EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Internal Audit Report

CGI Technology Risk Management

29 May 2023

CS2206

Overall Assessment	**Reasonable Assurance**

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2022/23 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2022. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

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

Although there are 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**

Overall opinion and summary of findings

Whilst control weaknesses were identified in the CGI technology risk management process, the design and effectiveness of the control environment provides reasonable assurance that risks are being managed.

The following improvement actions which should enhance the process have been identified:

- risk management framework – the end-to-end CGI technology risk management process is not contained within a single document which comprehensively details the approach taken and the process to be followed throughout.
- escalation process – the escalation process is unclear, during testing we were unable to see clear evidence of escalation of high risks to Board meetings.
- reconciliation of operational to overall risk logs: review and comparison of extracts of risks found that some of the risks were appearing in one log extract and not in the other. This was due to categorising the risk IDs to the wrong portfolios, with no reconciliations conducted to ensure accuracy.

Areas of good practice identified

- while there is a lack of an end to end documented process testing confirmed that risks are recorded, tracked, and managed in a logical manner with appropriate scrutiny
- the nature of risks considered are appropriate and includes operational technology, third party, change management, regulatory and compliance, and any other risks associated with CGI services that could potentially impact the Council
- Council risks are appropriately segregated from other client risks within the risk management system (RiskIT) operated by CGI. The RiskIT system contains comprehensive risk information which is updated on an ongoing basis by risk owners
- regular meetings are established between Digital Services and CGI to review and evaluate technology risks.

See Appendix 1 for Control Assessment and Assurance Definitions

Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
1. Risk Methodology and Governance	🔴	🟡	Finding 1 – Risk management framework	High priority
			Finding 2 – Escalation and review process	Medium priority
			Finding 3 – Reconciliation and tagging of risks	Low priority
2. Risk Identification and Evaluation	🟢	🟢	Linked to Finding 3 – Reconciliation and tagging of risks	Low priority
3. Risk Response	🟢	🟢	Linked to Finding 2 – Escalation and review process	Medium priority

Background and Scope

Technology risk management is the application of an enterprise's risk management methodology / framework to identify, assess, record, and manage its technology risks.

Technology risk is an important business risk that arises due to an organisation's adoption, ownership, use and operation of technology hardware, software or processes. For the majority of organisations, the impact of technology is pervasive as it is an enabler for growth, innovation and transformation, in addition to supporting ongoing service delivery.

Consequently, effective technology risk management is vital to ensuring that the Council can effectively deliver services and achieve its strategic objectives.

The Council's technology partner CGI manages and maintains the Council's three established technology networks (Corporate, Learning and Teaching, and Peoples Network) with support from external sub-contractors where required. CGI also supports technology change across the Council.

Schedule Part 8.1, Governance, of the contract between the Council and CGI defines CGI's responsibility to manage risks with appropriate input from the Council and to be reviewed by both parties at the Joint Risk Review Board. CGI captures and records its own IT related risks, that pertains to their own organisation and the risks they share with the Council using a bespoke tool (RiskIT), which supports extraction of any relevant Council risks (such as Security management, Business Continuity and Disaster Recovery) for discussion and review with Digital Services.

CGI also conducts a monthly Joint Risk Review Board with Digital Services to discuss technology risks impacting the Council, ensure visibility of actions to mitigate and / or manage these risks (including risk transference and risk acceptance where appropriate), and support escalation of any significant risks through the Council's established risk management structure.

Scope

The objective of this review was to assess the adequacy and effectiveness of controls established by CGI to ensure effective identification, assessment, recording, and ongoing management of technology risks that could potentially impact the Council, and their alignment with the CGI risk management responsibilities as detailed in the current contract.

This included assessment of the appropriateness of established governance and reporting mechanisms to provide the Council with oversight and assurance that these risks are being monitored and mitigated. Processes established for risk transference and risk acceptance were also considered.

Risks

- strategic delivery
- technology and information
- service delivery

Limitations of Scope

The following areas were excluded from scope:

- The Council's wider risk management framework and activities, including alignment to the Council's risk appetite statement.
- Technology risks associated with IT outwith the CGI contract including all shadow IT.

Reporting Date

Testing was undertaken between 11 October 2022 and 24 March 2023.

Our audit work concluded on 24 March 2023, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Risk management framework

Finding Rating	High priority

As part of the audit, the following documents which relate to the risk management process were reviewed:

1. Induction Risk slides
2. Risks and Issues Management Plan (2015)
3. Slide deck - Risk and Issues Management Joint review process (22 April 2021)
4. CGI Partnership Governance Model (1 February 2023)

From this review, it was difficult to comprehend the overall approach for IT Risk Management with no comprehensive guide on how risks would be extracted from RiskIT and the absence of a methodology to be followed to ensure tracking of risks and their mitigating actions in a consistent way.

The disjointed nature of the documents highlighted the following gaps:

- the matrix for scoring the risks is used for all solutions, is not limited to projects, and is based on CGI's Risk Management Methodology. From the inspection of Appendix B of the Risks and Issues Management Plan it clearly states under one (Time) of the Impact criteria that it is Project related and therefore it is unclear, how it relates to Service risks
- timeframes for completing mitigating actions at the various RAG statuses are not included in documents (II) and (III), CGI indicated that closure dates are established for each individual risk, however, the risk reports reviewed did not contain timeframes/closure dates and we were therefore unable to determine if actions were monitored to ensure timely completion
- it was noted that some abbreviations are used on register IDs such as NI, VM, AM, WR and it was not always clear what these referred to. Digital Services colleagues advised, that while there is a guide tab for Risk ID codes within the shared RAID log, it is not consistently kept up to date.

The RiskIT *Shared RAID log* report contains a weekly process sign off sheet, in the *Risk Management Process tab* of the log spreadsheet, which was not completed in the two versions of the log we received. CGI advised that completion of this tab is no longer part of the risk management process, and the sheet should be deleted from the log in future.

Risks

Strategic Delivery / Technology and information – absence of a risk management methodology may prevent consistent and effective technology risk management.

Recommendations and Management Action Plan: Risk management framework

Ref.	Recommendation	Agreed Management Action	Action Owners	Lead Officers	Timeframe
1.1	The current Risk and Issues Management plan (2015) should be updated to outline the risk management framework with the end-to-end process for managing IT risk for CEC and should be communicated to Digital Services. This should serve as a single source of	CGI will update the Risk and Issue Management plan covering all elements contained in the audit recommendation.	Deborah Smart, Executive Director of Corporate Services (CEC) Nicola Harvey, Service Director	Innes Davidson, Director of Delivery (Applications), (CGI) Heather Robb, Chief Digital Officer (CEC)	31/10/2023

	guidance for the management of risks, to be comprehensive and include: • a matrix which applies to all types of risk • indicative timeframes for completing mitigating actions • guidance on how to populate the 'Management Summary column' to include enough details in providing reasons on the various factors that may be causing a delay to mitigate that risk with indicative timeline (if possible). • the escalation process (see recommendation 2.2) • the risk categorisation reconciliation (see recommendation 3.2) • all relevant definitions		Customer and Digital Services (CEC) Mark Bulmer, Vice President Consulting Services (CGI)	Alison Roarty, Digital Services Commercial & Risk Lead (CEC) Jackie Galloway, Senior Manager – Commercial (CEC)	

Finding 2 – Escalation and review processes

Finding Rating	Medium Priority

The CGI Partnership Governance Model (1 February 2023) indicates that the monthly Partnership Board should undertake '*Review of highest rated risks and mitigations and overall joint risks'*.

Review of the Partnership Board report and minutes for January 2023 notes that whilst a set of risks (a mix of Red, Amber, and Green rated risks) were included in the report at Section 5.8 'Register detail' there is no direct reference to this section or record of a discussion within the minutes. Therefore, we are unable to conclude that the Partnership Board fulfilled is remit in relation to review of highest rated risks and mitigations.

CGI advised that escalated risks are captured and managed in the Consolidated Tracker and the monthly Partnership Board report includes a section on Risks and Issues per Service area. These sections are confirmed in the report; however, the minutes do not confirm that discussions on individual risks have taken place.

The Executive Board role includes *'Review of escalated risks from joint RAID'.* CGI advised that a classification field called 'Escalation Level within the RiskIT system was not used for the purpose of escalation to either of the Partnership, Executive Review, and Escalation Boards.

Review of the Executive Review Board meeting minutes for 15 February 2023 notes agreement to include risk management under the Audit section and that the CGI VP Account Lead will progress this. Minutes from this meeting, however, do not reference any discussion on risks, therefore we are unable to conclude if the review of escalated risks from the joint RAID log is taking place as per the remit.

The March 2023 Executive Board meeting pack includes a summary of the number of risks (sixty four service risks) by category. There is no further evidence of specific risk details being included for discussion.

Risks

Strategic Delivery / Technology and information – absence of an appropriate escalation process leading to failure to escalate to appropriate individuals or teams resulting in limited or ineffective risk response.

Recommendations and Management Action Plan: Escalation and review processes

Ref.	Recommendation	Agreed Management Action	Action Owners	Lead Officers	Timeframe
2.1	The risk management framework document at recommendation 1.1 should include details relating to the risk escalation process, specifying the rationale for escalation and the forum at which each set of escalated risks is reviewed.	Escalation process will be covered in the updated Risk and Issue Management plan.	Deborah Smart, Executive Director of Corporate Services (CEC) Nicola Harvey, Service Director	Innes Davidson, Director of Delivery (Applications), (CGI) Heather Robb, Chief Digital Officer (CEC)	31/10/2023

2.2	Board packs and associated minutes should clearly note which escalated risks have been discussed and any actions taken as a consequence.	Board packs and associated minutes will include the recommendations suggested.	Customer and Digital Services (CEC) Mark Bulmer, Vice President Consulting Services (CGI)	Alison Roarty, Digital Services Commercial & Risk Lead (CEC) Jackie Galloway, Senior Manager – Commercial (CEC)	31/12/2023

Finding 3 – Reconciliation and tagging of risks

Finding Rating	Low priority

Audit fieldwork included a review of risk reports and meeting minutes for November 2022 relating to a sample of three risk categories (service, security, and project risks).

The risk report which includes all risk categories is known as the *Account RAID log*. The risk report which is presented at the fortnightly Programme Board contains project risks and is called the *Shared RAID log*.

Comparison of the project risks in the Shared RAID log dated 1 November 2022 and the Account RAID log dated 9 November 2022 confirmed that both contained a total of 64 risks, however, 9 risks (2 Red, 4 Amber, and 3 Green) were not included in both. Four were in the Account RAID log but not in the Shared RAID log. CGI advised these were inaccurately tagged as project risks when they should have been tagged as service risks. Similarly, five were in the Shared RAID log but not in the Account RAID log. CGI advised they had been inaccurately tagged as service risks when they should have been tagged as project risks, which had been caused by an overwrite of formula cells in the report spreadsheets.

Other differences noted between the two reports were accounted for by the addition of new risks and the removal of closed risks between the dates the two reports were produced.

Digital Services also advised there were often discrepancies between the risk register extracts, and that a quality assurance process performed by CGI to provide confirmation of completeness would be beneficial.

Risks

- **Strategic Delivery / Technology and information –** formulae in report spreadsheets may be overwritten causing mis-categorisation of risks and potential for risks to be overlooked at management and escalation meetings and not managed appropriately.

Recommendations and Management Action Plan: Reconciliation and tagging of risks

Ref.	Recommendation	Agreed Management Action	Action Owners	Lead Officers	Timeframe
3.1	CGI and Digital Services should ensure an ongoing process of reconciliation is put in place to prevent inaccuracies in future risk categorisation, so that each risk is managed appropriately. This process should be included within the risk management framework document (recommendation 1.1). In addition, a quality assurance process to provide Digital Services with assurance on the completeness of the registers should be developed and agreed by CGI.	Updated Risk and Issue Management plan will include risk categorisation and the process to ensure that it is accurate. The process will ensure that Functional RAID logs can be easily traced back to the Account RAID log.	Deborah Smart, Executive Director of Corporate Services (CEC) Nicola Harvey, Service Director Customer and Digital Services (CEC) Mark Bulmer, Vice President Consulting Services (CGI)	Innes Davidson, Director of Delivery (Applications), (CGI) Heather Robb, Chief Digital Officer (CEC) Alison Roarty, Digital Services Commercial & Risk Lead (CEC) Jackie Galloway, Senior Manager – Commercial (CEC)	31/10/2023

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.