Minutes of the 61st Meeting of the

Office for Legal Complaints Audit and Risk Committee

Monday 15 January 2024

Members Present:
Harindra Punchihewa, Chair
Alison Sansome
Jane Martin (items 1 to 9)
Martin Spencer

In Attendance:
Elisabeth Davies, OLC Chair – observing-(joined mtg part way though risk assurance report).
Paul McFadden, Chief Ombudsman
Blessing Simango, Head of Finance, Procurement and ICT
Laura Stroppolo, Head of Programme Management and Assurance
David Peckham, Head of Operations, Business Transformation and Business Intelligence
Kay Kershaw, Board Governance Manager (Minutes)
Aaron Rock, Risk Manager (item 4)
Steve Moore, ICT Manager (items 11 and 12)
Steve Pearson, Deputy Chief Ombudsman (item 13)
Nawal Henry, Health and Safety and Facilities Officer (item 14)
Paul Conway, Performance and BI Manager (item 15)
Tom Harris, Deloitte
Ella Firman, National Audit Office
Sarah Hutchinson, Government Internal Audit Agency
Kasim Raja, MoJ, ALB Centre of Excellence – observing.
Clare Brown, LSB – observing.

Apologies:
Matthew Hill, Legal Services Board
Matt Ellis, Government Internal Audit Agency
Alex Clarke, National Audit Office

Item 1 - Welcome, apologies and declarations of interest

1. The Chair welcomed attendees to the meeting and introductions took place.

2. Apologies were noted.

3. The meeting was quorate.

4. There were no declarations of interest.

Item 2 – Deep Dive: Case management system and process

5. This agenda item was deferred from the October 2023 ARAC meeting.

6. The Head of Operations, Business Transformation and Business Intelligence presented a paper reporting on a deep dive of the case management system (CMS) and process.

7. Updates were provided on partially completed internal audit actions arising from two case progression audits undertaken in March and June 2021 and the actions being undertaken to complete them. The following points were made:

- Phase one audit action 1.1: This audit action had been delayed because of resource constraint, but some progress had been made following the implementation of a sign off process for Case Management System (CMS) guidance. Some CMS guidance was still to be reviewed and have an owner assigned to it; this would be progressed as part of project work to be completed at the end of 2025 after the completion of the LEAN process review.
- Phase one audit action 2.1: This audit action had been delayed because of changes in key personnel. Having successfully recruited a BI/SQL Developer, some progress had now been made on data warehousing and Power BI reporting; this provided greater assurance on data from source through to end reporting. A review of reporting was due to commence and it was expected that progress on the outstanding elements of this audit action would be made during Q4.
- Phase two audit action 1.1: It had not been possible to resolve a conflict between Outlook and Dynamics in-house so customer files continued to be set up in CMS to capture reportable data at the front end. A technological solution to address the GDPR compliance risks associated with a high volume of customer information being held within CMS files that were not progressed to a case entering the Pre- Assessment Pool (PAP) would be considered as part of the LEAN process review which commenced on 15 January 2024. To mitigate the GDPR compliance risk in the meantime, customers were asked to use the Customer Application Form instead of submitting complaints via Outlook and to only submit further information when it was requested.
- Phase two audit action 1.2: Having undertaken a costs / benefits analysis, the Executive had made a decision not to progress this audit action and would therefore not be terminating LeO's telephony service which was considered an essential element of the service and support provided to LeO's customers.

8. In discussion, questions were raised about whether the GDPR compliance risks that were identified by auditors related to the number of customer files or the volume of information held within the CMS; whether consideration had been given to alternative contracting arrangements for roles within IT and Business Intelligence; the level of satisfaction with the current CMS; the reason for the delay in scheduling a rolling

programme of guidance reviews; what other risks were linked to the CMS and process. In response, the following points were made:

- The GDPR compliance risks related to both the number of customer files and the volume of information held within the CMS that related to matters that were not progressed to a case in the PAP. It was anticipated that there may be scope to delete some of these customer files which would free up storage space and save on future costs once a technological solution had been identified to overcome the conflict between Outlook and Dynamics.
- Consideration had been given to alternative contracting arrangements for IT and Business Intelligence roles, however the Executive considered it would be more effective for staff in these roles to be employed by LeO as they would have a better understanding of the organisation and its processes and also work in a more agile way compared to contractors, ensuring continuous improvement. Steps had been taken to build resilience within the IT Team and a managed services contract was in place providing external support with CMS.
- The Executive considered the CMS to be a good system that met the organisations current needs. As part of an end-to-end review of business processes, the ICT Manager would consider ways to exploit the CMS capability to make further improvements.
- The Executive deemed it to be more effective to develop a rolling programme of guidance reviews which would be undertaken as part of the ongoing project work.
- In addition to the resource and system capability risks, a reporting risk associated with the CMS and process had been identified; mitigations were in place to manage this risk.

9. ARAC **noted** the update on the deep dive of the CMS and process, the technological and process improvements that had been made since the two internal audits on case progression had been undertaken in 2021 and the potential for further improvements following the completion of the LEAN review process.

Item 3 - Previous minutes, previous actions and matters arising.

10. The minutes of the ARAC meeting held on 2 October 2023 were **approved**, subject to the Board Governance Manager's review and clarification of ARAC members' attendance at the meeting.

ACTION: The Board Governance Manager to review and clarify the record of ARAC members' attendance at the ARAC meeting held on 2 October 2023.

11. ARAC **agreed** that action 6, paragraph 26 from the meeting held on 2 October 2023 should be closed following the discussion that had taken place between the ARAC Chair and members of the Executive on 12 January 2024 about further potential improvements to risk management and reporting, risk tolerance and relationship to risk appetite.

ACTION: The Board Governance Manager to close action 6, paragraph 26 from the ARAC meeting held on 2 October 2023.

12. ARAC **noted** the update on previous actions.

13. In line with ARAC's Terms of Reference, ARAC members had attended a private meeting with internal and external auditors on 15 January 2024.

Item 4 – Risk Assurance

14. The Head of Programme Management and Assurance presented the Risk Assurance report, updating ARAC on the position at the end of November 2023 on strategic risks and issues, business unit risks and internal audits. The following key points were drawn to ARAC's attention:

- The likelihood score for the strategic risk relating to the Edward House lease had reduced; this risk continued to be closely monitored. Engagement with landlords and the Government Property Agency continued regarding LeO's future ways of working.
- In February, the Board would be taking part on an attrition workshop, where consideration would be given to what aspects of the attrition risk were, and were not, within the OLC/LeO's control and what more could be done to mitigate the risk. It was anticipated that the Board's discussions would lead to the attrition risk being more clearly articulated on the strategic risk register.
- In December, the Board provided out of committee approval for the 2023/24 strategic risks and issues; this decision would be ratified at the January Board meeting.
- Resource was a common factor underpinning the high rated business unit risks. The cumulative impact of the resourcing issues across individual business units created the strategic level risk.
- Scoring for business unit risks was mostly driven by the impact of the risk. Whilst there was a high number of business unit risks, only two had the highest 'likelihood' scoring of 5. All business unit risks were closely monitored and targeted actions and controls were in place to reduce the likelihood of the risks occurring.
- Following discussion with the ARAC Chair on 12 January 2024, further enhancements would be made to risk management and reporting, including the introduction of more realistic target risk scoring; metrics to highlight the gap between residual risk scoring and target risk scoring; key risk indicators; more clarity on the mitigating action and the related timescales for reducing those risks some of which required a longer term approach; a process for escalating risks that were outside of tolerance to the Board. The Board's approval of the revised target risk scoring would be sought in due course.

- The number of overdue internal audit actions had reduced from ten to one. The remaining overdue audit action would be completed by the end of January 2024.
- All three completed internal audits for 2023/24 had received a substantial rating; no recommendations had been received for two of these audits.
- Meetings had taken place with internal auditors to scope the Q4 audit of Quality and the 2024/25 audit plan. A scoping meeting for the audit of Stakeholder Engagement would soon be taking place.

15. Having sought to understand whether there were any additional actions within LeO's control that could be taken to address the strategic issues that were outside tolerance and what further action ARAC could take if risk scoring persistently remained outside tolerance, the following points were made:

- Actions to address some strategic risks and issues were outside of LeO's control and others required a longer term approach to reducing risk scores.
- In exceptional circumstances, organisations had to accept the level of risk exposure. In such circumstances it would be important to ensure that the risks were well documented, with clear explanations about why the risks were there, why they are accepted with that level of exposure and when they were expected to reduce.
- The Executive had undertaken an attrition risk workshop to review the effectiveness of mitigating actions and consider what more could be done in both the internal and external environments to address the attrition risk. Further consideration would be given to this at the Board's strategic attrition risk workshop in February.
- As part of further enhancements being made to risk management and reporting, the scope for limiting the impact of those risks and issues that had a high likelihood of occurring would be considered.
- Concerns about the risks that persistently remained outside tolerance would be escalated to the Board for further consideration on whether more could be done to manage the risks.
- Strategic risks that remained persistently outside tolerance would only become strategic issues once they had crystallised.

16. Having sought to understand what collective impact business unit risks had on the organisation at an operational level, the ARAC Chair was advised that internal policies and governance ensured that business unit risks remained under control and were closely monitored by risk owners, the risk manager and the Executive. The Assurance Map would be presented to ARAC May 2024, this would show any movement in business unit risk scoring.

17. ARAC **noted** the Risk assurance update.

Item 5 - Internal Audit update

18. The 2023/24 internal audit plan remained on track for delivery, with three audits completed and the remaining two being scoped.

19. The audits on cyber security and grievances and staff complaints had each received a substantial rating.

20. The cyber security audit had provided assurance on the aspects of cyber security that were controlled by LeO/OLC, but not on aspects that had been outsourced to a third-party supplier.

21. A discussion took place about the next cyber security audit and whether it might focus on third-party supplier management and independent assurance. Having noted that there may not be scope within the third-party supplier's contract for GIAA to conduct such an audit, it was suggested that consideration might be given instead to auditing the robustness of the contractual framework for managing cyber security. Further consideration would be given to this as part of the 2024/25 internal audit planning.

22. Internal audit planning for 2024/25 had commenced and a risk-based proposal would be developed taking into account the risk register, business plan and the long-term audit plan. A draft proposal would be presented in Q4 and approval for the final audit plan would be sought in Q1. ARAC members were advised to forward any suggestions for potential audits to the Head of Programme Management and Assurance for discussion with GIAA.

ACTION: ARAC members to forward suggestions for potential audits to the Head of Programme Management and Assurance.

23. GIAA was considering some potential cross-departmental audits, if LeO/OLC was selected to take part in them it would provide an additional level of assurance.

24. ARAC was advised that the cost associated with cross-departmental audits would primarily be funded centrally by GIAA and that LeO/OLC would be notified at the earliest opportunity if taking part in a cross-department audit would have a cost implication.

25. ARAC **noted** the Internal audit update.

Item 6 - External audit update.

26. An initial planning meeting for the 2023/24 audit of Financial Statements had taken place in January with discussions focussed on the preliminary assessment of risks and the audit reporting timetable. A further meeting had been scheduled; this would focus on the detailed reporting timetable.

27. The Financial Statements audit would commence a week earlier than last year to allow more time to complete the work, deal with outstanding audit queries and ensure sufficient time to complete the financial statements.

28. Auditors had requested that the financial statements were drafted by the end of April.

29. The preliminary risk assessment was broadly in line with the previous year and included the management override of controls.

30. Auditors would not be reporting on accounting for leases as part of the 2023/24 audit because the level of risk had decreased.

31. ARAC members raised no objections to the preliminary materiality being set at £334,000, performance materiality being set at £250,000 and the error reporting threshold being set at £6000.

32. ARAC members **confirmed** that they were not aware of any frauds that had taken place during the year.

33. ARAC members **confirmed** that they were not aware of any ways that fraud could be perpetrated. Internal audits had not identified any areas of fraud risk for the Committee to be concerned about.

34. Recognising that LeO had a small finance team with limited segregation of duties, auditors stated that it would be important to ensure that the finance team did not get any smaller in order to mitigate the risk of management override of controls.

35. A new team of auditors would be conducting this year's audit; handover meetings and briefings had taken place to minimise the number of knowledge questions asked by the team.

36. Auditors were attending to the actions arising in response to the lessons learned from the 2022/23 Financial Statements audit to ensure a smoother audit and reporting process this year. This included creating a granular reporting timetable; a 'PBC' list that would be finalised well in advance of year end and regular catch up meetings with key staff.

37. ARAC members welcomed the attention given by Auditors to the lessons learned from the previous audit, commenting on the value of incremental learning to ensure the audit process was a smooth as possible.

38. ARAC **noted** the External Audit update.

Item 7 – Annual Report and Accounts 2023/24: Planning

39. The Head of Programme Management and Assurance updated ARAC on the planning and timetable for the 2023/24 Annual Report and Accounts, drawing attention to the following key points:

- Engagement had taken place with the MoJ and LSB to ensure alignment with LeO's planning and timetable for the 2023/24 Annual Report and Accounts.
- The high-level milestones for the 2023/24 Annual Report and Accounts process had been shared with external auditors.
- The earlier start date of the Financial Statements audit was manageable and was not expected to cause any issues.

- The next planning meeting with auditors would provide an opportunity to clarify details and address any issues before the audit commenced.
- Weekly meetings would take place with auditors throughout the audit.
- The internal Annual Report and Accounts project would be launched in February.
- The drafting of the Annual Report and Accounts had been outsourced to ensure resilience and capacity within the External Affairs Team. Proof-reading would be undertaken in-house.

40. ARAC **noted** the planning and timetable for the 2023/24 Annual Report and Accounts.

Item 8 – Financial Governance

41. The Financial Governance report was presented by the Head of Finance, Procurement and ICT. The following key points were made:

- Since issuing the Financial Assurance paper, the forecast underspend had increased by £47k. This was due to an unexpected credit from Birmingham City Council of £18k relating business rates in 2020/21, ombudsman attrition and recruitment challenges for specialist corporate roles. The forecast outturn position had therefore increased by £29k.
- Ninety-two per cent of the £250k capital budget would be spent on SharePoint migration; this work had commenced and the supplier had confirmed that work to the value of £230k would have been completed by 31 March 2024. The remaining capital budget would be spent on costs relating to furniture and fittings.
- The Executive aimed for the year end budget variance to be within the MoJ's 1% tolerance level; mitigating actions would be deployed if required to reduce any underspend.

42. Acknowledging the many variables and challenges that impacted the budget throughout the year, the ARAC Chair was keen to ensure that, where possible, all necessary spending was captured at the time the budget was set to avoid the need for mitigating actions to be deployed in Q4 to reduce any underspend.

43. ARAC **noted** the Financial Assurance report.

Item 9 – 2024/25 Budget: Assurance on budget setting process

44. The Budget Setting Assurance report was presented by the Heads of Finance, Procurement and ICT and Operations, Business Transformation and Intelligence.

45. In discussion the following key points were made:

- The report included ‘actual’ figures for 2024/25 and outlined the checks and balances that had been put in place to ensure the accuracy of all elements of the proposed budget and underlying key performance assumptions.
- The proposed budget had been tested extensively across all relevant business functions and the Performance Sub-Group (PSG) had thoroughly tested the assumptions and trajectories.
- The PSG had recommended some minor changes to the assumptions and trajectories having questioned the accuracy of the worst case scenario for demand.
- The PSG had also questioned whether reference to the ‘worst case’ was misleading as it implied that everything that could have an adverse impact on the assumptions and trajectories had been taken into account. Recognising that there may be some as yet unknown factors that could impact the assumptions and trajectories, it had been suggested that consideration was given to revising the terminology to reflect that this was a lower case estimate instead of the worst case scenario.
- The Executive was following up on the points raised by the PSG and would be presenting the revised assumptions and trajectories for lower, upper and likely case scenarios in addition to extenuating circumstances at the January Board meeting for further consideration.
- Stakeholder feedback in response to the 2024/25 Budget and Business Plan and 2024/27 Strategy consultation had broadly indicated support for the proposed budget; an overview of the consultation responses had been included in the paper.
- No changes had been made to the proposed budget.

46. Following discussion, the ARAC Chair stated that he had been satisfied that ARAC’s Budget Acceptance Criteria had been met, requesting that ARAC was alerted to anything that compromised any of the criteria during the remainder of the budget setting process.

47. ARAC **noted** the update on the 2024/25 Budget setting assurance process.

Item 10 – Attestations and single tenders report

48. The Head of Finance, Procurement and ICT presented the Attestations and Single Tenders report providing details of three single tender justifications for the period September to December 2023.

49. ARAC **noted** that attestations and single tenders report.

Item 11 – Annual security policy framework: self-assessment

50. This agenda item was deferred from the October 2023 ARAC meeting.

51. The ICT Manager presented the 2022/23 Cyber Security Framework Self-Assessment report, highlighting the findings of the self- assessment and the actions that had been taken to mitigate a few vulnerabilities that had been identified.

52. In response to questions from the ARAC Chair, the ICT Manager explained that:

- Cyber Essentials certification was not appropriate for an organisation like LeO. LeO had produced its own framework that incorporated elements of Cyber Essentials and discussions were taking place with the MoJ about the potential deployment of a formal framework for validating LeO's cyber security measures. This framework would be tested by LeO in 2025 before it was implemented in 2026.
- The managed service provider responsible for monitoring data security was approved through the Crown Commercial Framework and was a Microsoft Gold Partner.

53. ARAC **noted** the 2022/23 Cyber Security Framework Self-Assessment report.

54. Commenting on the need to maintain vigilance and develop mitigations to reduce the risk of new threats relating to cyber security, ARAC thanked the ICT Manager for their report and their continued focus on cyber security. Further, the suggestion was made to do some peer group benchmarking where possible.

Item 12 - Annual cyber security report

55. This agenda item was deferred from the October 2023 ARAC meeting.

56. The ICT Manager presented the annual Cyber Security Report; this report had been updated since it was first issued to ARAC in October 2023. ARAC's attention was drawn to:

- The security measures that had been put in place in 2022/23 and 2023/24 to improve the level of security and mitigate cyber security risks.
- A security incident arising from the exploitation of a vulnerability in a form on LeO's website; this was quickly resolved in collaboration with LeO's managed service provider for the website and no personal information or LeO data had been compromised by this incident.

57. In response to questions, the ICT Manager reported that:

- The security incident had been identified by the website's managed service provider as part of their routine monitoring of malicious or suspicious activity in line with their contractual responsibility.
- Contractual agreements were in place with all IT managed service providers to monitor malicious and suspicious activity and any future contracts awarded would also include this requirement.
- LeO was confident that the website vulnerability had not been exploited in the past.

- The action listed on the penetration test remedial plan to disable and delete old system admin accounts that were no longer in use had been completed.
- The action listed on the penetration test remedial plan relating to an outdated SharePoint version remained in progress. Migration to SharePoint 365 had commenced and this was expected to be completed by the end of May 2024.

58. ARAC **noted** the 2023 Cyber Security report.

Item 13 – Information rights and security incidents

59. Papers on Information Rights and Security Incidents for quarters 2 and 3 2023/24 were presented by the Deputy Chief Ombudsman (DCO). The following key points were drawn to ARAC's attention:

- The number of data breaches and statutory information requests had remained broadly stable over the last two quarters.
- Most security incidents related to 'incorrect recipient'; this remained consistent with previous quarters. Mitigating actions were in place to minimise the occurrence of these incidents. The viability of introducing additional controls continued to be assessed but, considering the small number of incidents involved and the likely adverse impact additional controls would have on operational performance, further controls were considered to be dis-proportionate at the present time. The Executive would continue to review this decision and further action would be taken if the level of incidents showed any significant and sustained increase.
- A small number of information requests had not been completed within the statutory deadlines, this was because of delays with a third party transcribing telephone calls, large volumes of information being requested and an information request being misdirected. In all instances, the information requestors had been kept updated about the delay; mitigating actions had been taken to reduce the risk of re-occurrence and learning had been fed back to staff.

60. In response to questions, the DCO advised that:

- The scale of the risk of information being sent to an incorrect recipient was minimal for both financial and highly sensitive information because LeO did not hold financial details and information relating to third parties or matters that were not part of the complaint being investigated were redacted from evidence bundles. The measures in place to mitigate the small risk of other personal or sensitive data being sent to an incorrect recipient was considered to be proportionate.
- The Security Forum regularly reviewed both the cause and volume of data breaches to determine whether current mitigating actions remained sufficiently robust and whether additional measures to mitigate the associated risk was required.

61. Following discussion, ARAC **noted** the Information Rights and Security Incidents for quarters 2 and 3.

Item 14 – Annual health and safety compliance report

62. The annual Health and Safety Compliance report was presented by the Head of Programme Management and Assurance.

63. In discussion, the following key points were made:

- Since the paper was written, further progress had been made on the new health and safety system which was on track to be implemented in January. The old health and safety system would remain open until all the data it held had been transferred to the new system.
- The dis-repair of the windows and security gates at the Birmingham office would be discussed with the Landlord as part of the lease negotiation process.
- All actions arising from DSE assessments up to December 2023 had been completed.
- An external health and safety audit was to be undertaken on 23 January 2024. The findings of this audit would be shared with the Executive and ARAC in due course.
- LeO's Health and Safety policy and associated procedures related to all staff, including those working from the hubs and home workers.
- It was confirmed that the Head of Programme Management and Assurance was the Executive sponsor for health and safety.

64. Following discussion, ARAC **noted** the annual Health and Safety Compliance report.

Item 15 - Annual data assurance report

65. The annual Data Assurance report was presented by the Head of Operations, Business Transformation and Business Intelligence. The following key points were made:

- LeO continued to automate data reporting wherever possible.
- In 2024/25 LeO would be undertaking a reporting project which would involve reviewing the current suite of reporting to ensure it was fit for purpose and that it was underpinned by quality data.

66. An ARAC member sought to understand the timescale for the introduction of ARAC and RemCo dashboards. The ARAC Chair requested that an update on this was provided to ARAC members outside of the meeting.

ACTION: The Head of Operations, Business Transformation and Business Intelligence to provide an update to ARAC members outside of the meeting

on the expected timescale for the introduction of ARAC and RemCo dashboards.

67. ARAC **noted** the annual Data Assurance report.

Item 16 – Escalations to Board

68. It was **agreed** that ARAC's concerns about the risks that persistently remained outside tolerance would be escalated to the Board so that consideration could be given to whether anything more could to manage the risks.

Item 17 - Any Other Business

69. There was no other business.