



Meeting: Joint Audit Committee

Venue: Teams

Date: 28th of July 2026

2.00pm – 17.00pm

<u>Members:</u>	Ms Kate Curran (KC) Chairperson Mr David Macgregor (DM) Ms Julie James (JJ) Ms Caroline Wheeler (CW)
<u>JAC Attendees</u>	Mr Dafydd Llywelyn, Police and Crime Commissioner (PCC) Ms Carys Morgans, Chief Executive Officer (CM) Ms Nicola Davies, Chief Finance Officer (ND) Mr Jason Blewitt, Audit Wales (JB) Ms Michelle Reynolds, T-Head of Finance (MR) Mr Steve Cadenne, Head of HR Service Delivery (SC) Mr Marc Jones, Head of ICT (MJ) Mr Jonathon Maddock, TIAA (JM) Mr Edwin Harries, Director of Finance (EH) Ms Liz Reed, Planning and Assurance cycle Manager (LR) Mr Richard Janas, Insp HMIC Inspection (RJ) Mr John Carrol, Supt Head of Service Improvement Unit (JC) Miss Ellen Jones, Quality of Service caseworker OPCC
<u>Apologies</u>	Mr Ifan Charles, Chief Constable Mr Gary Phillips, T/Deputy Chief Constable Mr Farhan Shakoore, JAC member (FS) Ms Gaynor Maddox, Head of Programmes and Change
<u>Declarations of Interest:</u>	None

1. To confirm the minutes of the meetings held on the 23rd of June 2026

The minutes of the meeting held on the 23rd of June 2026 were deemed to be a true and accurate record of the meeting held, pending some slight amendments to initials of a speaker.

2. Review of Outstanding Actions

Action N°	Action Summary	To be progressed by	Progress
ACTION SUMMARY FROM THE MEETING HELD ON THE 28 th of January 2026			
A 31	That the committee is invited to observe a business continuity testing exercise in the future	GM	In Progress – Staff are backfilling the Business Continuity Officer vacant post for the interim. The new business continuity was launched the week commencing the 1st of June, and the desktop testing is now due to commence end of July/August. Once the initial stages are complete and the rapid testing exercises commence, then the JAC will be sent invites to take part. Additionally, the planned TIAA audit on this area had been moved to October to allow sufficient time for the new processes to be fully implemented.
A35	Members of the Committee to test the guest access of a JAC Teams Channel.	OPCC	In Progress - two Members volunteered and guest access has been granted on their devices. Members provided their feedback on the current process advising that it would be improved due to technical difficulties. Discussion ensued regarding the importance of the channel and the benefits for wider Force meetings that the JAC members attend. Agreed that CM will discuss further with ICT.
ACTION SUMMARY FROM MEETING HELD ON THE 31 ST OF MARCH 2026			
A 36	That a further review is undertaken to establish whether there are sufficient controls in place when an	SC	In progress – Payroll are undertaking a review, and the report

	individual has changes made to their working hours with a view to avoiding overpayments.		will be provided to the 29 th of September JAC meeting.
A 38	That an additional meeting of the Committee be arranged for December	OPCC	Complete – Arranged for Monday the 14th of December.
A 39	OPCC to liaise with the CEO to establish what is required from the Statement included within the Terms of Reference "Review the governance and assurance arrangements for significant partnerships or collaborations" and feed back to the Committee.	OPCC	In progress – Following information provided by Gwent OPCC regarding all Wales collaboration oversight board it was agreed that further clarity was required regarding the committee's role. Agreed that CM will discuss with the Welsh OPCC's and further discussions to be held at all Wales JAC training day.
A 42	MM to provide JAC members with an update on the LRF partnership engagement arrangements.	MM / ACC	Complete – Minutes from the latest meeting to be circulated with members. Although further question raised by members around whether this LRF has ever been audited, and who monitors action plans and which of Boards does it report to? JAC members were satisfied that this query could be dealt with outside of the meeting through CM.
A 47	That a review of the Forces scoring of the risk register is to be reviewed.	LR / DC	Complete -Following clarity from the Force it was established that the Force only uses the 4T's for both our corporate and department (local) risk management.
ACTION SUMMARY FROM MEETING HELD ON THE 23RD OF June 2026			
A 49	That a further review be conducted in respect of the ICT Infrastructure audit, including consideration of the	Tiaa	Complete – Amended report on the agenda for discussion.

	Audit Planning Memorandum (APM) and an assessment of delivery against its intended scope.		
A 50	To provide clarification on the specific areas and controls tested as part of the ICT Change Management audit.	Tiaa	Complete – Amended report on the agenda for discussion.
A 51	That further information be provided to the Committee to clarify the nature, scope and extent of the review conducted as part of the ICT audit relating to SyAP Cyber Security, and that the audit report be updated accordingly to fully articulate the scope of the review and the work undertaken.	Tiaa	Complete – Amended report on the agenda for discussion.
A 52	That CM meets with the Deputy Chief Constable (DCC) to discuss audit governance arrangements and ensure that these are appropriately captured within the remit of the newly established Strategic Audit and Assurance Board.	CM	Complete – Inaugral meeting of Strategic Audit and Assurance Board was held with DM attending on behalf of the committee. Although further work was noted to be required in relation to the Terms of Reference. This will be progressed by the Board.

3. Joint Audit Committee Work Plan

Members considered the forward workplan for the JAC meetings. It was suggested that an additional meeting is to be scheduled for April 2027 to assist with the workload.

Action A 53 - An additional meeting of the Committee be arranged for April 2027

4. Review Corporate Governance Issues and Consider the Corporate Governance Framework

a. Updates from Corporate Governance Board

The Committee received an update on the Corporate Governance Board meeting held on 14 July 2026, chaired by the DCC.

EH advised the Members that the Annual Governance Statement (AGS) had been presented and approved, with several associated actions signed off. The Board also noted HMICFRS inspection arrangements and were advised that the draft accounts had been submitted to Audit Wales by the end of June in line with statutory requirements and that the audit process remains ongoing.

EH continued to advise that updates were also received on JAC matters, IT audit activity, the Strategic Audit and Assurance Board, and policy developments. The Board also considered emerging governance issues and national developments relevant to policing and corporate governance.

b. Updated from Strategic Audit and Assurance Board

The Committee discussed the Terms of Reference for the Strategic Audit and Assurance Board and discussed arrangements for reporting and governance oversight.

Members noted that amendments to the Terms of Reference had previously been proposed and that a revised version was expected. It was agreed that further amendments should be incorporated, including comments raised at the meeting and feedback relating to Audit Wales.

Discussion took place regarding reporting arrangements from the Strategic Audit and Assurance Board. It was noted that the Board's responsibilities are broader than those of the Committee and include matters which may require reporting through different governance routes.

Members also raised concerns regarding the wording of the Board's decision-making authority within the Terms of Reference, noting that



it lacked clarity and should better define the extent of the Board's authority.

It was suggested that, given the breadth of the Board's agenda, different elements of its work may need to be reported to different governance bodies to ensure effective scrutiny and oversight.

Action A 54 - CM to discuss future reporting arrangements for the Strategic Audit and Assurance Board with the DCC and ensure proposed amendments to the Terms of Reference, including Audit Wales feedback, are reflected in the revised document.

c. Annual Governance Statement (AGS) – Review of Actions

LR provided the committee with an update on progress against the actions arising from the previous AGS.

Members noted that actions 9.2, 9.5 and 9.6 had previously been completed and discharged. The Committee reviewed the latest updates and agreed to discharge actions 9.1, 9.3 and 9.4, noting that action 9.1 would continue to be monitored through a corresponding action within the 2025/26 AGS.

An update was provided on the remaining actions relating to Business Continuity and the Force Operating Model. Members noted that progress had been made on business continuity arrangements through the realignment of resources to support this work. However, recruitment to a dedicated post remained outstanding following an unsuccessful recruitment exercise, and the role would be re-advertised as a full-time position. The Committee also noted that the planned ICT Disaster Recovery Audit and Business Continuity Audit would be aligned within the current audit programme. Members welcomed the alignment of the ICT Disaster Recovery and Business Continuity audit activity and noted the positive progress being made.

In relation to the Force Operating Model, LR advised members that the programme of evaluations had commenced, with several reviews already reported through the appropriate governance structures and further reports scheduled during the current quarter.

The Committee also considered the new AGS actions for 2025/26 and noted the arrangements in place to ensure action owners provide regular progress updates. Members raised no concerns regarding the proposed actions, subject to the correction of a minor typographical error within the report.

The Committee confirmed that it was content to recommend the Annual Governance Statement to the CC and PCC.

5. Consider reports on the effectiveness of internal controls and monitor the implementation of agreed actions

a) Internal Audit reports

1. Outstanding 25/26 ICT reports

The Committee considered the three outstanding ICT Internal Audit reports and received an update on the actions taken since the previous meeting.

KC advised that additional assurance had been provided following further review of the reports, including input from FS, who had been unable to attend today's meeting. Members were also provided with a document outlining amendments made to the reports following the concerns raised at the previous meeting.

MR explained that, following the last JAC meeting, representatives from ICT and TIAA met to agree the required next steps. Revised draft reports were subsequently shared with ICT management for review and feedback before being returned to TIAA for amendment. Feedback provided by FS on the ICT Change Management and Cyber Security audits had been incorporated into the revised reports.

In relation to the Cyber Security audit, MR noted that clarification had been provided regarding the scope of the review, which focused specifically on the Strategic

Integrated Assurance Plan (SIAP) controls selected for testing rather than the wider cyber security environment.

Regarding the ICT Infrastructure audit, MR advised that detailed feedback had been provided by the Temporary Head of ICT (MJ) and supported by FS. Concerns centred on the audit's reliance on policies and procedures rather than testing the operational effectiveness and implementation of controls. Members noted that further comments had been received from FS earlier that morning.

MJ confirmed that they had met with JM to discuss the findings and welcomed the additional detail that had subsequently been incorporated into the reports. MJ highlighted the importance of clearly defining audit scope and ensuring this is understood by all parties at the outset to avoid misunderstandings regarding the purpose and outcomes of reviews.

KC and MJ both observed that some of the audit titles could create expectations that the reviews covered broader areas than were included within scope. Members agreed that future audit titles should more accurately reflect the specific focus of each review to support clarity and understanding.

JM advised that TIAA had reviewed all comments received from Members and ICT representatives following the previous meeting and had amended the three audit reports accordingly to provide additional clarity and assurance.

i. ICT Change Management

The Committee considered the revised ICT Change Management Audit report and received an update from JM on the amendments made following feedback from Members and ICT representatives.

JM advised that no changes had been made to the overall assurance opinion or recommendations, which remained at reasonable assurance with four

medium-risk and four low-risk recommendations. The principal amendments related to providing greater clarity around the scope of the audit. Additional detail had been included within the executive summary to more clearly set out both the high-level and detailed scope of the review, including the specific areas examined during audit testing.

Further detail had also been added to the report to better explain the testing undertaken and provide greater assurance regarding the audit findings.

DM welcomed the revisions made to the report and confirmed that he was content with the reasonable assurance opinion and the recommendations proposed. He noted that all eight recommendations had the same responsible officer and implementation deadline and sought assurance that the actions could be delivered within that timeframe.

MJ confirmed that the recommendations largely represented quick wins which were already in the process of being implemented.

DM further noted that the report highlighted previous weaknesses in the documentation, governance and follow-up of ICT changes, but accepted that improvements had now been identified and were being progressed.

Members confirmed that they were satisfied with the revisions made to the report and the approach taken in response to feedback.

ii. ICT Infrastructure

The Committee considered the revised ICT Infrastructure Audit report and received an update

from JM on the amendments made following feedback received at the previous meeting.

JM advised that the overall assurance opinion remained unchanged at substantial assurance, although one additional low-priority recommendation had been added following discussions with ICT management. As with the Change Management audit, the report had been revised to provide greater clarity regarding the detailed audit scope, testing undertaken and the evidence reviewed. Additional narrative had also been incorporated following discussions with MJ to strengthen the report and provide further context around the findings.

DM acknowledged the improvements made to the report but expressed reservations regarding the award of a substantial assurance opinion as he questioned whether the assurance grading was consistent with findings identified across the related ICT audit reports. In particular, he referred to observations concerning policy review arrangements and other areas requiring improvement, which in his view were more reflective of a reasonable assurance opinion.

In response, JM advised that the assurance opinion had been considered carefully and remained appropriate given the limited number and low priority of recommendations arising from the review. He confirmed that the opinion had been endorsed through TIAA's internal quality assurance processes and approved by the relevant Audit Director.

DM reiterated that his concern related to the consistency between findings across the suite of ICT audits rather than the performance of ICT staff. He noted that some findings highlighted weaknesses in governance documentation and policy review arrangements, which he felt should be reflected in the overall assurance assessment.

CW supported elements of DM's observations highlighting concerns that the patching policy had not been reviewed for a significant period and noted findings relating to cloud environment backup testing, which she considered important for business continuity and resilience.

MJ provided assurance that backup arrangements were actively utilised and tested through routine operational recovery activities. Whilst a full restoration of the entire cloud environment had not been undertaken, he confirmed that backup data was regularly restored and verified when required, providing confidence in the effectiveness of the arrangements.

EH noted that, whilst certain policies required updating, the audit report clearly evidenced that key technical controls were operating effectively. He referred to testing undertaken by auditors, including the review of screenshots and supporting evidence demonstrating patch compliance and other infrastructure controls.

Following discussion, Members acknowledged the differing views regarding the assurance grading but accepted the explanation provided by TIAA and the assurances given by ICT management

iii. ICT SyAP Cyber Security

The Committee considered the revised Cyber Security Audit report and received an update from JM on the amendments made following feedback received at the previous meeting.

JM advised that there had been no changes to either the overall assurance opinion or the number of recommendations. Amendments had been made within the executive summary to ensure the wording more accurately reflected the scope of the audit. References to wider cyber security assurance

had been revised to clarify that the review focused on selected controls within the Cybersecurity Improvement and Assurance Framework (CIAF) rather than the organisation's overall cyber security arrangements.

Members confirmed that they were content with the amendments made to the report and the approach taken in response to feedback.

b) Summary Internal Controls Assurance (SICA) Report

JM provide an overview of the Internal Audit Progress Report and an update on the delivery of the 2025/26 and 2026/27 Internal Audit Plans.

JM reported that no new audit reports had been finalised since the previous meeting, although the collaborative Risk Assurance Audit covering the four Welsh police forces had now been issued in draft form. Members also noted that the outstanding Priority 1 recommendation relating to the collaborative security review remained ongoing, with a further update to be provided separately.

JM advised that all audits within the 2025/26 Internal Audit Plan had now been completed and that the Annual Internal Audit Opinion could be finalised following agreement of the revised ICT audit reports. An update was also provided on delivery of the 2026/27 Internal Audit Plan, with several reviews already underway and the remainder scheduled for completion during the year.

Members noted that some reviews, particularly collaborative audits involving all four Welsh forces, had been deferred and would now result in a greater volume of audit reports being presented later in the year. JM advised that discussions were ongoing with Forces to bring forward reviews where possible and noted the positive engagement from MR and ND in supporting audit planning and scheduling.

To assist Members in managing the anticipated volume of reports, JM suggested that completed audit reports could be



circulated to Committee Members in advance of formal meetings, providing additional time for review and consideration before discussion at JAC meetings.

KC welcomed the suggestion, noting the potential benefits given the volume of reports expected between the September and December meetings. She highlighted that earlier circulation would allow Members more time to review reports in detail and help avoid delays in finalising audits where further questions arose.

Action A 55: TIAA to circulate draft Internal Audit reports to JAC Members upon completion in order to provide additional time for review and consideration before discussion at JAC meetings.

JM also advised that, following discussions at the previous meeting, draft scopes for upcoming collaborative audits were being shared with ICT representatives at an early stage. He confirmed that comments from FS on the collaborative Data Protection Audit would be incorporated into the final scope, and that the same approach would be taken for the forthcoming Counter Fraud Audit to ensure stakeholder input was reflected before fieldwork commenced.

c) Internal audit performance and open recommendations

The Committee received a presentation from MR on Internal Audit performance, delivery of the audit plan and the management of outstanding audit recommendations.

In relation to the 2025/26 Internal Audit Plan, MR confirmed that a total of 20 audits had been completed, comprising 11 substantial assurance, 7 reasonable assurance and 2 limited assurances.

The Committee also considered progress in implementing audit recommendations. MR reported that the number of open recommendations had reduced from 55 to 51, with 20 recommendations closed since the previous reporting period, whilst 16 new recommendations had been added. Members noted that increased oversight was being applied through

regular engagement with budget holders and through scrutiny at the Strategic Audit and Assurance Board, where requests for implementation extensions had been considered and challenged where appropriate.

Further work was underway with Information Management and ICT leads to review older outstanding recommendations and establish clear implementation plans and timescales. Members noted that the largest concentration of open recommendations related to People and Organisational Development, ICT, Data Protection, Data Storage and Cyber Security, reflecting the complexity and longer-term nature of these areas.

MR confirmed that only one Priority 1 recommendation remained open, relating to the Security of Seized Cash and Proceeds of Crime audit, and that progress continued to be monitored through established governance arrangements.

KC welcomed the revised reporting format and thanked MR for presenting the information in a clear and accessible manner.

DM also welcomed the additional analysis provided and suggested that future reports should include further detail on recommendations that remained outstanding more than 12 months after their original implementation date. He noted that, where recommendations had remained open for a significant period, it would be useful to understand revised implementation timescales and whether the original recommendations remained appropriate considering organisational changes and evolving risks.

MR agreed to provide additional detail on older outstanding recommendations and advised that work was already underway with Information Management and ICT colleagues to review these recommendations, assess their ongoing relevance and establish updated timelines for completion.

KC supported this approach, noting that longstanding recommendations should be reviewed to ensure they remain relevant and proportionate to current organisational priorities.

6. To consider the Treasury Management 2025/2026 Outturn Report

The Committee received the Treasury Management Outturn Report for 2025/26 and an update from ND on treasury management activity during the financial year.

ND explained that the report summarised treasury management performance and outlined the wider economic context in which borrowing and investment decisions had been taken. Members noted the continued volatility of financial markets and the persistence of relatively high interest rates, which continued to make long-term borrowing less attractive. As a result, the Force had maintained its strategy of relying on short-term borrowing arrangements whilst monitoring interest rate movements.

Members noted that the borrowing position at the end of March 2026 stood at just over £25 million, remaining within approved limits and in accordance with the Treasury Management Strategy. The Committee was advised that surplus cash balances continued to be managed prudently, with investment decisions prioritising security and liquidity.

ND reported that investment returns had remained strong during the year, with an average return of just over 4%. Investment income exceeded budget expectations, generating over £1 million compared to a forecast of approximately £500,000, reflecting the favourable interest rate environment.

KC welcomed the report and highlighted the continued slippage within the capital programme, noting that this remained a recurring issue and had contributed to lower borrowing requirements than originally anticipated.

In response, ND acknowledged that capital programme slippage had occurred during 2025/26 but advised that significantly greater scrutiny had been applied to the development and monitoring of the current year's capital programme. Members were informed that most projects had either commenced or were nearing completion, with only one project currently considered at risk of further slippage. Ongoing monitoring arrangements were in place to ensure delivery expectations remained realistic.

7. Audit enquiries to those charged with governance

The Committee received the annual Audit Enquiry to Those Charged with Governance letter from Audit Wales. JB confirmed that this is a standard annual requirement issued to all audited bodies and forms part of Audit Wales's audit process, with responses considered as part of their audit work.

Members sought clarification regarding declarations of interest for Independent Audit Committee Members. EH advised that, following a review of the Code and guidance from Audit Wales, declarations of interest were no longer required from Independent Audit Committee Members. This

represented a change in process for the current year and had been appropriately verified.

DM welcomed the improved quality of the responses provided within the document, noting that they had become more meaningful in recent years and were less reliant on content carried forward from previous submissions. He expressed his appreciation to EH and the team for the work undertaken.

Members concurred, recognising the significant effort involved in preparing and reviewing the responses and welcomed evidence of improvements, including strengthened compliance with ICO guidance.

8. Monitor the effective development and Operation of Risk Management

a. To consider the Force Risk Register

LR provided the committee with an update on the Force's Corporate Risk Register highlighting two key developments since the previous meeting.

DM suggested that the Committee should receive a future briefing on the Police Reform, including proposals relating to policing governance given the potential longer-term strategic implications for organisational governance and risk.

The PCC supported the proposal and advised that, whilst significant national discussions were ongoing, there remained considerable uncertainty regarding future governance arrangements. Members noted that a member of the OPCC team is seconded to the Association of Police and Crime Commissioners and is involved in discussions with the Home Office, providing useful insight into the emerging reform agenda.

ND advised that efforts were being made to secure attendance from a member of the national reform team at the forthcoming All-Wales training event to provide a broader update on developments.

LR noted that Police Reform actions are already being monitored through the AGS action plan and would continue to be reported through those updates. Any requirement for a more detailed report could be accommodated later in the year.

The Committee also discussed the emerging risks associated with Artificial Intelligence (AI).

KC queried whether AI-related risks had been formally considered within the organisation's risk management framework, noting significant impacts within her own sector from AI-generated complaints, information requests and associated resource pressures.

LR advised that AI had been discussed internally and that the organisation was currently undertaking limited trials of approved AI products. Early consideration was being given to governance, controls and future rollout arrangements.

CM highlighted that AI presents both opportunities and risks. Whilst internal trials had demonstrated benefits, learning from issues experienced elsewhere had reinforced the need for clear governance and usage parameters. She also noted increasing examples of AI-generated complaints and legal correspondence creating additional organisational pressures.

KC expressed concern that the growing operational and organisational impact of AI may not yet be sufficiently reflected within the risk framework and suggested that the matter warranted further consideration.

CM agreed and proposed that the issue be reviewed further to determine whether AI-related risks should be reflected within the Corporate Risk Register.

LR confirmed that she would examine whether AI-related risks were already captured at departmental level, including within Legal Services risk registers, and consider whether escalation to the Corporate Risk Register was appropriate.

CW supported this approach and suggested that AI should not be treated as a single risk. She observed that there were several distinct AI-related risks, including internal use, external misuse, legal implications, information governance concerns and resource impacts, which may require separate consideration and management.

Action A 56: OPCC to provide a Police Reform update to the Committee at the December meeting.

Action A 57: LR and CM to review AI-related risks across the organisation, including consideration of whether risks should be reflected within departmental and/or Corporate Risk Registers.

b. To consider the OPCC Corporate Risk Register

The Committee received an update on the OPCC Risk Register from CM.

CM advised that there were no significant changes to highlight since the previous meeting. Members noted that it had been proposed that the Sexual Assault Referral Centre (SARC) risk be moved from the Risk Register to the Issues Register, in line with the approach adopted by the Force. This proposal had been agreed following discussions between the Director of Commissioning and Partnerships, the Head of Assurance and Force representatives.

No further questions were raised by Members

9. Review the Assessment of Fraud risk and Potential Harm

a) Receive Reports on Fraud

Members noted the report that was provided and no further questions were raised.

10. Update from HMIC inspection

RJ provided an update on the Force's HMICFRS PEEL inspection.

RJ informed that the evidence-gathering phase concluded in June 2026 and that the Force is awaiting the draft report for factual accuracy checking, expected in August, with the final inspection report anticipated in the autumn. Members noted that significant work had been undertaken ahead of the inspection, with 35 previous areas for improvement (AFI's) addressed and signed off internally, subject to final HMICFRS confirmation.

Initial HMICFRS feedback was reported as largely positive, with no significant surprises identified. Work is already underway to address areas highlighted for improvement ahead of receipt of the final report.

Members welcomed confirmation that Dyfed-Powys Police had been assessed as Level 1 under HMICFRS's new Policing Performance System, meaning no enhanced monitoring or intervention is currently required.

The Committee also noted that eight AFIs remain open, comprising four awaiting HMICFRS sign-off and four arising from the recent Regional Serious and Organised Crime Inspection.

DM sought clarification regarding HMICFRS comments on supervisory oversight of Grade 3 incidents, and RJ explained that these relate to non-urgent scheduled incidents requiring more consistent oversight and timely progression.

Members welcomed the positive feedback received to date and recognised the significant preparation and improvement work undertaken by the Force.

11. Members Updates

DM provided an update from the Strategic Finance Board and the Strategic Audit and Assurance Board that he had attended. Members noted that the Force was currently reporting a broadly balanced budget position, with significant overspends in police pay and overtime being offset by underspends in police staff pay. DM highlighted the robust financial monitoring arrangements in place and the close oversight being exercised by both the Force and OPCC finance teams.

JJ advised that she had attended the Corporate Governance Board and confirmed that the update previously provided under that agenda item was a comprehensive reflection of the matters discussed.

KC and CW updated Members on a recent meeting with the Finance Team regarding the external audit process. Members noted that the session had provided a useful overview of audit progress and the use of the Inflow system for managing and tracking audit requests. CW commented positively on the system and welcomed the visibility it provided regarding progress against audit actions.

JB provided a brief update on the external audit, advising that audit fieldwork was approximately halfway complete and progressing well, with no significant concerns identified and all required information being provided in a timely manner.

12. Any other business

Members received an update on arrangements for the forthcoming All Wales Audit Committee Training Day scheduled for 9 September 2026. ND advised that the agenda was being finalised and would be circulated once speaker availability had been confirmed.



ACTION SUMMARY

Action N°	Action Summary	To be progressed by	Progress
A 53	An additional meeting of the Committee be arranged for April 2027.	OPCC	In progress – Dates being sought
A 54	CM to discuss future reporting arrangements for the Strategic Audit and Assurance Board with the DCC and ensure proposed amendments to the Terms of Reference, including Audit Wales feedback, are reflected in the revised document.	CM	In progress – Feedback has been provided to SIU with a request for amendments to the ToR to be made as per JAC discussions and previous OPCC feedback.
A 55	TIAA to circulate draft Internal Audit reports to JAC Members upon completion in order to provide additional time for review and consideration before discussion at JAC meetings.	TIAA	
A 56	OPCC to provide a Police Reform update to the Committee at the December meeting.	OPCC	In progress – Scheduled for the 14 th of December meeting.
A 57	LR and CM to review AI-related risks across the organisation, including consideration of whether risks should be reflected within departmental and/or Corporate Risk Registers.	LR / CM	In progress