

**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.

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.

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.