

**Minutes of the thirty-seventh meeting of the
Office for Legal Complaints Audit and Risk Committee
Thursday 19 April 2018
12.00 - 15:00
National Audit Office, London**

Present:

Michael Kaltz, Chair

Rebecca Hilsenrath

Annette Lovell (by telephone for items 1-4, 13 and 16)

In Attendance:

Rob Powell, CEO

Rebecca Marsh, Chief Ombudsman

Wanda Goldwag, OLC Chair (observer)

Emma Cartwright, Head of Finance, (by telephone)

Ali Morgan, National Audit Office (NAO)

Ed Bowie, Head of ALB Partnership and Assurance, MoJ

Andrea Emms, Government Internal Audit Agency (GIAA)

Chris Davis, GIAA

Marcus Passant, Head of HR (by telephone for item 10)

Steven Pearson, Senior Ombudsman (by telephone for items 1-7)

Gurmit Sangha, Compliance Officer (by telephone for items 1-7)

Apologies:

Alison Wedge, Deputy Director, ALB Governance, MoJ

David Eagles, Partner, BDO

Steven Corbishley, NAO

Archie Rwavazhinji, Assistant Manager, BDO

Neil Buckley, CEO, Legal Services Board

Board Secretary:

Kay Kershaw

Item 1 – Welcome and apologies.

1. The Chair welcomed those in attendance and introductions took place. Apologies were noted.
2. The meeting was quorate for items 1 – 4, 13 and 16. Decisions proposed during the meeting were ratified in item 16.
3. A conflict of interest was declared for all LeO staff present with respect to agenda item 10, Employee Value Proposition: Reward and Recognition Controls.
4. There were no other conflict of interests declared.

Item 2 – GDPR readiness review

5. Gurmit Sangha presented a paper setting out the progress made in meeting the requirements of the General Data Protection Regulation (GDPR) which comes into force with a new Data Protection Act on 25 May 2018.
6. It was **noted** that good progress was being made.
7. Information Asset Registers (IARs) have been introduced for each area of the business in line with the approach adopted by the National Archives. This would provide assurance on the safe handling of information assets and the mitigations in place to manage any risks. The Security Forum, attended by the SIRO, was confident that all IARs were complete. The development and review of IARs would be considered annually by the Security Forum.
8. Guidance had been sought from the MoJ, ICO and other ombudsman organisations, which had assisted LeO in establishing its grounds for processing personal data. During the investigation of a complaint, the grounds for processing personal data would be 'consent'. The grounds for processing employee data would be 'legitimate interests'. The grounds for processing personal data when undertaking activities permitted by the Legal Services Act such as data sharing with regulators, research and customer satisfaction surveys would be 'a task carried out in the public interest or in the exercise of official authority vested in the controller'.
9. Privacy notices have been updated for use from April. The privacy notice on the website would be updated by 25 May.
10. Technical and organisational measures to show that the organisation had considered and integrated data protection into its processing activities have been implemented. Any new processing of data would now only be authorised upon completion of a satisfactory privacy impact assessment (PIA). A new PIA template was now in operation and guidance on their use has been issued to staff.
11. Staff training is to be provided to raise awareness of data subjects' rights and how they would be handled within the organisation.
12. All contracts with partner organisations responsible for processing data had been reviewed. It was noted that whilst all partner organisations were compliant with the current Data Protection Act, they did not all meet the standard set by GDPR. The Crown Commercial Service has provided a template letter to be sent to all processors and a template contract setting out the GDPR data protection terms.

13. It was noted that under GDPR, LeO's suppliers would be responsible and accountable for any data breaches they cause. The Security Forum would monitor these data breaches and annually review the data management policies of partner organisations in order to ensure that they remained compliant with requirements of GDPR.
14. Internal Audit would review LeO's contracts with suppliers in order to provide feedback and further assurance.
15. A new reporting tool was being developed for staff to report data breaches. This would alert key officers to any data breaches so that they could establish the severity of the resulting risk to the data subject's rights and freedoms and decide whether that risk should be reported to the ICO and the data subject within the new 72 hour deadline. A record of decisions taken not to report data breaches would be retained in line with GDPR requirements. The Committee noted that no previous breaches had been assessed by the SIRO as requiring reporting to ICO (although they had been reported to the data subjects). It was acknowledged by the Committee and the management that some of those breaches may have been reportable had GDPR been in force.
16. Training and guidance on the new requirements for reporting data breaches would be provided to staff. The Committee requested sight of this guidance for information and noted that due to internal deadlines it would not be possible for them to request any amendments to this guidance prior to 25 May.
ACTION: The CEO to share staff guidance on reporting data breaches under GDPR with ARAC members.
17. In discussion it was noted that a good escalation process for dealing with data breaches would be imperative in order to ensure that the SIRO was able to take the necessary action within the new deadlines.
18. LeO has sought to comply with Article 30 of the GDPR by documenting mandatory information in regard to processing activities, risk assessment and data protection assurance.
19. The Committee commented on the additional burden that GDPR implementation could place on staff at a time when the organisation was already going through considerable change as a result of the Modernising LeO Programme. They noted that the timely action taken by the organisation had helped to reduce some of this additional burden.
20. The CEO updated the Committee on the recruitment activity taking place following the resignation of the Data Protection Officer.
21. The Committee thanked the Data Protection Officer for the sterling work he had undertaken on GDPR implementation and wished him every success in his new role.
22. The Committee **noted** the progress made and the arrangements in hand to complete GDPR compliance activities by 25 May.

Item 3 – Strategic risk register.

23. A paper summarising the position on the Legal Ombudsman’s strategic risk register was circulated prior to the meeting. This paper included an in-depth review of the operational resource and demand strategic risks.
24. The Committee **noted** that nine of the twelve risks were stable relative to the position at the end of quarter three. Two risks had increased: quality of service, as a result of concerns about quality issues including timeliness performance; and data security due to the resignation of the Data Protection Officer. The risks around operational resource had reduced as a result of additional recruitment using the increased 2018-19 budget and the expansion of the ombudsman pool. Four risks were at target and eight were not. All risks were being actively managed.
25. There were four operational risks scoring above 15, which all related to the impact and resources committed to the Modernising LeO programme. It was noted that the new case management system had gone live on 18 April and this was likely to result in a reduction to these risk ratings.
26. A discussion took place about the reputation and credibility risk and whether an impact evaluation had been undertaken to assess the involvement of level 2 ombudsmen in stakeholder engagement activities. It was noted that stakeholder engagement was a key element in the 2018/19 business plan where more work would be undertaken to properly segment LeO’s stakeholders and develop a refreshed communications and engagement strategy. In the meantime, the balanced scorecard would provide a record of the emerging measures on the impact of stakeholder engagement. A full impact assessment would be undertaken once the stakeholder strategy has been implemented in order to measure its success.
27. An Internal Audit of stakeholder engagement was planned for 2018/19 which would add further value and provide assurance about this area of work.
28. The Chief Ombudsmen reported that she would be introducing a granular review of quality in order to ensure that the organisation had the right resources to deliver a consistently high quality service.
29. The Chair requested the names of risk owners to be updated to reflect changes of staffing within the organisation.
ACTION: CEO to update the names of risk owners to reflect changes of staffing within the organisation.
30. Steve Pearson presented a paper setting out a detailed retrospective review of the demand and operational resource risk and advised that the OLC Board would be holding its annual strategic risk workshop on 23 April.
31. The Committee **noted** that the risk around demand had been significant due to an increase in the number of cases accepted for investigation and insufficient resource to meet the demand. This had led to poor performance against KPIs and a backlog of unallocated cases. Resource capacity had also been negatively impacted by the inability to over recruit to key roles and the delivery of the Modernising LeO Programme.

32. The procurement and implementation of a forecasting tool is beginning to provide greater visibility of the effects of changes in demand and available capacity.
33. The forecasting tool is continuing to be refined. With more accurate data being captured in the new case management system and the recruitment of a specialist forecasting and capacity modelling analyst, the organisation would have a better evidence-base to inform key operational decisions. But in the meantime, the forecasting tool was providing an evidence base to start initial demand and capacity modelling.
34. Annette Lovell suggested that the Executive reviewed the link between horizon scanning and forecasting to the risk register. The Committee also discussed whether elements of the delivery of the scheme could be further simplified.
35. Members **noted** the strategic risk update and the in depth review of the demand and operational resources risks.

Item 4 – Annual fraud report

36. The Head of Finance presented a paper setting out an annual update on the fraud risk register which included an assessment of LeO's overall position on fraud risk against Annex 4.7 of Managing Public Money, a copy of the fraud risk register setting out in some detail a number of fraud risks along with the detective and preventive controls in place to mitigate them, and the relevant extracts from LeO's assurance map.
37. It was **noted** that this paper was presented to ARAC in order to provide assurance about fraud risk to support the process of sign off of the 2017-18 Annual Report and Accounts.
38. Members **noted** that the overall level of risk was low and that there was a clear control framework in place, with a scheme of delegations and appropriate controls.
39. Members **noted** that there had been no additional risks added to the fraud risk register since June 2017 and **noted** the progress that had been made to date and that the remaining items listed had clear timescales in place for completion.
40. A detailed discussion took place around the fraud risks.
41. In response to a question from the Chair, the CEO responded about risks of conflict of interest in recruitment matters. The CEO was asked to check whether LeO's job application form required applicants to declare a conflict of interest (in the broadest sense of the term).
ACTION: The CEO to confirm whether LeO's job application form required applicants to declare a conflict of interest.
42. The CEO advised that all staff now completed an annual conflict of interest return.
43. 

Fol Exempt S.43 (2)

44. Chris Davis reported that he was pleased to see that a risk around corrupt behaviour in the decision making process was now included in the fraud risk register.
45. It was noted that LeO's travel policy stated that staff must book travel through Redfern. Redfern provides the CEO with a clear audit trail of all travel booked by staff.
46. The CEO reported that fraud risk around flexible working is low and there is good visibility about staff productivity when working flexibly.
47. Ali Morgan advised that, as part of the NAO's end of year process, the Committee would be required to state whether or not it was satisfied with the fraud controls LeO had in place.
48. The Committee confirmed that it was comfortable providing assurance on the fraud controls subject to the caveat that Annette Lovell was a new member of ARAC and therefore had no prior knowledge of the fraud controls that were in place or the actions that had previously been taken.
49. Members **noted** the contents of this paper.

Item 5 – Policy reviews

50. The CEO reported that the expenses policy, gifts and hospitality policy, procurement policy and asset management policy had all be reviewed in line with the rolling programme of policy reviews. No amendments were made as a result of this process. All four policies would be reviewed again in quarter 1 to ensure that they were correctly aligned with any MoJ communications and controls for the new financial year.
51. The Committee **noted** the review of these policies.
52. The whistleblowing policy had been reviewed and a number of minor changes had been recommended. The Committee commented on some inconsistency in terminology and overlapping concepts within the policy and asked for this to be rectified prior to internal publication. The Committee also asked the CEO to look again at section 3.3 to confirm that what was recorded was accurate.
53. Chris Davis suggested that rather than list examples of whistleblowing concerns, the policy should list the criteria around what would be considered a whistleblowing matter.
54. The CEO **agreed** to address the use of inconsistent terminology and overlapping concepts, confirm the accuracy of section 3.3 and amend the policy accordingly.
ACTION: The CEO to address the use of inconsistent terminology and overlapping concepts, confirm the accuracy of section 3.3 and amend the policy accordingly.
55. The Committee **confirmed** that they would not require sight of the amended policy and **approved** the whistleblowing policy subject to these additional amendments being made.

56. The Committee was asked to comment on a new critical incident policy that had been developed. The policy defined a critical incident and how the organisation would respond to one.

57. The Committee suggested including examples of critical incidents within the policy.

ACTION: The CEO to include examples of critical incidents within the policy.

Item 6 – Data handling incident report.

58. The Chief Ombudsman presented a paper on the actions undertaken this quarter to reduce the number of data handling incidents together with planned actions and interventions that would be implemented in the short and medium term. The paper included a summary of the data incidents for quarter four of 2017/18.

59. The Committee **noted** that in January new guidance had been issued to staff around handling information. Guidance on data security had also been reviewed and re-issued to staff. This has resulted in a positive improvement to data handling within the organisation.

60. Planning for the changes associated with GDPR continues. It is anticipated that these changes would result in improved data incident reporting and notification systems.

61. As part of the Modernising LeO Programme, all operational guidance had been reviewed and significant progress had been made in retraining operational staff on the new prescribed ways of working.

62. It was anticipated that the prescribed checkpoints and validations being introduced by the Chief Ombudsman as part of the new supervision model would contribute further towards increased data security and the early identification of issues.

63. In quarter four, the number of preventable data handling incidents reduced to 5. There were 5 breaches of policy which had no related loss.

64. In discussion it was felt that the spike in incidents in quarter 3 may have been caused by pressure on resources and also related to a number of incidents involving third party suppliers.

65. The CEO reported that the SIRO, Nikki Greenway, would present future Data Handling Incident Reports to the Committee.

66. It was noted that the SIRO would be ensuring that training for all Information Asset Owners (IAOs) is up to date.

ACTION: SIRO to ensure training for all Information Asset Owners if up to date.

67. **The Committee noted the issues highlighted in the paper.**

Item 7 – Update on internal audit actions

68. The CEO presented an update on internal audit actions.

69. Final audit reports for Attendance Management and Modernising LeO had now been received, both resulted in assurance ratings of Substantial. The recommendations of both reports were accepted and reflected issues that had already been identified by the organisation.

70. It was **noted** that seven of the 54 actions arising from internal audits since January 2016 were not yet fully remediated. Of these, two actions related to the performance audit and two to the audit of the financial control framework; remediation of these outstanding actions were dependent on the new case management system. One action related the Modernising LeO audit and was due for completion in June 2018 and two actions related to the Attendance Management audit which were both due for completion in May 2018.
71. Concern was raised about the overall priority of 'low' given to the actions in the Attendance Management audit as it was felt by the Chair and some members that the risk of not recording details of conversations with staff on sick leave should have led to a higher priority. Chris Davis confirmed that he was satisfied that the priority given to these actions was appropriate.
72. The CEO advised this audit action was part of a number of improvements being implemented within the business around people management.
73. The Committee **noted** the update on internal audit actions.

Item 8 – Internal Audit update

74. Chris Davis presented a paper providing an update on the progress made by Internal Audit against the audit plan for 2017/18. This paper set out the first draft of GIAA's annual audit opinion, which provided an overall level of substantial assurance.
75. He reported that, in line with the audit plan, five audits have been delivered; Modernising LeO, Assurance Framework, Attendance Management, Financial Control Framework and Performance Statistics follow up. Four received a substantial assurance rating, the Performance Statistics follow up audit received a moderate assurance rating, the second highest level of assurance available.
76. The Committee noted that the annual substantial assurance rating was an indicator of how far the organisation has progressed over the last 12 months. The Committee noted in particular the report on the Financial Control Framework and congratulated the Head of Finance on the strength of her achievement.
77. The work on auditing Performance Statistics would continue in 2018/19 in order to assess and provide assurance on LeO's new reporting solution through the business intelligence (BI) project.
78. The terms of reference for the BI project have been drafted and a mapping exercise of the old and new reporting systems has been undertaken.
79. Following discussion, the CEO agreed to provide the Chair with an update on the progress being made in regard to finalising KPI definitions.
- ACTION: the CEO to provide an update on the progress being made in regard to KPI definitions to the Chair.**
80. The Committee **noted** the progress made by internal audit.

Item 9 – External Audit update

81. Ali Morgan reported that work would commence on 21 May to audit LeO's 2017-18 annual report and accounts.
82. The Committee **noted** the proposed approach to the audit of the 2017-18 financial statements.

Item 10 – Employee value proposition: reward and recognition controls

83. The Head of HR presented a paper setting out a draft control framework applying to LeO's proposed reward and recognition framework, setting out how LeO proposed to allocate the non-consolidated bonus pot, the control framework and monitoring of equality and diversity issues under the Public Sector Equality Duty.
84. It was **noted** that the framework and controls drew on the MoJ's reward and recognition scheme and that the MoJ, NAO and Internal Audit had been asked to review the framework and controls and provide comments ahead of a meeting with RemCo on 27 April, when final proposals would be tabled for approval.
85. The CEO reported that the reward and recognition proposals had been informed by constructive discussions with the Staff Council.
86. There was a discussion about the risk that allocation to high profile transformation project work could impact equality of opportunity for reward and recognition. The Executive explained how the proposed framework sought to balance recognition of business as usual delivery and specific project work. The Committee recommended that the monitoring process include specific checks about the balance of project and business as usual delivery to ensure fairness.
87. There was a discussion about whether the benefits of the award scheme could be outweighed by the controls process.
88. The Committee recommended that paper include more detail about the criteria staff were required to meet in order to earn a reward. The Committee also asked for the paper to be more explicit about the circumstances in which the Remuneration and Nomination Committee might feel that reputational risks made it inappropriate to approve payment of annual awards.
89. The Head of HR **agreed** to update the paper in line with the Committee's comments.
ACTION: Head of HR to update the paper in line with the Committee's comments.
90. The CEO reported that staff communications would be agreed once RemCo had made a formal decision on the reward and recognition proposals.
91. The Head of HR and CEO **noted** the comments provided by the Committee.

Item 11 – Annual report and accounts

92. The Head of Finance reported that the production process for the Annual Report and Accounts for 2017/18 was currently on track within project timescales.
93. Preparatory work had begun on drafting the various sections in line with Government's Financial Reporting Manual (FReM) requirements and progress had been made on agreeing key dates.

94. Initial performance data became available after 3 April and a first full draft is to be compiled and send to ARAC on or around 2 May.
95. Confirmation of the target laying date of 17 July is awaited.
96. ARAC **noted** the update on progress being made with the Annual Report and Accounts.

Item 12 – Update on the Grant Thornton governance review

97. The CEO presented a paper providing an update on the progress made on implementing the governance review conducted by Grant Thornton in December 2015.
98. He reported that initial progress against the action plan had been monitored by the previous OLC Chair and Chairs of ARAC and RemCo, before being signed over to 'business as usual' following a paper to the OLC Board in December 2016.
99. There were 15 actions outstanding in December 2016, of which all but two had now been completed. One action was dependent on the new case management system, while the other (the redundancy policy) required a minor update when it was next reviewed.
100. ARAC **noted** the progress made on implementing the governance review.

Item 13 - ARAC self-assessment and terms of reference review

101. In line with ARAC's terms of reference, the Committee is required to assess its effectiveness and review its terms of reference annually.
102. The Committee **noted** the update on the actions arising from the ARAC self-assessment for 2017/18 as a light-touch annual review of its effectiveness.
103. In discussion, it was **agreed** that, due to changes in Committee membership, the full ARAC self-assessment should be deferred until the end of the financial year to allow time for new members to settle into their role.

ACTION: Board Secretary to add the annual ARAC self-assessment to the forward plan.

104. Some minor amendments to the ARAC terms of reference were recommended by the Board Secretary in order to reflect changes in committee membership and structural changes within the organisation. The Chair requested an amendment to reflect the changes around GDPR under the regulatory requirements of the Committee.
105. It was **agreed** that the amendments to the terms of reference would be circulated out of committee for review and approval.

ACTION: Board Secretary to amend the ARAC terms of reference and circulate out of committee for review and approval.

Item 14 – standing items

106. The Head of HR presented a paper setting out exception reporting which set out details of single tenders and attestations.
107. The Committee **noted** the updated on standing items.

Item 15 – Minutes of the previous meeting, matters arising and outstanding actions

108. Internal Audit requested that the previous minutes were amended to reflect that ARAC had approved the Internal Audit plan for 2018/19 at its meeting on 28 February 2018.

ACTION: Board Secretary to amend the previous minutes.

109. Subject to the amendment noted above, the previous minutes were **approved**.

110. The Committee **noted** the update on outstanding actions.

111. There were no matters arising.

Item 16 – Recap of decisions taken

112. The Chair provided an update on the decisions taken during the meeting which are outlined in the relevant section of minutes for the benefit of Annette Lovell who had not been in attendance for all agenda items. Annette Lovell confirmed her approval of the decisions made.

Item 16 – Any other business

113. There was no other business