Hinckley & Bosworth Borough Council
Audit Committee – 4 February 2026
Internal Audit Progress Report

Date Prepared: January 2026

Strictly private and confidential

forvis mazars

Contents

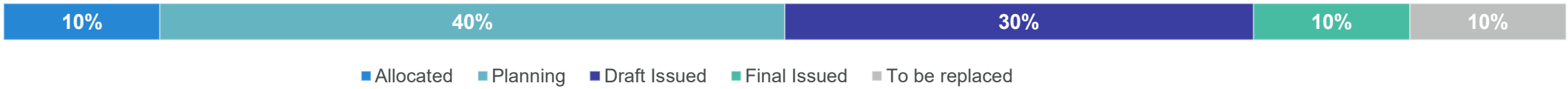
Disclaimer

This report ("Report") was prepared by Forvis Mazars LLP at the request of Hinckley & Bosworth Borough Council and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of Hinckley & Bosworth Borough Council and to the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk. Please refer to the Statement of Responsibility in this report for further information about responsibilities, limitations and confidentiality.

1. Snapshot of Internal Audit Activity

Below is a snapshot of the current position of the delivery of the 2025/26 Internal Audit Plan.



AC decisions needed

- Note the progress being reported and consider final reports included separately in the paper pack,

RAG status of delivery of plan to revised timetable — **Behind**

Key updates

The final report for Service Level Budgeting has been issued. The draft reports for Partnership Governance, Council Tax and NNDR, and Licensing have been issued and we are waiting for management responses.

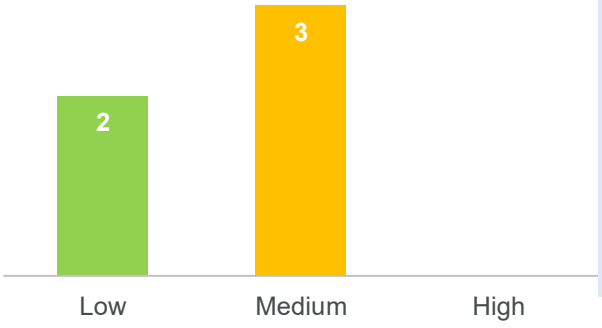
We have set the RAG status for plan delivery as Behind at the time of drafting this update as there are two audits that have not taken place when originally planned.
After we had issued a draft Terms of Reference for the Work Capacity audit, we were advised by the Interim Director (Resources and Streetscene Services) that the audit area was not relevant to the Council and a replacement audit area would be suggested by the Leadership Team, however we have not yet had those discussions.
The Business Continuity audit was meant to commence in January 2026, however we were unable to scope the audit despite a number of attempts to obtain key contact details. We will work with the Assistant Director Finance & Audit (S151 Officer) to have this re-scheduled.
Enforcement is scheduled for February 2026 and we are working with key contacts to plan this review.

An overview of the Internal Audit Plan is in Section 2.

Thought Leadership – Navigating Cyber Risks, can be found in Section 3.

Assurance opinions to date

Audit recommendations to date



2. Overview of Internal Audit Plan 2025/26

The table below lists the status of all reviews within the 2025/26 Plan.

Review	Original Days	Actual Days	Audit Sponsor	Status	Start Date	AC	Assurance Level	Total	High	Medium	Low
Partnership Governance	10	10	Interim Director (Resources and Streetscene Services)	Draft	September 2025	-	-	-	-	-	-
Corporate Governance	10	10	Interim Director (Resources and Streetscene Services)	Planning	TBC	-	-	-	-	-	-
Service Level Budget Monitoring	10	10	S151 Officer	Final	September 2025	-	-	-	-	-	-
Revenue and Benefits - Council Tax and NNDR	10	10	S151 Officer	Draft	October 2025	-	-	-	-	-	-
Licensing	10	10	Interim Director, Community Services	Draft	October 2025	-	-	-	-	-	-
Workforce Capacity*	10	10	TBC	To be replaced *	November 2025	-	-	-	-	-	-
Business Continuity	10	10	TBC	Planning	January 2026	-	-	-	-	-	-
Enforcement Action	10	10	TBC	Planning	February 2026	-	-	-	-	-	-
IT Audit	12	12	TBC	Planning	TBC	-	-	-	-	-	-
Follow up	5	5	S151 Officer	Allocated	March 2026	-	-	-	-	-	-
Management and reporting	15	15	-	-	-	-	-	-	-	-	-
Totals	**112**	**112**					**Totals**	**-**	**-**	**-**	**-**

*We were advised by the Interim Director (Resources and Streetscene Services) that this audit area is not relevant for the Council. An alternative area is yet to be agreed.

3. Thought Leadership – Navigating cyber risks: How LAs can build resilience against emerging threats

The recent cyber-attack on local authorities in November 2025 serves as a stark reminder of the evolving threats facing the public sector. As cyber risks grow in scale and sophistication, councils must adopt robust cybersecurity practices to safeguard essential services and sensitive data.

Key Cyber Risks Facing Local Authorities

Third Party Vulnerabilities:
Many councils rely on shared IT services or external suppliers. A breach in one area can quickly escalate, disrupting services across multiple authorities. Therefore, supply chain security is no longer optional, but it's essential.

Ransomware and phishing attacks:
Local authorities are prime targets for ransomware and phishing campaigns. These attacks can lead to service outages, data breaches, and significant financial losses.

Regulatory Compliance:
The Cyber Security and Resilience Bill (2025) requires councils to demonstrate resilience and report incidents promptly. Whilst the Bill is still progressing, aligning with its principles now will help future-proof your organisation.

Legacy Infrastructure:
Outdated systems are often harder to patch, lack modern security controls, and can serve as easy entry points for attackers. Many local authorities still rely on older technology that may no longer be supported by vendors, increasing exposure to exploits. While cloud adoption grows, many critical services and data still reside on-premises. Poorly secured on-premises systems can become a single point of failure.

Why cyber security matters for local authorities?

Local authorities manage critical services - from housing and social care to education and public safety. A successful cyber-attack can disrupt these services, compromise citizen data and erode public trust. With the Cyber Security and Resilience Bill (2025) introducing stricter requirements for incident reporting and resilience planning, now is the time to strengthen your cyber posture.

Best practices to mitigate risks:

- Modernise legacy systems;
- Incident response planning;
- Staff training and awareness
- Multi-Factor authentication (MFA);
- Patch Management;
- Data backup and recovery; and
- Collaboration with peers

For full explanations, please read the full article here.

Read full article here

Contact

Forvis Mazars

Peter Cudlip
Partner
Peter.Cudlip@mazars.co.uk

Sarah Knowles
Internal Audit Manager
Sarah.Knowles@mazars.co.uk

Sana Arshad
Assistant Manager
Sana.Arshad@mazars.co.uk

Statement of Responsibility

We take responsibility to Hinckley & Bosworth Borough Council for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or reply for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: 30 Old Bailey, London, EC4M 7AU, United Kingdom. Registered in England and Wales No 0C308299.

forvis mazars