Rossendale Borough Council

Internal Audit Service

Progress Report:
2025/26 Audit Plan Delivery
December 2025 – January 2026

ROSSENDALE
BOROUGH
COUNCIL

1 Introduction

1.1 This report supports Audit and Accounts Committee's responsibility under its terms of reference to consider performance reports from Internal Audit on progress with delivery of the 2025/26 audit plan agreed at the July 2025 Committee meeting.

2 Summary of progress

2.1 The table below reports progress with delivery of the 17 audits on the audit plan. We issued three final and two draft audit reports, are actively progressing six audits and have scheduled five audits for Quarter 4, including the four annual financial systems audits. We have agreed to defer the audit of the Rossendale Leisure Trust to 2026/27, when we will look at how the outcomes of the current review are being addressed.

2.2 We gave reasonable assurance over our audit of the Council's data management arrangements. We reported robust governance roles, secure technical controls, particularly within Revenues and Benefits, while noting gaps in policy coverage, inconsistent Data Protection Impact Assessment usage, and varying levels of training compliance. Access controls and data security were generally sound across all services, though improvements are needed in updating data governance policies, strengthening Legal Services' data handling through the planned system replacement, and re-establishing annual data management assurance activities.

2.3 Salford Technical Audit Service delivers the council's IT audits, and have issued a draft report on their audit of outsourced data centre physical security and environmental controls. The audit focussed on logical, physical and environmental security of sites hosting elements of the network infrastructure.

2.4 We are currently developing the Annual Internal Audit Plan 2026/27 in conjunction with the council's corporate management team, and will report the outcome separately to the committee for consideration once a full plan has been agreed.

2.5 Previous reports have notified the Committee of our ongoing recruitment activity to increase the size of the Internal Audit Service to build capacity and support long-term sustainability. As of this meeting we are now at full complement, although have three trainees on the team who will require time to develop their skills and progress to full audit delivery responsibilities.

2.6 We have included extracts from finalised audit reports in Annex A to this report.

Control Area	Audit Progress	Assurance
Governance and democratic oversight		
LGA Improvement and Assurance Framework	Progressing	
Rossendale Leisure Trust	Deferred	
Business effectiveness		
Capital Programme	Planning	
Contract Management	Planning	
IT - Patch and Vulnerability Management	Planning	
IT - Payment Card Industry Data Security Standards	Final Report	Limited (Low 5/10)
IT - Cyber Security: Outsourced Data Centre Physical Security and Environmental Controls	Draft Report	
Service delivery		
Asset Commercialisation	Draft Report	
Service support		

Data Management	Final Report	Reasonable
Business processes		
Council tax	Progressing	
Business rates/ NNDR	Progressing	
Housing benefits	Progressing	
Payroll	Final Report	Substantial
Accounts payable	Q4 start	
Accounts receivable	Q4 start	
General ledger and budget setting	Q4 start	
Income collection/ banking	Q4 start	

Stage of audit process	**Number of audits**
Not started	4
Planning	3
Progressing	4
Draft report	2
Completed - Final Report *or* no report necessary	3
Deferred/ cancelled	1
Total number of audits	17

3 Update on the National Fraud Initiative (NFI)

3.1 The most recent results from the council's involvement in the National Fraud Initiative NFI are shown below.

Category of data	**Number of matches**				**Frauds**	**Errors**	**Savings identified**
	identified	**processed**	**cleared**	**investigating**			
Housing Benefit	15	14	13	0	1	0	£26,926.13
Payroll	9	0	0	0	0	0	£0.00
Waiting Lists	89	5	5	0	0	0	£0.00
Council Tax Reduction	255	230	223	25	3	4	£22,844.96
Creditors	902	0	0	0	0	0	£0.00
Procurement	32	0	0	0	0	0	£0.00
Totals	**756**	**244**	**236**	**25**	**4**	**4**	**£49,771.09**

4 Use of this report

4.1 This report has been prepared solely for the use of Rossendale Borough Council and it would therefore not be appropriate for it or extracts from it to be made available to third parties other than the external auditors. We accept no responsibility to any third party who may receive this report, in whole or in part, for any reliance that they may place on it and we

expect the external auditors to determine for themselves the extent to which they choose to utilise our work.

Annex A

Extracts from Final Internal Audit reports

Data Management

Overall assurance rating

Reasonable

See Appendix A for Rating Definitions

Audit findings requiring action

Extreme	High	Medium	Low
0	0	4	0

The audit reviewed the Council's data management arrangements across key services and provides an overall Moderate assurance rating. The Council has established a solid governance framework, with responsibilities allocated for the roles of Senior Information Risk Owner (SIRO) and Data Protection Officer (DPO), defined data ownership, and some ongoing oversight activities. Strong technical controls, system security measures, and established operational processes, particularly within Revenues and Benefits, demonstrate positive practice. However, current policies do not fully cover essential data governance requirements such as GDPR principles and lifecycle management, areas normally addressed through a dedicated data protection policy.

Most Benefits and Council Tax applications were submitted online and supported by appropriate lawful bases, privacy notices, and an existing Data Protection Impact Assessments (DPIA). Across the areas reviewed, personal data was processed under Legal Obligation or Public Task, meaning consent was not required. The Garden Waste service collected only limited personal data but relied on a generic privacy notice and had no service-specific DPIA; transparency could be improved by adding clearer privacy information within FAQs and at the point of registration. Legal Services processed basic personal data, and occasionally special category data, within the IKEN system through document attachments and emails. System controls were limited, although data collection responsibilities remained with originating services. Planned system replacement is expected to strengthen data handling. Reintroducing the annual Data Management Questionnaire would further support compliance across all services.

Access controls were generally strong across all services, though the level of maturity varied. Revenues and Benefits demonstrated the most robust approach, with conflict-of-interest checks, annual access reviews, detailed audit trails, and external assurance. Garden Waste also had solid controls through role-based access, MFA for corporate users, and available audit logs. IKEN access was restricted to only four authorised users within the Legal Services team which minimised risk. Data was securely hosted across all services with Revenues and Benefits using ISO 27001-certified UK Tier 4 data centres with encryption and Garden Waste operated within Bartec's encrypted cloud environment. Legal Services stored limited information on the locally hosted IKEN system. No breaches or unauthorised access had been reported. Physical and server security remained strong, supported by enhanced building entry controls and virtual hosting with automated backups. Revenues and Benefits and Garden Waste had clear retention periods with automated deletion of out-of-date records. In contrast, IKEN relied on staff manually entering closure and deletion dates before data could be removed, a known issue that is expected to be resolved through the planned system replacement. Data sharing was managed through formal agreements that set out required standards for security, handling, and retention.

Freedom of Information (FOI) training delivered by Legal Services had recently been expanded to include Data Protection whilst comprehensive Information and Cyber Security training was available, though completion was not mandatory or consistently monitored. Evidence of uptake was only identified within Revenues and Benefits, indicating inconsistent embedding of training across the organisation.

Agreed actions from the audit	Priority
The Council should develop and implement a dedicated Data Protection Policy that combines all GDPR and Data Protection Act requirements, including roles and responsibilities, the full data lifecycle, expectations for DPIAs, privacy notices, incident reporting, training and data subject rights.	●
Develop and implement service-specific privacy notices and Data Protection Impact Assessments (DPIAs) for each area with distinct processing activities and make these easily accessible to data subjects.	●
Reinstate the annual Data Management Questionnaire capturing key data governance controls, including data quality, retention, privacy notices, DPIAs, security, and staff training. Ensure these are reviewed by the SIRO/DPO to strengthen organisational oversight and ensure early identification of compliance gaps.	●
The Council should introduce mandatory data protection and information security training for all relevant staff, supported by routine monitoring of completion rates and timely follow-up of non-completion.	●

2.1 Background

This audit has been undertaken in accordance with the 2025/26 Internal Audit Plan as approved by the Audit & Accounts Committee. The audit covers the period April 2025 to January 2026 and has been conducted in conformance with the Public Sector Internal Audit Standards.

2.2 Context

The Council relies on effective data management to support the delivery of its statutory services, safeguard sensitive information, and enable informed decision-making across the organisation. As the Council modernises through new digital systems, shared services, and greater use of data in service planning, ensuring the accuracy, accessibility, and security of its information become increasingly important. Robust data governance is essential not only for operational efficiency but also to ensure compliance with UK GDPR and the Data Protection Act 2018. This audit sought to assess the adequacy of the Council's data management arrangements, including policies, controls, and practices, to determine whether they effectively supported organisational objectives and mitigated risks related to data quality, security, retention, and usage. To achieve this, we looked at arrangements within Revenues and Benefits, Legal Services and the Operations Service.

2.3 Scope of Audit

In this audit we reviewed and tested the adequacy and effectiveness of the controls and processes established by management to mitigate the key risks relating to the following areas:

- Governance and accountability;
- Data collection, retention and sharing;
- Data storage and access; and
- Data handling and security risks.

Annex A

Scope, responsibilities and assurance

Approach

1 The Internal Audit Service operates in accordance with Public Sector Internal Audit Standards, 2017. The scope of internal audit work encompasses all the council's operations, resources and services including where they are provided by other organisations on its behalf.

Responsibilities of management and internal auditors

2 It is management's responsibility to maintain systems of risk management, internal control and governance. Internal audit is an element of the internal control framework assisting management in the effective discharge of its responsibilities and functions by examining and evaluating controls. Internal auditors cannot therefore be held responsible for internal control failures.

3 We have planned our work so that we have a reasonable expectation of detecting significant control weaknesses. We have reported all such weaknesses to management as they have become known to us, without undue delay, and have worked with management to develop proposals for remedial action.

4 Internal audit procedures alone do not guarantee that fraud will be detected. Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud or other irregularities which may exist, unless we are requested to carry out a special investigation for such activities in a particular area.

5 Internal audit's role includes assessing the adequacy of the risk management processes, key internal control systems and corporate governance arrangements put in place by management and performing testing to ensure those controls were operating effectively for the period under review.

Basis of our assessment

6 My opinion on the adequacy of control arrangements is based upon the result of internal audit work undertaken and completed during the period in accordance with the plan approved by the Audit and Accounts Committee. Sufficient, reliable and relevant evidence has been obtained to support the recommendations made.

Limitations to the scope of our work

7 Other than as set out in the audit plan for the year there have been no limitations to the scope of the audit work.

Limitations on the assurance that internal audit can provide

8 There are inherent limitations as to what can be achieved by internal control and consequently limitations to the conclusions that can be drawn from our work as internal auditors. These limitations include the possibility of faulty judgement in decision making, of breakdowns because of human error, of control activities being circumvented by the collusion of two or more people and of management overriding controls. Further, there is no certainty that internal controls will continue to operate effectively in future periods or that the controls will be adequate to mitigate all significant risks which may arise in the future.

9 Decisions made in designing internal controls inevitably involve the acceptance of some degree of risk. As the outcome of the operation of internal controls cannot be predicted with absolute assurance any assessment of internal control is judgmental.

Access to this report and responsibility to third parties

10 This report has been prepared solely for Rossendale Borough Council. It forms part of a continuing dialogue between the Internal Audit Service, the chief executive, Audit and Accounts Committee and management of the council. It is not therefore intended to include every matter that came to our attention during each internal audit assignment.

11 This report may be made available to other parties, such as the external auditors. However, no responsibility is accepted to any third party who may receive this report for any reliance that may be placed on it and, in particular, the external auditors must determine the reliance placed on the work of the Internal Audit Service.

Annex C

Audit assurance and residual risks

Note that our assurance may address the adequacy of the control framework's design, the effectiveness of the controls in operation, or both. The wording below addresses all these options and we will refer in our reports to the assurance applicable to the scope of the work we have undertaken.

- **Substantial assurance**: the framework of control is adequately designed and/ or effectively operated.
- **Reasonable assurance**: the framework of control is adequately designed and/ or effectively operated overall, but some action is required to enhance aspects of it and/ or ensure that it is effectively operated throughout.
- **Limited assurance**: there are some significant weaknesses in the design and/ or operation of the framework of control that put the achievement of its objectives at risk.
- **No assurance**: there are some fundamental weaknesses in the design and/ or operation of the framework of control that could result in failure to achieve its objectives.

Classification of residual risks requiring management action

All actions agreed with management are stated in terms of the residual risk they are designed to mitigate.

- **Extreme residual risk**: critical and urgent in that failure to address the risk could lead to one or more of the following: catastrophic loss of the county council's services, loss of life, significant environmental damage or significant financial loss, with related national press coverage and substantial damage to the council's reputation. *Remedial action must be taken immediately*
- **High residual risk**: critical in that failure to address the issue or progress the work would lead to one or more of the following: failure to achieve organisational objectives, significant disruption to the council's business or to users of its services, significant financial loss, inefficient use of resources, failure to comply with law or regulations, or damage to the council's reputation. *Remedial action must be taken urgently*.
- **Medium residual risk**: failure to address the issue or progress the work could impact on operational objectives and should be of concern to senior management. *Prompt specific action should be taken*.
- **Low residual risk**: matters that individually have no major impact on achieving the service's objectives, but where combined with others could give cause for concern. *Specific remedial action is desirable*.