighting the risks associated with lack of a Council wide significant incident management framework that is linked to Service Area incident management processes. If this proposal is accepted, the current resilience management framework will be shared with Directorates and guidance and support provided on how this can be linked with Service Area incident management processes. b) Resilience will develop guidance and promote best practice to enable managers to develop incident management procedures for their respective areas as they deem appropriate. 2. The process and rationale for archiving corporate resilience plans will be documented. 3. And 4 a) As part of the Resilience management review programme and priorities assessment Resilience will, on the basis of risk assessment and in conjunction with key internal stakeholders, document the review frequency for corporate resilience plans, aligning with government and Resilience Partnership set priorities and prioritising on a risk basis. b) Under this methodology the Major Incident Evacuation Plan and Bomb Threat and Suspicious Items will be reviewed by January 2019. c) The Council Business Continuity Plan (which was based only on the Council's structure) is being replaced on an interim basis by refreshed BIA data, based on each Council building, which will provide data to support a wider range of incident scenarios, including loss of premises – this is scheduled to be completed by November 2019. d) A full Council Business Continuity Plan is scheduled to be completed by December 2020, which will include contingency plans for essential activity areas.	1. a) and b) - 29 March 2019 2. 20 December 2018 3 and 4 a) - 28 June 2019 b) 31 January 2019 c) 29 November 2019 d) 18 December 2020

4. Resilience Training

Findings

Employees with resilience responsibilities across the Council receive training delivered by the Resilience team. However, there is no established process to ensure that all new employees or existing employees who have assumed resilience responsibilities receive the necessary training.

Additionally, whilst some evidence of training attendance was available (calendar invites and e mails), it is not formally recorded and monitored by the Resilience team.

Review of a sample of 20 employees with resilience responsibilities (including the Chief Executive; four Corporate Leadership Team Members; one Head of Service; and the Council Leader) confirmed that:

- 1 resilience coordinator had not yet attended the training;
- no evidence of training attendance could be provided for 2 cross-council resilience specialists; and

- no evidence of training attendance could be provided for 1 service area resilience coordinator.

Business Implication	Finding Rating
Employees with resilience responsibilities who have not received training may not discharge their duties effectively in the event of an incident.	Medium

Action plans

Recommendation	Responsible Officer
1. A process should be established to ensure that the Resilience team are made aware of all employees (new and existing) who have assumed resilience responsibilities, enabling them to be enrolled for training; 2. A training delivery tracker should be established and maintained to record training delivered to Council employees and identify potential opportunities for delivery of refresher training;	1. Service Areas and Resilience team 2. Resilience team
Agreed Management Action	**Estimated Implementation Date**
1. a) Resilience will provide an updated list of Council staff with a named resilience responsibility from the RMS to the CLT detailing all Resilience Coordinators and Specialists every 6 months to identify new employees with resilience responsibilities. (Resilience Deputies will be determined as part of the resilience plans being developed with each essential activity area.) b) Resilience will support Resilience Coordinators to undertake and complete a training needs analysis for direct resilience roles. c) Resilience to meet with HR (Margaret-Ann Love and Christine McFadzen, the HR Resilience Specialist) to discuss corporate resilience training needs. 2. The Resilience Training and Exercising records tracker will be updated and maintained.	1. 30 November 2018 2. 21 December 2018

5. Lessons learned from resilience exercises

Findings

Review of a sample of five internal and external resilience exercises established that:

- no debrief report was written for the Dark Star Phase 2 exercise completed in March 2017; and
- there was no evidence of a completion of a debrief for the Lothian Pension Fund workshop completed in October 2017.

Additionally, there was no evidence available to confirm that debrief actions had been implemented for the following resilience exercises / workshops:

- business continuity, completed in July 2017;
- Magpie, completed in September 2017; and
- Lothian Pension Fund workshop, completed October 17.

Business Implication	Finding Rating

Lessons learned are not incorporated into future exercises or live resilience incidents.	**Low**

Action plans	
Recommendation	**Responsible Officer**
1. Debrief reports or notes should be prepared or obtained for all Council-led resilience exercises performed and the outcomes shared with all participants and all relevant employees with resilience responsibilities; and 2. Evidence should be retained to confirm implementation of all debrief actions.	Resilience team
Agreed Management Action	**Estimated Implementation Date**
1. Debrief reports / notes will continue to be maintained for Council-led resilience exercises and outcomes shared with all participants and relevant employees with direct resilience responsibilities (as noted in the RMS). 2. Agreed Resilience debrief actions will be captured and monitored on Pentana as part of the resilience management review programme.	1. and 2 – 30 November 2018

Appendix 1 - Basis of our classifications

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

Appendix 2 – Terms of Reference

Draft Terms of Reference – Resilience Governance Review

To: Laurence Rockey, Head of Strategy and Insight
Mary-Ellen Lang, Resilience Manager

From: Lesley Newdall, Chief Internal Auditor Date: 20th February 2018

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

Background

In September 2017, the Council published its strategic business plan ("Programme for the Capital") to build upon Edinburgh's successes, and demonstrate a commitment to improve services and amenities across the City.

Five strategic aims are included in the business plan. One notable aim is to have:

- A resilient city, where citizens are protected and supported with access to sustainable and well-maintained facilities.

Certain services are a statutory requirement or are critical for citizens, such as health and social care and education. Ensuring that statutory and critical services continue to operate and are restored effectively in the event of a disaster or disruptive event, is a key priority for the Council.

Additionally, there is a legislative requirement for the Council to establish Business Continuity Management (BCM) arrangements under the Civil Contingencies Act (CCA) 2004.

The Council's Resilience team is currently accredited under the British Standards Institute's International Standard for Business Continuity (ISO22301) which specifies the requirements for a management system to protect against, reduce the likelihood of, and ensure business recovery from disruptive incidents.

As a capital city, one of the most significant disruptive events that could occur in Edinburgh is a terrorist attack. The Council participated in exercise Border Reiver (counter-terrorism exercise) in October 2017. This exercise, which forms part of the UK Home Office's National Counter-Terrorism Exercise Programme was designed to test effectiveness of emergency services; government; local authority; and other relevant agency responses to a terrorist incident.

It should also be noted that the Resilience team do not include the Health and Social Care Partnership within their Council wide remit, but provide resilience advice and support to the partnership an ongoing basis. This was agreed with the Health and Social Care Senior Colleagues.

The Council is currently undergoing a period of significant change and consequently Business Impact Assessments (BIAs) are being undertaken as structures are finalised by the Council. Resilience has confirmed that this is significantly impacting the ability to finalise and maintain council wide resilience plans.

Scope

We will assess the adequacy of design and operating effectiveness of the key resilience controls in place to mitigate the following Corporate Leadership Team risk:

Major incident - A sudden high impact event causes harm to people and damages infrastructure, systems or buildings. Buildings, staff and/or systems are non-operational for a time, resulting in a reduced ability to deliver services. Failure to deliver an appropriate level of service in the event of a sudden operational requirement may lead to harm to people and reputational damage to the Council.

Our review will focus on the adequacy and effectiveness of controls in the following areas:

- The Council's Resilience Management System (RMS);
- Emergency response plans;
- Oversight and governance of the RMS and emergency response plans; and
- Completion of resilience plans and BIAs for high risk Service Areas.

Limitations of Scope

The audit will not provide assurance on the following areas:

- Adequacy of Service Area resilience plans, and
- Adequacy of key third party suppliers' resilience arrangements.

Approach

Our audit approach is as follows:

- Obtain an understanding of the Council's RMS through interviews with key stakeholders, and review of supporting documentation;
- Identify the key risks related to the RMS, including oversight;
- Evaluate the design of the controls in place to address the key risks; and
- Test the operating effectiveness of the key controls.

Specific Control Objectives

Sub-process	Control Objectives
Resilience Management System	• A RMS is defined and implemented that is aligned with applicable legislation and standards. • Resilience roles, responsibilities and accountabilities have been clearly defined for both the Resilience team and Service Areas across the Council. • BIAs have been prepared by all Service Areas that clearly define the service delivered and its criticality. • BIAs completed by Service Areas have been consolidated (where possible) into appropriate resilience arrangements to support prioritisation for reinstatement of business-critical services across the Council. • BIAs are regularly reviewed and refreshed to reflect changes in service, and these changes are reflected in the overall Council resilience plan. • All third parties have been identified and prioritised on the basis of criticality of services provided to the Council, and the outcomes recorded in BIAs. • The RMS is subject to regular ongoing review to ensure that it remains aligned with changes within the Council; and changes to statutory and critical services. • A resilience training programme covering all areas of the Council that have a resilience responsibility has been established and delivered on an ongoing basis. The content of the training plan is sufficient to ensure that all those with a resilience responsibility are aware of the nature of resilience, external threats and their resilience responsibilities.

Resilience Exercising	• An annual resilience exercise programme has been established, and the test schedule approved by the relevant governance forum. Results, supporting evidence and lessons identified are recorded. • Performance against the overall plan and objectives is monitored and reviewed, and exercise outcomes are reported to management for review. Remedial actions are identified, and action plans for improvement are produced and authorised, and incorporated into the Council's resilience plan.
Incident Response and Management	• An incident response and management plan to deal with the Council's response to city wide incidents has been established and is regularly reviewed, refreshed and tested. • An incident response and management incident management team is in place, and includes appropriately senior levels of management who are responsible for providing direction, strategic & tactical decision making, and supporting the operational response. • All individuals in the incident response and management co-ordination group are fully aware of their roles and responsibilities, with new member and refresher training provided. • The incident response and management plan includes a communications strategy and plan to ensure that employees and citizens are aware of action being taken. • Incident response and management and communications plans are regularly tested with outcomes recorded and lessons identified factored into the incident response plan. • Incident response and management and communications plans have been updated to reflect the outcomes and lessons identified from the Border Reiver exercise that occurred in October 2017.
Oversight and governance	• Appropriate committees / governance forums have been established to provide scrutiny and oversight of the Council's RMS. • Committees / governance forums are supported by approved Terms of Reference that sets out roles and responsibilities. • The Council's overarching resilience plans have been approved.

Internal Audit Team

Name	Role	Contact Details
Lesley Newdall	Chief Internal Auditor	0131 469 3216
Fiona Mathewson	Internal Auditor	07802660187

Key Contacts

Name	Role	Contact Details
Laurence Rockey	Head of Strategy and Insight	0131 469 3493

Mary-Ellen Lang	Resilience Manager	0131 529 4686

Timetable

Fieldwork Start	05/02/2018
Fieldwork Completed	09/03/2018
Draft Report	16/03/2018
Receipt of Management Responses	23/03/2018
Final Report Issued	06/04/2018

Follow Up Process

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

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

Monitoring of outstanding management actions is undertaken via monthly updates to the Director and his executive assistant. The executive assistant liaises with service areas to ensure that updates and appropriate evidence are provided when required.

Details of outstanding actions are reported to the Governance, Risk & Best Value (GRBV).