POL00423460

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 9 May 2019 at 13.00 pm

Present:	Alisdair Cameron (Chair) (AC)	Interim Chief Executive Officer
	Priyanka Dewan (PD) (on behalf of Owen Woodley)	Senior Strategy Manager
	Ben Foat (BF)	Legal Director
	Rob Houghton	Group Chief Information Officer
	Mo Kang	Group HR Director
	Cathy Mayor (CM) (on behalf of Debbie Smith)	Finance Director, Retail
In Attendance:	Veronica Branton (VB)	Head of Secretariat
	David Parry (DP)	Senior Assistant Company Secretary
	Johann Appel (JA)	Head of Internal Audit
	Jenny Ellwood (JE)	Risk Director
	Jonathan Hill (JH)	Compliance Director
	Liz Robson (LR)	CIO – Retail (item 3.)
	Deana Herley (DH)	Senior Manager, Assurance (item 5.3)
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**

Following introductions round the table, Alisdair Cameron opened the meeting. He remarked that the pack needed to be streamlined and that papers should be condensed, identifying the most significant risks and issues, what we were going to do to address these and the timeframes for doing so.

2. Minutes and Action Lists

The minutes of the RCC meeting held 14 March 2019 were **APPROVED.** Progress on completion of actions as shown on the action log were **NOTED.**

3. PCI-DSS Update

Liz Robson provided a verbal update on PCI compliance.

She explained this update would focus on the progress made on the alternative approach to banking services under investigation which would result in these transactions not being processed through Horizon and therefore not being in scope for PCI compliance. The progress report requested by ARC had been circulated for noting.

Regarding retail transactions via pin pad devices in branch, the deployment of point-to-point encryption (P2PE) of the Pin-Pad estate remained on track to plan, with devices being shipped to enable the required software upgrade and physical swap-out in branch.

PCI accreditation linked to the pin pad devices expired in the next 12 months and steps had been taken with Global Payments (our acquirer) to extend this accreditation until 2023 following accreditation testing. Accreditation cover came with the proviso that no further software changes would be made to the pin-pad devices beyond P2PE. An update from the Branch Device and Strategy Review on the future

POL00423460

of Pin-Pad device for branches, along with other devices such as Paystations, was expected at the end of May.

Regarding banking transactions, positive progression had been made with Ingencio and Vocalink to process transactions directly with the banks via the Ingencio cloud. This approach removed the POL back-end from PCI scope, helping to simplify the process of achieving PCI compliance by moving these transactions out of scope. Design and planning sessions were in train with payment partners and a revised timeline plan plus associated costs was expected at the end of May 2019. P2PE deployment would not be impacted and remained crucial for PCI compliance being achieved. Work remained ongoing in parallel.

The recent Data Audit of the systems estate was almost complete, with low instances or no instances of PCI related data being identified. PCI data that had been identified was removed and users educated to prevent further occurrences. Audits for Computacenter and Accenture remained outstanding and completion dates would be confirmed with both partners.

The team had remained actively engaged with Nettitude, our Quality Security Assessor (QSA) and Global Payments throughout this activity, and our Acquirer was also fully aware and supportive of our plans. A full plan update would be provided at the end of May 2019.

A number of points were raised:

What challenges were associated with data encryption for banking transactions, as an alternative to processing data through Horizon? It was reported that there were two main challenges: 1) reconciliations and 2) banks needing to change their systems. A workshop was taking place with Ingenico and Global Pay to assess the technical feasibility of an alternative approach.

The timescale for achieving PCI Compliance. It was reported that we would not be PCI compliant by the end of the year and JE and LR were working on identifying the associated risks, including the views of our partners.

The following was **AGREED:**

1. The Data Audit paper would include a section on how a BAU process would be implemented to monitor/scan the systems estate to identify and action any appropriate remediation for any PCI-related data. **LR**
2. The Branch Device Strategy paper would include an assessment of requirements of pin-pad devices in the future if they were going to be used for data entry by customers. **LR**
3. Mark Siviter would provide an update on current negotiations with RMG on the solution for International Data Capture.

A holistic plan on achieving PCI compliance, our position on data security and management (structured and unstructured data) and our risk controls would be presented to ARC in May.

4. Internal Audit (IA)

4.1 Internal Audit Report (IAR)

Johann Appel reported that apart from two change reviews, which had been deferred as part of the re-prioritisation plan, the Audit plan for 2018/2019 had been completed. 17 reports had been finalised with seven cleared by management. There was no outstanding fieldwork required for completion, and at 30 April 2019, there were no overdue actions.

AC requested that JA pass on his thanks to the team.

The RCC discussed the contents of the reports and noted that whilst there were no significant areas for concern, the message(s) conveyed could be more clearly identified. It was felt the reports should be focussed so that ARC members were fully aware of the key risks, the expected impacts, whether there **To do: JA**

POL00423460

were any shortcomings and the mitigating actions. Where appropriate, reports should be benchmarked against other industries and we should indicate where lessons from one report could be applied to other parts of the business.

It was suggested that the Internal Audit Report on Cyber Security needed to bring out the extent of our vulnerability, how long it would take to reach an acceptable position with reference to industry benchmarks, the prime drivers of weaknesses (e.g. not having strong passwords) and the activities we were undertaking such as tightening of controls around critical data assets.

It was noted that the security issues with some Payzone devices was not within the scope of the audit but Jenny Ellwood would reference this in her risk report.

JA was asked whether he had any concerns in relation to future audit reports planned or any other issues he wished to flag. He reported that terms of reference have not been agreed with process owners yet. The ToRs were in place for the Pensions Internal Audit. The Telco Internal Audit was at an early stage of planning. JA and RH would discuss the proposed change assurance work for the payment technology programme.

The reports would be circulated to the ARC for noting.

5. Risk

5.1 Consolidated Risk Report

Jenny Ellwood presented the consolidated risk report.

She reported that PCI, Information Security, Litigation and Change workforce remained the key risks but that there had been positive progress in relation to Information Security, including piloting some testing of third party supplier information security arrangements.

Emerging risks included uncertainty around the stability of the Government; people risk because of measures in the pipeline such as the introduction of a redundancy cap and because there had been significant people changes in critical roles recently and further organisational design changes were planned; and, the risk of the regulator taking action to address loyal customers' potential disadvantage vis-à-vis new customers. It was suggested that we should include what our mitigating actions would be in response to the loyalty super complaint.

It was **AGREED** that we would:

- Check whether RMG was affected by LINK ceasing to settle for partner banks from 1 July 2019.
- Include an update on the Fit and Proper compliance risk.

5.2 Litigation Update

The second trial relating to the Horizon system was pending direction from the Court of Appeal following our application to recuse the managing judge, which had been denied. The trial was due to resume on 4 June 2019 until early July.

5.3 Annual Report and Accounts 2018/19 – key risks

Deana Hurley presented the Risk Report for the Annual Report and Accounts 2018/19.

The principal risks and top risks were noted.

DH commented that since the publication of the last Risk Report there had been two main changes. Firstly the risk of increased likelihood of litigation had been amended from unlikely to possible, and

POL00423460

secondly, the risk related to Technology and Business Interruption had increased in impact as a result of being unable to automatically failover the second datacentre.

AC requested a review of the wording of the report. RH remarked that the cyber security risk had reduced as control effectiveness had improved; we were still not within risk appetite but we would be providing more information on additional risk mitigations.

DH

The Executive Declarations were noted. The following was **AGREED**:

- Mitigating actions should be included.
- The GLO litigation should be included under the risk section and should be expanded to include details of the risk(s) involved, timings, costs involved (where available) and any operational changes that may be required.
- Health and Safety had not previously been included as a risk but should be referred to.

An updated paper would be presented to ARC in May.

6. Compliance

6.1 Compliance Report

Jonathan Hill presented the consolidated compliance report.

The following key points were noted.

Ofcom would investigate the text relay breach and assistance was being provided to respond to information requests from Ofcom. Difficulty had arisen in that Ofcom wished to understand the position dating back to 2002. JH believed the potential penalty was likely to be hundreds of thousands of pounds, but it was noted that the self-declaration and wish to settle early had been well received by the regulator and was likely be taken into consideration. The regulator had also recognised the mitigating actions we had completed to date.

6.2 Fit and Proper: Compliance with HMRC June 2019 Deadline

Since the last RCC meeting, the project team had focused on completing fit and proper returns. A large backlog of responses had been cleared and HMRC had agreed to extend the June 2019 deadline to September 2019 for MI data gathering purposes.

The RCC noted the improved and accelerated position but requested that the risks and how they would be tracked were identified. To do: JH

HMRC had increased branch registration fees from £130 per annum to £300 per annum from 1 May 2019. Fees would be in the region of £1.3 million and the plan was to stagger payments. Around 4,000 registered branches processed a limited number of transactions. Work was being undertaken on the implications of not providing a Forex service in those locations; however it was not thought that we should remove the service during the course of the litigation except where there were no transactions in a branch.

Appointed Representatives

Work remained ongoing with CAP ONE on the Appointed Representative appointment. Any new arrangement would need to be consistent with the current approach taken with our existing regulatory principals.

Approved person forms would need to be filed at Companies House once completed.

Vulnerable Customers' Policy

POL00423460

An external assessor had provided positive feedback on our vulnerable customers' policy and the associated training in branches.

Whistleblowing Policy
A question was raised about whether our whistleblowing policy was being used as we would hope. JH advised the whistleblowing hotline would become a Freephone number and that work was being undertaken by HR to encourage a culture which encouraged employees to raise issues of concern.

7. Cyber Security

RH advised that the main update of note was the work that had taken place on penetration testing of Payzone devices and the work now underway with the IT Security team to formulate a risk treatment plan to remediate vulnerabilities identified.

8. Business Continuity Plan and Policy

The paper and policy were **NOTED** but the item was deferred.

The POL policy template needed to be used and the risks and mitigating actions need to be clearer.

It was **AGREED** that with assistance from RH and JH, an updated paper and policy would be presented to the RCC and ARC in July 2019. **TA/RH/JH**

9. GDPR Update

The paper was **NOTED**.

AC felt that the paper should use less technical language and be simplified to bring out the key challenges and the next steps. We also needed to provide a complete picture of data and not just the personal data covered by GDPR to provide the ARC with a holistic view. Further work required on data should also be set out.

The RCC noted that some contract remediation was outstanding and that before the GDPR programme could be signed off, the transition from programme to BAU needed to be clarified. It was also proposed that privacy/GDPR champions should be established group wide.

It was **AGREED** that:

1. A revised paper would be presented to ARC showing the work completed to date, and the areas of outstanding work. **JH**
2. An Internal Audit would be completed in Spring 2020. **JA**

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

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

A consolidated report for Risk, Compliance and Internal Audit would be presented to ARC.

11. Any other Business

11.1 Meeting dates

It was noted that the next scheduled RCC meeting was on 4 July 2019.