Post Office Limited
ARC Committee Meeting

MINUTES OF A MEETING OF THE AUDIT, RISK AND COMPLIANCE COMMITTEE HELD ON TUESDAY 23rd NOVEMBER 2017 AT 20 FINSBURY SREET, LONDON EC2Y 9AQ AT 11.15AM

Present:	Carla Stent	Chair **(CS)**	
	Richard Callard	Non-Executive Director **(RC)**	
	Tim Franklin	Independent Non-Executive Director **(TF)**	
	Ken McCall	Senior Independent Director **(KM)**	
			Item
In Attendance:	Paula Vennells	Group Chief Executive **(CEO)**	
	Alisdair Cameron	Chief Financial and Operations Officer **(CFOO)**	
	Jane MacLeod	General Counsel & Company Secretary (Secretary) **(JM)**	
	Marla Balicao	Minute Secretary **(MB)**	
	Ashish Singh	Head of Risk **(AS)**	
	Nick Kennett	Chief Executive Financial Services and Telecommunications **(NK)**	*(item 2)*
	Tim Armit	Business Continuity Manager **(TA)**	*(item 4.5)*
	Rob Houghton	Group Chief Information Officer **(RH)**	*(item 4.6, 4.7)*
	Mick Mitchell	IT Security and Service Director **(MM)**	*(item 4.6)*
	Jules Harris	Head of Information Protection and Assurance **(JH)**	*(item 5)*
	Johann Appel	Senior Manager Internal Audit **(JA)**	*(item 7)*
	Peter McIver	Ernst & Young **(PM)**	*(item 8)*
	Claire Johnson	Ernst & Young **(CJ)**	*(item 8)*
	Michael Passmore	Group Financial Controller **(MP)**	*(item 4.1,8)*
	Mark Dixon	Head of Treasury, Tax and Insurance **(MD)**	*(item 9)*

Apologies:	None	
		ACTION

1. WELCOME AND CONFLICTS OF INTEREST

A quorum being present, the Chair opened the meeting. The Directors declared that they had no conflicts of interest in the matters to be considered at the meeting in accordance with the requirements of section 177 of the Companies Act 2006 and the Company's Articles of Association.

2. POMS ARC REPORT (VERBAL UPDATE)

2.1 The Chair welcomed Nick Kennett to the meeting to provide a verbal update on the work of the POMS Audit, Risk and Compliance Committee (ARC).

2.2 NK reported that POMS had not had a recent ARC meeting, with one due in December but a Board Strategy session had been held earlier in the week which looked at the strategy for the next 5 years and took into account a comprehensive market assessment. Once finalised, POMS management will share the strategy with POL.

2.3   NK reported the oversight of the AR relationship of POL remains the highest rated out of tolerance risk, with a further paper due at the POMS ARC in December. The key areas of focus for the POMS ARC were the contractual arrangements (in particular the MSA and Distribution Agreement) , controls over fitness and propriety of POL staff selling POMS products, training and competencies within the branch network and the arrangements for oversight of in branch sales.

2.4   NK noted the dependency by POMS on the EUM project for the significant enhancement of controls relating to fitness and propriety, training and competence and the ability to track MI to individual staff members which POMS believes is an important component of their overall process for ensuring compliance.

2.5   EUM has proved to be a complex implementation, particularly given the dependency on data held through SuccessFactors, which in turn is migrating from HRSAP. In response to a question from the Chair, NK advised that if EUM was unable to deliver overall solution by the targeted June 2018 delivery date, POMS would have to consider requiring POL to cease selling POMS products in branch. NK noted that in the event of a delay in delivery there may be manual interventions which could avoid an adverse outcome, and that the EUM project was reviewing its contingency plans to ensure this possibility was addressed. The Chair noted that this project needed continual close oversight and **asked that NK provide an update of the POMS position to the January 2018 ARC.**   NK

2.6   NK reported on the renewals issue and he explained that following the introduction of new legislation which took effect from April 2017; a number of expiring travel insurance customers would subsequently have received non-compliant letters. Following discussions with the FCA 6,687 letters were sent to policy holders who had received the wrong letter and had renewed their POMS travel insurance policy. Following the issue of these further letters, there had been minimal customer response and POMS believes that the issue is closed with the regulator.

2.8   Key projects:

(a)   **GDPR** – the project is being led by POL. The POMS ARC has requested an update on GDPR progress at its December meeting, with a further more comprehensive update at its first meeting in 2018. The POMS Board notes the importance of successfully implementing GDPR against tight timescales. In particular it notes the importance of maximising access to data across POL and POMS in order to deliver the POMS strategy.

(b)   **IDD** – delivery is tight; the legislation comes into effect in February 2018, and POMS must be able to demonstrate compliance within 12 months.

(c)   **Vulnerable Customers** –POMS is developing a vulnerable customer policy consistent with FCA expectations and aligned with the POL policy. A paper on the approach will be going to the POMS Board in December.

3.   MINUTES OF THE MEETING HELD ON 25th SEPTEMBER 2017, MATTERS ARISING AND ACTIONS LIST

3.1   The minutes of the meeting held on 25th September 2017 were approved as presented and the Chair of the Committee was authorised to sign them as a true record.

3.2   The actions status report was noted as accurate.

4.   **MANAGEMENT OF KEY OPERATIONAL RISKS**

4.1   **Financial Reporting & Control Update**

The Committee received the Financial Reporting Controls Report and AC took questions on the report. The Committee asked to AC to explain Appendix 2 to the Report ("EY control findings with assigned owners and deadlines") and in particular his level of confidence that the remediation activity would be undertaken by the specified dates. AC confirmed that he was confident delivery was on track.

4.2   **Financial Services Conduct**

The Committee noted the report and in particular, that although there was a red rating for mystery shopping results, BoI was comfortable with the remediation plan.
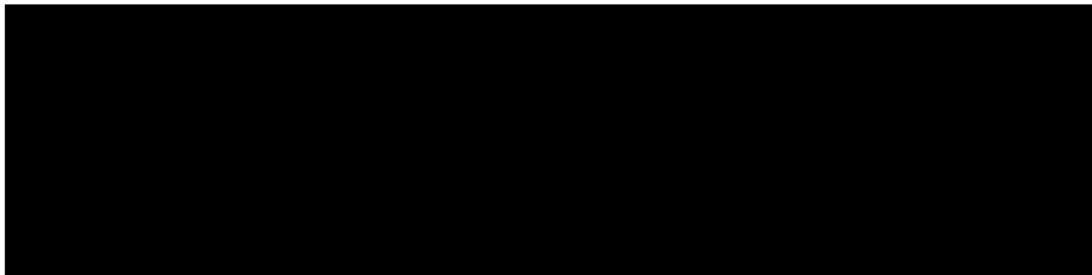
4.3   **Change**

The Committee noted the report and the following points were discussed:

(a)   AC reported that starting in the next financial year quarterly reports would be submitted to UKGI which would include updates on implementation of change activity. As a result, management and Board oversight of change was being reviewed and strengthened. **A pilot report would be submitted to the January Board and this should assist in aligning with management reporting.**   **AC/ RH**

(b)   The Committee challenged the governance of 'Change' projects and queried how management ensured that the change portfolio was properly prioritised; the Committee was also concerned that there seemed to be a significant number of projects where delivery had been delayed.   AC responded that the portfolio management team was being strengthened and work was underway to ensure more effective prioritisation and greater certainty around delivery and benefit realisation.

(c)   The Chair asked if there were effective reporting and management tools with controls in place. AC responded that there are reporting tools and controls however these are not operating effectively, and he was concerned about slippage across all programmes. In particular, management needed to reinforce the requirement that issues should be flagged as they arose, even if at that time appropriate remediation plans had not been developed. but this has been flagged. **The Committee asked for a further update on 'Change' implementation to be brought back to the ARC in January.**   **RH**

(d)   **The Committee also requested that a 'lessons learned' be undertaken regarding SuccessFactors and for the project sponsor to report these back to the Committee.**   **MK**

(e)   AC noted that the back office transformation was still ongoing and was complicated by the fact that Post Office was dependent on out of date applications and systems and the migration of these to current versions was proving more challenging than originally contemplated. The Committee

queried what level of confidence it should have in the target dates for completion as the report shows it moving to November.

4.4 Financial Crime

██

JM/ SS

4.5 & Business Continuity Planning and IT Disaster Recovery
4.6

Tim Armit ('TA'), Rob Houghton ('RH') and Mick Mitchell ('MM') joined the meeting as both agenda items would be covered together.

(a) TA reported that in the previous two weeks there had been a significant number of material incidents including 3 DDOS attacks, AEI failure and issues with the POCA contact centre being overwhelmed with high call volumes. He noted that the Business Protection Team (BPT) had worked well and addressed the issues quickly, and that the communication process had worked effectively. PV noted that communications and information had worked well and was a good test of how we can cope in these situations.

(b) RH provided more details around the three IT related issues:

DDOS Attacks

(i) These attacks were industrialised robotic attacks to the postoffice.co.uk site. Security responses had been increased after each attack and the Government cyber-security team had been informed. Work was underway to determine if there was any rationale as to why Post Office was identified, however he noted that such attacks were becoming more common across industry. **KM asked if we have discussed this with RMG to see whether they had been experiencing similar attacks. RH said he would follow up on this**. The Chair asked if there was anything else needed to assist the IT function to address the issues? RH responded that he was in discussions with Verizon to determine whether further protection was available.

RH

AEI Failure

(ii) Gemalto (who provide the software for AEI machines) had released a regular security patch that had inadvertently prevented access to 115 biometric verification booths. The resulting issue could then only be resolved through manual visits, and there were only 16 qualified engineers that could provide this service. RH explained that this was a control failure on Gemalto's part as they should have tested the patch before releasing on the AEI machines. PV has written to their CEO as this is high profile government work with customer critical

SLAs. RH will be looking at the contractual breach and reassurances that further planned patches will be properly tested. The current contract is not due for renewal till 2020 and we will consider what remedies are available to us. **The Committee requested an update on what contractual remedies are available**.

RH/JM

Contact Centre Issues

(iii)   Due to a letter sent out to POCA customers in accordance with regulatory requirements under the Payment Services Directive, the customer contact centre was inundated with so many calls that it was unable to cope with call volumes for more than a week. It has highlighted that we could not cope with the number of calls on one platform and are now running on BT and Horizon platforms as a contingency. RH summed up that there were two major learning points:

- Capacity forecasting and design to address unexpected volumes; and
- Recovery planning, as in this case it took too long and there were no contingency plans.

The Committee asked if they could be given comfort that the PO would not be left vulnerable during the holiday season. MM noted that there was a change freeze from 23rd November in place and IT management team are focusing on cover during the peak holiday season. KM emphasised that this should include assurances from suppliers that they are also able to support over the peak periods.

RH

(c)   The Committee commented that they had not had an update on remediation activity in relation to the joiners/ leavers process and that this remained an unacceptable risk. RH clarified that a comprehensive solution required both IT and business processes in order to work effectively. From an IT perspective he is now confident that if IT are told of a new leaver, then accounts will be de-activated and access will be promptly removed. Further, if an account was inactive for 40 days then it would be automatically suspended. RH noted that a manual reconciliation was undertaken on a weekly basis. KM noted his concerns over this and asked for next steps, actions, responsibility and business ownership. **PV noted that a separate paper on this would be provided for the next meeting. The Chair requested that the CEO oversee the corrective actions required to resolve the issues and embed the changes over the next 90 days. RH and TA should carry out spot checks every quarter and that business owners need to take responsibility here for this ongoing cycle**

PV/ JM

RH/ TA

(d)   In relation to implementation of the actions arising from the Deloitte security audit, progress had been made against all actions including encryption and procurement of the SOC, however further work remained. MM noted that a supplier for the SOC had been identified and the contract was being finalised. RH noted that it was important to get the contract right, and that once in place implementation could begin.

(e)   TA noted that the Chesterfield recovery solution with Sungard is in place and has been tested and although functional, is clunky and slow. Further

testing will be undertaken in early 2018 to ensure these issues are addressed. **The ARC asked to be kept informed of progress.**   **TA**

TA left the meeting.

4.7   **IT Control Update**

The Committee noted the report.

5.   **INFORMATION SECURITY**

5.1   **Deep Dive on Information Security**

Jules Harris joined the meeting. The Committee noted the report.

5.2   **Information Security and IT Security Policies Review**

JH noted that the Committee was requested to approve two policies:

* Acceptable Use Policy Cyber and
* Information Security Policy.

JH reported that these policies had been reviewed by the R&CC in November 2017 and were required to be reviewed annually. Both polices have been rewritten in the new template format and further work to communicate the policies is underway. JM added that there will be a wider communication piece to be rolled out with a range of different types of tools with the focus on information rather than IT. The Chair asked at what point would we be able to form a view that the cultural aspects had been embedded and were working, and whether this could be reviewed by Internal Audit? JA noted that IA are validating actions but should be able to provide a view following implementation of the final actions which are targeted for June. **The Chair asked for an update in March. PV noted a**   **JH** **further update should be provided for the ARC in January ahead of the Internal Audit review in June.**

5.3   JH requested the Committee to approve the two policies. **The Chair requested**   **JH** **that the definitions should be reviewed and checked to ensure they were consistent across both polices.** The Committee asked what would be the consequence to non-compliance of these two policies. In response to this ███████ █████████████ It was **resolved** that the two policies were approved by the Committee.

JH, MM, RH left the meeting.

6.   **RISK UPDATE**

The Committee noted the report.

7.   **INTERNAL AUDIT**

7.1   JA presented his report and provided the following highlights:

(a)   The internal audit plan has not changed however some changes will be made to the change assurance around certain projects: in particular paragraph 9 of his report shows the table of planned audits and reason for change, which included 2 additional reviews on back office transformation, 1 clarification on

the POLSAP project, and 1 postponed review relating to the effectiveness of the gating process as this needs to be reviewed in light of the proposed changes to Change Management. He also noted that 2 placeholders had been included for Project Panther and Customer Hub.

(b) JA stated that independent reviews would be undertaken on SucessFactors in two phases.

- Phase 1 – to review if there are any residual risks to 'go live' and
- Phase 2 – Deep dive into lessons learned.

AC noted that this had been discussed at the GE and that management supported this phasing. The Chair asked JA if he had sufficient resources to undertake the various reviews that had been identified. JA noted that a team member had recently given notice to resigned and JA had started the recruitment process for a replacement, but overall was comfortable with resourcing through access under the Co-source arrangements with Deloitte and PwC.

The Committee **approved** the changes to the Audit plan.

8. FINANCIAL REPORTING AND DISCLOSURE

8.1 <u>External Audit Plan</u>

Peter McIver and Claire Johnson presented their Audit Planning report and highlighted the following:

(a) The overview of their 2018 audit strategy would focus primarily on the following areas of risk:

- Improper revenue recognition
- Classification of capital and investment items
- Impairment of goodwill and long-lived items
- Capitalisation and disposal of fixed assets
- Valuation of the provision for Postmaster compensation
- Risk of management over-rides
- Pension valuation and disclosure
- Legal claims, including the Postmaster litigation
- Calculations of Network cash, and
- VAT accounting.

(b) It was noted that materiality was based on revenue rather than on the profit/loss impact and was therefore set again at £9.27m (1% of annualised revenue), performance materiality was £4.63m and audit differences of £463k. The Committee were asked to authorise the materiality levels and this was confirmed.

(c) PM had had a meeting with Michael Passmore's team to discuss the level of transformation that had taken place and to determine whether the systems were ready for testing.

(d) The EY team remains unchanged apart the addition of a new senior audit manager.

(e)   PM noted that the next report would be in March. The Committee requested that where possible, the audit work should be undertaken as promptly as possible to relieve pressure on the team at year end.   PM noted that a discussion was still required on the proposed audit fees.

8.2   Management Letter

The Committee **noted** the Management letter provided by EY.

9.   TAX UPDATE

9.1   Mark Dixon joined the meeting and presented the tax update and strategy paper. He informed the Committee that following the Finance Act 2016 companies are required to publish their tax strategy on their website so it is freely available to the public. Post Office Limited is required to publish its tax strategy by no later than 31 March 2018, and HMRC had issued guidelines to assist business comply with this new requirement. The Committee asked if any other companies had already published their tax strategy. MD noted that Post Office had engaged Grant Thornton to advise on this, however there were relatively few companies which have, as yet, made their tax strategies public, however we are monitoring the position.

The Committee **approved** the proposed Tax Strategy and **noted** the Tax Update.

10.   ANY OTHER BUSINESS

10.1   The Chair noted that she would provide an update of the Committee's business to the POL Board which was meeting later in the day.

10.2   There being no further business the Chairman declared the meeting closed at 13:30pm.

GRO

....

Chair

........29/01/2018........

Date