POL00423462

**POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE**
Minutes of a Risk and Compliance ("RCC") meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 4 July 2019 at 13.00 pm

| | | |
|---|---|---|
| **Present:** | Alisdair Cameron (Chair) (AC) | Interim Chief Executive Officer |
| | Chrysanthy Pispinis (CP) (on behalf of Owen Woodley) | Senior Strategy Manager |
| | Ben Foat (BF) | General Counsel |
| | Rob Houghton | Group Chief Information Officer |
| | Mo Kang | Group HR Director |
| | Cathy Mayor (CM) (on behalf of Debbie Smith) | Finance Director, Retail |
| **In Attendance:** | David Parry (DP) | Senior Assistant Company Secretary |
| | Johann Appel (JA) | Head of Internal Audit |
| | Jenny Ellwood (JE) | Risk Director (via telephone) |
| | Jonathan Hill (JH) | Compliance Director |
| | Mark Fabes (MF) | Interim Group CIO (items 1-3) |
| | Tony Jowett (TJ) | Chief Information Security Officer (item 4) |
| | Tim Armit (TA) | Business Continuity Manager (items 4, |
| | Ben Cooke (BC) | IT Director – Back Office (item 5) |
| | Barbara Brannon (BB) | Purchasing Director (item 7) |
| | James Scutt (JS) | Head of Customer Experience, Retail (item 9.3) |

**Apologies** Debbie Smith, Chief Executive Officer, Retail, Owen Woodley, Chief Executive Officer, Financial Services, Telecoms and Identity, Group Marketing and Group Digital & Innovation.

**1. Welcome and Conflicts of Interest** **Actions**

AC opened the meeting and remarked that the pack was too large and should be halved in length. Papers should be condensed to identify the most significant risks and issues faced by the Post Office, the mitigating actions that were being completed and the timeframes for doing so.

**2. Minutes and Action Lists**

The minutes of the RCC meeting held 5 May were **APPROVED.** Progress on completion of actions as shown on the action log were **NOTED.**

**3. PCI-DSS Update**

The paper was taken as read.

RH outlined that there are two types of transactions; retail and banking. Both transactions require pinpad upgrades with the banking transaction requiring a solution that avoids PAN data being brought into the POL environment (called the "banking solution" for ease).

AC sought and received confirmation from RH that no definitive plan had been received from Ingenico regarding the banking solution. A plan for collection, shipment and firmware upgrade and in-branch device swap had been agreed, and a pilot to update the pin-pad devices was scheduled to begin at the end of August, with a full roll-out planned in September on successful completion of the pilot.

POL00423462

It was noted that the pin-pad devices could only be upgraded by trained specialists and not in-house. For the banking solution, resource to commence the design activities had been provided by Vocalink and Fujistu, Ingenico had advised that they could not provide suitable resource until late August/early September.

In order to avoid further delay, AC requested that escalation with the senior executive of Ingenico be accelerated. **RH**

The RCC discussed further the banking solution and the two opportunities to improve POL's PCI compliance status currently being explored. Firstly, to identify whether there were any alternative providers (such as Global Payments) who could process banking transactions reducing POL's reliance on Ingenico, and secondly, to explore whether banking transactions could be excluded from PCI-DSS regulation. RH commented that POL's legal team had engaged with CMS (Solicitors) and the Payment Service Regulator (PSR) to confirm this position, and that feedback was expected by the end of July/early August.

The RCC noted that whilst banks comply with PCI, they are not certified/subject to PCI compliance, whereas merchants are. Additionally, PCI was recognised as a good industry standard to meet, and POL would strive to meet this as business as usual.

The recent Data Audit had now been completed and no further instances of PCI related data had been identified. A full report was expected by the end of July.

AC requested that a condensed paper of two sides be prepared ahead of the next ARC meeting (29 July) clearly communicating the current position.

MF left the meeting.

**4. Security Strategy**

4.1 The paper was taken as read.

TJ and TA entered the meeting.

TJ explained that the purpose of the paper was to provide an update of the current position. In line with best practice and to meet the recommendations of the Deloitte Review, the Cyber Security Team had now been expanded to cover IT Security and Business Continuity Management. Prioritisation had been given to meetings with key third parties to understand and align on security provision.

AC questioned when POL's position could be considered 'Good'. TJ responded that the process of designing 'Good' was in train, and that seven of the ten key recommendations from the Deloitte Review had now been met. Additionally, a number of initiatives throughout the year had identified POL's 'Crown Jewels' i.e. the business critical data/systems, its location and the controls in place to protect this.

CP questioned whether agent related data (such as agent pay) was considered part of the crown jewels. BF believed this should be treated as part of the 'Crown Jewels' and noted that the Secretariat department had good governance controls in place regarding the storage of business critical data such as financial data, litigation material and business reports. A cultural piece was required across POL to ensure that business critical data was treated with a greater sense of security.

He suggested that as a starting point, the team should review the document retention programme listing all corporate documents, owners and the retention period.

AC requested that the term 'Crown Jewel' be more clearly defined. Regarding third party data, this should clearly identify the type of data held/stored, the audit rights and when they can be exercised.

POL00423462

Further, it would be useful for the RCC to see a report that identified:

- What POL does well;
- What is at risk;
- What is POL doing about it i.e. mitigating actions;
- When will it be completed by.

TJ

AC reiterated that further resource could be provided if required and that due to the varying numbers of standards, one clear view should be established. Any issues should be escalated to him.

He requested a crisper report be published for ARC (29 July) identifying the current position.

4.2 **Cyber Risk Appetite**

AC questioned TJ's request to withdraw the Cyber Risk Appetite paper ahead of the meeting.

TJ commented that following discussions he and RH had had with Shirine Khoury-Haq (NED), and later conversations with JE and David Mann (Head of Information Security & Supplier Risk), it was agreed that the current proposal would be reviewed with further consideration given towards data criticality. An additional request was made to simplify the approach particularly around the key risk indicator element.

AC requested that a real world interpretation should be applied to show POL's risk appetite. He recognised that breaches such as hacking did occur and questioned what would happen to any data lost. JH remarked that in such circumstances, a financial penalty would be likely. Further, the regulator (ICO) expected companies to have established risk processes and controls in place.

The RCC discussed the potential of POL being attacked by hackers and felt that although this scenario was quite low, an attack on Horizon could have significant impact on POL. Having assurance from suppliers about the security of POL's data was critical, especially if POL is the data owner/processor.

Of greater concern to the team was the need to modernise the data centre.

AC thanked the team for their honest assessment and frank conversation. He requested that an updated paper be presented at September's RCC meeting and suggested JE and RH review the scores and the language used. Mitigating actions should also be highlighted/in place.

TJ and TA left the meeting.

**5. Transtrack, Back Office Transformation**

The paper was taken as read.

BC entered the meeting.

He explained that whilst Transtrack provided POL's supply chain capability for cash and logistics, he questioned the decision to appoint them in 2016 to manage this process.

The financial reconciliation issue (where not all financial transactions recorded in Transtrack are sent to POL's financial system) remained unresolved, but had significantly improved since Go-live, with the team ensuring that financials were robust enough to avoid any branch impacts.

At its peak, around 29,000 transactions (equivalent to c.£.250m) had been missed and the project team had now reduced this amount to c.20 missed transactions a day. The bulk of the missing historical transactions had also been processed.

POL00423462

A number of financial controls had been established to prevent further repeated occurrences which had also helped identify any technical issues requiring remediation before they arose. Further, Transtrack had strengthened their team in areas of weakness however it was noted that significant manual overhead was required by POL to ensure that there no impact is felt by the Post Masters or the financials.

Regarding Back Office Transformation, operational noise remained in place and any issues identified regarding Transtrack application architecture, development capacity, deployment approach and skills was circulated to the GE on a weekly basis.

The Committee questioned whether issues how branch incidents were escalated to the RCC but recognised that cultural change was required.

**6. Combined Risk, Compliance and Audit Update**

6.1 **Risk**

The report was taken as read.

JE reported that the top risks to POL included PCI compliance, the Group Litigation Order, Brexit, People Change and Payzone Payment Device Vulnerabilities.

*PCI Compliance*
PCI continued to report red. Ingenico had not provided a definitive plan regarding the banking solution and challenge remained with the timeline and costs of the new schedule.

*Horizon trial*
The second High Court trial relating to Horizon was due to conclude this week (week commencing 1 July). Deloitte had provided support via workshops to identify the risks, mitigation and owners, of the risks raised from the trial. Output from these sessions would be reviewed by Central Risk.

*Brexit*
Planning remained ongoing with continued and regular dialogue with BEIS. BEIS had confirmed that 'No Deal' plans should be 'shrink wrapped' and that businesses should plan for a 'Deal'. However, JE believed POL should continue to work on contingency plans for 'No Deal' particularly as it was felt the risk for 'No Deal' had not diminished. Brexit (and the associated risks) would continually be reviewed throughout September and October and the Brexit Operations Group would be re-established.

*People Change*
People change remains a key risk to POL in light of recent significant people changes and future planned organisational changes. The review to assess capability of senior positons including the identification of critical roles continues.

*Payzone Payment Device Vulnerabilities*
Work to remediate the security vulnerabilities identified following the Payzone Payment Device Penetration Test continue and are on track. It was expected that remediation would be completed by October from the recent work completed with Payzone and Information Security.

The current exposures were at device level and it was felt that this was holding at an amber position rather than red as previously thought.

BF questioned whether the risk reporting lines for Payzone should report to POL ARC, considering that Post Office Insurance did so. It was noted that whilst Payzone had a risk framework in place, it was not as comprehensive as Post Office Insurance. AC requested JE and BF discuss this outside of the meeting. — To do: JE/BF

AC further requested sight of the monitoring data (page 3 of the report) on retail partners and JE proposed that a deep dive be carried out in September. JE to send information to CM. — To do: JE/CM

POL00423462

6.2 **Compliance**

The report was taken as read.

*Text Relay*

POL provided a response to the second part of Ofcom's investigation on 21 June. He noted that Ofcom had recognised the actions POL had taken to date and the commitment to reimburse impacted customers. Where data is available, customers will be reimbursed. Where there is no data, a contribution will be made to Action for Hearing Loss.

*GDPR*

The programme was formally closed at the end of Q1. Compulsory data protection training has been rolled out for all employees, contractors and agents, with further mandatory training being developed for staff members who have high levels of daily access to sensitive personal data.

*Fit & Proper*

The team remains focused on gathering F&P returns, with fortnightly updates being provided to HMRC. It was noted that 29 of 43 of POL's commercial partners have responded in full; regarding non-commercial partners, 64% are fully compliant and a further 21% have submitted responses that now require review. A concerted final push is planned for late June/early July for the remainder returns.

A meeting is planned with HMRC next week to discuss the progress made to date, although it was noted that some commercial partners had not responded at all. One solution proposed should no return be forthcoming, is to switch off the branches capability to sell travel money.

*Moneylaundering*

The team continued to see a number of high value and complex cases relating to business banking deposits, where deposits are then used to purchase crypto currencies. Concern being the link between crypto currencies and money laundering. BF remarked that the legal risk lay with the banks rather than POL.

JH agreed that for Banking Framework transactions, so long as POL carried out its responsibilities, which it is, the banks hold the regulatory risk. However, POL does have duties and is also exposed to reputational risk should POL's network be caught up in money laundering by the banks' customers. It was **AGREED** that a money laundering analysis and risk appetite review should be conducted.

6.3 **Internal Audit**

The report was taken as read.

JA advised that 24 of 26 reviews planned reviews had been completed in the year and that the following recurring control themes had been identified:

- Internal controls not deployed through policies, procedures and systems and/or internal controls not yet designed or operating effectively enough.
- Ineffective identification and/or management of operational, fraud and change risk.
- Unavailability (or ineffective communication) of relevant, quality information to support the internal control function and decision making.
- Lack of clarity of structure, authority and responsibility.

The RCC recognised that progress had been made with regards to reporting clearance lines and the establishment of a clear escalation process to address any significant delays, however report turnaround (in terms of drafting the report and management review and comment) was below the requested internal service level agreement of clearing audits within 20 days. 10 days was considered ample time in which management should respond.

To do:

POL00423462

A number of changes to the content of the IA report summaries was requested by the RCC. These included: JA

- The use of shorter, simpler and clearer report summaries.
- Identifying the severity of any issues raised.
- Providing a broad recommendation such as the development of a new policy/system.
- Identifying whether current policies are suitable for purpose and if so, explaining how they are suitable.
- To have management responses prominently displayed as a headline.

**7. Supplier Contracts out of Governance**

The paper was taken as read.

The RCC noted that overall, the non-compliance value had dropped slightly since January from £26.4m to £26.1m, which was felt to be tolerable risk. The reduction had been primarily driven down by the closure of some material risks through compliant procurement awards, and contracts reaching a statute of limitation on a challenge period.

BB remarked that £17.5m of the £26.1m of non-compliance value had been planned/managed over the last six months, however some of this was unmanaged such as the appointment of professional services. She remarked that the risk of non-compliance could be further reduced with the appropriate quote process being used. Additionally, a new panel for procurement was being developed to reduce non-compliance.

The RCC commented that staff should use the CAF process as a matter of standard with appropriate consequences for staff who did not follow protocol.

The RCC requested a number of changes to the format of the report:

- Add a risk indicator to the table of high value open items
- Identify categories of non-compliance
- Remove POI data as this is subject to internal governance only.

BB left the meeting.

**8. Business Continuity Update and Policy**

The paper was taken as read.

TA remarked that whilst he was happy with the current position, an element of complacency had recently been observed. AC advised that appropriate support would be provided to avoid any slippage.

Evacuation tests had been successfully completed for all sites and IT tested in Swindon was found to be resilient, although he questioned the benefit of moving IT to Swansea. AC requested another evacuation test should be planned for Finsbury Dials.

The RCC requested that the following changes be made to the paper:

To do: TA

- To identify what was currently in place
- To identify what was not currently in place and how this would be fixed
- Description of actions taken to date.

*Business Continuity Policy*
The Business Continuity Policy was APPROVED for submission to the ARC on 29 July 2019.

POL00423462

TA left the meeting.

**9. Policies for Approval**

The policies were taken as read.

9.1 **Anti-Bribery and Corruption Review and Policy (including Gifts and Hospitality)**
The Anti-Bribery and Corruption Policy (including Gifts and Hospitality) was **APPROVED** for submission to the ARC on 29 July 2019.

9.2 **Whistleblowing Review and Policy**
The Whistleblowing Policy was **APPROVED** for submission to the ARC on 29 July 2019.

9.3 **Modern Slavery Statement**
The Modern Slavery Statement was **APPROVED** for submission to the ARC on 29 July 2019.

The RCC noted the statement required publishing on the POL website by 1 October 2019, and discussed the volume of work required to meet Section 54 of the Modern Slavery Act 2015.

It was felt that greater communication (to be led by the retail lead team) was required between the network and supplier base to ensure that suppliers were fulfilling their legal requirements. Vetting processes and cultural behaviour would also need to be improved.

JS left the meeting.

**10. GDPR Update**

The paper was taken as read.

JH reported that the GDPR programme (now closed) had established appropriate controls which gave POL the confidence that operational practices are compliant with GDPR. Some work remained outstanding on:

- contract remediation;
- records retention;
- data classification; and
- data storage.

He commented that the Data Protection Team was confident this work would be completed within the calendar year, and noted that GDPR would be reviewed by Internal Audit in Spring 2020.

The RCC questioned whether POL was fully compliant with GDPR. JH assured the RCC that POL was operationally compliant and could show the regulator (ICO) that established systems and processes were in place.

**11. Corporate Insurance Renewal**

The paper was taken as read.

The RCC noted the current position regarding the renewal process and that a further update would be provided to ARC in September.

**12. Review of draft Audit, Risk and Compliance Committee meeting agenda**

The draft ARC agenda for 29 July 2019 was **NOTED** and discussed.

**13. Any other Business**

POL00423462

**13.1 Meeting dates**

It was noted that the next scheduled RCC meeting was on 3 September 2019.