



## **2026/27 Internal Audit Plan**

# Contents

- Developing the Internal Audit Plan ..... 3
- Coordination and Reliance ..... 5
- Topical Requirements ..... 6
- Organisational Structure: High-level Auditable Areas ..... 7
- Risk Assessment..... 8
- Appendix 1: 2026/27 Internal Audit Plan ..... 9

# Developing the Internal Audit Plan

## Approach

The approach to preparing the Internal Audit (IA) plan is set out at Figure 1. The plan is driven by the requirements of the GIAS (UK Public Sector), the Council's objectives and priorities, and an assessment of the risks that could prevent the Council from meeting its objectives and providing services.

Changes in organisational structures, system developments, working practices and legislative requirements create a constantly changing control environment. Taking these factors into account, the highest risk areas are covered in the IA plan.

Internal Audit must consider the risk of fraud when performing risk assessments and developing the internal audit plan and evaluate governance and risk management processes for fraud prevention. The 2026/27 plan includes an initial assessment of exposure to fraud related risks for each audit.

## Engagement with key stakeholders

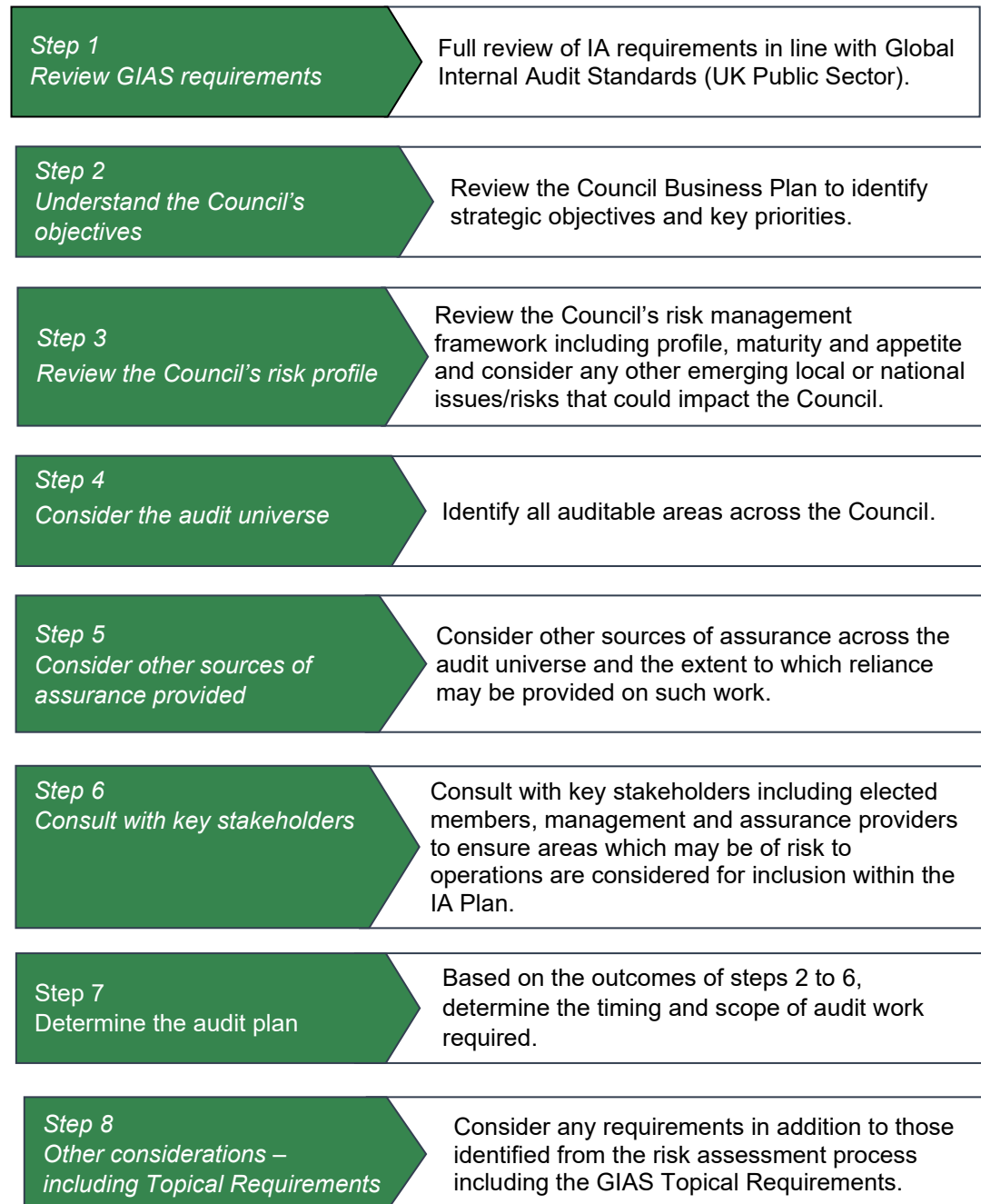
Key stakeholders including elected members, the Chief Executive, Directors, senior management and external assurance bodies are invited to provide input into the IA plan to help ensure that the relevant areas are targeted for review during the year.

## Internal Audit influence and value

IA is a valuable resource which can help services to achieve objectives and reduce exposure to associated risks. Where appropriate and without compromising its primary function and independence, IA will become involved in relevant emerging issues at an early stage and provide advice and guidance to prevent problems or weaknesses from arising and to ensure effective and efficient use of Council resources.

This is achieved through delivery of a flexible audit approach aligned to priorities and available resources, and an IA plan which includes a mix of engagement types from short, focussed reviews to more in-depth assurance reviews as well as advisory work.

Figure 1: Approach to developing the 2026/27 IA Plan



In addition, IA has established an agile auditing approach to provide assurance and support across the Council on an ongoing basis where relevant for example, ongoing project reviews, system development lifecycle reviews and major projects and programmes spanning several years.

### **Fraud Prevention and Fraud Risk Assessments**

[The Economic Crime and Corporate Transparency Act 2023](#) 'Failure to prevent fraud' offence, effective from 1 September 2025, sets out the requirement for management to undertake at least annual fraud risk assessments, document fraud prevention procedures, and regularly test the effectiveness of controls.

Internal Audit will review the effectiveness of the Council's fraud prevention policies and procedures including the timely completion of robust and accurate fraud risk assessments. Internal Audit will continue to review fraud controls as a standard objective for all internal audit reviews, as well as concluding on the overall effectiveness of fraud prevention controls in the IA Annual Report.

### **Types of Internal Audit Services**

**'Assurance services'** – traditional audits where IA perform objective assessments to provide assurance. Examples include compliance checks, operational/performance reviews, financial and technology assessments. The scope of assurance services are determined by IA. The majority of IA work is assurance related.

**'Advisory services'** – services through which IA provide advice to management without taking on any management responsibilities. Examples include advising on the design and implementation of new policies and frameworks, processes or systems and providing training or facilitation/participation in discussions about risk and control frameworks (such as working groups). The scope of assurance services are determined jointly between IA and management. Advisory audits do not get an overall rating however observations are provided a priority rating based on risk and suggest timescales for remediation.

**'Agile auditing'** – traditional audits have defined stages: planning, fieldwork and reporting over an extended period of time which can be up to 3 months. Agile auditing provides a dynamic and flexible approach to enable real-time feedback on new projects, processes or initiatives as they are developed. Agile auditing can be on an assurance or advisory basis depending on the area of risk.

# Coordination and Reliance

IA is only one source of assurance available; assurance can come from many sources. The **Three Lines Model**, as set out in the diagram, helps identify and understand the contributions of these various sources.

Defining the sources of assurance into the three categories on the following page helps to understand how each of them contributes to the overall level of assurance and how they can be best integrated and mutually supportive.

In line with the GIAS, when developing the IA risk assessment and plan, where relevant, we have considered other sources of assurance and a shared risk assessment to understand the extent to which reliance can be placed upon these other sources to avoid duplication in the work they do.

Key sources of assurance for the Council include:

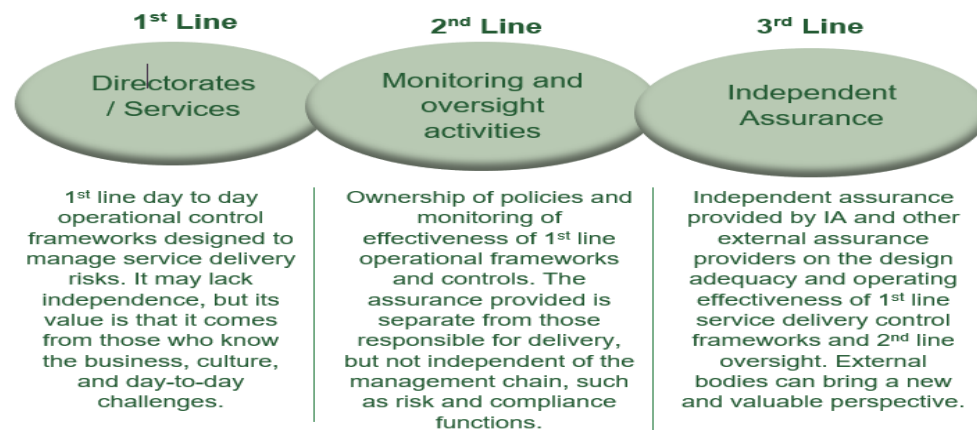
- Audit Scotland as External Auditors
- various regulators and inspection bodies
- Annual Governance Statements
- National Fraud Initiative
- Internal assurance teams

## Internal assurance teams

The following specific second line assurance activities are performed across the Council:

- **Corporate Risk Management** – responsible for designing, maintaining and embedding the Council’s Risk Management Framework.
- **Governance Team** - responsible for delivery of the Council’s governance functions and ensuring the Council meets legal responsibilities and follows government guidance.
- **Whistleblowing and Investigation Teams** – investigate employee related issues raised under the relevant policies including the Council’s Whistleblowing policy, Grievance policies and Disciplinary policies.

## Three lines model



- **Customer Fraud Team** – support the detection of customer fraud across benefits including the blue badge scheme, council tax and council tenancies.
- **Information Governance Unit** - responsible for helping the Council manage its information effectively and compliantly.
- **Corporate Health and Safety** - undertake health and safety audits to check compliance with the Council’s Health and Safety Policy and legal health and safety obligations as part of a rolling programme to monitor and report on health and safety performance, and to foster continual improvement.
- **Quality, Governance and Regulation Services** support the Chief Social Work Officer and social work/care related quality assurance across the Council and the Edinburgh Health and Social Care Partnership.
- The **Education Quality, Improvement and Curriculum Service** work with schools to ensure that the Council is meeting national and local priorities. This includes supporting schools with His Majesty's Inspectorate of Education (HMIE) inspections.
- The **Housing and Homelessness Service Improvement Team** performs quality assurance activities and monitors service delivery across key operational areas and compliance with relevant regulations

## Assurance Mapping

An assurance map is a matrix which sets out an organisation's risks and all the internal and external sources of assurance which cover these risks. This visualisation helps to expose coverage gaps and duplication. The map also helps to provide an overall view of assurance activity and helps to prevent audit fatigue in the areas and processes being reviewed.

The maturity of the Council's assurance map remains at a basic level. Understanding how first and second line assurance activities work together and can support the third line remains a key focus for Internal Audit. All audits now include information gathering on other assurance activities and bodies which should enable a great understanding and mapping of activities, to determine the extent to which reliance can be placed on these.

As part of the IA Strategy, IA will continue to coordinate with the Corporate Risk Team, internal assurance teams, and external assurance providers to support development an assurance map covering the Council's risk categories and high level key controls.

## Topical Requirements

Topical Requirements are a mandatory component of the International Professional Practices Framework and GIAS which will become effective over the course of 2026/27.

Topical Requirements aim to enhance the consistency and quality of IA services related to specific audit subjects. Each Topical Requirement supports internal auditors performing engagements in a specific risk area by providing a consistent and comprehensive approach to assessing the design and implementation of key governance, risk management and control processes in the topical area.

The following Topical Requirements have been issued so far:

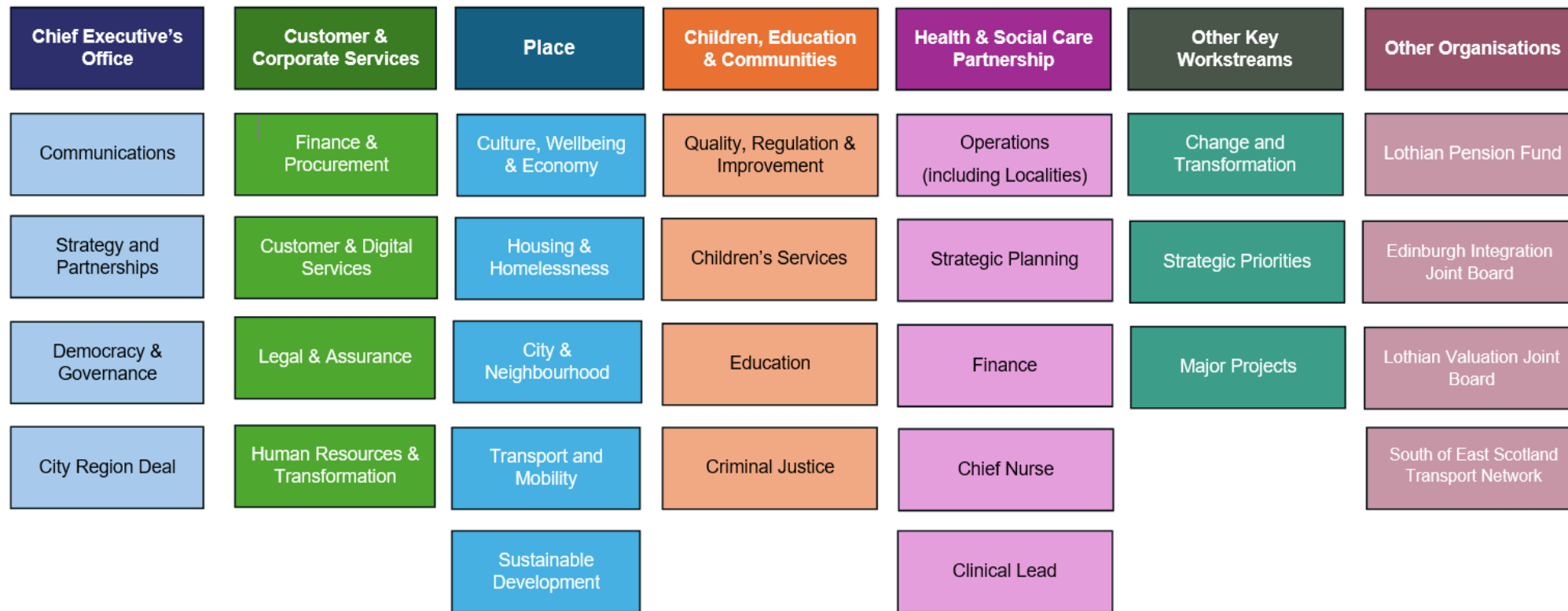
- **Cyber Security** – effective February 2026
- **Third Party** – effective September 2026
- **Organisational Behaviour** – effective December 2026
- **Organisational Resilience** – expected early 2027

IA must assess and record the applicability of each across any audits covering each Topical Requirement from their effective date. Internal planning arrangements for the 2026/27 plan will assess the applicability of the Topical Requirements for each audit.

# Organisational Structure: High-level Auditable Areas

The diagram below represents the organisational structure as at January 2026 including Council directorates and divisions, Health and Social Care Partnership and sets out the high-level auditable areas which form the basis of the IA plan.

In addition to the Council, IA provides audit services to several other organisations on an annual basis.



# Risk Assessment

It is a requirement of the GIAS (UK Public Sector) that the IA plan is based on a risk assessment.

To ensure a risk-based and proportionate approach to the IA plan which supports the GIAS requirement to produce an overall conclusion on the effectiveness of the Council's governance, risk management and control framework (annual report and opinion), when developing the 2026/27 IA plan, consideration was given to the Council's priorities as detailed in the [Council Business Plan 2023-27](#) and the Council's risk profile as at February 2026.

The Council's risk profile as at February 2026 included 14 risk categories and 21 risks across these categories.



The 2026/27 IA plan is informed by a review of the Council's risk profile as at February 2026 which included an assessment for each of the 21 enterprise risks based on management's view of the internal and external operating environments with actions required to manage the risks in line with the Council's agreed risk appetite.

Previously completed audits, emerging issues impacting the Council and the requirement to ensure regular assurance on key financial systems is also considered as part of the risk assessment process.

The audits included in the proposed IA plan at [Appendix 1](#) provide coverage across the 14 strategic risk categories.

## Dynamic risk review and audit scoping

While the IA plan includes a short summary of the area proposed for review, IA will meet with key officers prior to commencing each audit to further understand the key risks, and to develop and refine the scope of each review.

For assurance reviews, in line with the GIAS, IA is responsible for determining the scope of each audit. For advisory reviews, the scope is agreed jointly with IA and management.

It should be noted, that if areas are identified during testing that are out with scope but impact the risk and control framework, findings and recommendations will still be raised and reported on, where appropriate.

In line with the IA Charter, where relevant, IA reserves the right to raise findings on areas that have not been specifically included in the IA plan where significant or systemic control gaps are evident.

The IA plan is reviewed on a quarterly basis to ensure it maintains a clear focus on the link between the Council's priorities, business critical risks, the IA programme, and core controls. Proposed changes are reported to GRBV as part of quarterly IA activity reporting.

# Appendix 1: 2026/27 Internal Audit Plan

The proposed IA work programme for the period 1 April 2026 to 31 March 2027 is set out below and is based on strategic priorities, current and emerging risks and key areas of business change as at January 2026.

Internal Audit resource should be flexible to respond to emerging issues and risks impacting the Council. Therefore, audits have been categorised as 'Priority Q1 and Q2', 'Indicative Q3 and Q4'. Priority audits are those aligned to the Council's highest risks, which IA will aim to complete within Q1 and Q2. Indicative audits will be completed in Q3 and Q4 and will be flexible to enable IA capacity to react to changes in the Council's risk profile. In addition, agile audits on a range of emerging initiatives will be undertaken over the course of the year to enable real-time feedback to be provided as processes are developed.

Priority Q1 and Q2 Audits					
Directorate	Service Area	Assurance /Advisory	Audit Title and High-Level Scope	Fraud Risk	Days
Cross Directorate	CE Office / Education and Children's Services	Assurance	<b>1. Child Friendly Complaints</b> – review of the design of key processes established to ensure adherence to the <a href="#">SPSO Child Friendly Complaints Handling Principles</a> and supporting guidance.	Medium	40
	Place Education Corporate and Customer Services	Assurance	<b>2. Venue and Events Booking and Management</b> – will consider the design and operating effectiveness of key controls established to ensure compliance with the Council's <a href="#">Venue and Events Booking Policy</a> approved in January 2024 including income management controls, data governance, and key systems controls.	High	40
	Health and Safety / All directorates	Assurance	<b>3. Health and Safety Assurance: Management Controls and Compliance</b> – review of oversight and assurance over the effectiveness of the directorate management controls for health and safety including managing risks in public facing environments and compliance with statutory safety duties.	Medium	40
	HR / All directorates	Assurance	<b>4. Redeployment</b> – review of the design and operating effectiveness of key controls established to manage redeployment across the Council. Will include a review of a sample of cases and overall monitoring and oversight arrangements.	Medium	30
CE Office	Strategy	Assurance	<b>5. Carbon Emissions Reduction Plan</b> – to provide assurance over the effectiveness of arrangements supporting delivery of the <a href="#">CERP</a> including planning, performance management and reporting and whether these are sufficient to support achievement of agreed targets.	Medium	30
	City Region Deal	Assurance	<b>6. City Region Deal: Governance and Financial Management</b> – review of programme level arrangements to support governance and decision-making including risk management and	Medium	30

Priority Q1 and Q2 Audits					
Directorate	Service Area	Assurance /Advisory	Audit Title and High-Level Scope	Fraud Risk	Days
			performance monitoring to ensure appropriate oversight and accountability of programme funds and compliance with relevant requirements.		
Place	Regulatory Services - Licensing	Advisory	<b>7. Premises licensing and partner agency assurance</b> – assessment of how premises licensing by the Council manages safety risks for both permanent and temporary venues including effective coordination with key partners such as Police Scotland and the Scottish Fire and Rescue Service.	Medium	40
	Network Management & Enforcement	Assurance	<b>8. Road Safety Delivery Plan</b> – to provide assurance that governance, programme management and operational arrangements support the effective and timely delivery of the Council's <a href="#">Road Safety Delivery Plan</a> .	Medium	30
	Network Management & Enforcement	Assurance	<b>9. Port Facility Security Plan</b> - annual review of the existence and operation of the Port Facility Security Plan as per Department for Transport requirements.	Medium	25
	Strategy, Commissioning & Service Improvement	Assurance	<b>10. Transfer of Management Development Funding</b> – biennial review of the adequacy of key controls established to support management of transfer of development funding from the Council to registered social landlords, in line with the Scottish Government requirements.	Medium	25
	High Rise Management & Investment Area Based Regeneration & Shared Repairs Mixed Tenure Improvement Service	Assurance	<b>11. Management of Mixed Tenure Properties</b> – review will assess whether the Council has effective governance, financial and operational arrangements in place to manage mixed tenure properties including the role of the Mixed Tenure Improvement Service - considering factoring responsibilities, delivery of common services, and planning and delivery of preventative and programmed works, engagement with stakeholders and clarity of decision making, use of contractors/materials and securing best value for all owners and consideration of energy efficiency requirements including grant funding.	High	55
Customer and Corporate Services	Digital Services / CGI	Assurance	<b>12. CGI Privileged Access Management: Domain Administration</b> – assessment of how CGI managed high privileged roles are assigned, controlled, and reviewed against least-privilege and NCSC best-practice guidance.	High	30
HSCP	Assessment & Care Management	Assurance	<b>13. Self-Directed Support (Adult Services)</b> – review of the adequacy and effectiveness of key controls established to ensure compliance with the Council's Self-Directed Support (SDS) Policy implemented in November 2024, which aims to ensure consistency with the statutory	High	30

Priority Q1 and Q2 Audits					
Directorate	Service Area	Assurance /Advisory	Audit Title and High-Level Scope	Fraud Risk	Days
			guidance produced to support the delivery of Social Care (SDS) (Scotland) Act 2013 which was revised in November 2022.		
	Home First and Community Based Support	Advisory	<b>14. Reablement Services</b> - to provide assurance that the newly established reablement model is appropriately designed, governed and operating effectively to deliver safe, timely and outcome focused services that support independence and represent value for money.	Medium	30
<b>Q1 and Q2 Audits – Total Days</b>					<b>475</b>

Indicative Q3 and Q4 Audits					
Directorate	Service Area	Assurance /Advisory	Audit Title and High-Level Scope	Fraud Risk	Days
Cross Directorate	Resilience / All Directorates	Advisory	<b>15. Preparedness for the Terrorism (Protection of Premises) Act 2025</b> – agile review of the Council’s preparedness for implementation of the <a href="#">Act</a> , which is due to be implemented in 2027 and will require the authority to prepare for protection from a terrorist attack, in line with standard duty premises and enhanced duty premises.	Low	40
	All Directorates	Assurance	<b>16. Implementation of Assurance Actions</b> – review of directorate progress in implementing assurance actions across the range of assurance and inspection reports including the Care Inspectorate, Audit Scotland, HMIE and other relevant national reports. Will include oversight and validation of progress as well as approaches to lessons learned.	Medium	40
	Information Governance / All Directorates	Assurance	<b>17. Data Governance / Access Controls</b> – will assess whether the Council has an effective governance framework and control environment to manage access to corporate data, mitigate confidentiality risks and support transition from legacy shared drives to collaboration platforms such as SharePoint.	High	40
Cross Directorate	Digital Services / Education Culture – Libraries	Assurance	<b>18. Digital Safeguarding and Internet Safety in Schools and Libraries</b> – will assess whether arrangements for schools and libraries provide safe, proportionate and effective controls over public and student internet access, supporting safeguarding responsibilities while enabling appropriate use.	High	30
	Finance	Assurance	<b>19. Core Financial Controls – Non-pay expenditure</b> – to provide assurance that non-pay expenditure including mileage, vehicle use, training expenditure and other employee-	High	40

Indicative Q3 and Q4 Audits					
Directorate	Service Area	Assurance /Advisory	Audit Title and High-Level Scope	Fraud Risk	Days
	All Directorates		related non-pay benefits are properly authorised, recorded, monitored and controlled to prevent misuse, error and fraud.		
	HR All Directorates	Assurance	<b>20. Protecting Vulnerable Groups Disclosure Applications and Referrals</b> – to provide assurance that revised processes implemented in 2025 to address previously reported issues are adequately designed and operating effectively to ensure the Council meets all requirements of the Protection of Vulnerable Groups (Scotland) Act 2007.	High	30
	Strategy All Directorates	Advisory	<b>21. Equity in Service Delivery</b> – advisory review of how the Council designs and evaluates initiatives intended to reduce inequality and support those experiencing poverty. Will consider whether service models are informed by lived experiences, deliver meaningful outcomes and avoid unintended stigma or inequitable impacts.	Medium	40
	All directorates	Assurance	<b>22. Annual Validation review</b> - review of a sample of previously implemented and closed IA agreed management actions to confirm that they have been effectively sustained.	Depends on sample	40
Place	Neighbourhood Environmental Services	Assurance	<b>23. Waste and Cleansing Services: Operational Management</b> - to provide assurance that operational management controls are appropriately designed and consistently applied to support effective, compliant and accountable service delivery.	High	40
	Homelessness & Housing Access	Assurance	<b>24. Homelessness Services: Temporary Accommodation and Allocations</b> – to provide assurance that the Council’s homelessness services including temporary accommodation and allocations are effective, efficient and compliant, with robust governance, risk management and performance monitoring in place to support positive outcomes for people during the current housing emergency.	Medium	50
Customer and Corporate Services	HR	Assurance	<b>25. HR Case Management</b> – review of the efficiency and effectiveness of HR case management processes including grievance and disciplinary processes and linkage to whistleblowing or employee investigations. Will consider policy adherence, case recording and tracking, timeliness, consistency of outcomes and management reporting.	Medium	40
Children, Education and Communities	Education	Assurance	<b>26. Behaviours of Concern (focused follow-up)</b> – to assess progress made since the previous audit on managing behaviours of concern completed in 2021 including ensuring that school policies, practice, training and monitoring support children’s inclusion, engagement and wellbeing; protect staff from harm; and align with national guidance <a href="#">'Included, engaged and involved'</a> .	Medium	30

Indicative Q3 and Q4 Audits					
Directorate	Service Area	Assurance /Advisory	Audit Title and High-Level Scope	Fraud Risk	Days
	Education	Assurance	<b>27. Devolved School Management</b> - review of processes established to ensure compliance with the <a href="#">Scottish Government devolved school management guidance</a> which sets out how local authorities fund schools and the accountability and responsibility for financial decisions. Will include review of processes for a sample of schools.	High	40
	Quality, Regulation and Improvement	Advisory	<b>28. Safeguarding Processes</b> – review will consider the design adequacy of newly established processes for managing allegations involving adults working with children and vulnerable groups. Will consider governance, policies and procedures, referral and case management, interagency communications, training and monitoring arrangements.	High	30
HSCP	Adult Mental Health Services	Assurance	<b>29. Mental Health Officer: Waiting List Management</b> – will assess whether Mental Health Officer services are compliant with statutory duties, delivered within required timescales and whether management actions are adequately addressing service backlogs and waiting list pressures.	High	30
<b>Q3 and Q4 Audits – Total Days</b>					<b>560</b>

Agile Audits					
Directorate	Service Area	Assurance / Advisory	Audit Title and High-Level Scope	Fraud Risk	Days
Cross Directorate	Transactions Regulatory Services Business Growth and Inclusion	Advisory	<b>30. Visitor Levy for Edinburgh Implementation</b> – agile audit work will be undertaken to provide assurance of key considerations as the scheme develops including consideration of <a href="#">Visitor Levy (Scotland) Act 2024</a> requirements.	High	40
	Change and Transformation Finance All Directorates	Advisory	<b>31. Change and Transformation</b> – agile audit to provide assurance that the Council has robust governance arrangements, clear accountability and effective oversight mechanisms in place to manage change and transformation initiatives, ensuring alignment with strategic objectives, budget and savings proposals.	Medium	40
	Information Governance Digital Services	Advisory	<b>32. AI Governance, Ethics and Oversight</b> – agile audit to provide assurance that the Council's AI adoption is governed effectively, ethically and transparently to support service	High	40

Agile Audits					
Directorate	Service Area	Assurance / Advisory	Audit Title and High-Level Scope	Fraud Risk	Days
	All Directorates		transformation and efficiency including ensuring that AI driven processes are informed, accountable and ethically justified.		
	All directorates	Assurance	<b>33. Third Party Grant Funding</b> – review of arrangements for providing grant funding to third parties including compliance with <a href="#">Grant Standing Orders</a> and adherence to procedures and assessment processes and governance and oversight processes.	High	40
<b>Agile Audits – Total Days</b>					<b>160</b>

Other Organisations	Audit Service	Days
Lothian Pension Fund (LPF)	<b>34 – 37.</b> Four audits completed for LPF as part of established audit service arrangement.	120
	<b>38. Annual Validation review</b> - review of a sample of previously implemented and closed IA agreed management actions to confirm that they have been effectively sustained.	5
Edinburgh Integration Joint Board (EIJB)	<b>39– 41.</b> Three audits completed for the EIJB as part of established audit service arrangement.	110
	<b>42. Annual Validation review</b> - review of a sample of previously implemented and closed IA agreed management actions to confirm that they have been effectively sustained.	5
SEStran	<b>43.</b> One audit delivered for South-East of Scotland Transport Network as part of established audit service arrangement.	20
Lothian Valuation Joint Board	<b>44.</b> One audit delivered for Lothian Valuation Joint Board as part of established audit service arrangement.	25
<b>Total Audit Days for Other Organisations</b>		<b>285</b>

Other IA Activities	Days
Annual planning and annual reporting activities; quarterly committee reporting and attendance – CEC	40
Annual planning and annual reporting activities; quarterly committee reporting and attendance – Other Orgs	30
Internal Audit representation across a series of governance boards and working groups	100
Follow up to confirm that agreed management actions have been effectively implemented	150

<b>Other IA Activities</b>	<b>Days</b>
IA Quality Assurance including annual GIAS self-assessment	40
Provision of an External Quality Assessment as part of SLACIAG peer review group	40
GIAS implementation including Topical Requirements process development	60
Training (CPD, colleague induction, leadership, audit systems and general controls)	25
<b>Total other IA activities</b>	<b>485</b>
<b>Contingency – including extended scope, additional requests and ad-hoc advisory work</b>	<b>150</b>

<b>Area</b>	<b>Days</b>
Q1 and Q2 audits	475
Q3 and Q4 audits	560
Agile audits	160
Other Orgs Audits	285
Other Activities	485
Contingency	150
<b>Total Days</b>	<b>2115</b>