Internal Audit Report

CGI Filtering Management

3 August 2026

CS2504

Overall Assessment	Reasonable Assurance

Contents

Executive Summary 3
Background and Scope 5
Findings and Management Actions 7
Appendix 1 – Control Assessment and Assurance Definitions 12
Appendix 2 – Areas of Audit Focus and Control Objectives 13

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

The Council's filtering solutions are managed by CGI and play a key role in protecting users, including staff and children, from harmful and inappropriate content. The audit reviewed controls for governing the management and operation of these filtering solutions and the relevant services provided by CGI and noted key internal controls require strengthening.

The review did not identify that the filtering solutions were failing to provide the intended security and protection to end users. Rather, the findings relate to the management controls operated by CGI in administering and supporting the filtering platforms, specifically around privileged access management, change management, monitoring and governance processes associated with the FortiGate and Lightspeed environments.

These controls are fundamental pillars for maintaining the security, integrity and availability of solutions and allows the Council to protect its end users from harmful and inappropriate content, including corporate staff, public users (through Wi-Fi, libraries etc.), and teachers, children and young learners in schools and other educational establishments.

The following improvements to key control areas are recommended:

- CGI should agree with and provide the Council the documentation needed to evidence completion of privileged access reviews and what privileged activities should be monitored
- CGI should evidence to the Council their process for change implementation related to filtering changes including all approval gateways
- the Council should perform sample checks to confirm the completeness and accuracy of filtering rules applied across the Council's networks or work with CGI to ensure it is completed as part of CGI's managed service.

Areas of effective practice

- requests for updating website filtering are approved by the Council's delegates prior to being requested for implementation
- changes made following CGI's change process must have an approved rollback plan prior to the change being applied. Once these changes are made, a post-implementation review is conducted to check changes were applied as expected and did not have a negative impact on the filtering solution.

Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
Web Filtering Process Management			N/A – no issues noted	N/A
Logging and Monitoring of Web Activity			See Finding 3	See Finding 3
Access to Web Filtering Solutions			Finding 1 - Privileged Access Review and Monitoring of Activities	High Priority
Management of Change to Web Filtering Solutions			Finding 2 - Configuration and Filtering Rule Change Management Process	High Priority
Governance and Oversight			Finding 3 – Monitoring of Filtering Rules and CGI Service Performance	Medium Priority

See Appendix 1 for Control Assessment and Assurance Definitions

Background and Scope

Effective management of web filtering services is essential to protect users from inappropriate content or malicious websites, upholding child safeguarding obligations and delivering secure public facing services. Inappropriate content may include gambling, pornography, alcohol/drugs, violence and extremist-views, and malicious websites may include known phishing websites and websites hosting ransomware or other malware.

The City of Edinburgh Council's (the Council) IT environment supports a wide range of end users, including corporate staff, public users (through Wi-Fi, libraries etc.), and teachers, children and young learners in schools and other educational establishments.

The Council's digital environment is managed using FortiGate or Lightspeed web filtering platforms. These platforms provide distinct filtering solutions for the Council's networks – Corporate, Learning and Teaching and Peoples Network. The filtering solutions are tailored to each network as per its user population, security requirements and technical routing paths. Whilst filtering policies vary across the networks, the process for managing configuration, change, access and the overall operation of platforms should be consistently applied across the Council environment.

As part of the Council's IT services outsourcing contract to CGI, CGI operates and manages the Council's web filtering platforms and services. The Council's Digital Services function is responsible for determining the business rules and CGI is responsible for implementing and operating web filtering services in line with the business rules and maintaining the platforms. The web filtering service includes procedures for identifying new filtering needs, determining both block and allow requirements, managing configuration and system policy changes, accurate routing and policy application, and maintaining ongoing monitoring and oversight.

Scope

The objective of this internal audit was to assess the end-to-end process for managing web filtering and the web filtering solutions. The scope focused on the design and operating effectiveness of controls managed and operated by both CGI and the Council and included:

- Web Filtering Process Management
- Logging and Monitoring of Web Activity
- Access to Web Filtering Solutions
- Management of Change to Web Filtering Solutions
- Governance and Oversight.

Alignment to Risk and Business Plan Outcomes

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

- Resilience
- Technology and Information
- Supplier, Contractor, and Partnership Management
- Reputational.

Business Plan Outcomes:

- core services for people in need of care and support are improved
- people can access public services locally and digitally, in ways that meet their needs and expectations, contributing to a greener net zero city
- attainment, achievement, and positive destinations are improved for all with a particular focus on those in poverty
- the Council has the capacity, skills, and resources to deliver its priorities efficiently, effectively and at lower cost.

Limitations of Scope

The following areas were excluded from scope:

- investigation in relation to the incidents referenced in the ‘Empowered Learning - Filtering’ report, to the Governance, Risk and Best Value Committee on 16 September 2025
- review of the Council's employee or pupil Acceptable Use Policies (AUPs)
- a technical assessment of the effectiveness of the FortiGate or Lightspeed tools in blocking all malicious websites, beyond consideration of CGI's configuration and management processes
- an assessment of whether the web filtering rules are the right ones i.e. the specific websites which are allowed / disallowed. The internal audit only considered the roles, process and governance around management’s decisions
- analysis of network bandwidth performance or capacity
- Skills, capability and capacity assessment of the function/teams managing the web filtering service
- the Council's internal IT infrastructure or processes related to web access that are not within CGI's managed service remit for web filtering
- an assessment of adherence to the contractual agreements regarding web filtering.

Reporting Date

Audit work concluded on 15 June 2026, and the findings and opinion are based on the conclusion of work at that date

Findings and Management Actions

Finding 1 – Privileged Access Review and Monitoring

Finding Rating	High Priority

Privileged roles should be defined and accounts assigned with these roles should be monitored through access reviews and activity monitoring.

CGI Telecom Engineers have access to the Terminal Access Controller Access Control System (TACACS) which enables engineers to manage and support the Council's networks. This access provides unrestricted access to FortiGate, including activating/deactivating filtering solutions across the Council's networks, applying software and configuration changes and updating filtering rules.

Lightspeed is used to filter site and online content for schools' mobile devices i.e. iPads provided to students and education staff as part of the Empowered Learning network. User accounts assigned the 'Administrative' role can update Lightspeed filtering rules and integrate the Lightspeed solution with Mobile Device Management (MDM) solutions.

CGI management advised annual user access reviews are performed for both FortiGate and Lightspeed. However, evidence of user access reviews was not available at the time of the audit and, as such, this could not be tested by internal audit. There is also no monitoring or review of the privileged activities undertaken in FortiGate and Lightspeed to identify unauthorised and/or inappropriate activities.

This could result in unauthorised and/or inappropriate users having privileged access, and unauthorised and/or inappropriate activities remaining undetected. At the time of the review, 242 users had administrative access to TACACS, and 8 users had administrative access to Lightspeed.

Alignment to City of Edinburgh Council Risks

- **Technology and Information** – limited evidence of privileged access governance could reduce assurance over the appropriateness of administrative access
- **Reputational Risk** – weakness in privileged access controls could reduce confidence in the Council's ability to demonstrate that filtering controls are being managed appropriately managed by CGI.

Recommendations and Management Actions: Privileged Access Review and Monitoring of Activities

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
1.1	CGI should provide evidence of annual user access reviews for TACACS and Lightspeed to the Council.	CGI will implement reviews of AD Accounts for CGI members with access to TACACS and Lightspeed to ensure the joiners, leavers, movers process has been followed. Where discrepancies are found, access will be disabled. This will be managed through the Service Now system with the outputs recorded, available and shared with Digital Services as evidence that this activity has taken place.	Corporate Director, Customer and Corporate Services, CEC Vice President Consulting Services, CGI	Director, Infrastructure Engagement, Scotland East, CGI Cyber Security Manager, CEC	31/03/2027

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
1.2	Regular checks of the privileged activities undertaken in FortiGate and Lightspeed should be performed by CGI to identify unauthorised and/or inappropriate activities with outcomes of these checks reported to the Council.	There is a structured change management process including CAB approval, defined implementation procedures with prechecks, testing, validation, and rollback, multi layered governance involving Technical Authority, Subject Matter Expert, CAB and IAB review, post implementation verification and auditability of changes. These controls represent a mature and well governed change process. In addition, compensating controls exist, including Event logging of configuration changes, traceability of changes through system logs and change records, and incident driven detection and investigation mechanisms. The Security Operations Centre (SOC) includes firewall monitoring and management as part of the service. If an issue is identified, it will be managed through the appropriate incident process. Where malicious activity is detected or suspected, a Security Incident will be raised and managed in accordance with CGI's security incident response procedures. If an approved change results in a service disruption, the issue will be recorded and managed as a Service Incident through the established IT service management process. In cases where an unsolicited or unauthorised change is identified, the matter will be investigated and managed in line with organisational governance and disciplinary policies, as appropriate. If it is determined the above does not mitigate risk to an acceptable level, then a relevant change request should be made for regular checks of activities to be implemented. In the event that regular checks are requested CGI will provide evidence to Digital Services of the results of those checks carried out by CGI	Corporate Director, Customer and Corporate Services, CEC Vice President Consulting Services, CGI	Director, Infrastructure Engagement, Scotland East Cyber Security Manager, CEC Relations & Service Manager, Digital Services, CEC Digital Education Manager, CEC	31/07/2027

Finding 2 – Configuration and Filtering Rule Change Management

Finding Rating	High Priority

All software upgrades, and configuration and filtering rule changes should be approved, tested and authorised prior to being applied to the filtering solutions, FortiGate and/or Lightspeed. The end-to-end change process should be designed so that it cannot be bypassed.

CGI manage the software upgrade, and configuration and filtering rule changes to FortiGate and configuration and filtering rule changes to FortiGate and Lightspeed. Each change record has the Council's approval, test acceptance, post-implementation review and roll back planning, and change authority board (CAB) approval. Once a change is approved by CAB, changes to FortiGate and Lightspeed are made by CGI. CGI's Network and Telecommunications members make changes to FortiGate and authorised CGI and Digital Services personnel make changes to Lightspeed.

CGI Terminal Access Controller Access Control System (TACACS) users have unrestricted access to make changes to FortiGate and CGI users with Administrative User access to Lightspeed can update filtering rules. These accounts do not have enhanced restrictions (e.g. time-bound access, privileged activity session termination etc), enabling these users to bypass the change process. There is no detective control to retrospectively identify changes that may have bypassed the process. Ability to make changes to filtering solutions is not granted on a needs basis or timebound. At the time of the audit, 242 and 8 users were identified with the ability to make changes in FortiGate and Lightspeed, respectively.

The current change framework supports safe and secure operation of the filtering service but strengthening preventative and/or detective controls would improve assurance that all changes are fully governed and evidenced in line with expectations.

Alignment to City of Edinburgh Council Risks

- **Resilience –** existing change process may not be followed which could result in filtering solution service outage and extended recovery times
- **Technology and Information –** existing change process may not be followed which could result in filtering solutions and filtering rules not working as intended
- **Reputational Risk –** inappropriate and/or unauthorised changes to filtering solutions and rules could result in filtering solutions not operating as intended which will lead to reduced confidence in the Council's ability to protect its employees and the public from inappropriate and/or harmful content.

Recommendations and Management Actions: Filtering Rule Change Management Checks

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
2.1	CGI should improve monitoring and reporting of filtering related changes and provide evidence of this to the Council. This should include consideration of • preventative controls to prevent users from implementing changes to filtering solutions prior to change	Audit logs for changes made to Lightspeed and Fortigate are held and CGI have the ability to retrospectively monitor these to detect unauthorised or inappropriate changes made. CGI will work with Digital Services to strengthen the monitoring and reporting of filtering-related changes by implementing regular reviews of these audit logs. A clearly defined Change Request (CR) will be raised to introduce a formal process	Corporate Director, Customer and Corporate Services, CEC Vice President Consulting Services, CGI	Director, Infrastructure Engagement, Scotland East Relations & Service Manager, Digital Services, CEC	31/07/2027

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
	authority board (CAB) approval, and/or • detective controls to retrospectively identify unauthorised and/or inappropriate changes made e.g. changes that bypassed the CGI change process.	for the periodic monitoring and reporting of filtering solution audit logs.		Digital Education Manager, CEC Cyber Security Manager, CEC	

Finding 3 – Monitoring of Filtering Rules

Finding Rating	Medium Priority

FortiGate and Lightspeed are used to manage access to online content (i.e. web categories and websites) across the Council's networks.

For both Fortinet and Lightspeed, CGI manages the performance management, software updates, configuration management, access and filtering updates on behalf of the Council.

The Council conducts periodic checks to confirm that specific websites and online content are being filtered as expected. However, there is no periodic monitoring or analysis performed to check all web filtering rules are operating as expected i.e. reviewing the filtering rules in place for accuracy or analysing web traffic patterns.

Alignment to City of Edinburgh Council Risks

- **Technology and Information –** the lack of oversight and monitoring of filtering rules could result in incomplete and/or inaccurate rules remaining undetected and unresolved.

Recommendations and Management Actions: Sample Checks of Filtering Categories

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
3.1	The Council should perform checks to confirm the completeness and accuracy of filtering categories applied across the Council's networks to ensure they are working as expected.	The Council and CGI will meet quarterly to review the rules applied to filtering solutions used in the Council including review of categories blocked and allowed.	Corporate Director, Customer and Corporate Services, CEC	Cyber Security Manager, CEC Relations & Service Manager, Digital Services, CEC Digital Education Manager, CEC	31/03/2027

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
Web Filtering Process Management	• Defined processes exist to identify, prioritise and implement web filtering rules (i.e. through use of Internet Watch Foundation, IWF and URL list) across the Council's corporate, people, public, learning & teaching and empowered learning networks. • Defined process exists to manage requests related to web filtering by the Council.
Logging and Monitoring of Web Activity	• The Council's web filtering needs are understood, agreed by relevant stakeholders and updated on a regular basis. • Monitoring exists to make sure web filtering is operating as expected, including logging and auditing. • Processes exist to proactively monitor and update web filtering to, at a minimum, evolve with emerging risks. • There is monitoring to identify inappropriate and/or unauthorised changes to web filtering.
Access to Web Filtering Solutions	• There are defined processes and controls to manage access to web filtering solutions and filtering rules.
Management of Change to Web Filtering Solutions	• There are defined processes and controls to manage changes to web filtering software. • Processes exist to manage configuration, and other filtering rule changes, to the web filtering solution.
Governance and Oversight	• The Council monitor appropriateness and/or performance of web filtering services provided. • Web filtering arrangements are periodically reviewed for continued alignment with filtering policies and emerging risks.