Internal Audit Report

Organisational Resilience – Major Incident

6 October 2025

CD2502

Overall Assessment	Reasonable Assurance

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2025/26 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2025. 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 Global Internal Audit Standards (UK Public Sector) and as a result is not designed or intended to comply with any other auditing standards.

Although there are 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.

Executive Summary

Overall Assessment	Reasonable Assurance

Engagement conclusion and summary of findings

There is a generally sound system of governance, risk management and control in place enabling the Council to plan, respond, and recover from a major incident affecting the city or Council. The review has however highlighted key areas where alignment to strategic objectives and priorities, operational clarity, and incident responsiveness can be improved. These include:

- strengthening role clarity, training, and awareness through defining and communicating clear roles across the Council supported by tailored, timely training and ensuring sufficient resources are available to expand business partnering to all Directorates
- reinstate strategic oversight and governance including resuming reporting to CLT and ensuring sufficient resources are available to support directorate level governance structures, including completion of key documents / logs, appointment of deputies, as well as resuming multi-agency partnership forums which enable collaborative resilience planning
- validating and testing of protocols through multi-year testing and exercising schedules for all relevant internal plans and protocols and regular review of external contact information, together with involving all key stakeholders in exercises to support resilience readiness
- formalising incident response and on-call arrangements, including clarifying and communicating definitions and escalation protocols and expanding contractual on-call arrangements
- modernising the Council's Incident Response Centre to ensure it is fit for purpose, and is supported by regular testing and maintenance to enable timely access and response during a major incident
- embedding debriefs and action tracking, including mandating timely debriefs with clear criteria and reporting timelines, and tracking of all actions to ensure lessons learned are captured, communicated, and embedded into practice.

Areas of effective practice

- the Council's Resilience Governance Framework sets out the resilience governance approach across the organisation, and includes a comprehensive and detailed roles and responsibilities matrix
- organisational resilience risks are captured in the Corporate Resilience risk register, directorate risk registers, and divisional / service risk registers
- previous audit actions for Business Impact Analyses (BIAs) are complete, supported by the Resilience Team, with BIAs conducted across the majority of services
- the Resilience Team contribute to the Council's overarching Records Management Plan and provide regularly updates to the Information Governance Team on arrangements
- a contract is in place between the Council and its business continuity management system provider, there are contract management meetings with the provider every six months, and management information is provided by the supplier quarterly.

Phased implementation

Management recognises the need to establish a coordinated and consistent approach to managing resilience across the Council. A phased implementation approach will be adopted to ensure that detailed management actions are developed to address some of the findings and recommendations.

These management actions and implementation dates will be provided to Internal Audit by 31 January 2026. Following this, they will be reported to Committee.

Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
1. Risk Management			No Issues Identified	N/A
2. Policies, Procedures, and Training			Finding 1 – Role clarity, training and awareness	Medium Priority
3. Governance and Oversight			Finding 2 – Governance and Oversight of Resilience	High Priority
4. Business Continuity Planning			No issues Identified	N/A
5. Incident Response Preparedness			Finding 3 – Protocol Reviews and Testing	Medium Priority
			Finding 4 – Incident Response and On-Call Arrangements	High Priority
6. Coordination with Partners and External Stakeholders			See Finding 1	As per Finding 1
7. Post-Incident Review and Continuous Improvement			Finding 5 – Debriefs and Lessons Learned	Medium Priority
8. Information Governance			No Issues Identified	N/A
9. Service Level Agreements and Service Standards			No Issues Identified	N/A

See Appendix 1 for Control Assessment and Assurance Definitions

Background and scope

Organisational resilience refers to an organisation's ability to prepare for, respond to, and recover from, disruptive events, while continuing to deliver priority services. Organisational resilience is essential to ensure that statutory services, such as social care, waste management, public health and emergency coordination, can be maintained during periods of crisis. The Joint Emergency Services Interoperability Programme defines a major incident as an event or situation with a range of serious consequences which requires special arrangements to be implemented by one or more emergency responder agency. Examples include:

- severe weather (e.g. storms, flooding, or heatwaves)
- prolonged power or utility outages
- civil unrest or large-scale public events
- pandemic outbreaks or major public health emergencies
- large scale ICT failure or failure of a major contractor
- major fire in a high-rise residential block
- terrorist threats or security-related disruptions.

The Council's Emergency Plan defines a 'major incident' as any emergency that requires the implementation of special arrangements by one or more of the emergency services, the NHS, or the local authority for:

- rescue and transport of a large number of casualties
- involvement of large numbers of people
- handling of a large number of enquiries
- requiring large scale combined resources.

In addition, the Council defines 'serious emergencies' as having 'serious consequences but may not be termed a major incident. Such an emergency may nevertheless require a large scale and co-ordinated response from the Council to support and assist the emergency, health or other services.'

Between January 2023 and April 2025 there were 22 incidents recorded on the Incidents Register. As of 2025, the Council has never declared a major incident.

Performance of Organisational resilience arrangements is assessed against a range of statutory and regulatory guidance which include:

- Civil Contingencies Act 2004
- Counter Terrorism and Security Act (2015)
- Control of Major Accident Hazards (COMAH)
- The Radiation (Emergency Preparedness and Public Information) Regulations 2019.

As a local authority, the Council is a Category 1 responder under the Civil Contingencies Act 2004. Category 1 responders are at the core of the response to most emergencies and are subject to specific duties which include:

- assess the risk of emergencies occurring and use this to inform contingency planning
- put in place emergency plans
- put in place business continuity management arrangements
- put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform, and advise the public in the event of an emergency
- share information with other local responders to enhance co-ordination
- co-operate with other local responders to enhance co-ordination and efficiency
- provide advice and assistance to businesses and voluntary organisations about business continuity management (local authorities only).

City of Edinburgh Council Resilience Governance Arrangements

The Council Resilience Group develops and maintains the Council Resilience Governance Framework and drives and monitors the Council's resilience workstreams.

The Resilience Team provides specialist support and advice to Directorate Resilience Coordinators to maintain Business Impact Analyses (BIAs) and plan for, and respond, to a range of resilience incidents. There are five Resilience Coordinators, supported by a number of Resilience Deputies working within Directorates, in addition to five Resilience Specialists covering cross-Council services.

The Council has a Chief Officer On-Call Rota for resilience incidents that occur out of hours including weekends. There are 14 Chief Officers, and they comprise Corporate Directors and Service Directors, as well as the Chief Executive. The Council also has a Council Incident Coordination Centre in the City Chambers.

Resilience Arrangements

The Council Emergency Plan (2019), and information about the Edinburgh Major Incident Evacuation Plan (Evacuation Plans for Business and Residents), are available on the Orb and Council website, and each directorate has business continuity documentation. BIAs are stored and maintained through Meridian, a business continuity, resilience, and risk management system.

The Council periodically undertakes exercises using a range of methods, to raise awareness and test and validate current resilience arrangements. The Resilience Team has responsibility for arranging the validation of corporate plans and protocols, and directorates are responsible for arranging the validation of Directorate plans and protocols. Some recent examples of exercises undertaken include:

- October 2023 – exercise Safe Steeple: an in-person, multi-agency tabletop exercise led to test the city's preparedness in the event of a terrorist attack
- April 2024 – multi-agency exercise to test the Major Accident Hazard Pipelines Plan
- February 2025 – exercise Dark Smoke: an in-person, multi-agency tabletop exercise to validate the Council's INEOS Dalmeny Off-Site Emergency Plan.

Scope

The objective of this review was to assess the adequacy of design and operating effectiveness of the arrangements established to enable and support the Council to respond to a major incident impacting the city or Council including consideration of relevant plans and protocols including testing, working with key partners across the city, and roles and responsibilities including on call / out of hours arrangements. The audit considered arrangements for both major incidents and serious emergencies, as defined by the Council.

Alignment to Risk and Business Plan Outcomes

The review also considered assurance in relation to the following Corporate Leadership Team risk categories:

- Resilience
- Service Delivery
- Technology & Information
- People
- Reputational
- Health & Safety
- Legislative and Regulatory
- Supplier / Partnership Management
- Governance and Decision Making.

Business Plan Outcomes:

- The Council has the capacity, skills, and resources to deliver our priorities efficiently, effectively and at lower cost.

Limitations of Scope

The following areas were excluded from scope:

- Cyber Security Resilience – covered in the Directorates Cyber Incident Response audit issued in October 2024
- preparation for Martyn's Law – as this will be covered in a specific audit as part of the approved 2025/26 internal audit plan.

Reporting Date

Testing was undertaken between 9 June 2025 and 11 August 2025.

Audit work concluded on 28 August 2025, and the findings and opinion are based on the conclusion of work as at that date.

Findings and Management Action Plan

Finding 1 – Role Clarity, Training and Awareness

Finding Rating	Medium Priority

Role clarity

Adherence by Directorate Resilience Coordinators to some aspects of the Resilience Governance Framework is impacted due to a lack of clarity and awareness of respective roles and responsibilities. In addition, there are capacity challenges for coordinators when balancing resilience responsibilities with their principal roles as Directorate Operations Managers.

Business partnering

The Resilience Team operates a business partnering programme with team members currently assigned to Place, Children's Education and Justice Services, Customer and Corporate Services and the Chief Executive's Office. Due to ongoing resourcing issues within the Resilience Team, the Health and Social Care Partnership do not have assigned resilience business partners. The impacts of ongoing resourcing issues and pressures in the team were reported in the bi-annual Legal and Assurance Service Performance and Assurance Information report in 2024.

Resilience Awareness Training

The Civil Contingencies Act 2004 states that officers charged with resilience work should be competent to carry out their role. However, training for Directorate Resilience Co-ordinators consists of a 1-hour session delivered remotely.

The training sets out some of the Resilience Coordinator responsibilities under the Council Resilience Governance Framework, such as developing a workplan, leading on directorate incident debriefs, and developing directorate resilience plans.

The training directs officers to the Resilience Governance Framework which sets out the extensive list of responsibilities including being a 24/7 point of contact, however, no training is provided to support and guide coordinators on how to deliver all responsibilities.

Timing of training delivery

The Council's Resilience Learning, Development and Exercising Strategy and the Resilience Governance Framework do not provide a clear timeframe for delivery of resilience training, nor is there a requirement for regular refresher training. Resilience Team management advised a resilience knowledge check is in development and due for annual rollout in March 2026.

It was noted that two Resilience Coordinators received their Resilience Awareness training months after they assumed their resilience responsibilities. The Resilience Team advised this was due to scheduling issues.

Risks

- **Governance and Decision Making** – lack of awareness of roles and responsibilities leading to ineffective incident response management
- **Resilience** – insufficient training may impact understanding and operation of resilience roles, affecting the Council's incident response
- **Service Delivery** – insufficient resources leading to an ineffective incident response which impacts service delivery
- **Regulatory and Legislative Compliance** – failure to meet statutory and regulatory duties leading to penalties and reputational damage.

Recommendations and Management Action Plan: Role Clarity, Training and Awareness

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
1.1	The Council should review the resource requirements needed for coordinating and undertaking resilience related duties and tasks. This should include capacity within the Resilience team to enable effective support to all directorates via the business partner model and ensuring adequate resources are available within Directorates to support Directorate Resilience Coordinators and Deputies to effectively fulfil resilience duties while performing their principal roles.	Resilience Team to lead a corporate review of resourcing based around desired resilience outcomes. Report to be presented to CLT for consideration.	Corporate Director for Customer & Corporate Services	Head of Health, Safety, Risk & Resilience	31/01/2026
1.2	The Council should review the current resilience training to determine whether it provides an adequate understanding and awareness in preparing colleagues for undertaking resilience-related roles and responsibilities. This should include consideration of tiered role-specific training, with the depth and content tailored to the requirements and responsibilities of the role. It is recommended a resilience skills and competency assessment is performed for all colleagues with resilience roles and responsibilities so that gaps in knowledge or skills can be addressed through the training review. The timing and frequency of training should be confirmed, including induction training and requirement for refresher training to ensure that colleagues continue to be aware of their roles and responsibilities. The Council's Resilience Governance Framework or the Resilience Learning, Development and Exercising Strategy should be updated to include the outcomes of the review so that requirements and expectations are documented and clearly understood.	A review of training content delivered or provided by the Resilience Team to be carried out by the Resilience Team to ensure the training provision reflects the learning needs of learners. Key stakeholders to be engaged through this process including the Council Resilience Group.	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience	30/06/2026

Finding 2 – Governance and Oversight of Resilience

Finding Rating	High Priority

Corporate Leadership Team (CLT) oversight of resilience

The Council Resilience Group (CRG) meets every two months and has delegated responsibility from CLT for resilience work. Membership includes resilience officers, Directorate Resilience Coordinators, and a number of other service representatives. The CRG terms of reference states that CLT receives progress reports, through the Resilience Manager, on key issues and signs off corporate documents as appropriate. However, there is limited oversight of the group at CLT level, with the requirement for resilience annual reports to CLT stopping during the pandemic.

Directorate Resilience Governance

The Resilience Governance Framework (last updated in May 2025) sets out the roles and responsibilities assigned to each directorate including the responsibilities assigned to the Directorate Resilience Coordinators overseeing resilience governance arrangements within directorates, including appointing a Resilience Deputy, delivery of resilience training, and maintaining and coordinating a resilience team or group. The draft framework was provided to Resilience Coordinators in February 2025 with a request to provide feedback. The CRG Terms of Reference states that one of the purposes of the group is to review and approve the Governance Framework. However, it was not approved by the CRG in the March 2025 meeting, but it was shared via email to CRG members in February 2025; it was subsequently signed off by the Chief Executive in May 2025. Review of directorate arrangements in line with requirements highlighted:

- Resilience Deputies are not in place for the Health and Social Care Partnership (HSCP)
- Resilience Coordinators in Customer and Corporate Services, Place, and Children's Education and Justice Services (CEJS), were not aware of Resilience Deputy arrangements for their directorates
- no directorates have performed an assessment of training needs, or the extent of resilience protocol coverage
- no directorate has completed Directorate Resilience Arrangements Logs, which list the resilience plans and protocols
- no directorates have an exercising programme to test protocols
- Place and CEJS have not established a directorate governance forum for resilience. A Customer and Corporate Services forum was established in June 2025.

The Resilience Team were not aware of the lack of adherence to the Framework by directorates, nor was it highlighted through the CRG. All of these requirements are stated in the Resilience Governance Framework.

Activity and performance reporting

There is limited reporting for resilience activities, including the Council's response to resilience incidents, directorate adherence to the Framework, and completion of resilience training and exercising programmes. The bi-annual Legal and Assurance reporting provided information on resilience team activities, including progress with updating plans and protocols and Council debriefs, and ongoing issues but this reporting ceased in October 2024 as the relevant Directorate performance and review meetings were discontinued. There have been, however, incident debriefs for specific events such as Operation Unicorn and Storm Éowyn.

Key resilience partnerships and forum meetings

The Edinburgh Community Resilience Group has not met since 2019. The Resilience Team advised this is due to reduced capacity within the Resilience Team. The other key external governance forum, the Local Resilience Partnership resumed quarterly meetings, beginning in August 2025. The group had not met previously since 2019.

Risks

- **Resilience –** colleagues are unaware of their responsibilities and resilience requirements are not adhered to consistently across the Council leading to an ineffective or delayed incident response

- **People –** insufficient capacity and resource within the Resilience Team and directorates to enable the Council to adequately prepare, respond, and recover from a major incident
- **Supplier, Contractor and Partnership Management** – a lack of engagement and planning with local communities could impact the Council's front-line resilience defences and collaboration with key partners
- **Governance and Decision Making –** lack of reporting on resilience activities and performance at a senior level leading to a limited strategic oversight, assumptions that resilience is embedded and effective, and lack of awareness on resource challenges, gaps, and areas for improvement
- **Strategic delivery, and Regulatory and Legislative Compliance** – lack of visibility of activity at a senior level may mean that the interdependency of resilience risks with other strategic risks including cyber, fraud, and service delivery are not understood and assessed.

Recommendations and Management Action Plan: Governance and Oversight of Resilience

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
2.1	A review of the governance and oversight arrangements for resilience should be undertaken. This should include regular reporting on resilience activities and performance to the Corporate Leadership Team (CLT) at an agreed frequency to ensure that senior management have effective oversight of resilience. Reporting could be via the Council's Resilience Group to CLT and should include, but not be limited to: • adherence to relevant legislation • summary of recent resilience activities and incidents • effectiveness of incident response arrangements • resilience exercising and protocol validation work • lessons learned from incident and exercising debriefs and key themes. In addition, all significant updates to key Council resilience guidance should be reviewed and approved by the Council Resilience Group prior to being finalised.	Report to be taken to CLT setting out revised Governance and Oversight for Council-wide arrangements. This will include frequency of reporting to CLT to ensure sufficient oversight and reassurance on key matters of organisational preparedness.	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience	31/01/2026

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
2.2	a) All directorates should establish a directorate resilience group with key officers. The directorate resilience groups should ensure that the requirements set out in the Resilience Governance Framework are clearly understood and arrangements established to monitor assurance with the requirements across the directorate, including establishing key measures to evidence adherence including, but not limited to: • directorate adherence to the Governance Framework • coverage and scope of directorate-level plans and protocols • exercising and validation of directorate-level plans and protocols • training completion • review and coverage of BIAs and BCPs. Regular updates on directorate arrangements should be provided to the Resilience team via the Council's Resilience Group. The resource to support this should be considered as part of the review set out at 1.1.	A phased implementation approach will be adopted to ensure that detailed management actions which address the findings and recommendations are developed. Management actions and implementation dates will be provided to Internal Audit by 31 January 2026.	N/A	N/A	N/A
	b) Oversight and support to establish directorate arrangements should be provided to directorates from the Corporate Resilience Team. The resource to support this should be considered as part of the review set out at 1.1.				
2.3	The Council should review the role and value of the Edinburgh Community Resilience Group with a view to confirming if meetings for this group should resume. If the group does not resume, the Council should ensure that any statutory requirements for the Council, which were previously mitigated via participation in this group, are adequately covered in other arrangements.	The Resilience Team will carry out a review of the activity of the Edinburgh Community Resilience Group, will engage with key stakeholders and report back to CLT with proposals on the future Community Resilience approach.	Corporate Director of Customer & Corporate Services	Head of Health Safety, Risk & Resilience	31/10/2026

Finding 3 – Protocol Reviews and Testing

Finding Rating	Medium Priority

Plan and protocol Review and testing

The Council's Resilience Learning, Development and Exercising Strategy lists eight potential learning methods. It recognises that 'live exercises are often viewed as the best way to validate a particular plan, short of its actual invocation in an emergency. Live exercises can be complex to arrange and resource intensive'. The Council has not undertaken or significantly participated in a live exercise since November 2018. Resilience Team management advised this is partially due to the impact of Covid-19 and the resulting changes to Council working patterns.

The Resilience Team workplan sets out tasks to be performed each year including testing and exercising of plans and protocols for each year. The testing workplan does not go beyond 12 months and testing schedules have not been established for the Council's plans and protocols with the exception of the INEOS FPS Ltd. Dalmeny External Emergency Plan.

Where there are no statutory requirements, plans and protocols are reviewed every 2 years, but they are tested on an ad hoc basis, not in line with any assigned schedules. The Resilience Team advised this is due to continued resourcing constraints within the team. They advised that some protocols have proven to be effective during some recent incidents (such as the Notification and Escalation Protocol and the Warning and Alerting Procedures), so responses to actual incidents also provide a relevant testing platform.

Resilience Protocols

There are 11 Council plans and protocols for key potential resilience incidents, which the Resilience Team are responsible for maintaining. Two of the 11 documents had not met the assigned review schedule:

- the Control of Major Accident Hazards Regulations 2015 requires the multi-agency INEOS FPS Ltd. Dalmeny External Emergency Plan to be reviewed and tested every 3 years. Testing occurred in 2019 but due to the pandemic was not tested in 2022. The Resilience Team advised the Health and Safety Executive (HSE) and an interim multi-agency testing exercise was undertaken in February 2025
- the Major Incident Evacuation Plan should be reviewed every 2 years. It was last reviewed in October 2022, but the next scheduled review is October 2025.

Council and External Partner Contacts

The Council's Incident Contacts Directory includes contacts within the Council and 41 external contacts, including the emergency services, NHS Lothian, and the Scottish Government. The Resilience Team circulates the Directory bi-monthly to all relevant Council officers, asking for confirmation of any additions, removals, or changes. A similar exercise is not regularly undertaken with external contacts to confirm details remain up to date. The Resilience Team advised that all contact details were tested regularly prior to the pandemic but this has not been possible more recently due to resource and capacity constraints in the team.

Inclusion of key stakeholders in exercising

The Chief Officer On-Call Rota consists of Corporate Directors and key Service Directors, who have a key role in the Council's resilience incident responses out of normal working hours. There have been instances where some officers have not been involved in, or notified of, exercises. Resilience Team management advised that invitees to exercises are determined by the nature and level of exercise scenario that is covered: strategic, tactical or operational.

Risks

- **Resilience –** lack of or irregular validation and testing of resilience plans, protocols and contact information may lead to an unprepared, delayed or ineffective response and a reactive response to unplanned issues
- **Regulatory and Legislative Compliance** – failure to review and test plans may lead to a breach of statutory duties and enforcement action, prosecution or fines.

Recommendations and Management Action Plan: Protocol Reviews and Testing

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
3.1	The Council should lead or participate in regular live multi-agency exercises to test the effectiveness of plans and protocols and provide assurance on the planned incident response approach.	Programme of plan testing aligned to planned revision of plans and protocols to be developed. This is required at a Council and Directorate level.	Corporate Director of Customer & Corporate Services	Head of Health and Safety, Risk & Resilience	31/03/2026
3.2	All resilience protocols and plans (not including guidance documentation) should be updated to include a minimum schedule for testing where appropriate. A longer-term testing programme (beyond 1 year) should be developed to schedule dates and ensure that all plans and protocols are tested on an ongoing rolling basis.	A long-term Plan/protocol schedule of testing will be developed, tracked through the CRG, and reported on as part of the revised Governance arrangements proposed above.	Corporate Director of Customer & Corporate Services	Head of Health and Safety, Risk & Resilience	31/07/2026
3.3	Review and testing programmes should be established with key partners for major and multi-agency plans to ensure exercises are undertaken in line with statutory requirements. Repeated issues or delays to coordinating with partners should be escalated to the Corporate Leadership Team for formal escalation.	Programme of plan testing aligned to planned revision of plans and protocols to be developed. Through the monitoring to be conducted by CRG, where plan testing and revision is being held up by partners this will be escalated to CLT for external escalation as appropriate.	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience Corporate Director of Customer & Corporate Services	31/03/2026
3.4	Contact details for Council officers and external resilience partners listed in the Council's Incident Contacts Directory should be confirmed regularly to ensure that they remain up to date.	Process to be established to ensure validation of contacts on an annual basis. This will be documented within the Resilience Team Manual.	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience	31/01/2026
3.5	Relevant senior officers with resilience responsibilities should be included in resilience exercises and events where capacity allows. Where capacity to participate is an issue, senior officers should attend on a rolling basis to ensure	The development of a long-term Plan and protocol testing regime will allow long notice periods to potential attendees of exercises, creating a	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience Corporate Resilience Manager	31/03/2026

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
	adequate training and understanding, unless the exercise relates to their specific service area or directorate.	greater opportunity for Senior Officers to protect time for their attendance.		Senior Resilience Specialist	

Finding 4 – Incident Response and On-Call Arrangements

Finding Rating	High Priority

Incident definitions and response arrangements

Definitions of what the Council considers a major incident, and a serious emergency are included within the Emergency Plan and resilience incidents are defined in the Generic Notification and Escalation Protocol. These definitions are not sufficiently clear and do not provide examples of incidents which would fall into each category. For example, a 'resilience' incident is defined as: '*serious emergency, major incident or terrorist attack which causes severe disruption to normal activities across the city and / or significant business continuity issues within the Council*'.

The lack of clarity on the categorisation of incidents has led to confusion and delay in responding to emergencies, with some colleagues advising they have not known whether to include the Resilience Team to the facilitate incident escalation and response.

Resilience on-call arrangements

The Resilience Incident Generic Notification and Escalation Protocol states that it is the responsibility of the Resilience Team to escalate a resilience incident to the Corporate Director of Customer and Corporate Services outwith standard office hours.

The Resilience Team have a key role in the Council's initial incident escalation and response, however, they do not operate an out of hours on-call rota and instead use a 'failing whom' basis whereby phone numbers for resilience colleagues held in the Council's Incident Directory are called by the Customer Contact Team until a member of the Resilience Team responds. The absence of a formalised on-call procedures means colleagues in the Resilience Team are not contractually entitled to disturbance allowance or other overtime payments and there is a reliance on the goodwill of colleagues to support.

The lack of a Resilience Team on-call rota has led to confusion amongst colleagues who are involved in out of hours incident escalation as to whether to include resilience colleagues in incident responses, which can mean the response can become fragmented, and inconsistent with the approved framework, plans and protocols.

Chief Officer on-call arrangements

The Resilience Response and Strategic Overview guidance sets out a gold, silver and bronze hierarchy for incident response, with gold reflecting senior leaders and a strategic response, silver involving middle managers who translate strategy to actions and coordinate resources, and bronze where operational leads carry out front-line onsite operations. The Council's Chief Officer On-call arrangements only provide for one senior colleague to be on-call and coordinate an incident response.

Council Incident Coordination Centre

The Council Incident's Coordination Centre (CICC) functions as a coordination and communications hub during a serious emergency or major incident. The CICC Operations Guide was reviewed in 2022 and then updated in August 2025 during the audit. Not all CICC rooms are functional and are cluttered with storage boxes, files, and redundant computer equipment and other technology. The technology and equipment in the CICC is dated, with no videoconferencing equipment to support hosting hybrid and remote meetings with colleagues and partners.

A library of hard copies of plans and protocols is in place, but this is not regularly reviewed and updated to ensure current versions are available.

The Resilience Team are responsible for routine testing and maintenance of the CICC and its equipment and ensuring a programme of regular tests results recorded in an equipment testing log (although the regularity of these tests is not defined). However, this work is not currently taking place, and an equipment testing log is not maintained.

The Resilience Team advised ad hoc visits are undertaken to check the equipment is functional, but there is no set frequency, and the results are not documented.

Risks

- **Resilience –** lack of awareness and agreement on what constitutes a major incident or a resilience incident or inadequate on call arrangements leading to delayed response, escalation, and deployment of protocols
- **Resilience** – an outdated incident response centre may lead to delayed response times and lack of remote conferencing will impact real-time collaboration across colleagues, services and external partners
- **People –** over-reliance on informal arrangements and individual availability places pressure on colleagues, can undermine the importance of incident response arrangements, and create key-person dependencies
- **Governance and Decision Making** – a lack of formal on-call arrangements may result in unclear decision-making authority and the potential to bypass protocols with decisions made via assumptions rather than a structured governance framework
- **Health and Safety** – old equipment and cluttered workspaces may create hazards and lead to health and safety incidents, especially in a high-pressure environment such as a response to a major incident
- **Technology and Information –** outdated, untested, and non-operational equipment and records may impact the effectiveness of the incident response with time required to fix or replace equipment instead of managing the incident and / or force reliance on personal non-approved devices with increased risk of data breaches.

Recommendations and Management Action Plan: Incident Response and On-Call Arrangements

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
4.1	The definition of what the Council considers a 'resilience incident' should be reviewed, agreed and relevant documents updated to include examples and increase clarity in the incident escalation process. Updated documents should be communicated to relevant officers and the examples of incidents included in training materials.	Defining a Resilience Incident will be prepared in consultation with CLT to ensure the support that follows as part of the resourcing for Resilience matches expectations. The definition will be included in the report referenced at 1.1.	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience	31/01/2026
4.2	On call arrangements for the Resilience Team should be reviewed with consideration of a formal on-call rota and associated remuneration arrangements are in place to ensure that other colleagues involved in incident response and escalation have clarity as to who to contact.	A phased implementation approach will be adopted to ensure that detailed management actions which address the findings and recommendations are developed. Management actions and implementation dates will be provided to Internal Audit by 31 January 2026.	N/A	N/A	N/A
4.3	The Council should review the on-call arrangements for teams involved in the out of hours resilience incident escalation and response process including the Chief Officer on-call arrangements. This should include consideration of the use of the strategic, tactical and operational hierarchy to				

	implement appropriate arrangements aligned to the size, nature and complexity of the Council and to ensure effective resilience incident responses.				
4.4	The Council should undertake a review of the CICC to determine the future requirements for use. If the CICC will not be retained, then clear arrangements to ensure a fit for purpose on-site incident coordination centre can be stood up quickly for incident events where physical coordination, secure access, and public safety is required.	The Resilience Team will carry out a review of the CICC, taking input from CLT and reporting to CLT with the report outcome and recommendations.	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience	31/03/2026
4.5	If the CICC is to be retained, it should be upgraded and maintained to a useable standard including disposing of redundant technology, files and boxes to clear both desk and floor space. In addition, technology and equipment should be updated to ensure that it is secure, fit for purpose and in good working order. This should include Wi-Fi and integration with key systems.	Head of Health, Safety, Risk and Resilience to oversee any upgrade in line with agreed requirement from CLT and will put in place the necessary arrangements to ensure it is operationally ready at all times. This will be reported to CRG and CLT as part of future reporting on organisational resilience preparedness.	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience	31/03/2026
4.6	An inventory of the plant and equipment in the CICC should be created and maintained. Testing of the equipment in the CICC should be undertaken on a regular basis to ensure it remains operational and fit for purpose for use during an incident. A schedule for testing should be documented in the CICC Operations Guide and the results of the tests recorded in an equipment testing log with any issues reported to the Corporate Property Helpdesk or IT helpdesk to ensure timely and effective resolution.	The Resilience Team will establish an inventory list and set out appropriate testing regimes to ensure facility and equipment are fully operational at all times. This will be included in the CICC Operations Manual.	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience	30/04/2026
4.7	A process should be established to ensure that current hard copy versions of the relevant Council's policies, protocols and frameworks are stored securely within the CICC. Appropriate records	The Resilience Team will put in place secure copies of policies, plans, protocols and frameworks within the CICC and review periodically to ensure	Corporate Director of Customer &	Head of Health Safety, Risk & Resilience	31/10/2025

	management arrangements should be put in place for destruction of previous copies and any related sensitive or personal data.	an up-to-date set of arrangements are maintained.	Corporate Services		

Finding 5 – Debriefs and Lessons Learned

Finding Rating	Medium Priority

Incident Debriefs

The Incident Debrief Template and Guidance includes both a debrief template that colleagues should use following an incident debrief, and guidance for undertaking these debriefs. The Guidance was last reviewed in January 2022. The Resilience Team advised that capacity and resourcing has been an issue, however not every document requires regular review.

The requirement for a debrief following a resilience incident is decided on a case-by-case basis by the Council Resilience Group (CRG). There is no clear criteria to determine whether a debrief should be completed at either the corporate or directorate level. The guidance states the debrief of an incident that affects only one directorate should be discussed at CRG within six weeks of the incident taking place, however there is no set timescales for an incident that affects more than one directorate, including when a debrief should be undertaken, or when a debrief report should be circulated.

The Resilience Team maintains an Incident Log for resilience incidents. Between January 2024 and June 2025, 12 resilience incidents recorded:

- 5 incidents required a debrief; 3 were completed but formal reports were produced for two
- significant delays were noted between the incident and the debrief being held – a debrief of an incident in May 2024 was held in March 2025, and a debrief for an incident in January 2025 in March 2025, with the formal debrief report circulated in June 2025
- 2 incidents in March and May 2024 are not fully recorded in the Incident Log with a status of 'update required'.

The Directorate advised that updates for both incidents were provided to the Resilience Team by email in January 2025. The delay in holding incident debriefs and updating the Incident Log indicate communication and working arrangements require improvement and that the CRG meetings should include monitoring of debrief completions and associated reporting.

Action Tracking

The Incident Debrief Template states that all corporate action points will be captured and monitored by the Resilience Team, and that the directorates will be responsible for the capture and monitoring of any actions relevant to them. Actions resulting from incidents that affect more than one directorate or are the responsibility of the Resilience Team should be added to the CRG Decision Log. For the five incidents that required an audit debrief:

- 1 of 3 debriefs had the respective actions recorded on the CRG's Action Decision Log
- no actions from the January 2025 incident are recorded on the Decision Log. The Resilience Team advised the debrief report was circulated in June 2025, and there had been no CRG meeting in the interim.

The March 2025 incident lists 5 actions, 3 of which are assigned to the Resilience Team; however, these actions have not been added to the Decision Log. The Resilience Team advised they have not been added as they have not received a formal debrief report from the directorate. The Resilience Coordinator for the directorate advised a formal debrief report was completed, however it was not provided to the Resilience Team, and the Operations Manager was not aware of the requirement to provide the debrief report.

Risks

- **Resilience –** delays in completing incident debriefs can reduce the ability to recall events accurately and can undermine the seriousness of the incident, and in addition early warning signs or issues that may impact another system or service may not be identified and communicated
- **Governance and Decision Making –** failure to capture and monitor actions arising from debriefs may lead to a lack of accountability, repeat failures, and a failure to embed changes in practice.

Recommendations and Management Action Plan: Debriefs and Lessons Learned

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
5.1	The Incident Debrief Template should be reviewed to include: • a clear criteria to determine whether a debrief should be completed at either the corporate or directorate level • a defined period for completion of an incident debriefs after an incident takes place • a timeframe for discussion of debriefs at CRG when incidents affect one directorate • a timescale for producing and circulating a debrief report to relevant stakeholders should be agreed • guidance on who should attend incident debriefs • requirement for adding actions to the CRG Action Decision Log. Once agreed, the requirements should be communicated and adherence to the requirements monitored regularly by the Resilience Team and the CRG. A regular review schedule should be established for the Incident Debrief Template and added to the Resilience Plans and Protocols Review Schedule.	The Resilience Team will review the current debrief form in consultation with the Council Resilience Group. This will be complemented by the development of a guide setting out how to conduct debriefs and a guide timescale to complete and report. The guide will outline how actions should be tracked by Council or Directorate. The CRG will review the Incident Debrief Template and guidance thereafter as part of a rolling work programme.	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience	31/03/2026
5.2	The Corporate Resilience Incident Log should be updated regularly following incidents and debriefs, and it should be a standing agenda item at all CRG meetings.	Corporate Resilience Incident Log to be added as standing item to all CRG meetings.	Corporate Director of Customer & Corporate Services	Head of Health, Safety, Risk & Resilience Corporate Resilience Manager Senior Resilience Specialist	31/01/2026
5.3	Debrief actions should be consistently recorded, and completion monitored with clear ownership and timescales to ensure completion and embed required changes in practice.	The debrief guide will outline how actions should be tracked where Council (CRG) or Directorate. As part of the standing Incident Log at CRG, the CRG will monitor the assignment of action owners,	Corporate Director of Customer & Corporate Services	Head of Health Safety, Risk & Resilience Corporate Resilience Manager	31/03/2026

		timescales to complete actions, and will use this to report on organisational learning from incidents as part of CLTs future resilience preparedness reporting.		Senior Resilience Specialist	

Appendix 1 – Control Assessment and Assurance Definitions

Control Assessment Rating		Control Design Adequacy	Control Operation Effectiveness
Well managed		Well-structured design efficiently achieves fit-for purpose control objectives	Controls consistently applied and operating at optimum level of effectiveness.
Generally Satisfactory		Sound design achieves control objectives	Controls consistently applied
Some Improvement Opportunity		Design is generally sound, with some opportunity to introduce control improvements	Conformance generally sound, with some opportunity to enhance level of conformance
Major Improvement Opportunity		Design is not optimum and may put control objectives at risk	Non-conformance may put control objectives at risk
Control Not Tested	**N/A**	Not applicable for control design assessments	Control not tested, either due to ineffective design or due to design only audit

Overall Assurance Ratings	
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

Appendix 2 – Areas of Audit Focus and Control Objectives

Audit Areas	Control Objectives
Risk Management	• risks related to organisational resilience are identified, recorded, and managed within Directorate and service risk registers, and regularly reviewed to ensure appropriate mitigating actions are in place and remain effective, with escalation to divisional and directorate level risk committees where required.
Policies, Procedures and Training	• there are up-to-date and clear policies and procedures in place for organisational resilience which include Category 1 responder requirements which are adhered to, and are reviewed, and updated, in line with the relevant legislation, requirements and guidance, and following any changes to practice • training and development requirements for officers involved in organisational resilience are clearly understood, and relevant requirements are communicated with monitoring arrangements to ensure training is completed and up to date.
Governance and Strategic Oversight	• there is a clear governance structure for Organisational resilience, with defined leadership, responsibilities, and resources • there is effective committee oversight of Organisational resilience work.
Business Continuity Planning	• each directorate has up-to-date and fit-for-purpose Business Continuity Plans that identify all priority services and set out clear recovery priorities and timelines • Business Continuity Plans are aligned to corporate resilience strategies and reviewed following major or serious incidents / at scheduled intervals • plans consider concurrent risks (e.g. loss of access to buildings, power outages affecting digital services), and mitigations are in place to ensure continuity.
Incident Response Preparedness	• the Council has a defined and tested incident response framework / suite of protocols, including emergency management roles, escalation protocols, and communication plans • relevant colleagues are trained and equipped to respond effectively to incidents, with simulations and exercises conducted to test preparedness and learn lessons • the Council Incident Coordination Centre is operational and fit-for-purpose • the Council has the capacity to respond to major incidents or serious emergencies, both within the directorates and the Corporate Resilience team. This includes out-of-hours arrangements such as evenings and weekends, and the use of rotas.
Coordination with Partners and External Stakeholders	• the Council works collaboratively with emergency services, regional resilience groups, and key service delivery partners to ensure joined-up preparedness • roles, responsibilities, and communication lines with third parties are defined, documented, and periodically tested.

Audit Areas	Control Objectives
Post-Incident Review and Continuous Improvement	• there are processes in place to capture lessons learned from incidents and exercises, and these are systematically used to improve resilience arrangements • actions arising from post-incident reviews are tracked, assigned to accountable officers, and monitored for completion.
Information Governance	• information governance risks for organisational resilience are clearly understood, and effective controls have been established to ensure adherence to relevant Council information governance policies and procedures.
Service Level Agreements and Service Standards	• where services are provided by another Council area, team or third party to support organisational resilience, there is a service level agreement in place which sets out the types or services provided, relevant service requirements, timescales, and performance requirements.