ISLE OF ANGLESEY COUNTY COUNCIL	
Report to:	Governance and Audit Committee
Date:	3 February 2026
Subject:	Internal Audit Update
Head of Service:	Marc Jones Director of Function (Resources) and Section 151 Officer MarcJones@anglesey.gov.wales
Report Author:	Marion Pryor Head of Audit and Risk MarionPryor@anglesey.gov.wales

Nature and Reason for Reporting:

The Governance and Audit Committee's terms of reference has an explicit requirement for the committee to oversee the council's internal audit arrangements as part of its legislative duties under the Local Government (Wales) Measure 2011. (3.4.8.10.1)

The committee is required to consider updates on the work of internal audit including key findings, issues of concern, management responses and action in hand as a result of internal audit work. It is required to consider summaries of specific internal audit reports as requested, including the effectiveness of internal controls and will monitor the implementation of agreed actions. (3.4.8.10.10)

This report fulfils the requirements of the Global Internal Audit Standards (UK public sector) consisting of the Global Internal Audit Standards (GIAS) of the IIA, the Application Note: Global Internal Audit Standards in the UK public sector and the CIPFA Code of Practice for the Governance of Internal Audit in UK Local Government.

It is also consistent with the recommended practices for the oversight of internal audit as determined in CIPFA's Position Statement: Audit Committees in Local Authorities and Police 2022.

1. Introduction

1.1 Standard 11.3 of the Global Internal Audit Standards (GIAS) requires the chief audit executive to communicate the results of internal audit services to the board and senior management periodically and for each engagement. In addition, Standard 15.1 requires the chief audit executive to disseminate the final communication to parties who can ensure that the results are given due consideration.

1.2 This report updates the committee, as at 21 January 2026, on the audits completed since the last update as at 21 November 2025, the current workload of internal audit and our priorities for the short to medium term going forward.

2. Recommendation

2.1 That the Governance and Audit Committee considers:
- the outcome of Internal Audit's engagements,
- the assurance provided and
- our priorities going forward.

Internal Audit Update

February 2026

Marion Pryor BA MA CMIIA CPFA ACFS

Head of Audit & Risk

Contents

Summary of Assurance Work Completed Since Last Update

1. This section provides an overview of assurance reports finalised since the meeting in December 2025, including the overall assurance rating and the number of issues/risks/opportunities raised.

2. We have finalised **one** piece of work in the period, summarised below and discussed in more detail later in the report:

Title	Assurance Level	Critical	Major	Moderate
Physical security and environmental control of data centres	Reasonable	0	0	1

Assurance Ratings

3. It is current practice in public sector internal audit teams to provide a summary opinion and assurance rating in the internal audit report. However, there is no standard definition or terminology, and it is for each head of internal audit to determine an appropriate methodology.

4. As organisations in the public sector increasingly work collaboratively with other public bodies, senior managers and audit committee members across the public sector were finding themselves receiving reports from more than one set of internal auditors. Auditors were being challenged about the consistency of their opinions because of the use of different terminology.

5. This led to CIPFA's Internal Audit Special Interest Group reviewing existing practices and considering the case for a common approach. The group published a briefing in 2020, recommending the case for standardising the terminology and proposed a set of opinions and supporting definitions for internal audit teams to use.

6. The council's assurance ratings mirrored the ratings proposed by the group and the assurance definitions largely reflected the definitions proposed by the group.

7. Members of the Governance and Audit Committee agreed the definitions at a meeting of the committee in April 2019, with minor changes following the publication of the CIPFA briefing in July 2020.

8. For the benefit of the new members of the committee, these assurance rating definitions are detailed to the right. This may help members to understand the levels of assurance applied to each audit and what assurance they may take from the level applied.

9. As discussed in a recent meeting, the level of assurance applied is not formulaic and does not directly equate to the number of issues, risks or opportunities raised.

10. In applying the most appropriate level of opinion, the auditor will use their professional judgement and consider the overall level of risk exposure, including the impact on the organisation as a whole. The ultimate decider is the response to the key question.

Assurance Rating Definitions

Level of Assurance	Definition
Substantial Assurance	Arrangements for governance, risk management and internal control are **good**. **We found no significant or material Risks/Issues.**
Reasonable Assurance	Arrangements for governance, risk management and/or internal control are **reasonable**. **There are minor weaknesses in the management of risks and/or controls but there are no risks to the achievement of objectives. Management and heads of service can address.**
Limited Assurance	Arrangements for governance, risk management and internal control are **limited**. **There are significant weaknesses in the management of risks and/or controls that put the achievement of objectives at risk. Heads of service need to resolve, and Leadership Team may need to be informed.**
No Assurance	Arrangements for governance, risk management and internal control are **significantly flawed**. **There are fundamental weaknesses in the management of risks and/or controls that will lead to a failure to achieve objectives. The immediate attention of Leadership Team is required, with possible Executive intervention.**

Physical and environmental control of data centres

Reasonable Assurance	Issues / Risks / Opportunities	
	0	Critical
	0	Major
	1	Moderate

11. Our review sought to answer the following key question:

    Does the council have adequate arrangements in place to minimise the key risks associated with physical access and environmental risks within the council's key IT infrastructure?

12. The audit of the council's two data centres confirmed that physical security and environmental controls are generally effective, with both sites featuring near-identical safeguards to protect IT hardware and minimise risks of data or service loss. Security at the primary site is robust, while the secondary site presents a minor residual risk due to external visibility of servers. CCTV, fire detection, and suppression systems are in place, though external monitoring and resilience against false triggers require attention.

13. Environmental controls, including airflow, temperature, humidity, and power supply arrangements, are functional but limited by insufficient monitoring and unresolved UPS error messages. Water ingress risks are minimal at the primary site but are present at the secondary site due to ground-level server positioning and absence of leak detection sensors.

14. Contingency and disaster recovery arrangements are reasonable but would benefit from formal documentation. As the council advances its 'cloud-first' strategy, physical risks will diminish, shifting focus to third-party contract management.

15. Overall, the outcome of the review was positive, with five recommendations raised by Salford Council IT auditors. When assessed against the council's risk assessment matrix, only one was assessed as moderate with the remainder classified as minor (green).
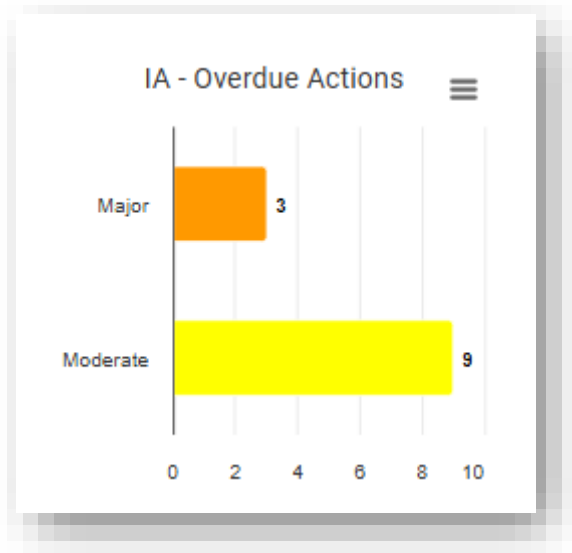
Work in Progress

16. The following pieces of work are currently in progress:

Area	Reason for Audit	Stage
Regulation and Economic	Investigation	Fieldwork
IT Audit: IT Asset Management	Strategic Risk Register (YM3)	Postponed until 2026-27 at the request of the Chief Digital Officer
Adult Social Care Finance: Financial Assessments – Residential and Nursing Care	First Follow Up	Fieldwork
Managing the Safeguarding Risk: • Follow Up • Supply Teachers	Strategic Risk Register (YM10 / YM12)	Fieldwork (delayed due to Care Inspectorate Wales visit)
Early Education and Childcare Grant Programmes	First Follow Up	Fieldwork
Financial Management	Strategic Risk Register (YM1)	Fieldwork
Disabled Facilities Grants (DFGs)	Second Follow Up	Fieldwork
Financial Systems – Payroll	IA Strategic Priority 2025-26	Fieldwork
Financial Systems – Creditors	IA Strategic Priority 2025-26	Fieldwork
Financial Systems – Bank Reconciliation	IA Strategic Priority 2025-26	Scoping
Financial Systems – General Ledger	IA Strategic Priority 2025-26	Scoping
Financial Systems – Treasury Management	IA Strategic Priority 2025-26	Scoping

Outstanding Actions

17. Work is progressing to support services with addressing all 'Issues / Risks / Opportunities' raised and implementing all outstanding actions.

18. As at 19/01/26, there are currently three 'major' actions and nine 'moderate' actions that have reached their target date for completion which have become 'overdue'.

19. These actions relate to two audit reports that are currently being followed up and the outcome of which will be reported to the next meeting:

- Early Education and Childcare Grant Programmes
- Adult Social Care Finance: Financial Assessments – Residential and Nursing Care

Priorities

Short/Medium Term Priorities

20. Our current workload can be seen in Work in Progress detailed earlier in this report. Delivery of the Internal Audit Strategy for 2025-26 has progressed well and many audits are nearing completion. Enough work will have been completed by the end of the year to enable the Head of Audit annual audit opinion to be provided.

Longer Term Priorities

21. Implementation of the requirements of the new Global Internal Audit Standards in the UK Public Sector will continue over the next 18 months.

22. Following their introduction in April 2025, the Global Internal Audit Standards in the UK Public Sector have since been reviewed and amended to include the Institute of Internal Auditors' (IIA) Topical Requirements. These are a mandatory component of the IIA's International Professional Practices Framework (IPPF), but do not automatically apply to internal audit in the UK public sector.

23. The Internal Audit Standards Advisory Board (IASAB), on behalf of the Relevant Internal Audit Standard Setters (RIASS), has determined that the IIA Cybersecurity topical requirement and user guide are fully applicable for the UK public sector from 5 February 2026. In the UK, additional standards are also relevant in this area and UK auditors will also consider the National Cyber Security Centre assessment framework (CAF).