

**Post Office Limited
("the Company")
Terms of Reference of Risk and Compliance Committee**

The Risk and Compliance Committee (RCC) is a standing committee of the Strategic Executive Group (SEG). Its authority is subject to the powers and duties of the Company Board, as set out in the Articles of Association and the Framework Document.

A. Purpose

1. The purpose of the RCC is to support the SEG in fulfilling their responsibilities in the effective oversight of risk management, internal control and assurance, and compliance in the Group.¹

B. Duties and Responsibilities

2. The RCC shall **review** and **approve for recommendation** (where applicable) to the Audit, Risk & Compliance Committee all papers and decisions prior to submission to the Audit, Risk and Compliance Committee.²
3. The RCC shall also:

Risk Management Framework

- i. **Review** the effectiveness of the risk management framework and maintain oversight of the development and implementation of the components of the risk management framework;
- ii. **Monitor** the current risk exposures of Post Office Group and advise on future risk strategy;
- iii. **Review** the identification and effective management of current key risks and identified mitigating actions and regular reviews of emerging risks.;
- iv. **Review** areas of risk, which should include enterprise and linked intermediate risks.³
- v. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee the draft annual risk management framework;

¹ The Group is defined as Post Office Limited and its subsidiary undertakings: Post Office Management Services Limited (Post Office Insurance) and Payzone Bill Payments Limited. For the avoidance of doubt, the Committee is responsible for overseeing the Historical Matters Business Unit.

² See the Board Table of Delegated Authorities for decisions requiring Audit, Risk & Compliance Committee approval.

³ This includes, but is not limited to, Strategic risks, Governance risks (including those related to the financial services businesses operated by the Group and the Company's joint venture (First Rate Exchange Services Holdings Limited), Operational risks, Legal risks, Health & Safety risks (including pandemics), Financial risks, Commercial risks, People risks, Technology risks, Information risks, Security risks, Change risks, Reputation risks and Marketplace & Brand risks.

Post Office Limited
Terms of Reference of the Risk & Compliance Committee (RCC)

- v. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee the draft annual internal audit plan;
- vi. **Review** risk reports from subsidiaries, as appropriate;
- vii. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee the draft risk section of the Annual Report and Accounts;

Internal controls and assurance

- viii. **Review** the adequacy of the Group's internal controls and make recommendations for the improvement of the Group's internal controls, processes and systems (including financial controls);
- ix. **Monitor** the implementation of key recommendations and management action plans;
- x. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee Key Group Policies;⁴
- xi. **Review** and **approve** Non-Key Group Policies;⁵

Fraud, Theft and Ethics

- xii. **Review** with management their fraud assessment, detection measures and their investigation of illegal acts, as appropriate;
- xiii. **Review** any summary of frauds, thefts and other irregularities of any size;
- xiv. **Review** with the internal auditors the results of any review of the compliance with the Group's codes of ethical conduct and similar policies including whistleblowing;

Compliance

- xv. **Monitor** compliance with legal and regulatory obligations, including any significant breaches and horizon scanning for changes in the legal and regulatory landscape; and

⁴ Key Group Policies are those that require Board/Committee sign-off due to legal or regulatory obligations. A list of Key Group Policies can be found on the Intranet.

⁵ Non-Key Group policies are operational policies that do not require Board/Committee sign off.

Post Office Limited
Terms of Reference of the Risk & Compliance Committee (RCC)

Other

- xvi. **Review** and **approve for recommendation** to the Audit, Risk & Compliance Committee the Group Insurance provision (including any renewals).

C. Reporting Responsibilities

- 4. The RCC shall ensure the timely and appropriate reporting to the SEG, the Audit, Risk and Compliance Committee and Board (as requested).
- 5. The minutes of each RCC meeting shall be noted at the subsequent meeting of the Audit, Risk and Compliance Committee.

D. Authority

- 6. The RCC 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.

Post Office Limited
Terms of Reference of the Risk & Compliance Committee (RCC)

E. Composition and Governance

Membership

7. The RCC shall consist of:
 - i. Group General Counsel (Chair)
 - ii. Chief Transformation Officer
 - iii. Retail Engagement Director
 - iv. Group Chief People Officer
 - v. Finance Director, Commercial

(or those holding positions with responsibility for such roles, howsoever named).
8. In the event the Chair cannot attend a meeting, the Committee may nominate a member present to chair that meeting only.
9. Members of RCC may send a nominee to deputise on their behalf with prior approval of the Chair.
10. The following individuals shall be permanent invitees of the Committee:
 - i. Compliance Director;
 - ii. Head of Risk;
 - iii. Director of Internal Audit;
 - iv. Financial Controller;
 - v. Group Legal Director; and
 - vi. Group Assurance Director.

(or those holding positions with responsibility for such roles, howsoever named).
11. Permanent invitees may send a nominee to deputise on their behalf with prior approval of the Chair.

Quorum

12. Quorum shall be three members of RCC.

Committee Secretary

13. The Company Secretary, or his or her nominee, shall act as Secretary to the RCC and shall attend all meetings to keep minutes and record actions.

Frequency

14. The RCC shall meet at least six times a year and as otherwise required. Meetings shall be planned in accordance with key reporting and financial planning dates.

Governance

15. Meetings may be held in person or by telephone or other electronic means, so long as all participants can contribute to the meeting simultaneously.
16. Notice of each meeting shall be given to all those entitled to participate at least three working days before the meeting.

Post Office Limited
Terms of Reference of the Risk & Compliance Committee (RCC)

17. In exceptional circumstances, written requests for approval by RCC may be circulated by email, if agreed by the Chair.
18. Meetings for the RCC will be convened by the Secretary in consultation with the Chair. The Secretary will be responsible for setting the venue date and time of meetings in conjunction with the Chair. All papers supporting the meeting will be issued in good time, three working days in advance of the meeting date.
19. Minutes of each RCC meeting will be circulated to all members of the RCC.
20. The attendance of other Group employees for part or the whole of any RCC meeting shall be solely at the discretion of the Chair.

F. Annual Review and Approval

21. The RCC will undertake an annual review of its performance and the Terms of Reference. The outcome of these review will be recommended to the SEG for approval (notwithstanding amendments approved by the SEG whenever so required).

Approved by:	Date:	Version:	Effective from:
Group Executive	July 2016	1.0	July 2016
Group Executive	8 December 2020	2.0	9 December 2020
Group Executive	6 July 2022	3.0	7 July 2022
Group Executive	7 June 2023	3.1	8 June 2023
Strategic Executive Group	19 June 2024	3.2	20 June 2024