•EDINBVRGH•
THE CITY OF EDINBURGH COUNCIL

Internal Audit Report Draft

CGI Incident Response

9 July 2025

CS2402

Overall Assessment	**Reasonable Assurance**

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2024/25 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2024. 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 sound system of governance, risk management and control over how CGI design and deliver incident response capability for the Council. This includes clearly defined roles and responsibilities for CGI and the Council, with processes and procedures for incident escalation, resolution, risk management and service improvement. However, the following areas for improvement were identified, which will further strengthen the control framework and support the achievement of an effective incident response process for the Council.

One medium priority, two low priority and one advisory finding were identified:

- the CGI Service Continuity Plan, which is the overarching IT Disaster Recovery plan for Council services requires updating and approving by both parties
- incident closure procedures that would govern the closure of incidents impacting Council services should be defined and documented
- the CGI Incident Communications Plan should be updated to reflect current tools, technologies and processes
- the source of risks, which aids effective risk analysis, should be recorded in the joint Council/CGI Risks, Actions, Issues, Dependencies (RAID) log.

Areas of effective practice

- there is a defined operational framework structure which defines the scope of incident response and sets out roles and responsibilities for both CGI and the Council
- there are processes between CGI and the Council for identifying service improvement opportunities, including regular service reviews, analysis of trends and feedback from end-users.

Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
1. Disaster Recovery planning	🟢	🟠	Finding 1 - Outdated Service Continuity Plan	Medium Priority
2. Incident Response Lifecycle	🟠	🟠	Finding 2 - Incident Closure procedures not documented	Low Priority
3. Incident Response Lifecycle	🟢	🟠	Finding 3 - Review of Incident Communication Plan	Low Priority
4. Risk Management	🟢	🟢	Finding 4 - Recording risk source in RAID logs	Advisory

See Appendix 1 for Control Assessment and Assurance Definitions

Background and Scope

The Council depends on CGI for the provision of managed IT services, encompassing critical systems that underpin daily operations and citizen services. This dependence makes it essential for CGI to have a robust and effective Incident Response plan for services provided to the Council. In the event of service disruptions which may include cyberattacks or technical failures within the scope of services supported by CGI, a well-defined plan helps to achieve minimal downtime, swift recovery, and the protection of sensitive and business critical data. It enables the Council to maintain business continuity, preserve public trust, and fulfil its obligations to citizens by minimising the impact of any IT incidents originating from CGI.

The importance of comprehensive CGI Incident Response processes and supporting documentation is essential due to the business-critical nature of the Council's IT environment. Handling sensitive citizen data, managing critical infrastructure, and ensuring a proactive approach to maintaining a stable environment. Both parties must have a thorough understanding of their assigned actions and accountabilities during an incident. This shared understanding, facilitated by a well-structured incident response plan, supports efficient communication, streamlined escalation procedures, and a more effective and coordinated response to any IT incidents that may arise.

Scope

The objective of this internal audit was to assess the adequacy of design and operating effectiveness of the CGI Incident Response processes for the Council including lifecycle, governance and oversight and evidence of adequate testing/exercising of the plan. This involved:

- evaluating the adequacy and effectiveness of the key controls established within CGI’s plans, processes and procedures established to respond to service disruptions impacting the Council systems and services.
- reviewing the CGI incident response plan lifecycle, including incident escalation, incident diagnosis, resolution and incident closure.
- reviewing the CGI post-incident processes to evaluate how they identify lessons learned and drive continual service improvement.

Audit sample testing covered the period 31 January 2024 to 28 February 2025.

Alignment to risk and Business Plan Outcomes

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

- Resilience
- Technology and Information
- Supplier, Contractor, and Partnership Management
- Service Delivery
- Reputational Risk

Business Plan Outcomes:

- the Council has the capacity, skills, and resources to deliver our priorities efficiently, effectively and at lower cost
- people can access public services locally and digitally, in ways that meet their needs and expectations, contributing to a greener net zero city.

Limitations of Scope

The following areas were excluded from scope:

- physical security controls at CGI’s facilities or the Council’s premises
- ITIL practices of problem management, change management, knowledge management or service level management
- technical testing of the Disaster Recovery plan or review of ITDR test outcomes, as such no assurance was provided on the design, coverage, effectiveness, management testing or viability of identified Disaster Recovery plans
- vulnerability management and patching controls
- incident response capabilities of CGI’s third-party vendor
- major cyber incident response plans or their testing.

Reporting Date

Audit work concluded on 2 July 2025, and the findings and opinions are based on the conclusion of work at that date.

Findings and Management Action Plan

Finding 1 - Outdated Service Continuity Plan

Finding Rating	Medium Priority

CGI's Service Continuity Plan (SCP), which serves as the overarching IT Disaster Recovery plan for the Council, is outdated. The current draft version has remained in draft form since June 2024, with unresolved comments regarding CGI's responsibilities, missing contact details for the Council and disagreement over the length of time for review periods. These disagreements have been escalated to CGI senior management but remain unresolved in April 2025. The last approved version is outdated having been signed off in August 2022.

CGI design and deliver service continuity through an integrated framework of service level continuity plans and procedures which are governed by the SCP. The SCP sets out CGI's obligations and approach to service continuity and IT disaster recovery for the council. Complete and up-to-date planning documentation, as represented by the SCP, is integral in preparing and executing an effective disaster recovery response.

The SCP requires regular review and updates to confirm the information is valid and agreed between both CGI and the Council. The Council has proposed changing the review period from every six months to annually, but this change has not been agreed by CGI and remains an outstanding comment on the unapproved draft.

Two key appendixes were also omitted from the SCP potentially impacting the SCPs effectiveness and alignment with contractual obligations in a disaster scenario.

Discussions over review frequency, combined with the protracted review and approval process for the draft version itself, highlights an opportunity to improve communication and collaboration between CGI and the Council, and to establish a mutually agreed and timely review cycle for the SCP.

Risks

- **Resilience:** in a disaster scenario, relying on outdated information can lead to ineffective recovery efforts, prolonged service disruptions, and potential data loss.
- **Technology and Information:** critical systems may be overlooked during recovery, resulting in further delays and potential data integrity issues and the lack of up-to-date information may hinder effective prioritisation and resource allocation during a disaster.
- **Supplier, Contractor, and Partnership Management:** the protracted review and approval process for the SCP draft could erode trust and create tension, impacting the overall effectiveness of the partnership.
- **Service Delivery:** relying on outdated information can delay service restoration, impacting end-users and potentially causing significant disruption to the council's operations.
- **Reputational:** Prolonged service disruptions, data loss, and perceived lack of preparedness can erode public trust and confidence.

Recommendations and Management Action Plan: Outdated Service Continuity Plan

Ref.	Recommendation	Agreed Management Action	Action Owners	Lead Officers	Timeframe
1.1	CGI and Digital Services should finalise and approve the SCP (v2.1), resolving all	CGI will provide CEC Digital Services with a final SCP for approval.	Director Consulting Delivery, CGI	CGI Senior Service Delivery Manager	31/12/2025

Ref.	Recommendation	Agreed Management Action	Action Owners	Lead Officers	Timeframe
	open comments, including agreement of the review frequency. CGI and Digital Services should establish a robust review and update process, ensuring regular reviews at the agreed-upon frequency, timely resolution of comments, and effective version control.	The SCP will then be subject to annual review (as opposed to bi-annual) and follow the review guidelines as stated in SP8.6 of The Agreement.	Executive Director, Corporate Services, CEC	Service Director, Customer and Digital Services, CEC Chief Digital Officer, CEC ICT Senior Manager – Commercial, CEC ICT Commercial and Lead Risk Officer, CEC Technical Architect, CEC	

Finding 2 - Incident Closure procedures not documented

Finding Rating	Low Priority

There is no documented process to govern incident closure procedures between CGI and the Council. Management advised that a standard practice is followed, but the lack of defined and documented processes deviates from ITIL best practice to which CGI align, which emphasises the importance of defined processes for all stages on the incident lifecycle. This lack of a documented process creates ambiguity around incident closure criteria and procedures.

Inconsistencies in incident reporting have emerged due to this ambiguity. These include discrepancies between actual and reported resolution times, e.g.an NEC housing incident remained 'open' for an additional 16 hours after service resolution, and delays in incident report production with two of the sample of three incidents missing supplementary performance targets.

In addition, the current process communicates incident closure decisions by Microsoft Teams chat, which functions effectively in practice but does not provide a robust audit trail of decisions made. Incident close records from ServiceNow do not capture these discussions or the rationale behind closure decisions, including any agreed-upon monitoring periods which are determined ad-hoc based on the nature of the incident. Defining this process, including recording of joint incident management calls and the decisions made e.g. monitoring periods, incident closure agreement, in the incident records would provide an audit trail of decisions made.

Risks

- **Service Delivery** – delays in incident report production, as observed in the sample testing, and incomplete documentation hinder accurate performance reporting and service improvement efforts, ultimately impacting service delivery quality and transparency. The lack of documented joint calls further obscures communication and decision-making related to incident closure.
- **Resilience** - incomplete or inconsistent closure procedures increase the risk of recurring incidents and hinder effective problem management, potentially impacting service stability and resilience.
- **Supplier, Contractor and Partnership Management** - the lack of a documented process, coupled with inconsistent reporting e.g. discrepancies in resolution times as observed in the NEC housing incident, can erode trust and create tension between CGI and the Council, impacting the effectiveness of the partnership. This may create ambiguity around SLA adherence.

Recommendations and Management Action Plan: Incident Closure procedures not documented

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
2.1	CGI should define and document its incident closure procedures, aligning them with ITIL best practice. These should be agreed with the council and added to the Operational Framework Document.	CGI will update the Operational Framework Document (OFD) to reflect the current Incident Closure process in place and refer to any specific further documentation that is applicable. CGI will work with CEC Digital Services for the additional information to be approved (not the whole OFD).	Director Consulting Delivery, CGI Executive Director, Corporate Services, CEC	CGI Senior Service Delivery Manager Service Director, Customer and Digital Services, CEC Chief Digital Officer, CEC ICT Senior Manager – Commercial, CEC ICT Commercial and Lead Risk Officer, CEC	31/12/2025

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
				Digital Services, Relations & Service Manager, CEC	
2.2	CGI and CEC Digital Services should implement a process for documenting joint incident management calls with the council including key decisions and any agreed-upon actions.	CGI will update the Operational Framework Document (OFD) to confirm, where applicable, CGI or CEC Digital Services will agree one or both parties to document joint incident management calls, noting a high-level summary of key decisions and agreed upon actions. CGI will work with CEC Digital Services for the additional information to be approved (not the whole OFD).	Director Consulting Delivery, CGI Executive Director, Corporate Services, CEC	CGI Senior Service Delivery Manager Service Director, Customer and Digital Services, CEC Chief Digital Officer, CEC ICT Senior Manager – Commercial, CEC ICT Commercial and Lead Risk Officer, CEC Digital Services, Relations & Service Manager, CEC	31/12/2025

Finding Rating	Low Priority

Finding 3 – Review of Incident Communication Plan

CGI's Incident Communications Plan for the council is outdated, not having been reviewed since 2018. The plan makes references to Remedy ITSM, a tool no longer in use by CGI which suggests potential inaccuracies in the plan. The outdated state of the plan is due to a lack of regular review and update processes in CGI.

Effective incident communication requires a current and accurate communication plan that reflects current systems, processes, and contact information. Regular reviews are essential to validate the plan's ongoing relevance.

The outdated plan, referencing obsolete systems and potentially inaccurate contact information, increases the risk of ineffective communication during incidents. This can hinder timely escalation and resolution, potentially impacting service restoration for the council.

Risks

- **Service Delivery -** the outdated plan, with its reference to obsolete systems and potentially inaccurate contact information, increases the risk of ineffective communication during incidents. This could hinder timely escalation and resolution, potentially impacting service restoration and disrupting service delivery to the council.
- **Reputational** ineffective communication during incidents, stemming from an outdated plan, can damage both CGI's and the council's reputation. Delays in incident resolution and perceived lack of communication can erode trust and confidence among end-users.

Recommendations and Management Action Plan: Review of Incident Communication Plan

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
3.1	CGI should review and update the Incident Communication plan making sure it reflects current tools, technologies and processes. A regular review schedule should be established to prevent future obsolescence.	CGI will review and update the Communication plan and get internal approval of the document. This will then be subject to annual review.	Director Consulting Delivery, CGI Executive Director, Corporate Services, CEC	CGI Senior Service Delivery Manager Service Director, Customer and Digital Services, CEC Chief Digital Officer, CEC ICT Senior Manager – Commercial, CEC ICT Commercial and Lead Risk Officer, CEC Digital Services, Relations & Service Manager, CEC	30/09/2025

Finding 4 – Recording risk source in RAID logs

Finding Rating	Advisory

The Joint CGI/Council RAID log does not record the source of the risk; it only lists the cause of identified risks.

Effective risk management benefits from documenting both the source and cause of risks, providing a more comprehensive understanding of the risk landscape and enabling more targeted mitigation efforts. The source of a risk is the underlying factor that creates the potential for risk, while the cause of a risk is the specific event or action to trigger the risk to actually occur.

The absence of documented sources provides an opportunity to enhance CGI's risk identification and documentation practices.

The practice of recording the cause provides valuable information, but omitting the source limits the comprehensiveness of risk understanding and may hinder the development of fully targeted mitigation strategies. This may impact the effectiveness of risk monitoring and control design.

Recommendations: Recording risk source in RAID logs

Ref.	Recommendation
4.1	CGI should update its risk documentation practices making sure that both the source and cause of all identified risks are recorded in the Joint RAID log.

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 exist, 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
Incident Response Lifecycle	• CGI has documented incident response policy and procedures, with clear roles and responsibilities for CGI and the Council. • CGI has established incident escalation procedures ensuring alignment with agreed-upon communication channels. • CGI has processes for investigating and diagnosing major incidents to restore service within agreed SLAs. Post-incident reviews are conducted in collaboration with the Council to capture lessons learned, identify service improvement opportunities, and, where appropriate, instigate Problem Management processes to undertake root cause analysis. • CGI have established procedures for implementing resolutions and restoring services within SLAs, ensuring the Council is informed of progress and impacts in line with SLAs. • CGI have established incident closure procedures, including verification of resolution with the Council, documentation, and communication of closure to relevant stakeholders. • Post-incident reviews for major incidents, involving both CGI and the Council are conducted to identify lessons learned and drive service improvements for both parties.
Continual Improvement	• CGI and the Council have processes for identifying opportunities to improve service performance and identify and remediate recurrent problems, implementing corrective actions to drive service improvements.
Risk Management	• Risks related to CGI Incident Response are identified, recorded and managed within the Digital Services and CGI risk register, and regularly reviewed to ensure appropriate mitigating actions are in place and remain effective, with escalation to appropriate risk committees where required.
Disaster recovery planning	• CGI has established a Disaster Recovery Plan, and there is evidence that this plan exists and is subject to documented reviews. Where an incident requires activation of the Disaster Recovery Plan, CGI has a mechanism to enact it as part of the Incident response process. • The audit did not assess the effectiveness or viability of this plan or its technical testing.