POL00423466

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

MINUTES OF A MEETING OF THE AUDIT AND RISK COMMITTEE OF POST OFFICE LIMITED HELD ON MONDAY 29 JULY 2019 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 14.30 PM

Present:	Carla Stent	Chair **(CS)**
	Tim Franklin	Non-Executive Director **(TF)**
	Tom Cooper	Non-Executive Director **(TC)**
	Ken McCall	Senior Independent Director **(KM)**
In Attendance:	Alisdair Cameron	Interim CEO **(AC)**
	Tim Parker	Chairman, PO Limited **(TP)**
	Andrew Paynter	Group Audit Partner, PwC **(AP)**
	Lucy Mason	Group Audit Senior Manager, PwC **(LM)**
	Ben Foat	General Counsel **(BF)**
	Charlotte Webster	Internal Audit Manager **(CW)** deputising for Johann Appel
	Jenny Ellwood	Risk Director **(JE)**
	Jonathan Hill	Compliance Director **(JH)**
	David Parry	Senior Assistant Company Secretary **(DP)**
	Rob Houghton	Group Chief Information Officer (item 4)
	Mark Fabes	Interim Group CIO (MF) (item 4.1)
	Phey Rasulian	Programme Manager Payment Services, Retail (PR) (item 4.1)
	Tony Jowett	Chief Information Security Officer (item 4.2)
	Ben Cooke	CIO Back Office (items 7, 8)
	Tim Armit	Business Continuity Manager (items 8, 9)

Apologies:

Action

1. Welcome and Conflicts of Interest

The Directors declared that they had no new 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. Update from Subsidiaries

TF provided an overview of the key issues discussed at recent Post Office Insurance (POI) Audit and Risk Committee meeting of 18 July:

- POI Accounts for the year end 2018/19 are being finalised pending a small number of outstanding audit deliverables. There are no items of concern and POI Board is expected to approve these by 31 July 2019.
- The auditors have flagged a recurring issue of ineffective controls regarding the removal of leavers from IT systems. Further work on control remediation is required to ensure this is managed more effectively going forward.
- POI Board has re-approved the appointment of PwC as External Auditors.
- Good progress has been made closing Internal Audit actions within period.
- Updates from Sally Smith on Anti-Money Laundering, Anti-Bribery and Corruption, Countering Financing on Terrorism and Whistleblowing were received. It was agreed POL ARC would receive an overview of the annual POI MLRO report.
- A deep-dive on Complaints was received looking at data, identifying emerging trends and reviewing the effectiveness of current policies/processes.
- The quality of branch sales and disappointing mystery shopping results remain a concern.
- ERV has now been successfully established as underwriter replacing TIF.

POL00423466

- Brexit remains a key risk with a 'hard' exit on 31 October 2019 now a significant risk. Existing mitigation plans are in place and will be refreshed for review in September.

3. Minutes and Matters Arising

3.1 The minutes of the meeting of the Audit and Risk Committee held on 29th May 2019 were **APPROVED** and **AUTHORISED** for signature by the Chairman.

3.2 Progress with the completion of actions as shown on the action log was **NOTED**.

3.3 The draft minutes of the Risk and Compliance Committee held on 4 July 2019 was **NOTED**.

4. PCI-DSS Update and Cyber Security Update

4.1 **PCI DSS**

The paper was taken as read.

PR and MF presented an update on current status.

Following senior level talks held in June with Ingencio, engagement had now been brought forward by one month and workshops to review the detailed design and to refine the delivery plan were underway. A high level plan expected at the end of next week would be circulated to the Committee. **Action: MF/PR**

MF remarked that the team was investigating the possibility of alternative solutions to manage both retail and banking transactions under one single solution. Unlike banks, POL completed both retail and banking transactions which made it unique to the market place. Further, Ingencio had limited experience when dealing with banking transactions.

KM sought and received confirmation that the level of risk was being managed effectively. The banks received monthly updates on PCI compliance and had been informed that full compliance was expected to be achieved between Q2 – Q4 2020.

Following a query from TC on the processes/products that were not PCI compliant, PR explained that an operating model workstream was analysing these and that a holistic approach had been taken requesting providers modify their processes/products to be compliant.

In terms of the risk to POL not being PCI compliant, TJ advised the biggest risk was reputational, however he believed POL's security was effective against attack and that the team was vigilant to any threats.

The Committee requested the project be kept on track to avoid further delay.

4.2 **Cyber Security**

The paper was taken as read.

TJ noted the recent regulator fines for data protection breaches in the UK and America, and stated that the team was proactively assessing whether any lessons could be learnt. A cyber threat intelligence provider (Recorded Futures) had been on-boarded which ensured closer liaison with the National Cyber Security Centre.

Good progress had been made to implement the recommendations from Deloitte's audit on IT and Cyber security, however implementation of RSA Archer for the Security Operation enhancements (SOC) was behind schedule due to internal organisational changes. The team was still aiming to complete implementation of RSA Archer by January 2020 and Deloitte's recommendations by March 2020.

POL00423466

Security reviews have commenced with third party suppliers to ensure that suppliers are governing themselves in line with POL's Cyber Security policy and standards. KM requested that outstanding questionnaires be followed up with suppliers and that a plan be established to deal with third party governance highlighting the key risks to POL.

The Committee discussed and noted TJ's current concerns with third party providers and questioned whether audits of these suppliers should be completed. RH noted an audit of Computacentre had been completed, but that the recommendations had not been tested to date.

Regarding maturity scores against Deloitte's Maturity Review, POL had focused on the categories that had the worst rag ratings and the largest maturity gap. Following a query from TC on how current the data was, TJ explained the maturity scores represented data taken from Deloitte's client base in 2018 and refreshed annually.

RH, PR, TF & TJ left the meeting.

5. Annual Report and Accounts – Audit update and GLO and Starling disclosures

5.1 **Audit**

The paper was taken as read.

AP remarked that the audit was on the last straight with sign off this Thursday (1 August). He was comfortable with the numbers presented and noted the approach regarding the GLO disclosure had been endorsed by PwC Technical Partner – to be treated as a contingent liability.

Talks are still in the early stages and the outcome at present is unknown.

5.2 **Starling disclosure**

[redacted]

5.3 **GLO disclosure**

Regarding the GLO disclosure, BF explained this claim related to 555 claims being heard against POL currently over a series of at least four trials.

AC commented that in view of the judgement from the common issues trial (the first trial), POL's new strategy was to consider alternative dispute resolution through mediation. This meant that an economic outflow within this financial year was possible, however, a sensible number could not be provided because:

- POL was unaware of the claimants expectations for settlement or whether they are prepared to settle; and

POL00423466

- the claim valuation is unreliable.

KM questioned whether POL could have foreseen this happening and questioned whether it was sensible not to include a set of costs.

The Committee noted that the reasonableness test had been passed and that under IAS 37, a provision should only be made when the following criteria had been met:

a. an entity has a present obligation (legal or constructive) as a result of a past event;
b. it is probable that an outflow of resources embodying economic benefits will be required to settle the obligation; **and**
c. a reliable estimate can be made of the amount of the obligation.

However, POL had:

a. no present obligation;
b. a probable outflow but no reasonable assumption could be provided; **and**
c. ~~a robust defence~~ a reliable estimate cannot be made.

Carla Stent

AP remarked that whilst the regulator could question why provision had not been made, he recognised that POL was unaware of the claimant's expectations for settlement and that mediation was under consideration.

The Committee discussed whether it would be appropriate to include a statement on the Criminal Cases Review Commission (CCRC) cases within the disclosure. In view of making a full and transparent disclosure and of being true and fair, the Committee **AGREED** that a separate sentence should be included within the GLO disclosure. **Action: BF**

The Committee noted the disclosure.

Following a discussion of the disclosures and audit progress made, the Committee **RECOMMENDED** that the Annual Report and Accounts for 2018/19 be submitted to the POL Board for approval.

It was noted the GLO and Starling disclosures would be discussed in further detail at the next POL Board meeting.

The Chair thanked the auditors and the financial team for all their hard work.

6. Consolidated Report from Risk, Compliance and Internal Audit departments

6.1 **Risk**

The report was taken as read.

JE presented an update on POL's current risk profile.

She remarked that there had been no significant change to POL's risk profile with continued focus on Litigation, Change Portfolio, PCI-Compliance, Brexit and Key personnel changes all remaining 'red'.

GLO Litigation

The findings/outcomes from the second trial are expected in early September. Deloitte are assisting the team with workshops to record risks, mitigations and to allocate owners.

Change Portfolio

POL00423466

TC noted that there are a number of projects that would assist with GDPR compliance and remarked that contract remediation was a large job to undertake. JH reported that this was currently being reviewed and that a progress report would be discussed at the Risk and Compliance Committee meeting.

Privacy and Electronic Communications Regulations notifications

CS sought further information on the two Privacy and Electronic Communications Regulations notifications. JH remarked these were as a result of error in the Telecoms centre. Training had been reviewed and refreshed, however he assured the Committee this was not a systematic issue.

Fit & Proper

The team remained focused on gathering agent returns and data was shared with HMRC on fortnightly basis to evidence progress. It was noted the regulator had agreed to extend the deadline until September. Returns from four commercial partners remained outstanding along with 1162 outstanding responses from non-commercial partners.

Despite repeated warnings to commercial partners and agents, the Committee sought and received assurance that a strong stance would be taken to switch off Partners/Agents Travel Money and MoneyGram services on 30 August 2019 should their returns not be completed by 23 August 2019.

Compliance with Money Laundering Regulations
TC noted the large number of Bureau de Change non-conformance cases (66 identified between 24 April and 19 June 2019) where customers had purchased in excess of €15k in 90 days and sought to understand who the culprits were.

JH replied that this was under investigation but that this information could not be divulged for confidentiality reasons.

Mystery Shopping
TF sought and received confirmation that mystery shoppers do not identify what was said by agents in their reports. Results have declined since April which JC explained could be attributed to the re-structure and re-focus of the Area Manager teams, with less time given towards supporting client relationship managers who were on the front line.

The Committee noted and discussed the decline in mystery shopping standards and requested that Amanda Jones be invited to discuss the FS quality of sales in the network at the next ARC meeting in September.

Further, it was felt that senior level staff should be held more accountable for declining standards.

5th Money Laundering Directive
JC advised that the 5th Money Laundering Directive would be adopted in the UK coming into force in January 2020. The directive set about tighter regulations regarding money laundering, due diligence and ownership and control of companies and a requirement to list politically exposed persons.

POL00423466

The Change portfolio remains at 'Amber' and a new transformation director has been appointed to expedite the change process as it is apparent that some changes are not at the required/expected level of change.

PCI Compliance

PCI continues to report as 'Red' with no significant progress being made since last year.

Brexit

Dialogue continues on a fortnightly basis with BEIS regarding a 'No Deal' Brexit on 31 October 2019. Remediation work on a 'No Deal' is ongoing particularly POL's engagement with third parties who are yet to respond to POL's questionnaire. However it was noted that all key partners have been contacted and services will remain the same.

JE remarked the Operations Working Group would be re-established to review the original contingency plans and to agree any new actions. Consideration was being given to IT and Marketing releases and to cash supply and distribution. Overtime will be sanctioned to ensure cash centres can manage any upsurge.

Branches would be closed should there be any security issues and electricity supply to Northern Ireland branches would be provided by companies from both Northern Ireland and the Republic.

KM sought and received confirmation that JE had been liaising with industry contacts and AC noted the possibility of civil unrest in October.

Key personnel changes

In view of key personnel changes at senior positions, the review and assessment of the capability of senior positions continued, along with a review of career progression to understand current and future requirements for talent development.

Payzone

Remediation work following the Payzone penetration testing remains ongoing and is on track, with all security vulnerabilities expected to be resolved by October. A Payzone risk workshop is planned for 30 July 2019 to help develop Payzone's risk management framework and governance.

TF commented that it would be useful to understand the levels of engagement POL had with Deloitte and PwC, and to confirm whether there were any conflicts of interest or Chinese walls to be aware of.

6.2 Compliance

The report was taken as read.

JH highlighted the following key compliance issues:

Text Relay
Ofcom had requested further information to evidence when senior managers were informed of non-compliance, which the team was collating. He believed the regulator was becoming more stringent than before, and a provision of £200k had been set aside to cover a potential fine.

GDPR
The GDPR project was formally closed at the end of Q1 and compulsory data protection training had gone live for all employees.

POL00423466

6.3 Internal Audit

The report was taken as read.

CW, deputising for Johann Appel, was welcomed to the meeting.

She reported that eight reviews had been finalised since the last ARC meeting and good progress had been made with the 2019/20 Internal Audit plan. 24 of the 26 audits for 2018/19 had been completed with the two outstanding audits on assurance being included under the change audit in the 2019/20 plan.

The Committee discussed and noted the recurring key themes and root causes of audit actions reported in 2018.2019. These included change delivery, control activities, information & communication and risk assessment.

KM noted that the average time to clear internal audit report was still higher than the agreed target. AC provided assurance that governance and turnaround had improved with formal closure meetings for each audit with the GE sponsor and management executive and a clear escalation process to prevent significant delay. The Committee acknowledged that standards had improved.

TC requested the Payzone Master Services Agreement be completed to avoid any future risks.

7. Transtrack

The paper was taken as read.

BC and TA entered the meeting.

BC presented an update on Transtrack.

He advised that Transtrack was a Dutch company who provided POL with software support for cash logistics and process operations. There had been a number of issues over the last 6 years of service including reconciliation discrepancies between Transtrack's software (CWC) and POL's financial system, and issues surrounding personnel capability at Transtrack.

He noted that the Auditors had accepted the Transtrack reconciliation gaps following evidence that showed the introduction of work arounds/financial controls had helped to reduce the gaps. Additionally, Transtrack had introduced a working improvement plan that included a ring-fenced team to provide adequate airtime to deal with POL issues.

The Committee questioned whether alternative providers should be considered in view of the fact that cash was central to POL's business and the large amount of time and resource that had been allocated to rectify reconciliation issues.

8. Belfast Data Centre Disaster Recovery testing

The paper was taken as read.

BC explained the centre (operated by Fujitsu) hosted POL's Horizon, counter trading application and other business critical applications and that resilience had not been tested since 2013.

The team planned to carry out a test exercise over the August Bank holiday weekend when trading was significantly lower than usual trading days, whilst noting that the bank holiday Monday is a normal trading day in Scotland.

POL00423466

He advised the primary system would be switched off on Saturday evening to the back-up system, so Sunday trading would be on the back-up system. On Sunday evening, the team would revert to the primary system ready for Monday trading in Scotland.

The team was technically confident the exercise would be a success and remarked that a workshop had been recently held to run through the risks and mitigating actions.

TA remarked that there is little contingent processes in place to manage a full loss of Horizon. Whilst there was no optimum time in which to test the centre's resilience, the team recognised the close proximity to the publication of the judgements from the second trial and the reputational risk to POL of the Horizon system not working.

The Committee wished the team good luck.

BC left the meeting.

9. Business Continuity Update and Policy

9.1 The paper was taken as read.

TA advised that business continuity was now established in POL and had moved from development to business as usual and was pleased with the progress made to date.

A system had been implemented to communicate to all branches when Horizon failed and Business Continuity recovery strategies are now in place and tested for all locations. Resilience in building design is being improved across all key locations and regular evacuation testing takes place across all sites.

KM noted the improved changes but advised that he was alarmed with the volume of red rag ratings in the risk appetite paper which suggested a live risk.

TA assured the Committee this was not the case and that many of the red items were only red because 3rd party plans had not yet been evidenced and validated. Action plans including mitigating actions and deadline dates would be included in the risk appetite to allay any fears. **To do: TA**

TA left the meeting.

9.2 Business Continuity Policy

The ARC **APPROVED** the Business Continuity Policy.

10. Change Update

The Chair advised the paper would be removed from the agenda to be reviewed at a later date. The paper had not been discussed at the Risk and Compliance Committee meeting.

11. GDPR

The paper was taken as read.

JH explained the programme was formally closed at the end of Q1 with controls established to ensure the POL was operationally compliant.

Further work is required on contract remediation, records retention, data classification and data storage to enhance POL's ability to evidence that effective compliance has been achieved. Additionally, a 'Privacy forum' is being proposed to meet quarterly to support the business manage data compliantly with oversight provided by the data protection team.

Action:

POL00423466

CS queried the number of "right to be forgotten" requests. JH advised he would investigate this and revert accordingly. **JH**

It was agreed that GDPR would be reported on a 6 monthly cycle until further notice.

12. AOB

The following policies were reviewed by the Committee:

- **Modern Slavery Statement** – it was agreed the statement should be re-reviewed at a later date as it was unclear whether progress had been made. The Committee required examples of what had been completed at a practical level to provide assurance that the actions had been completed.
- **Anti-Bribery and Corruption Update and Policy** – the Committee noted the update and **APPROVED** the policy.
- **Whistleblowing Policy** - the Committee noted the update and **APPROVED** the policy.

There being no further business, the meeting closed.

Carla Stent ..... 23/09/19.....

Chairman **Date**

Actions from meeting

Minute	Action	Lead	Due Date
4.1	**PCI-DSS** – circulate high level plan to the ARC following Ingencio workshops on detailed design and the refined delivery plan.	MF/PR	ASAP
5.3	**ARA 2018/2019** – to include a sentence/comment on the Criminal Cases Review Commission cases in the GLO disclosure.	BF	ASAP
11	**GDPR** – to confirm the number of "right to be forgotten" requests.	BF	Sept

POL00423466