Minutes of NHS Ayrshire and Arran Audit & Risk Committee Meeting

held on Thursday 19th March 2026 at 09:30hrs hours via Microsoft Teams

Present	Sukhomoy Das, Non-Executive Board Member (Vice Chair acting as Chair) Jean Ford, Non-Executive Board Member (Chair) (until Item 4.3 incl.) Neil McAleese, Non-Executive Board Member Joyce White, Non-Executive Board Member Marc Mazzucco, Non-Executive Board Member Marie Burns, Non-Executive Board Member
In attendance	Lesley Bowie, Board Chair Gordon James, Chief Executive Derek Lindsay, Director of Finance David Stonehouse, Interim Director of Finance Amanda Dowse, Assistant Director of Finance (Governance and Shared Services) Rachael Weir, Internal Auditor, Azets Paul Kelly, Internal Auditor, Azets (Item 4.1) Fiona Mitchell-Knight, External Auditor, Audit Scotland David Jamieson, External Auditor, Audit Scotland Kirstin Sharp, External Auditor, Audit Scotland Debbie McCard, Risk Manager (Item 3.1) Nicola Graham, Director of Infrastructure and Support Services (Item 4.1 – 4.3) Fraser McNeil, Head of Estates (Item 4.3) Marie Richmond, Assistant Director of Digital Services (Item 4.1 – 4.3) Sarah Leslie, Director of Human Resources (Item 4.3) Graham Armstrong, Head of Occupational Health & Safety (item 4.3) Shona McCulloch, Head of Corporate Governance (Item 6.1) Zoe Fance, Head of Procurement (Item 6.1) Shirley Taylor (Minutes)

1. Apologies and declarations of interest

1.1 Apologies

The Vice Chair welcomed everyone to the meeting, apologies were received from David Eardley and Crawford McGuffie.

1.2 Declarations of interests

None noted.

2. Minutes of Meeting held on 22 January 2026

The minute of the previous meeting was agreed as an accurate record of the discussion.

3. Matters Arising

3.0 Action Log

The Chair provided an update on the action related to the risk register. A meeting has taken place with the Risk Manager to understand what the risk system can do. One item was used as an example and feedback was requested from Non-Executive Directors as to whether the information contained was adequate. Most are supportive with a few amendments suggested. This will be taken forward into the risk appetite statement and a revised format is expected in September 2026.

Discussions have taken place regarding the NHS in Scotland report and specifically the more staff less efficiency piece and this will be built into the budgeting process for this year with a board workshop scheduled for October 2026 to look at headcount against activity.

Action 6.1 regarding the external audit recommendations was discussed and noted that this work has largely been completed and there has been good progress in the past few weeks as budgets and plans become available for 2026/27.

With regard to the Terms of Reference there had been questions as to whether the Directors were required at every meeting. It was agreed that the Nurse Director and Director of Pharmacy could be removed but as the Medical Director holds responsibility for risk they should remain as the risk executive. The option will remain that colleagues can be invited to attend if required.

3.1 Risk Appetite Statement Implementation Plan (Action 6.5 20/11/2025)

The Risk Manager shared the Risk Appetite Statement Implementation Plan and noted that the plan is for education and awareness with a timescale for completion by end of April 2026. As part of the process all strategic risks will be revisited prior to the Risk and Resilience Scrutiny and Assurance Group in July. From this a further paper detailing the revised risks will be presented to the committee in September 2026.

It was agreed it would be useful for a schedule to be produced for the May committee to show when each risk will be reviewed to align with the other committees.

ACTION – Debbie McCard

Some confusion arose regarding the risk appetite statement and the plan presented as this did not look like an appetite statement. Chair provided a recap

on the journey so far. A short Life Working Group was developed to review the risk appetite statement in 2025, a revised risk appetite statement and framework was then proposed to the Audit and Risk Committee in November 2025 and approved by the Board in December 2025. The Audit and Risk Committee requested an implementation plan be presented at a later committee which was the plan being presented at this meeting.

In light of confusion Chair will consider what if any further communication is required to members.

ACTION – Jean Ford

3.2 Committee Workplan 2025/26

The committee workplan was received with changes noted in red. It was highlighted that the external audit recommendations and register of gifts and hospitality have been carried forward to may meeting due to other pressures. Due to being so close to the deadline it was agreed that an update on the external audit recommendations would not be helpful and should be replaced with a timeline for this year's audit instead.

ACTION – Amanda Dowse

4. Internal Audit

4.1 Internal Audit Report – Cyber Security

The Internal Auditor presented the Cyber Security Internal Audit report and advised that specific areas of audit had been requested by Management due to a recent NIS review which had highlighted areas for improvement. An increase on reliance on third party providers to provide digital solution has been identified however any risk or cyber security issues would be the responsibility of the customer.

The audit received a rating of amber – substantial improvement required due to weaknesses in design of controls, a lack of oversight, no ownership or policies identified and no risk assessments or due diligence carried out when purchasing services. There is no vendor management process in place to confirm that third party providers maintain good cyber security throughout the life cycle of the contract and that incident response plans are being maintained. In some cases due diligence has been carried out but not kept up to date.

A further weakness was found whereby third parties who have been allowed access to the network did not have expiry dates put in place so the accounts remained live.

Members agreed that the report was welcomed and discussion took place on the timescales for completion. It was responded that the timescales are realistic due to the issues being systemic and not immediate to resolve. It was recognised by the department that there were weaknesses within the processes and a number of areas to improve on and it will take time for processes to be embedded. It was also confirmed that this work is being included on the pipeline and the structure will be redesigned to include specific vendor management posts going forward.

A member raised concerns with regard to the number of reports which show issues in terms of operational or administrative procedures and how these are not followed consistently. Assurance is required that the importance of this is recognised.

A question was raised as to whether the actions from the report would have sat within the delivery improvement plans. It was responded that as the weakness was identified by NIS it would sit within their own action plans however the issues highlighted are high on all agendas. Reassurance was also given to members that this was the only area within the NIS audit where the score was not up to standard. Verbal feedback from NIS has shown improvement so far. It was recognised that these issues do not exist across all of cyber security and is concentrated around the contract and supplier management.

The Chief Executive advised that the audit should be taken as a positive step and gives an area of focus as well as opportunities for learning. Procurement in this area will be strengthened and will form part of the SFI's.

Outcome: *The committee received the report for onward distribution to the Information Governance Committee for monitoring of actions*

4.2 Internal Audit Progress Report

The Internal Auditor presented the progress report and advised that two substantive audits have been completed since the last update. The scope and timing of the remaining audits have been agreed, and the plan remains on track to deliver the annual audit opinion in May. The management action follow-up for Q4 has also been completed. One audit has been deferred to 2026/27, with audit days reallocated to support follow-up work on CRES, which will remain a high priority on Members' agenda.

Outcome: *The committee received the report*

4.3 Internal Audit Report – Health and Safety

The Committee considered the audit report covering four key statutory compliance areas: water safety (including legionella), fire safety, electrical safety and health and safety. A number of issues were identified, including out of date risk assessments, overdue fire safety reviews and weaknesses in ensuring that risk assessments were implemented in a timely manner.

An overarching theme from the audit was a fragmented approach to governance, with differing processes across areas. The overall risk exposure was rated as red – immediate major improvement required. The Internal Auditor advised that, while there had been good and constructive engagement with management, the clearance process had been lengthy. Work is now underway to address the issues raised.

Members expressed concern regarding statutory processes not being followed and the length of time to reach an agreement on the overall risk rating. It was also agreed that the management comments within the report were not found to be helpful.

The Director of Human Resources reported that a short summary had been prepared in advance of the Committee, highlighting the control objective issues. At the time of audit, required evidence was not available. Although management believed safety risks were minimal, the audit was assessed at level four, with 24 actions relating to design controls. Ongoing monitoring would continue, with a governance report returning to Committee due to the status of actions. As detailed within the management response there is note of the human dimension and challenges associated with an ageing estate, including both NHS-owned and private facilities. A number of statutory compliance activities had been paused for around three years following COVID. There is currently one compliance officer for the whole Board. Key weaknesses related to capturing emerging risk, lack of formalisation, and insufficient documentation was evidenced. It was reiterated that safety risk during the audit was assessed as minimal, and that immediate action had been taken. The audit was acknowledged as a valuable learning exercise, involving review of over 200 files.

The governance improvements were outlined which includes a strengthened processes for technical governance. The Health, Safety and Wellbeing Committee has been reviewed and strengthened, and the Statutory Compliance and Best Practice Group will be further reinforced. This group will feed into CMT via quarterly and annual reporting, then through Staff Governance and onward to the Board. Assurance audit and training capability within the Health and Safety team has been strengthened, and any high-risk audit issues will be escalated to CMT and ARC as required.

The Director of Infrastructure and Support Services acknowledge the efforts of those involved in the audit which was a lengthy piece of work. Assurance was provided to members that there is a strong commitment to make improvements and the identified weaknesses was in the paperwork which will be examined to see what can be done differently in the future.

It was agreed that further updates would be required by the committee over the coming months. It was also agreed that the two audit reports received at the meeting would be put forward to RARSAG due to the emerging themes.

Discussion took place on the reporting that is required to get this to the Board and this will be discussed further.

ACTION – Lesley Bowie

Outcome: *The committee received the report for onward distribution to the Healthcare Governance Committee for monitoring of actions*

4.4 Internal Audit Follow Up Report

The Internal Auditor presented the follow up report and advised that 50 actions were followed up within the period. 21 of these were brought forward and 29 are new actions. Eight actions have been marked as complete and 24 are not yet due. 18 actions are partially complete and have passed their due date. 13 of

these are high or very high and a request was made that particular attention be given to finalising these.

Concerns were expressed that due dates are not being met .The Chief executive assured members that this is high on the CMT agenda and is reported on a monthly basis.

The Assistant Director of Finance advised that work is completed for one action however this could not formally be marked as complete until the SFI's were agreed and the governance processes followed.

Outcome: *The committee received the report*

4.5 Internal Audit Plan 2026/27
The Internal Auditor presented the revised Internal Audit plan taking account of comments by committee members at the January meeting. It was highlighted that the plan remains unchanged in terms of the number of audits to be concluded. The plan was supported for submission to the Board for approval.

Outcome: *The committee supported the audit plan for onward submission to the NHS Board*

5. External Audit

5.1 External Audit Plan 2025-26
The External Auditor presented the Board's audit plan for 2025/26 which sets out the plan to meet the audit responsibilities.

The key point of the plan is the significant risk of material misstatement to the financial statements as summarised with the report. Attention was drawn to one significant risk, that being fraud caused by management override of controls with significant adjustments made last year. To reflect the audit findings a quality assurance review will be completed on the accounts before they are submitted for audit on 4th May 2026.

The wider scope of the audit as set out by the Code of Audit Practice focuses on four key areas: financial management, financial sustainability, vision and leadership and governance and the use of resources to improve outcomes. In terms of financial sustainability, this will include a review of the final 2026-27 financial and delivery plans. The Auditor General will be kept informed of exhibit three sets out planned audit response, also keep auditor general informed of boards financial position to see if further section 22 reports are appropriate.

The signing of the independent auditor report and issue of the annual audit report are planned to take place by 30th June 2026. There has been an increase to the 2026/27 audit fee due to the significant risk in the wider scope area.

A question was raised as to whether a high level tracker is requested for the May committee. It was confirmed that as the timetable stands a draft report should be available for the next meeting. In terms of best value it was noted that the Director of transformation and Sustainability is leading on this and discussions

are ongoing to see how best to report on this work. A paper regarding the timetable for the accounts and key actions of the wider team is on the agenda for the CMT next week.
Outcome: *The committee received the audit plan*

6. Governance and Risk

6.1 Code of Corporate Governance
The head of Corporate Governance presented the Code of Corporate Governance and noted that this is being presented in two papers with a note of the changes made in the appendix. A review of the SFIs and Scheme of Delegation was commissioned separately the yearly Code of Corporate Governance update. There have also been slight amendments to how the sections are reflected and updated to allow individual sections to be presented to ARC and the Board if required in the future. Assurance was given to members that the full document will be provided to Board members for approval whilst providing detail of any changes.

The Director of Finance informed members that agreement is required on section 2.2 and 2.3 of the SFI's which sets a limit to the threshold for authorisation. Discussion took place on what this should be and it was agreed that a proposal would be made to the Board that the threshold should be set at £1m in line with other areas.

Outcome: *The committee endorsed the report for submission to the NHS Board for approval*

7. Any other competent business

7.1 ARC Workplan 2026/27
A committee member raised a query with regard to private meetings with the Internal and External Auditors and whether these would be reinstated. It was responded that these meetings will be reinstated twice per year.

It was also highlighted that the Internal Auditor term will be concluded at the end of this year and a decision is required as to whether this will be extended for a further one year period.

Outcome: *The committee agreed the workplan for 2026//27*

8. Key issues to report to the NHS Board

The following items were agreed to be reported to the Board:

- Internal audit progress and follow up reports
- Internal Audit Report – Cyber Security
- Internal Audit Report – Health and Safety
- External Audit Plan 2025/26
- Code of Corporate Governance and SFI's

9. Risk issues to report to the Risk and Resilience Scrutiny and Assurance Group

It was agreed that the Internal Audit reports on Cyber Security and Health and Safety would be reported to the Risk and Resilience Scrutiny and Assurance Group to be aware of in terms of possible trends.

10. Date of next meeting

Thursday 19th May at 9.30am via Microsoft Teams

Approved by Chair of the Committee:

..... Date: .....