

Internal Audit Report

CGI Service Stability

30 July 2025

CS2403

**Overall
Assessment**

**Substantial
Assurance**

Contents

Executive Summary 3

Findings and Management Action Plan..... 5

Appendix 1 – Control Assessment and Assurance Definitions..... 8

Appendix 2 – Areas of Audit Focus and Control Objectives 9

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

Substantial
Assurance

Engagement conclusion and summary of findings











CGI have an established service management approach in the provision of services to the Council. The approach includes defined roles and responsibilities for service management, along with processes for system availability monitoring and alerting, capacity planning, risk mitigation and problem management. However, the following areas for improvement were identified, which will further strengthen the control framework and enhance service stability for the Council.

- for non-critical services where resilience planning has not been included as a contractual obligation the High-Level Design documents (HLDs) should include documented rationale of the agreement between CGI and the Council to exclude resilience planning.
- once the Service Continuity Plan (SCP) has been approved by CGI and Digital Services, the SCP and HLDs should be reviewed to check alignment between failover capabilities.
- application availability requirements, associated KPIs and reporting mechanisms for all OBS should be reviewed and agreed by CGI and the Council.

Areas of effective practice

- there is a structured and effective service performance monitoring process that leverages automated tools like Zabbix and AI Ops.
- the integration of availability management with the change management process ensures that changes to designs and requirements are properly managed and assessed for their impact on availability. This controlled approach minimises the risk of unplanned outages.
- a structured problem management framework, including formalised Root Cause Analysis (RCA), ensures thorough investigation of problems, documented root cause identification where provided, and effective remediation.
- regular Problem Review Boards with the Council provide transparency over problems and facilitate continuous improvement in service stability.
- there is integration of capacity planning in the change management process which ensures capacity requirement are considered whenever changes are implemented, which seeks to address any risks of shortage of resources.
- there are regular, collaborative review meetings between the Council and CGI to discuss ongoing performance, problem identification and management, trend analysis and continuous improvement opportunities.

Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
1. Monitoring and Alerting			Finding 2 – Application Availability Requirements and Reporting	Low Priority
2. Problem Management			No issues noted	N/A
3. Risk Management			No issues noted	N/A
4. Capacity Management			No issues noted	N/A
5. CGI - Availability Management			Finding 1 – Resilience Documentation	Low Priority

Background and Scope

The City of Edinburgh Council (the Council) relies on CGI for managed IT services encompassing critical systems that underpin daily operations and citizen services. This dependency makes it essential for CGI to have a robust and effective Service Management approach, defined as consistent performance at agreed levels with minimal disruption. CGI is contractually obligated to adhere to ITIL v4 best practices for IT service stability and the Council's Digital Services team retains ultimate accountability. Key ITIL-aligned processes include system availability monitoring and alerting, capacity planning, risk mitigation and problem management.

Given the sensitive citizen data and critical infrastructure involved, proactive IT service monitoring and capacity planning are essential for maintaining a stable environment. A clear understanding of roles and accountabilities between both parties is crucial for stable and effective IT service delivery.

Scope

The objective of this internal audit was to assess the adequacy of design and operating effectiveness of the CGI processes and controls in place to limit service disruptions and achieve service stability. This involved:

- evaluating the adequacy and effectiveness of the key controls established within CGI's processes and procedures to monitor, detect and limit service disruptions impacting the Council systems and services and resolve recurrent problems to improve service stability
- evaluating the adequacy and effectiveness of the key controls defined to capture and reflect on lessons learned, to analyse and identify the root cause of service outages to reduce future occurrences
- reviewing the CGI capacity planning lifecycle and service availability management controls, including any controls embedded in systems architecture design processes to achieve sufficient service availability.

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

Alignment to risk and Business Plan Outcomes

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

- Resilience
- Technology and Information
- Service Delivery
- Reputation
- Supplier, Contractor, and Partnership Management.

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 premises
- technical testing of DR plans or review of IT DR test outcomes, as such no assurance is provided on the design, coverage, effectiveness, management testing or viability of identified DR plans
- vulnerability management and patching controls
- incident response and recovery capabilities of CGI or third-party vendors
- major cyber incident response and recovery plans or their testing
- suitability of the specific SLAs and KPIs agreed with CGI in the contract
- specific threats to service stability for specific services, or evaluation of any defined controls to mitigate those specific risks.

Reporting Date

Testing was undertaken between 28 April and 30 May 2025.

Audit work concluded on 16 June 2025, and the findings and opinion are based on the conclusion of work at that date.

Findings and Management Action Plan

Finding 1 – Resilience Documentation

Finding Rating	Low Priority
----------------	--------------

The Joint Design Authority (JDA) process, in accordance with the JDA Terms of Reference, governs the creation and review of High-Level Design documents (HLDs) or Full Specification HLDs which address availability, Disaster Recovery (DR) and business continuity. These documents, prepared by CGI and jointly reviewed with the Council, incorporate architecture principles for various areas and cover non-functional requirements including backup, DR and business continuity. Such resilience planning is crucial for ensuring business continuity and minimising disruption from incidents. By proactively identifying potential vulnerabilities and incorporating appropriate mitigation strategies into the design phase, CGI can significantly reduce the impact of outages, data loss and other disruptive events.

Documentation inconsistencies were identified in the following areas, potentially impacting the effectiveness of resilience and recovery efforts:

- The Service Continuity Plan (SCP), which serves as the overarching IT DR plan for the Council, is outdated. The current version has remained in draft form since June 2024. The last approved version was signed off in August 2022. This issue was also identified in the CGI Incident Response Internal Audit completed in June 2025. As a result of the outdated SCP, CGI are unable to verify how failover capabilities defined in individual HLDs align with the overall DR strategy for the Council.

- In addition, for non-critical services (e.g. the provision of residential Wi-Fi), where resilience planning has not been included as a contractual obligation, the HLD's do not include a documented rationale for excluding resilience planning. Without this justification, it is unclear if exclusions are based on a thorough risk assessment.

Risks

- **Resilience:** the lack of resilience planning for services provided by CGI to the Council may result in unexpected service disruptions and extended recovery times. An outdated SCP further heightens this risk by hindering a complete understanding of failover capabilities.
- **Service Delivery:** gaps in resilience and DR planning, stemming from the outdated SCP and a lack of clear alignment between continuity measures and business requirements, may impact service availability and performance, resulting in non-compliance with contractual availability obligations and ITIL 4 best practices. This could lead to ineffective recovery strategies and delayed response to incidents.
- **Supplier, Contractor, and Partnership Management:** incomplete documentation makes it difficult for the Council to assess CGI's adherence to contractual obligations regarding service availability and DR.

Recommendations and Management Action Plan: – Update of Resilience Documentation

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
1.1	For services considered non-critical and where there is no contractual requirement for a resilience plan, Digital Services and CGI are agreed that CGI should make sure	CGI will update the High-Level Design (HLD) documentation template to include a mandatory 'Resilience' section. This section must capture one of the following:	Corporate Director, Customer and Corporate Services, CEC Director Consulting Delivery, CGI	CGI Enterprise Architect Chief Digital Officer, CEC ICT Senior Manager – Commercial, CEC	31/12/2025

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
	any future HLDs include the rationale for the exclusion of this.	<ul style="list-style-type: none"> A summary of the resilience approach included in the design (e.g. DR, HA, failover mechanisms), or Where resilience is not included, a rationale explaining its exclusion will be included in the HLD. <p>Future HLDs will use this documentation template for incorporation when a HLD is developed as part of a project.</p>		<p>ICT Commercial and Lead Risk Officer, CEC</p> <p>Digital Services, Technical Architect, CEC</p>	
1.2	Once the SCP has been approved by CGI and Digital Services, both parties are agreed that any future SCP and HLD's should be reviewed to check alignment between failover capabilities.	The SCP has now been reviewed and approved. CGI will review all new HLDs to assess and document alignment with the SCP. Where gaps are identified, these will be highlighted in the HLD as a risk in accordance with the Risk Management process. This guidance will be added to the HLD template.	<p>Corporate Director, Customer and Corporate Services, CEC</p> <p>Director Consulting Delivery, CGI</p>	<p>CGI Enterprise Architect</p> <p>Chief Digital Officer, CEC</p> <p>ICT Senior Manager – Commercial, CEC</p> <p>ICT Commercial and Lead Risk Officer, CEC</p> <p>Digital Services, Technical Architect, CEC</p>	31/12/2025

Finding 2 – Application Availability Requirements and Reporting

Finding Rating

Low Priority

CGI is responsible for ensuring the availability of Output Based Specifications (OBS) for the Council, using automated tooling such as Zabbix and AI OPS, and reporting this data in the monthly Client Service Review (CSR). The CSR compares the target and actual achieved availability, including Key Performance Indicators (KPI), and provides trend analysis. These reports are jointly reviewed by the Council and CGI in monthly meetings.

A review of a sample of Priority 1 OBSs identified that the CSR does not include reporting over OBS - 316 (HR and Payroll). This is due to a hosting change (from on premise to Oracle). Availability reporting against the Oracle HR and Payroll application is now provided to the Council separately, by email. Similar reporting mechanisms exist for other applications following technology changes.

Digital Services have informed Internal Audit that the Council is content with these reporting arrangements. CGI and the Council intend to review application availability requirements, associated KPIs and reporting mechanisms during the contract review in 2029. However, completing the review earlier will result in consistent tracking and reporting of OBS, highlighting availability issues and proactive problem-solving and service improvement.





Risks

- **Technology and Information:** Outdated application availability requirements, associated KPIs, and reporting mechanisms pose a risk to the overall effectiveness and accuracy of the technology and information systems used for monitoring and reporting.
- **Supplier, Contractor, and Partnership Management:** The delay in reviewing application availability requirements, KPIs, and reporting mechanisms until 2029, increases the risk of inconsistencies in monitoring and reporting going undetected.

Recommendations and Management Action Plan: Application Availability Requirements and Reporting

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
2.1	Application availability requirements, associated KPIs and reporting mechanisms for all OBS should be reviewed and agreed by CGI and the Council.	CEC Digital Services intend to complete a full review of application availability requirements, associated KPIs and reporting mechanisms during the contract review in 2029. However, this does not impact the Council's ability to review and revise KPIs at any time prior to then which is done and will continue to be done through the current change process with CGI.	Corporate Director, Customer and Corporate Services, CEC Director Consulting Delivery, CGI	Director Consulting Delivery, CGI Chief Digital Officer, CEC ICT Senior Manager – Commercial, CEC ICT Commercial and Lead Risk Officer, CEC Digital Services, Relations & Service Manager, CEC	31/03/2029

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
Monitoring and Alerting	<ul style="list-style-type: none"> • Documented availability requirements are in place for critical services provided by CGI to the Council, and these are monitored to ensure requirements are consistently met. • The Council receives assurance from CGI that service and event monitoring is in place to identify potential issues before they impact stability of CGI provisioned services in line with the contract. • The Council receives assurance from CGI that appropriately configured alerts are in place, which are supported by documented escalation and response procedures for CGI provisioned services.
Problem Management	<ul style="list-style-type: none"> • A structured problem management framework is in place to identify, track, and resolve recurring issues to CGI provisioned services. • The Council receives assurance from CGI that processes are implemented and operating to perform root cause analysis and implement solutions to identified problems. • Lessons learned from stability issues are documented and integrated into operational processes, and this is tracked through to completion.
Risk Management	<ul style="list-style-type: none"> • Risks related to service stability 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.
Capacity Management	<ul style="list-style-type: none"> • Documented capacity plans are in place to maintain sufficient resources for current and future service demand, supporting stability. • CGI can demonstrate that defined thresholds are in place to pre-empt and address potential capacity issues.
CGI – Availability Management	<ul style="list-style-type: none"> • CGI can demonstrate that system and application architectures are designed and implemented with redundancy and failover mechanisms to enhance stability and meet the documented availability requirements in line with the contract (validated for a sample of applications only).