Registers of Scotland
ros.gov.uk

Audit and Risk Committee (ARC)

Minute of Meeting

14 May 2024
1030hrs
St Vincent Plaza, Glasgow

Chair	Andrew Harvey, Audit and Risk Committee Chair
Present	Dónall Curtin, Audit and Risk Committee Member Christine Martin, Audit and Risk Committee Member Julie Wardhaugh, Audit and Risk Committee Member Tim Wright, Audit and Risk Committee Member
In attendance	Chris Kerr, Director of Policy and Corporate Services and Accountable Officer Chief Finance Officer (HB) Head of Finance (DM) Head of Risk and Information Governance (AR) Head of Enterprise Risk Management (CI) Head of Information Governance (AK) Senior Internal Audit Manager (KM), Scottish Government Directorate for Internal Audit and Assurance (SGDIAA) Associate Partner (PK), Deloitte Martin Burns, Director of Digital, Data and Technology – *item 8.1* Policy and Post Registration Lead (KF) – *item 8.2* Communications Manager (KM) – *item 9*
Apologies	Internal Audit Manager (AB), SGDIAA Senior Manager (LM), Deloitte
Secretariat	Senior Executive Assistant to the Director for Customer and Business Development (JM) Senior Executive Assistant to the Director of People (VB)

1. Introduction, apologies, and chair's matters

1.1 The Chair welcomed everyone to the meeting and noted the apologies and guest attendees as above. It was highlighted that the Internal Audit Manager, SGDIAA is now on maternity leave. Introductions were made around the room for new attendees.

2. Declaration of interests

2.1 No new interests were declared.

3. Minute of meetings and outstanding actions

3.1.1 The minutes of the meetings held on 13 February 2024 and 26 March 2024 were accepted as a true record of the discussions held.

3.1.2 The Committee reflected on the Hybrid Working and Culture report discussion on 26 March around the work done to benchmark the RoS hybrid working approach against other organisations and agreed that the Accountable Officer will bring a progress update on this and any horizon scanning undertaken to the February 2025 meeting.

Action – Accountable Officer to bring a progress update on the RoS hybrid working approach, including benchmarking against other organisations and horizon scanning, to the February 2025 meeting.

3.2 The Committee reviewed the outstanding action log and agreed:

Action 5869 – Guidance on data handling has been produced and shared with Non-Executive Directors (NXD) and ARC members Action closed.

Action 6156 – ARC recruitment is underway with interviews taking place in June. New members will be invited to observe the August meeting to allow substantial overlap between new and old members. Action ongoing.

Action 6160 & 6268 – Guidance for ARC deep dives was discussed and agreed under agenda item 7.1 Action closed.

Action 6163 – Output from the Scottish Government Audit Committee Chairs' Network review of Key Performance Indicators (KPIs) is awaited and will be brought to a future ARC meeting once available. Action ongoing.

Action 6165 – People and Change progress update is planned for the August 2024 meeting. Action ongoing.

Action 6167 – A full update on the planned organisational resilience scenario exercise was presented under agenda item 8.1 Action closed.

Action 6267 – Statistical information was included in the Hybrid Working and Culture report, as presented to the March meeting. Action closed.

Action 6269 – ARC feedback on the wording of key risk 13 has been incorporated. Action closed.

4. Matters arising not covered on the agenda

4.1. No other matters were raised.

5. Internal Audit

5.1. Annual Assurance Report 2023/24

5.1.1 The Senior Internal Audit Manager presented the annual assurance report 2023/24 which found an overall 'Reasonable' assurance opinion. Consistency of approaches throughout the organisation was noted, with 74% of all recommendations made found to be fully implemented during follow up reviews. It was highlighted that while 74% is reasonable, 80% would be a good improvement to aim for next year.

5.1.2 The Committee reflected on the weighting of evidence and heard that whilst the auditors do work from a background checklist, subjective experience and judgement is applied to consider appropriate weightings. The Committee further reflected on the new Global Internal Audit Standards (released in January 2024 and which will become effective in January 2025) and heard that it is unknown whether these would have had any impact on the overall opinion should these have been applied retrospectively. The internal audit team will be reviewing the new standards to understand any impacts in due course and, if there are any, will incorporate those in future work.

5.1.3 The Committee highlighted a typographical error in page 18 of the report where question marks were inserted in the follow up review table instead of zeros.

5.1.4 The Committee was pleased to note the 'Reasonable' assurance opinion and in particular the positive progress made to achieve 74% full implementation of all recommendations made in follow-up reviews, agreeing that setting realistic dates at the outset is key to success. Thanks were expressed to all the Scottish Government (SG) and RoS colleagues involved.

5.2. Audit & Risk Committee Progress Report 2023-24

5.2.1 The Senior Internal Audit Manager provided an oral update on the internal audit plan 2023/24 progress. Fieldwork on the Registration KPI Outcomes assurance review planned for Q1 begins on 20th May, and planning for Q2 activities with the RoS Assurance Service is underway.

5.2.2 It was highlighted that a new resource matrix for audits is being applied and working well, and that a number of internal audit roles are currently being advertised, including that of the Director of Internal Audit and Assurance.

5.2.3 The ARC Chair expressed thanks to Chris Martin for providing input into the KPI Outcomes assurance review terms of reference.

6. External Audit

6.1 Interim Management Update

6.1.1 The Associate Partner, Deloitte, provided an oral progress update. This year's annual audit is on track, with the lessons learned from last year's audit incorporated into the audit plan and no new material standards of note. Both RoS and Deloitte colleagues will be on site on agreed dates, but with a degree of flexibility should additional on-site presence be required during the audit. It was highlighted that questions are known and can be reacted to in advance, however the RoS team are fully aware that some flexibility is required and are ready to respond.

6.1.2 The Committee reflected on the query raised in last year's audit regarding the valuation of Meadowbank House as a property asset and was reassured to hear that this issue was resolved as part of last year's audit with the figures found to be correct. This will be reviewed again in a three yearly cycle to align with SG guidance.

7. RoS Assurance Framework Update

7.1.1 The Head of Information Governance provided an oral overview of the RoS assurance framework progress since the last meeting in February 2024, and sought ARC support for a proposed deep dive schedule 2024-25 and draft deep dive guidance for colleagues.

7.1.2 The Committee welcomed the deep dive guidance and was content to approve this subject to the following minor amendments:

- A request for presenters to include a glossary of any technical terms and acronyms.
- The first paragraph to reflect that the deep dive will provide informal assurance to supplement the formal assurance from other sources.
- To reflect that deep dives will provide assurance on risk mitigation.
- To reflect that this is an opportunity for presenters to discuss challenges and highlight any issues as part of risk mitigation.

Action – Head of Information Governance to update the deep dive guidance to reflect Committee feedback.

7.1.3 It was further agreed that it is essential that presenters follow this guidance to ensure appropriate preparation, and that RoS Secretariat will ensure all presenters are made aware of the expectations.

7.1.4 The Committee reviewed the proposed deep dive schedule 2024-25 and was content to endorse, however suggested that it may be helpful to develop a rolling deep dive cycle and to consider adding a potential AI deep dive into this year’s programme. It was further discussed that the planned Automation deep dive is likely to touch on AI, and the Accountable Officer and Head of Risk and Information Governance agreed to consider how best to address the AI issue.

ACTION – The Head of Information Governance to consider developing a rolling deep dive cycle.

ACTION – The Accountable Officer and Head of Risk and Information Governance to consider how best to incorporate AI into the deep dive programme.

7.1.5 The Committee reviewed the assurance framework and key risk register and discussed as follows:

- Noted the changes to key risk 14, which has been delegated to the Customer and Business Development risk register and re-assessed as a threat. The Committee noted its concerns however accepted the decision and agreed that this can be brought back as a key risk in the future should this become necessary in the changing political landscape. It was further agreed that the Key Risk Owner / appropriate Director should be invited to provide a briefing to the Feb 25 ARC meeting with an updated EMT view of the current position. The ARC Chair would be happy to address ARC concerns with the former Key Risk Owner in the meantime.

- Noted that key risk 3 route is on track although part 2 of the route to target may extend into Q2, and received assurance that although the timeline has shifted slightly for good operational reasons, this will have no significant impacts or change the overall benefits.
- Welcomed an explanation of the income modelling used in key risk 1.
- Welcomed an explanation of the decision to add a new clause added to key risk 5.
- Noted that key risk 9 is closed and delegated as Individual Product risks to the DDAT register, as this has moved from general to specific risks. There is the potential for this to be escalated in the future if need be.
- Discussed the target scores on key risks 1,3,4 and 9 and the activities undertaken to reduce these over Q2.

7.2. Key Risk Register – Financial Impact Review

7.2.1 The Head of Enterprise Risk Management and the Chief Finance Officer presented the key risk register – financial impact paper which was taken as read. The Committee was asked to consider whether it continued to find this annual review helpful, noting that this was initially undertaken at the request of the RoS Board in March 2021.

7.2.2 The Committee discussed the information provided and considered that this report provides a clear understanding of the range of risks faced by RoS, and that there is some assurance gained from the last financial year end position.

7.2.3 The Committee reflected on potential consequences should the risks on the key risk register materialise, and agreed that while these are covered in our framework agreement, the Keeper may find it appropriate to update SG on the current exposure position.

ACTION – ARC Chair to raise with the Keeper, ARC suggestion that it they may find it appropriate to update SG on the current financial exposure position.

7.2.4 The Committee considered the work required to produce this report, whilst noting the work undertaken to manage the risks and the reasonably static range, and agreed to ask the RoS Board to consider if there is sufficient benefit to support this annual exercise going forward.

ACTION - ARC Chair to raise with the RoS Board whether there is sufficient benefit in the annual financial impact review exercise to support this continuing in the future.

8. Other Forms of Assurance

8.1. Cyber Threat Response Assurance

8.1.1 The Director of Digital, Data and Technology (DDAT) joined the meeting to receive questions on the cyber threat response assurance paper, which provided an update on cyber-attack threat response plans and invited members to provide critical feedback. It was highlighted that the planned exercise will involve key business areas including communications, and be run as a real life example with only a few named individuals aware in advance. Furthermore, discussions are underway to determine how best to test properly whilst protecting RoS systems and data.

8.1.2 The Committee was supportive of the exercises as outlined, however stressed the importance of only 1 person knowing the planned date in advance, and of ensuring the Communications team are fully involved not only to note and communicate decisions during the scenario, but also to be fully involved in the decision making.

8.1.3 The Committee thanked the Director of DDAT for the opportunity to comment, and expressed an interest in seeing a review of the outcome and lessons learned at a future ARC meeting. The Director of DDAT thanked the Committee for the very helpful feedback.

Action – The Director of DDAT to bring a review of the cyber-attack threat exercise outcome and lessons learned to a future ARC meeting.

8.2. Fraud Policies and Process

8.2.1 The Policy and Post Registration Lead joined the meeting to receive questions on the amalgamated fraud policy and draft internal fraud response plan, which have been updated following the amalgamation of the registration fraud and internal fraud officer roles into a single office of ‘fraud officer’.

8.2.2 The Committee was content with the proposed policy and draft plan; however, the following suggestions were made:

- To consider renaming the ‘fraud policy’ to ‘anti-fraud’ policy.
- To ensure the communications to staff encourage best practice behaviours when the mandatory online training and policy read is launched.
- To consider re-wording paragraph 1.1 of the policy to ensure the stated action aligns with the fraud response plan and Scottish Public Finance Manual.
- To consider signing up to the National Fraud Database.

Action – The Policy and Post Registration Lead to consider ARC feedback on the Fraud Policies and Process.

8.2.3 The Committee thanked the Policy and Post Registration Lead for the opportunity to comment on the amalgamated policy and draft plan, and was similarly thanked for the very helpful feedback.

9. Draft Annual Report 2023/24

9.1 The Communications Manager joined the meeting to present the most recent draft of the annual report 2023/24 and receive any comments. Members were thanked for all their helpful ’out of committee’ feedback received to date.

9.2 The Committee discussed the draft report and agreed it to be easy to read, concise and well structured. It was suggested that while the approach taken aligns with best practice examples from other public sector organisations, it would be prudent to continue to look at other examples ahead of next year’s report. Andrew Harvey and the Associate Partner, Deloitte would be happy to provide some suggestions should this be helpful.

9.3 The Committee was content with the draft report and look forward to seeing the next iteration, however suggested that a more suitable alternative to the word ‘score’ in pages 85 and 86 of the paper pack should be considered.

9.4 The Committee thanked the Communications Manager for their hard work on the draft report to date.

10. Outstanding Recommendations Log

10.1 The Committee reviewed the outstanding recommendations log and noted the helpful additional written summary provided. It was highlighted that recommendation 146 was added to the ‘for discussion’ tab in error and is actually on track.

10.2 The Committee was content to note those marked on track and agree those proposed to close. The following recommendations were discussed and agreed:

UID	Report	Recommendation	Agreement
155	Information Security Risk Management	Review of IT – Technical Risks	To remain on the log for review at February ARC to allow sufficient time to check that risk scenarios are covered in BCPs.
156	Information Security Risk Management	Mandatory Reading	ARC noted the update provided at item 11.8 and agreed to close this item from the recommendations log as the original recommendation has been met and the Policy and Practice Group (PPG) has accepted responsibility for mandatory reads compliance and enforcement. It was further agreed that ARC will continue to track through the ARC action log until PPG embeds its new assurance role into practice.

ACTION – ARC noted that PPG has accepted responsibility for mandatory reads compliance and enforcement and agreed to track this through the ARC action log until the PPG has embedded its new assurance role into practice. Action assigned to the Accountable Officer who is a PPG member.

10.4 The Committee reflected that at times, the recommendations and management responses had been unclear, and received assurance that internal colleagues now review all management responses for suitability.

11. Items for noting

11.1 The Committee noted the following items, highlighting a numerical error on the Board papers publication table in the 2024 Transparency Review paper.

1) Finance Update
2) Performance Reporting
3) RoS Board Minute - 12 December 2023
4) 2024 Transparency Review
5) National Fraud Initiative (NFI) Governance and Self-Appraisal Checklist 2024/25
6) Review of Key Accounting Policies and Judgments
7) Government Procurement Card Information
8) Information Security Risk Management – Audit Outcomes

12. Items for Information

12.1 The Committee noted the following items:

1) Q3 2023/2024 Information Assurance and Governance report
2) Q3 2023/24 Employment Law Report
3) PPG Forthcoming Matters Tracker

13. Any other competent business

13.1 No other business was raised.

14. Items for Escalation to RoS Board

14.1 Item 7.2 ‘Key Risk Register – Financial Impact Review’ will be escalated to the RoS Board for its consideration as discussed.

15. Meeting close

15.1 The meeting closed at 1250hrs. The next meeting(s) will be held on:

ARC Informal Check-In
09 July 2024 (apologies noted from Tim Wright)
0930hrs
Remote via Teams

ARC BAU Meeting
13 August 2024 (with current and new Committee members in attendance)
1030hrs
Meadowbank House, Edinburgh