Post Office Ltd – Confidential

| Risk and Compliance Committee (R&CC) | | Reference: R&CC September |
|---|---|---|
| Date: 8 September 2016 | Venue: Boardroom, Finsbury Dials | Time: 13:00 – 16:00 |
| **Members:** | | |
| Jane MacLeod (JM) | General Counsel | Chair |
| Alistair Cameron (AC) | Chief Finance Officer | Member |
| David Hussey (DH) | Transformation Director | Member |
| Martin George (MG) | Commercial Director | Member |
| Kevin Gilliland (KG) | Network and Sales Director | Member |
| Nick Kennett (NK) | Financial Services Director | Member |
| Paula Vennells (PV) | Chief Executive | Member |
| **Attendees:** | | |
| Jonathan Cormack | Director, Learning, Resourcing and Talent | On behalf of Group People Director |
| Victoria Moss | Deputy Company Secretary | On behalf of Company Secretary |
| Mike Morley-Fletcher (MMF) | Head of Risk and Assurance | Report (Papers 6 & 7) |
| Georgina Blair (GB) | Risk Business Partner | Secretariat |
| Julie George (JG) | Chief Information Security Officer | Report (Paper 2) |
| Rob Houghton (RH) | Chief Information Officer | Report (Paper 2) |
| Jonathan Hill (JH) | Head of Risk, Banking Regulation and Strategy | Report (Paper 3) |
| Owen Woodley (OW) | Sales Director, Network and Sales | Report (Paper 3) |
| Tom Moran (TM) | General Manager, Network | Report (Paper 11) |
| **Apologies:** | | |
| Alwen Lyons | Company Secretary | Member |
| Neil Hayward | Group People Director | Member |
| Jon Waples | Business Continuity Manager | Report |

## The meeting began at 13.00

The Chair declared the committee quorate and opened the meeting.

JM noted that the meeting agenda was full, and that the key things for the Committee to focus on were the papers going to ARC, including in particular the Cyber Update, FS Deep Dive paper and Financial Crime papers, and the three policies put forward for approval.

## Agenda Item 1, RCC minutes and actions

The Committee agreed the minutes of the previous meeting and reviewed the open actions.

**AP 1742 (Vulnerable customers)** – MG explained that the Vulnerable Customer policy had been updated after the last RCC. The aim was to develop a practical approach to dealing with Vulnerable Customers, firstly ensuring we meet legal requirements, before progressing for more. Actions were being developed. JH noted that the FCA and BBA (British Bankers' Association) had recently released an update on this topic.

**AP 1740 (Compliance with the Corporate Governance Code)** - JM updated the Committee on a recent discussion with Carla Stent, ARC chair, in which she agreed that as the statement about compliance with the Code had been downgraded in the Annual Report it was not necessary at this stage to undertake a gap analysis with the Code and any review would be deferred until at least Q3 in 2017.

**AP 1738 (Quarterly Lead Team Risk Reviews)** – JM noted Committee members had been requested to ensure risk was discussed at least quarterly at their lead team meetings.

Post Office Ltd – Confidential

**AP 1737 (Brexit Risk)** – MMF explained that the impact of the Brexit vote had been incorporated into individual risks in the Group Risk Profile and that an External Affairs Steering Group had been set up.

**AP 1726 (GE Objectives)** – MMF explained that we were still awaiting agreement of the TOM, before including a standard reference to risk and control in GE members job descriptions. JC agreed to work with MMF on this.

**AP 1732 (Vetting policy)** – JC noted that NH had not given it final approval because the budget and process for implementing the improvements needed for compliance with the policy had not yet been defined. NK noted that the policy was a requirement under the Banking Framework Agreement. JC said that he was confident that the necessary improvements would be implemented by January 2017, however he noted that approval of the policy was important.

**AP 1733 (Disaster Recovering policy)** – AC explained that he had requested for the policy to be revised and was waiting for an updated version.

## Agenda Item 2, Cyber/IT Security update

JG and RH joined the meeting to present paper 2.

JG summarised the key points of paper 2, explaining that although a framework of controls was in place to mitigate cyber security risks further investment would be required to reduce the risk further, including an enterprise wide Security Operations Centre (SOC) and technological monitoring and detection improvements. The Committee noted that Deloitte had recently performed assurance work over cyber security implementation, and although the report had not been finalised the draft conclusions suggested the current IT framework did not appropriately mitigate cyber security risk. It was agreed that there was a need to raise the awareness and understanding of IT security issues in order to inform business decision making. The Committee agreed the actions needed to bring the cyber security risk back within appetite should be articulated and a plan covering the necessary improvements in people, process and systems should be included in the paper presented to ARC.**(Action 1746)**

JG and RH left the meeting

## Agenda Item 3, Financial Services Deep Dive

OW joined the meeting

JH summarised the key points of paper 3, noting at ARC it would be preceded by a paper from POMS and a paper from the Bank of Ireland (BoI), and that this paper was to demonstrate to the ARC that POL was addressing the concerns of its two Principals. The Committee requested that the paper be reformatted in the appropriate board paper format. JH explained that BoI's top two concerns were pre-recruitment vetting and performance management and monitoring. Action was being taken to implement improvements in the vetting process (see Action 1732). There were currently gaps around the monitoring of transactional sales of Over 50s life insurance, travel insurance and savings products made in the wider branch network (i.e. not by Financial or Mortgage Specialists, or Customer Relationship Managers) but proposals had been made to instigate cost-effective monitoring activities. OW noted that it was necessary to have a clear whistleblowing process available to branches selling financial services. The Committee noted that the extent of monitoring required was directly linked to the extent to which financial services were sold over the branch network.

The Committee discussed repeated instances where branches have been located with retailers who are also appointed representatives (ARs) of other financial services firms or where retailers have changed their regulatory status after taking on a branch. Controls have been recommended to prevent further instances and there are currently eight branches affected. KG explained that there was a temporary solution in place in five branches, and three remained to be resolved. The Committee requested that NK, KG and JM find a solution for the three remaining branches before 28 Sept.**(Action 1747)**

Post Office Ltd – Confidential

OW left the meeting

## Agenda Item 4, Financial Crime

PH joined the meeting

### (b) BCV lessons learned

AC gave a verbal update on the current status of the lessons learned exercise from the BCV ('batch control vouchers') fraud, noting that the issue would be discussed in the Group Executive (GE) meeting on Monday 12 September. Two further attempts to obtain cash via this method had been made since monitoring started, but these had been successfully rebuffed. An action plan was being finalised with the help of Deana Herley, Senior Assurance Manager and a paper would be produced for ARC.

The Committee discussed the issue of product fraud and noted that agents' losses are currently increasing. The Committee requested that a list of frauds be presented at each RCC meeting.(**Action 1748**)

PH left the meeting

### (a) AML update

JM updated the Committee on progress with the HMRC Regulatory Activity project, detailed in paper 4. The Thistle risk assessment was running late but a draft report on residual risk was expected to be presented next week, and this information would be included in the ARC paper.

Branch premises registration with HMRC was now up to date but HRMC was still to confirm whether it would be imposing any fines. The Committee discussed the registration process, noting that it currently involved teams from three business areas (Network, Financial Services and the Financial Crime team in Corporate Services). KG offered to take over the entire process within Network, and the Committee requested that the process be reviewed and simplified.(**Action 1749**)

## Agenda Item 5, Internal Audit Report

MMF updated the Committee on audit activity since the last meeting, referring to paper 5. The Committee discussed the function of Post Implementation Reviews (PIRs), noting that there was undoubted value in reviewing lessons learned. The Committee also noted that some PIRs were taking place so long after the event that the key people involved in the project had left the business.

JM and DH proposed that they would collate findings from relevant BTA and audit work to date for the next RCC meeting, in order for RCC to consider the extent to which the business had taken on board such lessons and recommendations.(**Action 1750**)

PV asked AC to update the Committee on work on the Financial Controls Framework. AC confirmed that a paper will be going to ARC. There are nine workstreams all being progressed and the common issue that was being highlighted as making improvements difficult was the fragmented nature of POL's data holding system.

Post Office Ltd – Confidential

## Agenda Item 6, Risk Report

MMF updated the Committee on progress against the risk framework project plan (paper 6, appendix 1) and emphasised the important of the support of the Committee in making the risk register work in their own business areas.  In particular it was necessary to ensure that the risk registers were linked to the top risks.  The Committee agreed that a yearly risk workshop in each business area would be helpful in achieving this aim.

The Committee discussed the collection and presentation of risk incidents.  The Committee queried whether too much was being asked of the business in the collection of data in general in light of other work priorities.  The Committee recommended a wider GE discussion on prioritisation.  Referring specifically to the collection of risk incidents, GB explained that successful collection of risk incidents occurred where there are existing data streams (e.g. IT incident reporting, property incident reporting) and so the collection of those incidents posed no extra demands on the business.  In other areas where no data was collected on incidents it was necessary to consider whether a process should be in place, or whether the incident data was of no value and should not be collected.  JM noted that the incident reporting process was not yet fully functional, but the aim was for it to be developed so it would provide information to help identify control breaches.

## Agenda Item 7, Group Risk Profile

MMF summarised the changes in the Group Risk Profile presented in paper 7 which had occurred in the six months since the Committee last reviewed the business's risk profile, and asked the each member of the Committee to look at the key further actions listed against their risks and let him know post-RCC if they had any further amendments.

The Committee discussed the number of red risks and the process by which risks were categorised (thus resulting in 18 red risks).  The Committee noted that consolidation of some risks may hide specific risks that needed further actions and some risks may reduce in evaluation significantly over the next few months (e.g. 1) Pension Costs, 4) Third Party Relationship Management, 7) Industrial Relations).  The Committee agreed that it was necessary to view the risk profile as a whole and consider the impacts of risks to the whole organisation, and that the best way to do this would be in a GE discussion.  The Committee requested that a GE session to discuss the Group Risk Profile be held before the November ARC meeting.(**Action 1751**)

## Agenda Item 8, Business Continuity

JM gave a brief update on the Business Continuity and Crisis Management Project, explaining that Jon Waples, Business Continuity Manager was unwell.  The Committee requested an update at the next RCC meeting on progress of Business Impact Assessment plans as compared with the position that was shared with the Committee last October.(**Action 1752**)

## Agenda Item 9, Policy approvals

The Committee discussed the three policies put forward for approval.  NK requested some amendments to the Treasury Policy, and AC agreed to follow this up with NK.(**Action 1753**) The Committee approved the Investigations Policy and the Physical Security Policy.

## Agenda Item 11, Property Compliance update

TM joined the meeting.

JM explained that Carla Stent, ARC Chair, was due to brief the Board about Property Compliance, so an update would be going to ARC.  TM updated the Committee on progress in managing risks in property compliance, noting that significant progress had been made

Post Office Ltd – Confidential

over the past five months, and that improvements in reducing the risk profile in this area were on track. The Committee agreed that going forward reports on Property Compliance should go to the Health and Safety Committee, and that the RCC should get reports from the Health and Safety Committee.(**Action 1754**)

TM left the meeting.

## Agenda Items 10, 12 – 18

The Committee briefly discussed the Horizon scanning paper (paper 10) and JH explained that the work that they are currently doing with POMS and the Bank of Ireland was helping them to prepare for the Senior Managers' Regime. The Committee suggested that the proposal for workers on boards should be considered for the next paper.(**Action 1755**)

JM explained that it had not been possible to write a paper on Contract Management in time for the Committee meeting as insufficient information on the contracts had been received. The Committee noted that it was important to capture contractual obligations, and to make sure that this was recorded so it was not lost if people moved roles or left the business.

The following papers were noted:

Paper 13 – Agents Remuneration lessons learned
Paper 14 – Horizon outage lessons learned
Paper 15 – Items scheduled for the next RCC
Paper 16 – POMS RCC minutes
Paper 17 – ARC agenda

## The meeting closed at 16.10

**Next Meeting – 3 November 2016 Room 1.19 Wakefield 13.00 – 16.00**