POL00423386



# x) Review of RCC Terms of Reference

Author: Georgina Blair Sponsor: Jane MacLeod Meeting date: 09 March 2017

# Executive Summary

## Context

In line with best practice and as recommended by the UK Code of Corporate Governance a clear Terms of Reference ('TOR') for the Risk and Compliance Committee ('RCC') should be in place and reviewed on an annual basis. This year's review was completed in February 2017.

## Questions this paper addresses

1. Does the RCC have a clear and agreed TOR?
2. Has the Committee fulfilled the requirements of the TOR over the last year?
3. How will the Committee ensure it uses its time effectively in future and fulfils the requirements set out in its TOR?

## Conclusion

1. The requirements specified by the current TOR (see Appendix 1) are clear and approved by the Group Executive (GE).
2. The analysis carried out (see Appendix 2) confirms that the RCC has fulfilled the requirements of its TOR with the exception of receiving reports from three sub-committees.
3. The draft RCC timetable set out in Appendix 3 is a proposed forward agenda for RCC meetings which will ensure the RCC fulfils the requirements of its TOR in 2017/18.

## Input Sought

The members of the RRC are asked to:

1. Confirm they believe they have fulfilled the requirements of the RCC TOR in 2016/17 as specified by the Group Executive.
2. Feedback to the Chair any comments on the proposed forward agenda for 2017/18.

POL00423386



# The Report

1. The RCC is responsible for supporting the Group Executive (GE) in fulfilling their responsibilities in the effective oversight of risk management, internal control and assurance, and compliance in the company.

2. The areas of the TOR have be assessed against the Committee agendas, papers and decisions to ensure that the Committee has fulfilled its requirements to the Group Executive (see Appendix 2):
   a) The 'Purpose' of the Committee is clear and agreed by the Group Executive.
   b) The 'Composition and Terms of Office' have been met at each meeting during the year.
   c) The 'Meetings' have been convened in accordance with the TOR.
   d) The 'Responsibilities' have been discharged, with the exception of:
      i) Review of risk reports from sub-committees, namely Transformation, Information Security, Security and Business Continuity. Transformation Risk has been reported as a separate item at each meeting from November 2016 onwards. The Information Security Committee has not provided reports to RCC during the year, and nor has the Security Committee [does this in fact exist?]. There has not been a Business Continuity sub-committee during the year but the Committee has received regular updates on the implementation of the Business Continuity framework.

3. Areas of specific risk have been reported throughout the year and key further actions agreed.

4. The draft RCC timetable set out in Appendix 3 is a proposed forward agenda for RCC meetings which will ensure the RCC fulfils the requirements of its TOR in 2017/18. The scheduling of the various agenda items is yet to be finalised and will be aligned with the ARC timetable.

POL00423386



# Appendix 1

**TERMS OF REFERENCE OF THE POST OFFICE**
**RISK AND COMPLIANCE COMMITTEE**
Approved July 2016

## Purpose

1. The purpose of the Risk & Compliance Committee ("RCC" or the "Committee") is to support the Group Executive (GE) in fulfilling their responsibilities in the effective oversight of risk management, internal control and assurance, and compliance in the Company.

## Composition and Terms of Office

2. The Committee shall serve as a standing committee of the GE. It shall consist of all members of the GE.

3. The quorum shall be two members which will be deemed competent to exercise all or any of the authorities and powers vested in or exercisable by the committee.

4. The Committee shall meet at least six times a year and otherwise as required.

5. The Committee is authorised to seek any information it requires from anyone in the organisation in order to perform its duties including calling anyone to the meeting to be questioned as required.

6. The Committee is authorised to obtain outside legal or other professional advice on any matter within its terms of reference.

7. The Head of Risk and Assurance, the Senior Audit Manager and the Chief of Staff (or those holding positions with responsibility for such roles, howsoever named) will be permanent invitees.

8. The Committee shall report to the GE on its proceedings on all matters within its purpose and responsibilities highlighting significant risk and compliance matters for their attention.

9. The Committee shall report to the Board and Audit, Risk and Compliance Committee as requested.

10. The Committee shall input into the Post Office annual reporting as appropriate.

## Meetings

11. Any member of the committee may convene a meeting.

12. Meetings may be held in person or by telephone or other electronic means so long as all participants can contribute to the meeting simultaneously.

13. Notice of each meeting shall be given to all those entitled to participate at least 2 working days before the meeting.

14. Meetings shall be planned in accordance with key reporting and financial planning dates.

POL00423386



**Other Governance Responsibilities**

15. The Committee will

    a. Review and update its terms of reference annually.

    b. Conduct an annual review of its own performance to ensure it is operating effectively and recommend any changes it considers necessary to GE for approval.

**Risk Management Framework**

16. The Committee will:

    a. Review the effectiveness of the risk management framework and maintain oversight of the development and implementation of the components of the risk management framework.

    b. Maintain oversight of the current risk exposures of Post Office and advise on future risk strategy.

    c. Review the identification and effective management of current key risks and identified mitigating actions and regular reviews of emerging risks.

    d. Consider and review areas of risk, which should include, but is not limited to, sufficient coverage of:

        i. strategic risk,
        ii. major change initiative risk,
        iii. operational risk,
        iv. financial risk, and
        v. legal and regulatory risks, and
        vi. reputational risk,

        plus more specifically,

        vii. people risk,
        viii. fraud risk,
        ix. technology risk and cyber security,
        x. risk relating to the investment strategy and funding requirements of existing and new pensions schemes, and
        xi. conduct risks relating to the financial services businesses operated by both Post Office Limited and its subsidiaries and joint ventures.

    e. Receive and review risk reports from the following management Sub-Committees:

        i. Transformation
        ii. Information Security
        iii. Security
        iv. Business Continuity (once formed)

17. The Committee will receive and review the draft annual risk management plan for onward reporting to the Board Audit, Risk and Compliance Committee.

18. The Committee will receive and review the draft annual internal audit plan for onward reporting to the Board Audit, Risk and Compliance Committee.

POL00423386



**Internal controls and assurance**

19. The Committee will:

    a. Consider and review the adequacy of the Company's internal controls and make recommendations for the improvement of the Company's internal controls, processes and systems.

    b. Monitor the implementation of key recommendations and management action plans.

    c. Review the adequacy of policy governance and recommend changes.

**Fraud, Theft and Ethics**

20. The Committee will:

    a. Review with management their fraud assessment, detection measures and their investigation of illegal acts, as appropriate.

    b. Review any summary of frauds, thefts and other irregularities of any size.

    c. Review with the internal auditors the results of any review of the compliance with the Company's codes of ethical conduct and similar policies including whistleblowing.

**Compliance**

21. The Committee will monitor compliance with legal and regulatory obligations, including any significant breaches.

POL00423386



# Appendix 2

## Analysis of performance of RCC against requirements

| Verbatim Extracts from TOR | | Meeting Dates & topics of papers reviewed | | | | | |
|---|---|---|---|---|---|---|---|
| **Responsibilities -** | | **May-16** | **July-16** | **Sep-16** | **Nov-16** | **Jan-16** | **Mar-17** |
| **Risk Management Framework** | | | | | | | |
| a. Review the effectiveness of the risk management framework and maintain oversight of the development and implementation of the components of the risk management framework. | | Risk framework project plan | | | Risk framework project plan; risk appetite; risk exceptions process | Risk appetite | |
| b. Maintain oversight of the current risk exposures of Post Office and advise on future risk strategy. | | Principal risks for annual report | Group risk profile | Group risk profile | | Group risk profile | |
| c. Review the identification and effective management of current key risks and identified mitigating actions and regular reviews of emerging risks. | | Horizon scan | Key further actions; Horizon scan | Key further actions; Horizon scan | Horizon scan | Key further actions; Horizon scan | Horizon scan |
| d. Consider and review areas of risk, which should include, but is not limited to, sufficient coverage of: (see i. – ix. in Terms of Reference above) | | Financial Services; AML; Property Compliance | AML; Property Compliance | Financial Services; AML; Property Compliance; Cyber Security | Network Conduct Risk; FS Conduct Risk; AML | Financial Crime; AML; Network Conduct Risk; Legal Risk | Financial Controls; IT Controls; Financial Services Conduct; Safety; Pensions update |

POL00423386



| **Verbatim Extracts from TOR** | | **Meeting Dates & topics of papers reviewed** | | | | | |
|---|---|---|---|---|---|---|---|
| **Responsibilities -** | | **May-16** | **July-16** | **Sep-16** | **Nov-16** | **Jan-16** | **Mar-17** |
| e. Receive and review risk reports from the following management Sub-Committees:<br>i. Transformation<br>ii. Information Security<br>iii. Security<br>iv. Business Continuity (once formed) | | Business Continuity and Crisis Management implementation plan | Business Continuity and Crisis Management implementation plan | | Transformation Risk | Business Continuity; Transformation Risk | Business Continuity; Transformation Risk |
| The Committee will receive and review the draft annual risk management plan for onward reporting to the Board Audit, Risk and Compliance Committee. | | | | | | | |
| The Committee will receive and review the draft annual internal audit plan for onward reporting to the Board Audit, Risk and Compliance Committee. | | | | | | | Internal Audit plan 2017/18 |
| **Internal Controls and Assurance** | | | | | | | |
| a. Consider and review the adequacy of the Company's internal controls and make recommendations for the improvement of the Company's internal controls, processes and systems. | | Implementation of General Controls Framework | | Agents Remuneration lessons learned; Horizon outage lessons learned | Executive Declarations & Control Self Assessment; Financial Reporting controls | Telco Cyber Attack; IT Controls | Executive Declaration and Control Self Assessment |

POL00423386



| Verbatim Extracts from TOR | | Meeting Dates & topics of papers reviewed | | | | | |
|---|---|---|---|---|---|---|---|
| **Responsibilities -** | | **May-16** | **July-16** | **Sep-16** | **Nov-16** | **Jan-16** | **Mar-17** |
| b. Monitor the implementation of key recommendations and management action plans. | | Internal Audit Actions | Internal Audit Actions | Internal Audit Actions | Internal Audit Actions | Internal Audit Actions | |
| c. Review the adequacy of policy governance and recommend changes. | | Policy Framework Project | Policy Framework Project | | Policy Framework Project | | Code of Conduct; Conflict of Interest; Vulnerable customers |
| **Fraud, Theft and Ethics** | | | | | | | |
| a. Review with management their fraud assessment, detection measures and their investigation of illegal acts, as appropriate. | | | | | | | |
| b. Review any summary of frauds, thefts and other irregularities of any size. | | | | BVC Lessons Learned | | | |
| c. Review with the internal auditors the results of any review of the compliance with the Company's codes of ethical conduct and similar policies including whistleblowing. | | Review of whistleblowing procedures 2015-16 | | | | | Review of whistleblowing procedures 2016-17 |
| **Compliance** | | | | | | | |

POL00423386



| Verbatim Extracts from TOR | | Meeting Dates & topics of papers reviewed | | | | | |
|---|---|---|---|---|---|---|---|
| **Responsibilities -** | | **May-16** | **July-16** | **Sep-16** | **Nov-16** | **Jan-16** | **Mar-17** |
| The Committee will monitor compliance with legal and regulatory obligations, including any significant breaches. | | Modern Slavery Act | Risk incident report | Contract management; Risk incident report | Contract management; Risk incident report | Modern Slavery Act; Risk incident report | Risk incident report |

POL00423386



# Appendix 3 – THIS NEEDS TO BE UPDATED FOR CHANGES TO ARC AGENDA

**RCC Forward planner – proposed topics (assuming 6 meetings per year) – scheduling to be confirmed**

| Items | | Proposed | | | | |
|---|---|---|---|---|---|---|
| | 1) Jan | 2) Mar | 3) May | 4) July | 5) Sep | 6) Nov |
| **1. Standing Agenda Items** | | | | | | |
| • Minutes and actions from previous RRC meetings | √ | √ | √ | √ | √ | √ |
| • Minutes from POMS RCC meetings | √ | √ | √ | √ | √ | √ |
| **2. Governance Items** | | | | | | |
| • Review of RCC Terms of Reference | | √ | | | | |
| • RCC effectiveness against ToR self-assessment | | √ | | | | |
| **3. Risk Management, Internal Control and Assurance** | | | | | | |
| • Group Risk Profile | | √ | | | √ | |
| • Key Further Actions & Risk Incidents | √ | √ | | √ | √ | |
| • Internal Audit update | √ | √ | √ | √ | √ | √ |
| • Internal Audit – approval of the upcoming plan | | √ | | | | |
| • Business Continuity – approval of annual plan | | √ | | | | |
| **4. Financial Reporting and Disclosure** | | | | | | |
| • Risk disclosures for annual report and accounts | | | √ | | √ | |
| • Board Annual Assessment (including Executives Declaration, Key Policies and Control Self Assessment) | | | √ | | | |
| • Corporate Governance Statements | | | √ | | | |
| **5. Compliance** | | | | | | |
| • Regulation | | | | | | |
| ▪ Anti Money Laundering | √ | √ | √ | | √ | √ |
| ▪ Anti Bribery & Corruption | √ | | | | | |
| ▪ Competition Law | √ | | | | | |
| ▪ Data Protection | √ | | | | | |
| • Conduct/ People | | | | | | |
| ▪ Customers (e.g. Vulnerable, Conduct issues) | | √ | | | | |

POL00423386



| Items | | Proposed | | | | |
|---|---|---|---|---|---|---|
| | 1) Jan | 2) Mar | 3) May | 4) July | 5) Sep | 6) Nov |
| ▪ Ethics and Code of Conduct | | √ | | | | |
| ▪ Fraud and Theft | | √ | | | | |
| ▪ Whistleblowing | | √ | | | | |
| 6. **Deep Dives** | | | | | | |
| ▪ FS Deep Dives on specific issues | √ | | √ | | | |
| ▪ Pensions | | √ | | | √ | |
| ▪ Health and Safety | | | | | √ | |
| ▪ Incident Management, Disaster Recovery & Crisis Management | | | | | √ | |
| ▪ Transformation Risk | √ | | | | √ | |
| ▪ Cyber / IT Security | | | | | √ | |