POL00423505

1

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 28 JANUARY 2020 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 09.30 AM

Present:	Carla Stent	Chair **(CS)**
	Tom Cooper	Non-Executive Director **(TC)**
	Ken McCall	Senior Independent Director **(KM)**
	Zarin Patel	Non-Executive Director **(ZP)**
In Attendance:	Nick Read	Chief Executive Officer **(AC)**
	Alisdair Cameron	Chief Finance Officer **(AC)**
	Andrew Paynter	Group Audit Partner, PwC **(AP)**
	Sarah Allen	Audit Senior Manager, PwC **(SA)**
	Ben Foat	General Counsel **(BF)**
	Johann Appel	Head of Internal Audit **(JA)**
	Mark Baldock	Head of Risk **(MB)**
	Jonathan Hill	Compliance Director **(JH)**
	David Parry	Senior Assistant Company Secretary **(DP)**
	Jeff Smyth	Digital Technology Director, CIO FST & Identity **(JS)** (Item 4)
	Rob Wilkins	Portfolio Director **(RW)** (Item 4)
	Tony Jowett	Chief Information Security Officer **(TJ)** (item 4)
	Andrew Goddard	Managing Director, Payzone **(AG)** (Item 5)
	Mark Dixon	Head of Treasury, Tax & Insurance **(MD)** (items 6,7)
	Dan Zinner	Chief Transformation Officer **(DZ)** (item 8)
	Sally Smith	Money Laundering Report Officer and Head of Financial Crime **(SS)** (Item 9)
	Tim Armit	Business Continuity Manager **(TA)** (Item 10)
	Meredith Sharples	Director, Telecoms **(MS)** (Item 11.16 – 11.19)
Observers:	Rebecca Barker	Head of IT & Digital Risk **(RB)**
	Audrey Cahill	Risk Business Partner, Central Risk **(AuC)**
Apologies:		

Action

1. Welcome and Conflicts of Interest

1.1 The Chair welcomed ZP and MB to their first Committee meeting along with observers RB and AuC. All papers were taken as read.

1.2 ZP declared the following conflicts of interest:

- As a member of the HM Treasury Committee, ZP does not see the detail of any funding request, but the Committee agreed to note her role in both HM Treasury and POL and to ensure that should any sensitive matter arise, her papers would be redacted and ZP would be excused from the discussions, as required.

1.3 The remaining 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

POL00423505

The Chair provided a quick overview of the key issues discussed at the last ARC POI meeting in November 2019, based on discussions with the POI ARC Chair:

- Quality of Sales – there have been some improvements made but simple issues remain such as not discussing the wider product range or asking suitable questions. Training and the use of technology is key to this.
- Data breach – a marketing agency was inadvertently sent data files of 104 customers without encryption. Culture and training to raise staff awareness is required, pending an automated solution which requires Windows 10.
- The Senior Manager and Certification regime is now effective and has been implemented on time and under budget.
- GI pricing remains an area of regulator focus, in terms of the difficulty customers face when switching providers and instances of higher premiums being charged to loyal customers who do not negotiate or switch providers.

A fuller update would be provided in March to cover POI ARC's February and March meetings.

3. Minutes and Matters Arising

3.1 The minutes of the meeting of the Audit and Risk Committee held on 25 November 2019 were **APPROVED** and **AUTHORISED** for signature by the Chairman.

3.2 The minutes of the closed session of the Audit and Risk Committee held on 25 November2019 were **APPROVED** and **AUTHORISED** for signature by the Chairman.

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

3.4 The draft minutes of the Risk and Compliance Committee held on 14 January 2020 were **NOTED**.

4. PCI-DSS and Cyber Security Update

4.1 *PCI-DSS*

JS presented a verbal update on PCI-DSS. Following CEO level talks with Ingenico in December 2019, an executable and granular level plan had now been received (27 January 2020) and a steering committee (attended by NR and Ingenico) established to maintain visibility and track progress.

4.2 Compliance with the legislation was now expected in Q2 2021, six months behind the previously advised deadline. Martin Kearsley (Director of Banking Services) will use this additional time to converse with POL's banking partners (between August and December 2020). To date, the banking partners appear supportive.

4.3 NR remarked he would prefer compliance to be completed by December 2020, but consideration needs to be given to the busy trading period before Christmas. The Committee urged the management team to press for compliance pre-Christmas, even if roll out was delayed until after the **Action: NR**

Christmas trading period. NR did feel more assured with the joint effort/approach to compliance.

4.4 JS confirmed the first technical delivery would be in March 2020 and the first retail deliverable would be received in August 2020. POL's dependence upon Ingenico and Fujitsu was noted. It was **AGREED** monthly progress reports (signed by Ingenico's CEO) would be provided to the Committee. **Action: JS**

4.5 The Committee reiterated their concern that Ingenico must be held accountable, and that non delivery in August (or news of a further delay) would be unacceptable. TC purported financial penalties should be levied where compliance is not met by the proposed deadline.

4.6 A progress report would be presented to the Committee in March. **Action: JS**

4.7 *Cyber Security*

TJ presented an update on Cyber Security. Following the Travelex ransomware attack, focus had been on reviewing and strengthening cyber defences where required (considered suitable at present). A verbal update had also been received from FRES that their systems are suitable. A more formal confirmation is due in two weeks. Following a question from the Committee, it was confirmed that POI is included in the POL work, but Payzone have yet to be tested.

4.8 Regarding JML (joiners, movers, leavers), TJ had a good understanding of the processes involved and a plan would be rolled out in March to ensure accessibility rights was continually managed. Currently there is good basic coverage but some slippage occurs. There are currently 90 contractors in POL, 235 at its peak in October 2018. A full plan on JML will be shared with the ARC at the next meeting. **Action: TJ**

4.9 Regarding data security, the biggest risk to POL remained internal breaches. Attacks via tower providers to POL were unlikely as there are no direct connections from tower companies to Horizon, however, a cultural change is required regarding the usage of and respect for confidential data (with proportionate consequences for non-compliance).

5. Payzone Risk Report

5.1 AG provided a progress report on risk within Payzone.

5.2 The team continued to develop their risk management framework to align with POL's, and an assessment of all key risks (GDPR, integration of POL policies, Brexit, terminal communication issues, risk forecast revenues) had been completed with plans in place to resolve these issues by the end of FY 2019/20.

5.3 Regarding the terminal communication issue, TC queried whether the quick turnaround and limited testing could have been handled more effectively, and whether there are any lessons that can be learnt to use for on-boarding future energy providers.

5.4 AC advised testing had been compressed into a short period following lengthy negotiations leaving little time before launch. (POL had been

required to meet a commercial deadline.) In future additional resource would be provided to speed up negotiations.

5.5 KM believed POL should take a firmer negotiation stance and to pushback on unrealistic deadlines. NR acknowledged that a dedicated field team could be introduced to improve engagement, however British Gas was satisfied with the programme to date, especially as POL had demonstrated adaptability and negative social media coverage had been limited.

5.6 AG noted a number of other energy providers were in the pipeline to use Payzone services.

5.7 The Chair noted that Payzone had been added to POL's risk management framework and commented on the good progress made.

6. Tax Update and Annual Tax Strategy

6.1 MD presented the annual tax update and provided a brief overview of issues arising in the three main tax areas. The primary risk remains VAT, particularly paying and claiming the correct amount. The following minor issues were discussed in relation to Employment Taxes:

6.2
- Dualists – a number of senior employees (now no longer with POL) had been appointed and were subsequently deemed to have more than one permanent place of work. HMRC and staff members involved have been informed and settlement for 2018/2019 has been made through the annual paye settlement agreement (PSA). The impact on earlier years is being evaluated.
- IR35 – there has been increased focus on new legislation to assess whether a contractor should be included on the POL payroll or whether they could be invoiced as a 3rd party as a result of the imminent implementation in the private sector. HMRC has updated its assessment tool. POL has revisited earlier evaluations and concluded that certain classifications may have been erroneous. POL was working with Deloitte to understand the implications. AP advised that a client of his (a recruiting firm) was now providing this service.
- Payzone – integrating Payzone into the VAT group. AP confirmed that he was comfortable with the Payzone tax strategy and held quarterly meetings with their finance team.

6.3 AC noted POL sought to be as transparent as possible with HMRC around all its tax matters.

6.4 The Annual Tax Strategy was **APPROVED**.

7. Corporate Insurance Renewal

7.1 The Committee **RATIFIED** their email approval of 2 December 2019, where approval was sought to the increase the spend from IRRELEVANT to IRRELEVANT

8. Strategic Portfolio Office Change Control Environment Update

8.1 DZ presented an update on transformation. Progress was mixed in his opinion, with improved governance controls particularly around spend, project reporting and the quality of challenge. However, accountability, communication, understanding the need for change, and desire/wish to change required improvement.

8.2 He believed the project portfolio was too large (86 open) and should be shrunk to fewer large projects, with smaller projects moved into day to day business. All projects would need to be reviewed and graded against the strategic purpose (once agreed and defined) taking into consideration any regulatory/legal requirements, with capability/capacity also to be reviewed.

8.3 The Chair thanked DZ for his update and noted the improved controls that had been implemented.

9. Money Laundering Reporting Officer (MLRO) Annual Report

9.1 SS presented the annual MLRO report on the effectiveness of key anti-money laundering and counter terrorist financing controls.

9.2 She reported controls are generally effective but that the following areas require improvement:

- the timely provision and completion of return of Fit and Proper returns;
- ensuring all compliance training is completed;
- the first line of defence being aware of their responsibilities and understanding compliance policies;
- to reduce the number of cash gifts received.

9.3 A more proactive approach to supervision, with increased scrutiny and focus on money laundering and terrorist financing, was being taken by the regulator. The team size and workloads had increased since the prior year. HMRC registration fees had increased from IRRELEVANT It was agreed that the ability to recover any of these increases should be discussed as part of the retail offering.

9.4 Following a number of high volume and high profile investigations where money had been laundered through Post Office counters, the team had visited c.50 sites in East London to remind staff of their obligations and the importance of completing suspicious activity reports. SS suggested that to establish an audit trail, cash deposits via Post Office counters should be completed via a chip and pin process, similar to that of making cash withdrawals.

9.5 The Committee agreed with this was a good idea and should be pursued with the banks, noting that this would require investment on their part.

9.6 The Committee recognised that work-loads had increased and suggested that the only way to improve culture was to take a stricter approach towards non-compliance.

9.7 The Chair thanked SS and her team for their work.

10. Business Continuity and Resilience Update

10.1 TA presented the Business Continuity and Resilience Update.

10.2 He considered resilience to be suitable for purpose, but identified the following key risks:

- *Horizon failure* – testing for a total failure has not been completed. It was noted that manual operations would be impossible to complete due to increased regulatory change. Additionally, there are no

instructions for branches should this scenario materialise. Moving to the cloud (Belfast exit) would enable a more automated solution.

- *Retail partner failure* – the sudden loss of a key retail partner had identified that c.80-100 stores would need to re-open within two days to serve POCA and vulnerable customers. A new pop-up, fully functional Post Office - 'Post Office on Wheels'- (tested in December 2019) could alleviate this issue.
- *Telco business* – currently there is no disaster recovery plan in place for the Telco business. The contract does not contain a disaster recovery provision which means that should the data centre be lost, time would be required to source new hardware as well as build an appropriate environment. It was unknown how long this would take or costs involved. It was agreed that the disaster recovery plan will be assessed in the supplier retender.

JA advised that business continuity and disaster recovery was on the Internal Audit agenda.

10.3 A brief discussion was held on the flexible nature of and the positive commercial opportunities the 'Post Office on Wheels' presented to the business.

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

11.1 The Chair invited each presenter to highlight the key matters, taking the reports as read.

11.2 **Risk**

MB presented an update on POL's current risk profile, highlighting the following risks:

11.3 *Coronavirus*

This is a new emerging risk considered by the World Health Organisation as a public health emergency of international concern. There are two known cases in the UK to date, however its spread is being closely monitored by the UK government.

11.4 *Purpose, Strategy, Growth*

NR's new organisational structure is due to be launched on Wednesday (29 January 2020). Consideration will be required for any settling period whilst people understand new roles/objectives etc.

11.5 *Brexit*

Brexit remains a challenge whilst POL understands the full implications to the organisation. Ongoing dialogue with BEIS continues.

11.6 The implementation of RSA Archer (an integrated risk management solution) was progressing well and People Risk would be added to the Risk Register following a request from the Chair.

11.7 **Compliance**

JH noted the following compliance issues:

11.8 *Ofcom Text relay*

POL00423505

The issue (where vulnerable customers had been overcharged for using relay services) has now been closed by Ofcom. An early settlement resulted in a fine of £175k with a summary of findings published on Ofcom's website. There has been limited publicity.

11.9 *Data Protection, use of Cookies*

Updated guidance by the regulator (ICO) clarified the use of management of cookies on websites. POL is now non-compliant against regulation and work is underway to develop solutions for mitigation. It should be noted that all solutions will impact on POL's use of marketing data. The Committee requested this be kept under review. **Action: JH**

11.10 *GDPR*

Progress has been made to close down and remediate non-compliant contracts and the project is due for completion in July 2020. TC requested that the non-compliant contracts and those contracts signed outside of standard governance processes should be reviewed at Board level.

11.11 It was **AGREED** that an update on non-compliant contracts would be presented to ARC every quarter. **Action: DP**

11.12 *Whistleblowing*

It was noted that the contract with the current provider had expired but would be transferred to a new supplier by the end of the financial year. Work was underway to train agents to ensure that whistleblowers were confident that processes would result in their fair treatment.

11.13 **Internal Audit**
JA reported the IA plan was on track. Good progress has been made with four audits of the 2019/20 programme being finalised since the last ARC meeting in November: (PCI Programme (requires significant improvement), Cyber Security follow-up (requires improvement), CFS Controls (requires improvement), Third Party oversight (satisfactory)) and two overdue actions (FS Training and Purchase to Pay).

11.14 The Chair commended the good report.

11.15 **PSD2 Implementation**
MS explained that PSD2 (Payment Services Directive) is an EU directive that came into force in Jan 2016. It is designed to create a more level playing field and an integrated platform for the payments industry in Europe, enabling bank customers to give third party providers access to their data.

11.16 The FCA had previously advised telecoms firms in 2016 that they could either pay a full institution payment or apply for a waiver (exemption licence) so long as customers were not overcharged for using premium rate services (caps exist for premium calls and overall monthly charges). An independent audit would be required for this exemption and the deadline for applying for the waiver was 13 January 2018.

11.17 He noted that POL had received differing legal advice on whether PSD2 applied to the Telco business, but was informed last year (February 2019)

that compliance was required. Work was underway with Fujitsu to find an appropriate solution and POL had recently applied for, and received, a waiver (14 January 2020) with the regulator. Refunds of charges levied in excess of the specified caps would be made to affected customers (currently estimated at IRRELEVANT per annum since 2016).

11.18 The Committee noted the poor position this presented, but recognised the positive actions taken by management and the approval of the waiver by the regulator.

12. Policies for Approval

12.1 The following policy was **APPROVED:**

- Cyber and Information Security Policy.

13. AOB

13.1 AP presented the 2019/20 Audit fees of IRRELEVANT which had been agreed with management (broken down as fee proposal of IRRELEVANT and additional amounts billed of IRRELEVANT).

13.2 He noted the progress made: the GLO settlement had been agreed and that a good discussion with KMPG (auditors to FRES) had been held. He believed their understanding of POL had improved, along with communication lines in terms of knowing who to speak to for information. He also noted that issues with access remained (as had been noted in 4.8 above).

13.3 The Committee questioned and discussed the proposed fee increase, noting the change of scope not previously anticipated during the tender process, as well as the change in the external audit environment following the reviews of the industry.

13.4 The Committee **APPROVED** the Auditor's fees for 2019/20.

13.5 There being no further business, the meeting was closed.

Carla Stent

..... 20/05/2020

Chair 22/05/2020 13:00 **Date**

Actions from meeting

Minute	Action	Lead	Due Date
4.3	**PCI-DSS** The Committee urged the management team to press for compliance pre-Christmas, even if roll out was delayed until after the Christmas trading period. He did feel more assured with the joint effort/approach to compliance.	**NR**	
4.4	**PCI-DSS**	**JS**	

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

	It was **AGREED** monthly progress reports (signed by Ingenico's CEO) would be provided to the Committee.		
4.8	**Cyber Security - Joiners, movers, leavers** Regarding JML (joiners, movers, leavers), TJ had a good understanding of the processes involved and a plan would be rolled out in March to ensure accessibility rights was continually managed. Currently there was a good basic coverage but some slippage occurs. There are currently 90 contractors in POL, 235 at its peak in October 2018**. A full plan on JML will be shared with the ARC at the next meeting.**	**TJ**	**March 2020**
11.9	**Compliance - Data Protection, use of Cookies** Updated guidance by the regulator (ICO) clarified the use of management of cookies on websites. POL is now non-compliant against regulation and work is underway to develop solutions for mitigation. It should be noted that all solutions will impact on POL's use of marketing data. The Committee requested this be kept under review.	**JH**	**Ongoing**
11.11	**GDPR/Contracts Governance** It was **AGREED** that an update on non-compliant contracts would be presented to ARC every quarter.	**DP**	**March 2020**

POL00423505

Voting Results for January Minutes for Signature

The signature vote has been passed. 1 votes are required to pass the vote, of which 0 must be independent.

Vote Response	Count (%)
For	1 (100%)
Against	0 (0%)
Abstained	0 (0%)
Not Cast	0 (0%)

Voter Status

Name	Vote	Voted On
Stent, Carla	For	22/05/2020 13:00