POL00183698

FINAL

TERMS OF REFERENCE FOR THE RISK AND COMPLIANCE COMMITTEE

1. Purpose

The purpose of the Risk & Compliance Committee ("R&CC") is to support the Executive Committee in fulfilling their effective oversight of governance, risk and compliance by:

- Overseeing the coordination of governance, risk and compliance activities across the organisation.

- Ensuring the effective establishment and application of: a) Risk, Internal control and Policy frameworks. b) Risk appetite setting.
  c) A positive risk and compliance culture.
  and the embedding of the above across the organisation.

- Advise the Audit Risk and Compliance Committee and the Executive Committee on risk and compliance matters.

2. Composition and Governance

2.1 Composition

The Committee is a management committee and the Chair and members shall be appointed by the Chief Executive Officer:

- The committee shall comprise at least three executive committee members including the Chief Financial Officer and Director of HR and Corporate Services (Chair) and at least one from the Chief Information Officer, Commercial Director and Strategy Director.

- The Chair of the Committee may invite the Chief Executive and other senior managers to attend all or part of meetings as appropriate. The Head of Risk & Compliance and Head of Internal Audit shall be regular attendees.

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

POL00183698

2.2 Governance – Meetings

- The committee shall meet at least four times a year at appropriate times and otherwise as required.

- The frequency and timing of meetings will, where possible, be organised to occur sufficiently ahead of the Board Audit Risk and Compliance committee meetings[1].

- Meetings of the committee shall be called by the Committee Secretary as timetabled and at the request of any of its members as approved by the Chairman.

- Unless otherwise agreed, notice of each meeting confirming the venue, time and date together with an agenda of items to be discussed, shall be forwarded to each member of the committee any other person required to attend no later than five working days before the date of the meeting. Supporting papers shall be sent to committee members and to other attendees as appropriate, at the same time.

- Draft minutes of committee meetings shall be circulated promptly to all members of the committee. Once approved by the Chair, minutes shall be circulated to all other members of the Executive Committee unless it would be inappropriate to do so.

- The Minutes will also be included with a summary report to be sent to the Audit, Risk and Compliance committee. The secretary to the committee will produce the summary report.

2.3 Governance – Authority

- The committee is authorised by the Executive committee:
    - To seek any information it requires from any employee of the organisation in order to perform its duties.
    - To obtain outside legal or other professional advice on any matter within its terms of reference.
    - To call any employee to be questioned at a meeting of the committee as and when required.

[1] This is to allow the committee time to prepare its activity report and items to note for the ARC. The R&CC should meet 3-4 weeks prior to the upcoming ARC.

POL00183698

2.4 Governance – Reporting Responsibilities

- The committee chairman shall report to the Executive committee on its proceedings after each meeting on all matters within its duties and responsibilities.

- The committee chairman shall report to the Audit, Risk and Compliance committee highlighting significant risk and compliance matters arising for their attention. The committee shall make whatever recommendations to the Executive Committee it deems appropriate on any area within its remit where action or improvement is needed.

- The committee shall produce inputs to the Post Office annual reporting as appropriate and directed by the Board.

2.5 Governance – Risk and Compliance functions

The Committee will:

- Oversee and receive reports from the risk and compliance management teams.

- Consider and approve the remit of the risk and compliance management function and ensure it has adequate resources and appropriate access to information, management and staff to enable it to perform its function effectively and in accordance with the relevant professional standards.

- Ensure free and effective communication between the Committee, external auditors and internal auditors and hold separate sessions, or informal meetings and contact as required.

- Ensure lines of communication are maintained with the Board and the Executive Committee as a whole.

- The committee shall also ensure the department has adequate independence and is free from management or other restrictions.

2.6 Governance – Other

POL00183698

The Committee will:

- Have access to sufficient resources in order to carry out its duties.
- Oversee any investigation of activities which are within its terms of reference.
- Arrange for periodic reviews of its own performance and, at least annually, review its constitution and terms of reference to ensure it is operating at an effective level; and recommend any changes it considers necessary to the Executive committee for approval.

3. Duties and Responsibilities - Risk

The Committee will:

- Advise the Executive and Audit Risk & Compliance committees on the Post Office's overall governance, risk and compliance strategy.
- Advise on Risk, Internal Controls and Policy frameworks.
- Oversee and advise the Executive committee on the current risk exposures of the business and emerging risks.
- Review the company's current risk portfolio profile including;
    - Strategic/Executive Committee level risks.
    - Directorate level risks, including but not limited to sources of risk identified in the Risk Universe (viz: Financial[2], Investment, Strategic, Environment, Reputation and Operational risk).
- Review the overall risk assessment processes that inform management decision making including
    - Business capability to identify and manage current and emerging risks.
    - Qualitative and quantitative metrics used.
    - Parameters used in these measures and the methodology adopted.
    - Accurate and timely monitoring of risk exposures with critical importance.
- Ensure that risk function is properly and timely involved and consulted during all strategic decisions and investments. That such involvement includes evaluation

[2] From time to time the ARC may also invite senior executives to present on risk management in their areas as part of the ARC's oversight role.

POL00183698

of risk being undertaken is within the stated risk appetite. The committee may take independent external advice where appropriate and available.

- Ensure that day to day operational changes and investments have appropriate risk input from key departments such as health and safety, security etc).

3.1 Risk Response

The committee will:

- Review any material breaches of risk limits and the adequacy of proposed action.

- Review actions planned and underway by the business in response to risks raised by the business, the board, internal and external audit and other stakeholders or third parties.

- Review the adequacy and security of the arrangements for its employees and contractors to raise concerns, in confidence including;
    - Arrangements allowing proportionate and independent investigation of such matters and appropriate follow up action.
    - Application of policy and procedures for preventing detecting and responding to fraud and bribery risk[3].

4. Duties and Responsibilities - Compliance

The committee will:

- Review relationships with the regulatory authorities in the UK where appropriate and to review developments and prospective changes in the regulatory environment.

- Review whether satisfactory controls are in place to ensure that customers are treated in accordance with policies and regulatory requirements; and to review any risk mitigation plans arising.

[3] Note: The ARC will, on a periodic basis, assess the company's overall approach to fraud and bribery risks.

POL00183698

- Review significant breaches, or near misses, of regulation and the steps taken to ensure that the underlying root causes of any regulatory control failures are being addressed or prevented.

- Review material or prospective legal actions involving the business, any lessons learned from them about risks and controls being applied where appropriate.

- Review the procedures relating to prevention of financial malpractice, including money laundering and to note any material issues which arise and monitor their resolution.

- Review the adequacy and quality of the Risk & Compliance functions.

5. Committee timetable.

A timetable shall be produced each calendar year showing the current membership of the Committee and the major annual activities of the Committee, in a similar format to that set out in the appendix.

R&CC Membership December 2012

Chairman	Susan Crichton
Members	Christopher Day
	Susan Barton
	Martin Moran
	Lesley Sewell
Secretary	Rob Bolton
Head of Risk & Compliance	Malcolm Staite (interim)
Head of Internal Audit	Malcolm Zack
Business Risk Assurance Manager	Nigel Tuppen

POL00183698

FINAL

TERMS OF REFERENCE FOR THE RISK AND COMPLIANCE COMMITTEE

Appendix[4]

Annual Timetable	**Jan**	**Mar**	**Jun**	**Sept**
1. Risk Management Framework				
Effectiveness of Risk Management Framework			✓	
Review of Risk Policy Framework	✓	✓	✓	✓
Review of Risk Appetite and Tolerances	✓		✓	
Review of Risk Universe			✓	
2. Risk and Compliance portfolio				
20 Top Risks status	✓	✓	✓	✓
Summary Compliance status	✓	✓	✓	✓
3. Internal Control Framework				
Effectiveness of Internal Control Framework Controls Self Assessment process				✓ ✓
4. Other				
Items directed by the Board/ARC/Executive	✓	✓	✓	✓
Risk issues /highlights from Internal Audit	✓	✓	✓	✓
Information Security Risk		✓		
Physical Security			✓	
Fraud Risk				✓
AML	✓			
Data Protection		✓		
5. – Governance				
Annual review of ToR, self assessment			✓	
Effectiveness of 3 Lines of Defence			✓	

[4] **The current timetable sets out standing agenda items. It may be modified by the risk and compliance committee in light of specific requests or actions arising from meetings. The months indicated are provisional and subject to change as are the number of meetings to be called.**