WEST LINDSEY DISTRICT COUNCIL

Internal Audit Progress Report

25 November 2025

CONTENTS

Key messages 3

Appendices

Appendix A: Progress against the internal audit plan 2025/26 5
Appendix B: Other matters 6
Appendix C: Key performance indicators 7

KEY MESSAGES

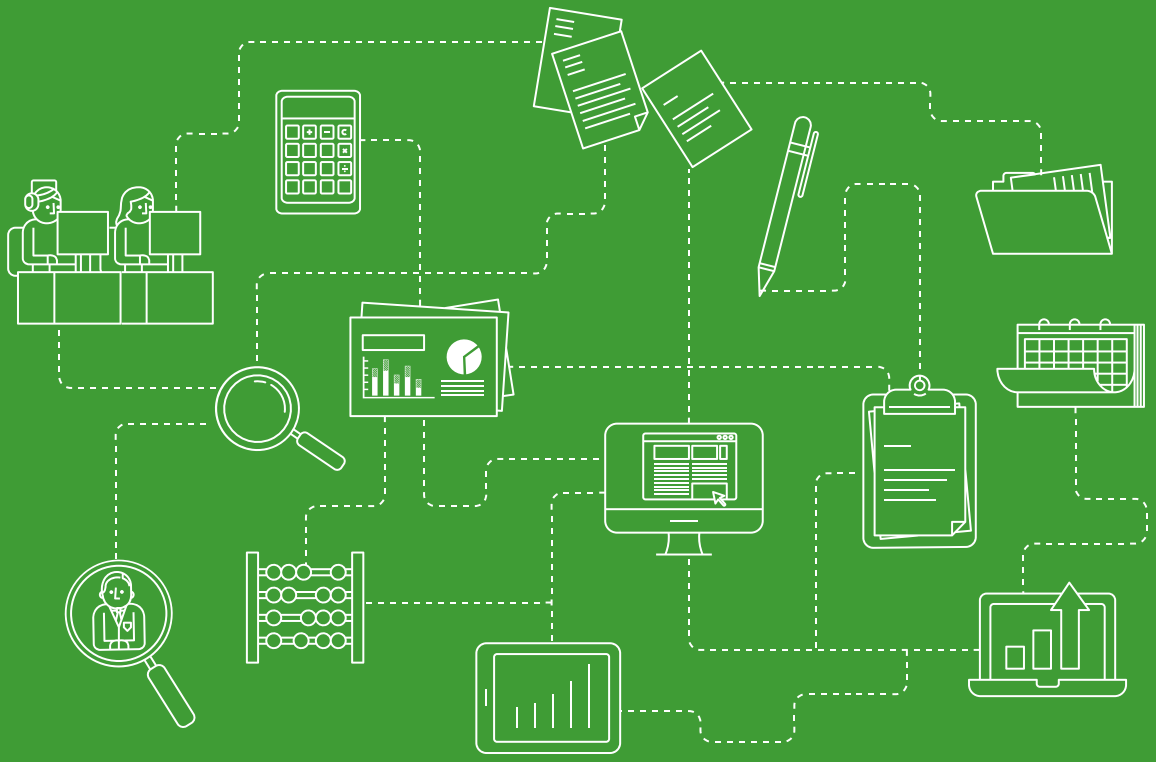
The internal audit plan for 2025/26 was approved by the Governance and Audit Committee at the 11 March 2025 meeting. This report provides an update on progress against the plan and summarises the results of our work to date.

We have issued two reports as final as part of the internal audit plan since the Governance and Audit Committee meeting in September 2025. These are Cyber Security Operations (3.25.26), and Members Onboarding and Training (4.25/26).

- Although the Members Onboarding and Training report has been finalised by management in the specific audit area, this will now be presented to the January 2026 meeting. This is due to the timings of the Management Team meeting to formally approve the report taking place the day before the Chairs Briefing, thus not allowing enough time to be included in the papers. **[To note]**
- Details of the progress made against the internal audit plan are included at Appendix A. **[To note]**
- Fieldwork dates have been agreed with management for all of the internal audits scheduled for 2025/26 to ensure that all fieldwork will be completed by the end of the year, and our Head of Internal Audit Opinion can be provided at the first meeting of the 2026/27 financial year. Details are included in Appendix B. **[To note]**

Appendices

02



APPENDIX A: PROGRESS AGAINST THE INTERNAL AUDIT PLAN 2025/26

Assignment	Status / Opinion issued	Actions agreed				Target Governance and Audit Committee meeting	Actual Governance and Audit Committee meeting
		Advisory	Low	Medium	High		
Fraud Risk Assessment - Follow Up	Final Report Issued / Reasonable Assurance	0	1	3	0	July 2025	July 2025
Follow Up 1	Final Report Issued / Reasonable Progress	0	3	1	0	September 2025	September 2025
Cyber Security Operations	Final Report Issued / Substantial Assurance	0	1	1	0	November 2025	November 2025
Members Onboarding and Training	Final Report Issued / Substantial Assurance	0	2	0	0	November 2025[1]	
Grant Funding and Grant Management	Fieldwork commencing 20 October 2025					January 2026	
Financial Resilience and Scrutiny	Fieldwork commencing 3 November 2025					January 2026	
Procurement	Fieldwork commencing 1 December 2025					January 2026	
HR System Readiness	Fieldwork commencing 1 December 2025					January 2026	
Combined Assurance	Fieldwork commencing 1 December 2025					January 2026	
Planning Enforcement	Fieldwork commencing 5 Janaury 2026					March 2026	
Emergency Planning / BCP	Fieldwork commencing 26 January 2026					May 2026	
Climate Change Strategy	Fieldwork commencing February 2026					May 2026	
Follow Up 2	Fieldwork commencing 9 March 2026					May 2026	

[1] Although this report has been finalised by management in the specific audit area, this will now be presented to the January 2026 meeting. This is due to the timings of the Management Team meeting to formally approve the report taking place the day before the Chairs Briefing, thus not allowing enough time to be included in the papers.

APPENDIX B: OTHER MATTERS

Quality assurance and continual improvement

To ensure that RSM remains compliant with the PSIAS framework we have a dedicated internal Quality Assurance Team who undertake a programme of reviews to ensure the quality of our audit assignments. This is applicable to all Heads of Internal Audit, where a sample of their clients will be reviewed. Any findings from these reviews are used to inform the training needs of our audit teams.

As part of the Quality Assessment and Improvement Programme, none of your files were selected for Internal Quality Monitoring programme during 2024/25. From the results of the reviews undertaken across our client base, there are no areas which we believe warrant flagging to your attention as impacting on the quality of the service we provide to you.

In addition to this, any feedback we receive from our post assignment surveys, client feedback, appraisal processes and training needs assessments is also taken into consideration to continually improve the service we provide and inform any training requirements.

Post assignment surveys

We are committed to delivering an excellent client experience every time we work with you. Your feedback helps us to improve the quality of the service we deliver to you. Following the completion of each product, we include a link to a brief survey in each report we issue.

APPENDIX C: KEY PERFORMANCE INDICATORS

Delivery				Quality			
	Target	Actual	Notes*		Target	Actual	Notes*
Audits commenced in line with original timescales*	Yes	Yes		Conformance with PSIAS	Yes	Yes	
Draft reports issued within 10 days of debrief meeting	10 working days	*6 working days (average)*		Liaison with external audit to allow, where appropriate and required, the external auditor to place reliance on the work of internal audit	Yes	Yes	
Management responses received within 10 days of draft report	10 working days	*10 working days (average)*		Response time for all general enquiries for assistance	2 working days	*2 working days*	
Final report issued within 3 days of management response	3 working days	*2 working days (average)*		Response for emergencies and potential fraud	1 working day	*N/A*	

Notes
This takes into account changes agreed by management and the Governance and Audit Committee during the year. Through employing an agile or a flexible approach to our service delivery we are able to respond to your assurance needs.

FOR FURTHER INFORMATION CONTACT

Rob Barnett, Head of Internal Audit

Email: Robert.Barnett@rsmuk.com

Aaron Macdonald, Managing Consultant

Email: Aaron.Macdonald@rsmuk.com

AUDIT OUTCOME OVERVIEW – CYBER SECURITY OPERATIONS

Background:

We have conducted a review of the Council's cyber security – operations controls, ie IT asset management, logging and monitoring, and incident management arrangements. The objective of this review was to assess whether the controls and processes in these areas were appropriately designed and operating effectively to support the security, integrity, and resilience of the Council's IT environment.

Effective management of IT assets, logging, and incident response is essential for maintaining control over the Council's technology environment and ensuring operational resilience. Accurate inventories and asset registers help identify and protect critical assets, while robust logging and monitoring enable timely detection of security incidents. Strong incident management processes, supported by disaster recovery procedures, help minimise the impact of disruptions and support business continuity. Together, these controls reduce cyber and operational risks, ensure regulatory compliance, and maintain stakeholder confidence.

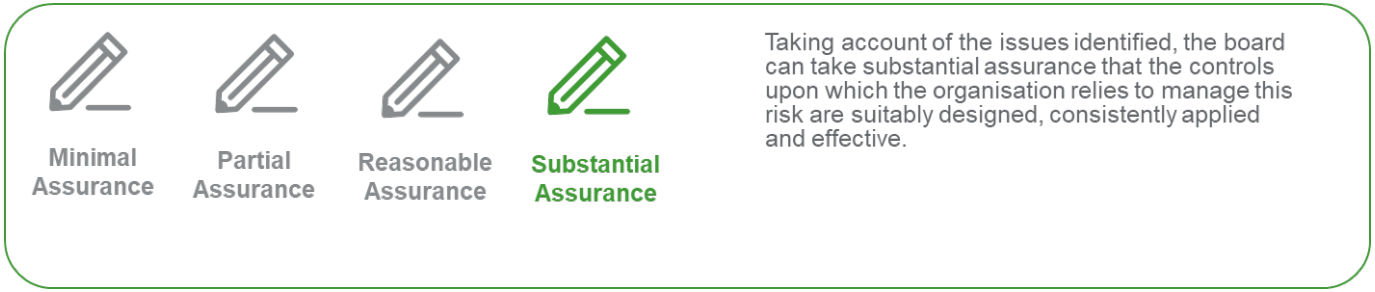
Conclusion:

Our review found that the Council has implemented key controls across asset management, logging and monitoring, and incident management. The Council uses LanSweeper as its asset management tool for both hardware and software. A Security Information and Event Management (SIEM) solution has also been implemented, capturing logs from the firewall, internet traffic, end-user devices, email systems, and Microsoft Defender, which serves as the anti-virus solution. In addition, Active Directory activity is monitored through AD Audit Plus and Microsoft Defender, covering events such as login failures, account modifications, deletions, creations, password changes, and account lockouts. For Incident Management, the Council has developed a Cyber Incident Response Plan to guide the incident monitoring, detection and response. The ICT Business Continuity Plan, which is regularly reviewed in conjunction with Lincolnshire Resilience Form (LRF)'s requirement, helps ensure timely response and resolution for major disruptions. In addition, staff receive training on identifying and reporting cyber incidents, and cyber-related staff undergo more specialised training on incident escalation and subsequent recovery procedures.

However, we have identified areas requiring improvement to strengthen Council's cyber security controls. In particular, there is no clear ownership, formal approval, or timely review of key IT policies and procedures, including the Information Systems Asset Management Policy, Cyber Security Monitoring Policy, Change Management Procedure, and ICT Disaster Recovery Policy. In addition, the Council has not established a documented log retention policy defining the retention period and scope of logs maintained within its SIEM tool, Microsoft Sentinel.

As a result, we have agreed one medium and one low priority action.

Internal Audit Opinion:



Audit themes:

Policies and Procedures

- Several key IT governance documents, including the Information Systems Asset Management Policy, Cyber Security Monitoring Policy, and Change Management Procedure, are not subject to appropriate ownership, approval, or timely review. For example, the Asset Management Policy has not been reviewed since its approval in February 2024, the Cyber Security Monitoring Policy is not scheduled for review until 2028, the Change Management Procedure lacks clear ownership and evidence of formal approval, and the IT Disaster Recovery Policy has not been reviewed since 2022, as per its scheduled review cycle. The absence of defined ownership and review cycles increases the risk that security controls may be based on outdated or incomplete requirements, reducing the Council's ability to respond to emerging cyber threats. This could lead to gaps in monitoring, change management, asset governance, and incident response, increasing the likelihood of unauthorised access, data breaches, and prolonged recovery following a cyber incident. **(Medium)**

Information Technology

- The Council has implemented a monitoring and alerting framework using Microsoft Sentinel, which aggregates logs from key sources, including the firewall, antivirus, internet traffic, end-user devices, and email systems through tools such as Microsoft Azure and Defender. Security events are actively monitored, categorised by severity, and assigned to responsible personnel for investigation.
- Active Directory is monitored through AD Audit Plus and Microsoft Defender, capturing events such as login failures, account modifications, deletions, creations, password changes, and lockouts. Additional metadata, including IP addresses and user activity types, is also collected. Any incidents identified are automatically notified to designated personnel within the IT Helpdesk for investigation.

Record Keeping

- The Council has implemented LanSweeper as its asset management solution, maintaining both the hardware and software asset registers. LanSweeper is deployed across all hardware within the estate and automatically scans devices as they connect to the Council's network. Exports reviewed confirmed that the registers capture key asset details such as make and model, operating system, purchase type, support arrangements, warranty status, serial numbers, and scan history. More granular information can also be accessed for specific assets, including build version, active/inactive status, physical location, last scan dates, and SCCM server details.

Log Retention

- A Security Information and Event Management (SIEM) solution is in place (Microsoft Sentinel), capturing logs from the firewall, internet traffic, end-user devices, email systems, and Microsoft Defender, which serves as the anti-virus solution. However, the Council has not formally documented the retention period of these logs within any approved policy or procedure. **(Low)**

SUMMARY OF MANAGEMENT ACTIONS

The action priorities are defined as:

High	Medium	Low
Immediate management attention is necessary.	Timely management attention is necessary.	There is scope for enhancing control or improving efficiency.

Ref	Action	Priority	Responsible Owner	Date
1	Management will ensure that key IT policies and procedures, including the Information Systems Asset Management Policy, the Cyber Security Monitoring Policy, Change Management Procedure, and IT Disaster Recovery Policy, are: • Formally approved and assigned clear ownership. • Dated and subject to version control. • Reviewed on a regular basis, with the frequency appropriate to risk and regulatory requirements, and following any significant changes to the environment, to ensure they remain accurate, relevant, and aligned with best practice.	Medium	ICT Shared Services Manager	31 March 2026
2	Management will formally document its log retention policy within an appropriate governance document, such as the Cyber Security Monitoring Policy. This documentation may include: • The retention duration (e.g. 90 days) • The scope of logs covered (e.g. security, application, system logs) • A schedule for periodic review to ensure continued relevance and alignment with regulatory requirements.	Low	ICT Shared Services Manager	31 March 2026