POL00397878

# Post Office Ltd – Strictly Confidential

[ SHAPE * MERGEFORMAT ]

## Risk and Compliance Committee (R&CC)

See Distribution

Reference: R&CC/MIN/SEP12
Date: 17 September 2012

**MINUTES OF THE POST OFFICE RISK & COMPLIANCE COMMITTEE HELD IN 148 OLD STREET AT 15.30 HRS ON 17 September 2012**

| | | | |
|---|---|---|---|
| Present | Susan Crichton | **HR & Corporate Services Director** | Chair |
| | Martin Moran | **Commercial Director** | Member |
| | Sarah Hall | **Financial Controller (for Chris Day)** | Member |
| | Lesley Sewell | **Chief Information Officer** | Member |
| | Susan Barton | **Strategy Director** | Member |
| | John Scott | **Head of Security** | Report |
| | Craig Tuthill | **Head of Network Services** | Report |
| | Malcolm Staite | **Head of Risk & Compliance** | Report |
| | Stephen Collins | **Risk & Assurance Manager (RMG)** | Report |
| | Nick Kennett | **Financial Services Director** | Report |
| | Jonathan Hill | **Senior Relationship Manager** | Report |
| | Andy Jones | **Quality & Standards Manager** | Report |
| | Mark Ward | **IT Security Specialist** | Report |
| | Nigel Tuppen | **Business Risk & Assurance Manager** | Secretary |
| | Rob Bolton | **Risk & Assurance Advisor** | Assistant Secretary |
| Apologies | Chris Day | **Chief Financial Officer** | Member |

| Item (a) | Discussion & Decisions (b) | Action (c) |
|---|---|---|
| 1. Introduction | 1.1 The Chair welcomed everyone to the meeting and there were brief introductions. Apologies had been received from Chris Day and Sarah Hall was attending in his absence. | |
| 2. Minutes of Previous Meeting | 2.1 The minutes of the last meeting had been circulated and were accepted as an accurate record by those present. | |
| 3. Outstanding Actions from the Previous Minutes | 3.1 Nigel Tuppen went through the previous actions.<br><br>Action 1478. An update had been provided prior to the meeting. It was agreed the action should be closed for the present however Nick Kennett advised that this would be re-visited again in the future and that an update would be provided to the November meeting<br><br>Action 1486 An update on the IARM plan was an agenda item<br><br>Action 1491 Scheduled for November meeting agenda<br><br>Action 1492 In progress, audit to be completed in November or December | |

POL00397878

# Post Office Ltd – Strictly Confidential

| | | |
|---|---|---|
| | Action 1494 Action Completed<br><br>Action 1498 Agenda item<br><br>Action 1499 Update provided in advance of the meeting and this action linked to the monthly forum being set up with the network field team<br><br>Action 1501 An update had been provided by John Scott prior to the meeting but he also provided a further verbal update at the meeting. He confirmed that Post Office Ltd had successfully achieved re-certification for PCI DSS for the Branch Network and Data Centre. Martin Moran asked about the period of the certification and John confirmed this was 12 months. The meeting welcomed the update but it was felt that a further report should be provided to the next meeting covering all of Post Office Ltd payment channels<br><br>Action 1502 Update provided and this action in progress<br><br>Action 1503 Update provided and this action in progress. Nigel advised this would be referred to in the ERM agenda item<br><br>Action 1504 Agenda item<br><br>Action 1505 An update provided in the form of a visual representation of the governance structure. Nigel confirmed that this was a initial view and that it was a work in progress with some work still to do in identifying the complete governance structure<br><br>Action 1506 Agenda item<br><br>Action 1507 Action in progress and update to be provided to the next meeting<br><br>**Action 1508 Report to be provided to the November meeting on updated position for Credit Card sales pilot**<br><br>**Action 1509 Full report on PCI certification covering all payment channels in Post Office Ltd to be provided to the November meeting and plans to ensure PCI compliance is established as a rolling business as usual programme.** | 1508 – NK<br><br>1509 - JS |
| 4 Enterprise Risk Management (ERM) update | 4.1 Nigel Tuppen explained that the target was to fully implement the Stratex risk tool by the end of September and to start using it from October. He confirmed that training on the tool was currently taking place covering the risk champions and the risk co-ordinators. Malcolm Staite explained that it was also the intention to get time with each of the ExCo members in the near future to talk through and explain functional risk management<br><br>4.2 Nigel provided a spreadsheet identifying risk champions and risk co-ordinators and explained that there were some gaps in both of these roles. This was discussed and the following confirmed:<br>• Paul Brown was the appointed risk champion for Commercial<br>• Simon Baker was the appointed risk champion for Chief Information Officer<br>The risk representatives for Strategy and Financial Services to be discussed with and confirmed by Susan Barton and Jonathan Hill respectively<br><br>4.3 John Scott suggested that the conversation had identified that Communications was the only directorate not represented on the Risk & Compliance Committee. Susan Crichton suggested that she discuss this with the Communications Director. | |

POL00397878

# Post Office Ltd – Strictly Confidential

| | | |
|---|---|---|
| | **Action 1510 Discuss a Communications representative on the R&CC with the Communications Director**<br><br>**Action 1511 Discuss and confirm the Strategy and Financial Services directorate risk representatives** | 1510 - SC<br><br>1511 – NT/SB/JH |
| 5. Key Risks | 5.1 Nigel Tuppen talked through the paper on key business risks which had been circulated prior to the meeting. He explained that the Business as Usual (BAU) risks had been generated by the Risk Champions within the directorates. Martin Moran queried some of BAU risks and the rationale behind them appearing together on the slide such as the failure to meet the Mails Distribution Agreement and the collapse of the Euro. Malcolm Staite explained that the top ten risks were identified across the Business and therefore it was normal for different levels of risks to be identified together<br><br>5.2 There was a general debate on the risk data and the consensus was that there was further work to be done on the identification of risks. It was also felt that the current process was very "bottom up" and that it should also include a "top down" view of the ExCo. Sarah Hall also felt that risk profiling was not being performed consistently across the Business and she thought it would have been a good opportunity to include this within the training that is currently being delivered. She suggested that training on risk identification and profiling could have been considered and included<br><br>**Action 1512 Re-engage with Risk Champions, via a workshop or face to face meetings, on the identification of key risks and risk scoring and review outputs by ExCo meetings scheduled.**<br><br>**Action 1513 Consider the inclusion of risk identification and risk profiling in the current training being delivered on the risk software** | 1512 – NT<br><br>1513 – NT/MS |
| 6. EY Management Letter | 6.1 Lesley Sewell and Andy Jones provided a brief summary of the Management Control audits performed over the last 2 years by Ernst & Young. Andy Jones reviewed the slides that had been circulated prior to the meeting focusing on the 4 findings. It was recommended to management that controls in place are sufficient to mitigate the existing low risk exposure. It was proposed that the committee should agree the acceptance of the risks associated with these audit findings<br><br>6.2 It was suggested that there was a requirement to evidence the existence of the mitigating controls and to confirm the strength of those mitigating controls in place and to this end the assistance of Internal Audit was required particularly in the area of the 4 findings previously discussed.<br><br>**Action 1514 Co-ordinate with IARM the follow up on the non SAP elements of the E&Y Audit, in particular the 4 findings identified within the R&CC update. Follow up activity to include a mitigation statement over the remaining risk**. | 1514 - LS |
| 7. Internal Audit Plan Update | 7.1 Stephen Collins provided an update on the 2012/2013 internal audit plan for Post Office Ltd. He identified progress against the activities identified within the original plan and also the reviews that had been cancelled in agreement with Post Office Ltd<br><br>7.2 Stephen confirmed that from the original plan of 500 days there was now some surplus time available due to the review cancellations. This extra time had now been allocated to additional reviews – Critical Business Controls, LINK and the E&Y Audit follow up | |

POL00397878

# Post Office Ltd – Strictly Confidential

| | | |
|---|---|---|
| 8. Business Continuity Management | 8.1 Nigel updated the meeting on current status and the resource proposal for Business Continuity. John Scott queried the resource proposal and whether this had been agreed as he felt that this was the main issue<br><br>8.2 There was a discussion about the resource issue and it was confirmed by Lesley that the principle had now been agreed of a split between the governance and operational (1st and 2nd line) BCM activities. It was therefore agreed that the resource proposal recommended within the BCM update be progressed and that a revised business case be submitted.<br><br>**Action 1515 Progress and submit business case for the resource proposal identified in the BCM update (2 x 3A managers and admin support)** | 1515 – NT |
| 9. Network Audit Findings | 9.1 A detailed report and a summary slide had been provided in advance of the meeting and Craig Tuthill talked through the summary slide relating to network audit findings.<br><br>9.2 There was a discussion about the data provided and the reporting requirements going forward. It was agreed that the reporting needed to pick up the key themes and trends from the audit activity that is being performed. It was agreed that that next report would reflect this. | |
| 10. Internal Controls Framework | 10.1 Nigel Tuppen provided an initial overview of the progress in developing an internal controls framework for Post Office Ltd. The supporting work that had been completed was then described including the approach and the initial outputs.<br><br>10.2 It was explained that the legacy 26 Critical Business Processes (CBPs) had been mapped to the APQC process framework and this had not only driven the identification of a new set of critical processes but had also suggested gaps in the legacy CBPs (Communications & Brand and Procurement).<br><br>10.3 15 new critical processes had now been identified and the supporting sub-processes from the APQC framework together with the legacy existing controls were mapped to these. This exercise revealed gaps in the existing controls e.g. the Strategy & Vision slide. It was explained that the documented existing controls needed to be validated to confirm if they still existed and were still operating effectively.<br><br>10.4 The Committee were informed that that there would be IARM support going forward Plans were already in place to discuss 2 of the new critical processes (Governance and Security) and fill in the gaps in the framework and to check the validity of the identified existing controls. | |
| 11. Any Other Business | 11.1 The reporting pack was discussed but no major issues revealed | |
| 12. Next Meeting | The next meeting of the Risk and Compliance Committee is scheduled to be held on 19th November 2012. Meeting to be held in the POL Boardroom from 13.30pm - 15.30pm. | |

**Rob Bolton**
**Risk & Assurance Adviser**

POL00397878

# Post Office Ltd – Strictly Confidential

| 13. Summary of Actions | Ref | Action | Lead | Status |
|---|---|---|---|---|
| Carried Forward | 1491 | **Perform a review of new Financial Branch Performance Profile findings and provide a further report of the findings to the November Risk & Compliance Committee meeting** | John Scott | Agenda Item |
| Carried Forward | 1505 | **To provide a list of all the governance boards for the next meeting**. | Nigel Tuppen | Initial view developed but further enhancement required which is in progress |
| Carried Forward | 1507 | **Nigel Tuppen to confirm list of key stakeholders of MI in liaison with David Mason.** | Nigel Tuppen | In progress – new management forum being developed |
| New Action | 1508 | **Report to be provided to the November meeting on updated position for Credit Card sales pilot** | Nick Kennett | Update received and included with supporting papers |
| New Action | 1509 | **Full report on PCI certification covering all payment channels in Post Office Ltd to be provided to the November meeting** | John Scott | Agenda item – to be delivered by Mark Pearce |
| New Action | 1510 | **Discuss a Communications representative on the R&CC with the Communications Director** | Susan Crichton | For discussion at meeting |
| New Action | 1511 | **Discuss and confirm the Strategy and Financial Services directorate risk representatives** | Nigel Tuppen / Susan Barton / Jonathon Hill | IT & Change Risk Champion also currently covering Strategy. Risk representatives for Financial Services & Strategy to be advised |
| New Action | 1512 | **Re-engage with ExCo members, via a workshop or face to face meetings, on the identification of key risks and risk scoring** | Nigel Tuppen | Ongoing – workshops or face to face meetings to be arranged |
| New Action | 1513 | **Consider the inclusion of risk identification and risk profiling in the current training being delivered on the risk software** | Nigel Tuppen / Malcolm Staite | Noted and will be incorporated where required as part of ongoing training |
| New Action | 1514 | **Co-ordinate with IARM the follow up on the non SAP elements of the E&Y Audit, in particular the 4 findings identified within the R&CC update. Follow up activity to include a mitigation statement over the remaining risk** | Lesley Sewell | Agenda item |
| New Action | 1515 | **Progress and submit business case for the resource proposal identified in the BCM update (2 x 3A managers and admin support)** | Nigel Tuppen | Agenda item |