Cherwell
DISTRICT COUNCIL
NORTH OXFORDSHIRE

Internal Audit Progress Report 2025/26

Date: 16 July 2025

APPENDIX 1

Veritau
Assurance for the public sector

CONTENTS

3	Background
3	Internal audit progress
4	Follow up
8	Annex A: Internal audit work in 2025/26
9	Annex B: Current audit priorities
10	Annex C: Summary of key issues from finalised audits
13	Annex D: Assurance engagement opinions and finding priorities

BACKGROUND

1 Internal audit provides independent and objective assurance and advice about the council's operations. It helps the organisation to achieve its overall objectives by bringing a systematic, disciplined approach to the evaluation and improvement of the effectiveness of risk management, control, and governance processes.

2 The work of internal audit is governed by the Accounts and Audit Regulations 2015 and relevant professional standards. These include the Global Internal Audit Standards and the Application Note: Global Internal Audit Standards in the UK Public Sector.

3 In accordance with the Global Internal Audit Standards (UK Public Sector) the Head of Internal Audit is required to report progress against the internal audit plan (the work programme) agreed by the Accounts, Audit & Risk Committee, and to identify any emerging issues which need to be brought to the attention of the committee.

4 The internal audit work programme was agreed by this committee in March 2025.

5 Veritau has adopted a flexible approach to work programme development and delivery. Work to be undertaken during the year is kept under review to ensure that audit resources are deployed to the areas of greatest risk and importance to the council.

6 The purpose of this report is to update the committee on internal activity up to 30 June 2025.

INTERNAL AUDIT PROGRESS

7 A summary of internal audit work currently underway, as well as work finalised in the year to date, is included in annex A. Annex A also details other work completed by internal audit during the year.

8 Since our last report to this committee, two audits have been finalised. These were the two ICT audits in the 2024/25 programme and both received ratings of Substantial Assurance.

9 Three audits from the 2024/25 work are nearing completion. Draft reports have been issued for the risk management and performance management audits and are currently being considered by officers. Fieldwork for the governance and decision-making audit, which was started late in 2024/25 (as a replacement for the deferred LATCO governance audit), has been completed. A closing meeting will be held, and a report drafted, during July.

10 The 2025/26 audit of cybersecurity is in progress. Four other 2025/26 audits are in the planning stage. Contact will be made with officers over the coming weeks to agree specifications and begin fieldwork.

11 The work programme, showing current priorities for internal audit work, is included at annex B. This reflects the efforts being made to conclude prior year work, and that the 2025/26 programme is underway. The remaining three audits in the 2025/26 programme are currently scheduled to be delivered in the second half of the year.

12 The two ICT audits that have been finalised since the last report to this committee are included in annex C. The annex summarises the key findings from these audits, and includes actions agreed with officers to address identified control weaknesses.

13 Annex D lists our current definitions for finding priorities and overall assurance levels.

FOLLOW UP

14 All actions agreed with services as a result of internal audit work are followed up to ensure that underlying control weaknesses have been addressed.

15 With the support of Corporate Leadership Team (CLT), we have recently agreed a follow-up and escalation procedure. This sees any non-responses (or unsatisfactory responses) to requests for evidence of completion brought to the attention of increasingly more senior members of staff and, ultimately, to this committee.

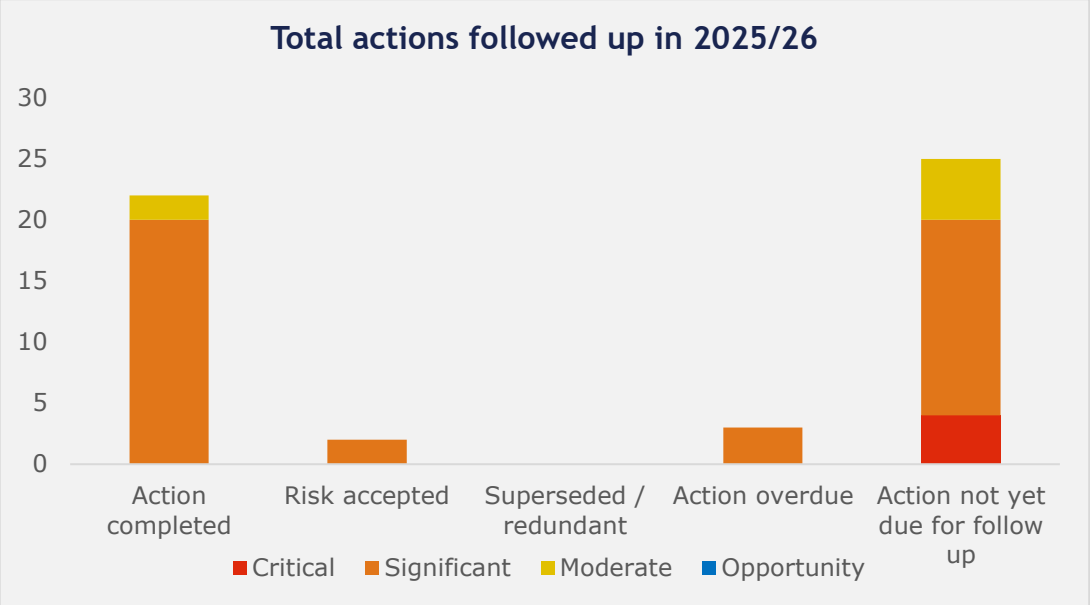
16 This procedure sets out when and with whom contact will be made to confirm completion of actions. It includes a series of escalation points which are used where a satisfactory response has not been received and so actions are considered overdue. These escalation points involve, in order:

- Notifying the relevant director
- Presenting overdue actions to CLT (monthly)
- Reporting unresolved overdue actions to the Accounts, Audit & Risk Committee

17 In figure 1 on the following page, the status of agreed actions from follow-up activity undertaken in the first quarter of 2025 is shown. Actions have been categorised by the rating of the finding from which they were raised (i.e. from a scale of opportunity to critical – see annex D for definitions).

18 For clarity, figure 1 is showing the results of all actions followed up in Q1 2025, regardless of when they were originally due (i.e. it may also include actions which fell due prior to the reporting period but which are still being followed up). For completeness, it also shows the number of actions which have been agreed in finalised audits but which have either (a) not yet fallen due and so have not been followed up or (b) which have been followed up and a revised completion date has been agreed.

Figure 1: Total actions followed up in 2025/26



19 In the table 1, below, the rating of the finding from which the action was agreed is presented. This is shown to illustrate the relative importance of the actions agreed with management that have been followed up.

Table 1: Number of actions by finding rating 2025/26 YTD

	Finding Rating				Total
	Critical	Significant	Moderate	Opportunity	
All actions followed up in 2025/26	2	36	3	0	41

20 A total of 41 agreed actions have required follow up this year[1]. Of these, 22 have been satisfactorily implemented.

21 An additional 2 actions have been marked as risk accepted[2]. The risk accepted status is used when senior management has decided to accept the risk of not completing the action. In practice, this is usually because circumstances have changed and so the actions are now redundant for the purposes of follow-up.

[1] For information, a further 11 actions have been agreed which are not due for follow up at the time of reporting.
[2] These relate to 2 actions related to frequent emissions monitoring and reporting from the 2022/23 Climate audit which officers have identified as not being in line with standard practice or being realistic to implement.

22 A total of 14 actions have had their original implementation timescale extended (i.e. a revised date has been agreed with the action owner). These relate to the following audits:

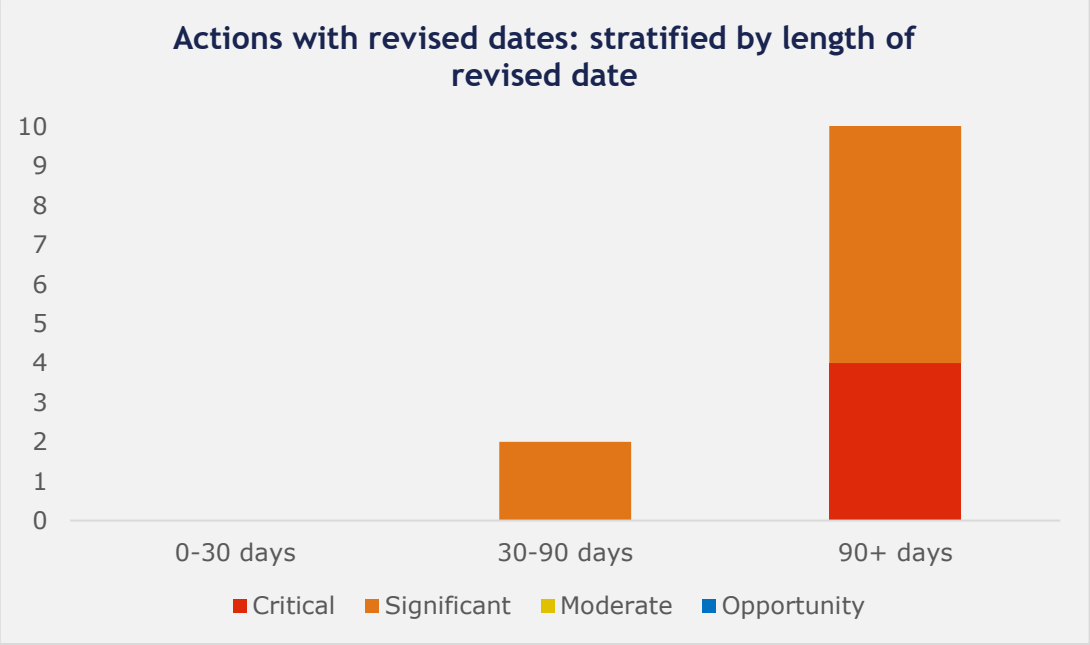
- HR
- Revenues and Benefits IT Application
- Direct Payments
- PCI
- Utilities
- Corporate Health and Safety
- GDPR
- Climate

23 The figure below groups agreed actions by how far from the implementation date the revised date has been set, and the priority of the action.

24 We agree revised dates where the delay in addressing an issue will not lead to unacceptable exposure to risk and where the delays may be unavoidable. However, the committee should be aware that lengthy or continued revised dates do inevitably lead to a degree of risk exposure to the council.

25 From figure 2, below, the committee can see that 2 actions have been revised between 30-90 days from the original implementation date. Of these, both were linked to 'significant' rated findings. In addition, 10 actions linked to 'significant' rated findings and 4 actions linked to 'critical' rated findings have been revised 90+ days from the implementation date.

Figure 2: Length of revised dates for action implementation



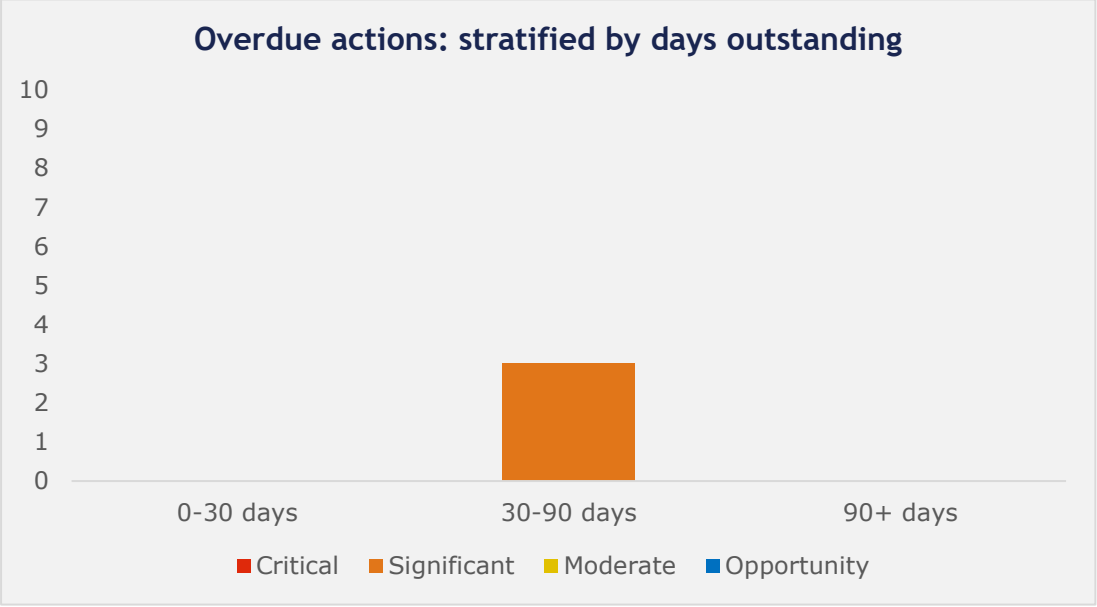
26 At the time of reporting, 3 agreed actions are overdue. These relate to the following audits:

- Corporate Health and Safety
- Climate

27 Actions are categorised as overdue when the implementation date (either original or revised) has passed, and we have not had an adequate response from the action owner to confirm completion.

28 Figure 3, below, demonstrates that all 3 actions are overdue by between 30-90 days from the agreed implementation date.

Figure 3: Length of time actions have been overdue



ANNEX A: INTERNAL AUDIT WORK IN 2025/26

Final reports issued

Audit	Reported to Committee	Opinion
Cloud, network and security management and monitoring	July 2025	Substantial Assurance
ICT applications: third party assurance	July 2025	Substantial Assurance

Audits in progress

Audit	Status
Risk management	In draft
Performance management	In draft
Governance and decision-making	In progress
Cybersecurity: user awareness and training	In progress
Licensing	Planning
LATCO governance: Crown House and Graven Hill	Planning
Utilities management	Planning
Treasury management	Planning

Other work completed in 2025/26

Internal audit work has been undertaken in other areas during the year, including those listed below.

- Follow up of agreed actions, including preparation of regular reports to Corporate Leadership Team (CLT).
- Development of follow-up and escalation procedure
- Attendance at, and support to, CLT, Corporate Oversight Governance Group, and the Statutory Officers' Group.
- Contribution to the council's governance dashboard.
- Contribution to the council's annual governance statement.

ANNEX B: CURRENT AUDIT PRIORITIES

Audit / Engagement	Rationale
Category 1 (do now)	
Risk management	Key cross-cutting system of governance.
Performance management	Provides coverage of key assurance area. Risks and controls are changing.
Governance and decision-making	Provides coverage of key assurance area. Being undertaken following a request from senior management.
Cybersecurity: user awareness and training	Provides coverage of key assurance area.
Licensing	Key operational system with no recent coverage.
LATCO governance: Crown House and Graven Hill	Provides coverage of key assurance area. Being undertaken following a request from senior management.
Utilities management	Being undertaken as a follow-up audit, in response to the identification of significant control weaknesses in a previous audit.
Treasury management	Key financial system with no recent coverage.
Category 2 (do next)	
Section 106 agreements	Risks and controls are changing.
Category 3 (do later)	
Procurement Act compliance	-
ICT asset management	-

ANNEX C: SUMMARY OF KEY ISSUES FROM AUDITS FINALISED SINCE THE LAST REPORT TO THE COMMITTEE

System/area (month issued)	Opinion	Area reviewed	Comments / Issues identified	Management actions agreed
Cloud, network and security management and monitoring (May 2025)	Substantial Assurance	This audit reviewed arrangements for its co-managed service contract for managed cloud support, data platforms, network service, and security operations centre.	A comprehensive call-off contract exists between the provider and the council under the G-Cloud 13 framework agreement, with supporting statements of work and service definitions for each service purchased. There are clear roles and responsibilities for the management of the contract, with experienced officers providing informal training to officers overseeing day-to-day management activities. Governance, risk management and reporting arrangements established for the oversight of the contract reflect the council's expectations for a contract of this scale. Two areas for improvement were identified. Firstly, the terms of the contract could be more clearly defined in relation to quality assessment of changes	The council will contact the provider to get clarity, in writing, of the arrangements for: ▲ Quality assessment standards for changes made ▲ Secure data destruction ▲ Prioritisation of service restoration in the event of provider failure ▲ Exit plan A formal monitoring schedule will be established, to include reviews of provider activity logs, periodic due diligence checks and certification reviews. The council will consider scheduling audit

System/area (month issued)	Opinion	Area reviewed	Comments / Issues identified	Management actions agreed
			made by the provider, secure data destruction, and service restoration in the event of provider failure. Secondly, at the time of the audit, contractual monitoring arrangements were still being established. Monthly performance discussions with the provider were not being documented.	activity to exercise the right to audit the provider.
IT applications: third party assurance (May 2025)	Substantial Assurance	The audit sought to provide assurance that sufficient due diligence is carried out to verify that third party cloud-based applications are secure and accessible, and that performance is regularly reviewed to ensure that business needs continue to be met.	Suitable processes are in place to ensure the council's digital needs and existing resources are considered before procuring third party cloud-based applications. Due diligence is carried out during the procurement process. This is done using questionnaires which assess compliance against technical and security requirements. However, no periodic checks are performed during the contract period to confirm that the provider has maintained its accreditation. Performance reviews are held with supplier account managers to discuss the application's performance and ability to	A formal schedule and central log of annual security credential reviews for third-party application providers will be maintained. Responsibility will be assigned to Customer Success Leads to verify up-to-date certifications and security documentation from suppliers. Regular performance review meetings will be held with all third-party application providers for key systems.

System/area (month issued)	Opinion	Area reviewed	Comments / Issues identified	Management actions agreed
			meet business needs. However, these review meetings had not been held for one system and had not been consistently documented for the other applications tested.	Responsibilities and expectations for these meetings will be clearly defined to service areas by Customer Success Leads.

ANNEX D: ASSURANCE ENGAGEMENT OPINIONS AND FINDING PRIORITIES

Audit opinions

Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on four grades of opinion, as set out below.

Opinion	Assessment of internal control
Substantial assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Finding ratings

Critical	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Significant	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Moderate	The system objectives are not exposed to significant risk, but the issue merits attention by management.
Opportunity	There is an opportunity for improvement in efficiency or outcomes but the system objectives are not exposed to risk.