POL00423520

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 Group Executive (GE). 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 GE in fulfilling their responsibilities in the effective oversight of risk management, internal control and assurance, and compliance in the Group.[1]

Commented [RW1]: Addition of the call out for the HMU was requested by the RCC.

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** ~~Maintain oversight of~~ 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. ~~Consider and~~ **Rreview** areas of risk, which should include~~, but is not limited to, sufficient coverage of~~ enterprise and linked intermediate risks.[3]

~~iii.~~ ;

[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.

POL00423520

~~iv. strategic risk,~~

~~v. major change initiative risk,~~

~~vi. operational risk,~~

~~vii. financial risk, and~~

~~viii. legal and regulatory risks, and~~

~~ix. reputational risk,~~

~~x. plus more specifically,~~

~~xi. people risk,~~

~~xii. fraud risk,~~

~~xiii. technology risk and cyber security,~~

~~xiv. risk relating to the investment strategy and funding requirements of existing and new pensions schemes, and~~

~~xv.~~v. ~~conduct risks relating to the financial services businesses operated by both Post Office Limited and its subsidiaries and joint ventures.~~

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

~~Transformation~~
~~i. Information Security~~
~~i. Security~~
~~i. Business Continuity (once formed)~~

Commented [RW2]: Amendment agreed with Mark Baldock as per GE approved enterprise risks signed off in Feb 2020.

Commented [R3]: These don't exist anymore....

Formatted: Font: 11 pt

v. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee the draft annual risk ~~management~~ management framework~~plan~~;

vi. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee the draft annual internal audit plan;

vii. **Review** risk reports from subsidiaries, as appropriate;

viii. **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

~~vi.~~ix. **Review** the adequacy of the Group~~Company~~'s internal controls and make recommendations for the improvement of the

POL00423520

Group~~Company~~'s internal controls, processes and systems (including financial controls);

~~vii.~~x. **Monitor** the implementation of key recommendations and management action plans;

~~viii.~~xi. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee Key Group Policies;[4] ~~the adequacy of policy governance and recommend changes;~~

xii. **Review** and **approve** Non-Key Group Policies;[5]

Fraud, Theft and Ethics

~~ix.~~xiii. **Review** with management their fraud assessment, detection measures and their investigation of illegal acts, as appropriate;

~~x.~~xiv. **Review** any summary of frauds, thefts and other irregularities of any size;

~~xi.~~xv. **Review** with the internal auditors the results of any review of the compliance with the Group~~Company~~'s codes of ethical conduct and similar policies including whistleblowing;

Compliance

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

Other

~~xiii.~~xvii. **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 GE, 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.

[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. ~~This includes policies which apply solely to Post Office Limited.~~

POL00423520

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.

E. Composition and Governance

Membership

Commented [RW4]: Membership is as proposed by the RCC at its meeting on 12 November 2020.

7. The RCC shall consist of:
   i. Group Chief Financial Officer (Chair)
   ~~ii. Group Chief Executive Officer~~
   ~~iii. Group Chief Commercial Officer~~
   ~~iv.~~ii. Group Retail and Franchise Network Director
   ~~v.~~iii. Group Chief Information Officer
   ~~vi.~~iv. Group Chief People Officer
   ~~vii. Group Operations and Supply Chain Director~~
   v. Group General Counsel
   ~~viii.~~vi. Finance Director, Commercial

8. In the event the Chair cannot attend a meeting, the Committee may nominate a member present to chair that meeting only.

~~8.~~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. Head of Internal Audit; and
   iv. Financial Controller.

10. Permanent invitees may send a nominee to deputise on their behalf with prior approval of the Chair.

Quorum

~~9.~~11. Quorum shall be ~~two~~ three members of RCC.

Commented [R5]: This aligns with GE.

Committee Secretary

~~10.~~12. 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

~~11.~~13. 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

~~12.~~14. Meetings may be held in person or by telephone or other electronic means, so long as all participants can contribute to the meeting simultaneously.

POL00423520

~~13.~~15. Notice of each meeting shall be given to all those entitled to participate at least three working days before the meeting.

~~14.~~16. In exceptional circumstances, written requests for approval by RCC may be circulated by email, if agreed by the Chair ~~Group Chief Financial Officer~~.

~~15.~~17. 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.

~~16.~~18. Minutes of each RCC meeting will be circulated to all members of the RCC.

~~17.~~19. The attendance of other Group employees for part or the whole of any RCC meeting shall be solely at the discretion of the Chair.

Commented [R6]: Previously two but three is in line with GE

Commented [R7]: New, but in line with GE

Commented [R8]: Minutes to the ARC is included above in Reporting section

F. Annual Review and Approval

~~18.~~20. 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 GE for approval (notwithstanding amendments approved by the GE whenever so required).

Approved by:	Date:	Version:	Effective from:
Group Executive	July 2016	1.0	July 2016
Group Executive	12 December 2020	2.0	13 December 2020