POL00447840

GROUP POLICY

Internal Audit Charter

Version – V0.2

POL00447840

POL00447840

1. Overview

1.1. Introduction by the Standard Owner

The Charter is a formal agreement between the Director of Internal Audit & Risk, the CEO, the Group CFO and the Chair of the Audit, Risk and Compliance Committee (ARC).

1.2. Purpose

This Policy has been established to set out the main purpose of Internal Audit, how the function approaches its work and the rights and arrangements in place to provide quality assurance to the Board and the ARC.

The Policy also sets out an independence policy designed to identify and manage possible conflicts of interest, to ensure Internal Audit remains independent and objective in its work.

1.3. Core Principles

The Charter describes how we apply the ten core principles of the Internal Audit function to the work we do. Our principles, based on guidance from the Chartered Institute of Internal Auditors, are:

1. ***We act with integrity***
2. ***We demonstrate competence and due professional care***
3. ***We are objective and free from undue influence (independent)***
4. ***We are aligned with the strategies, objectives, and risks of Post Office***
5. ***We stay appropriately positioned and adequately resourced***
6. ***We produce high quality results and seek continuous improvement***
7. ***We communicate effectively***
8. ***We provide risk-based assurance***
9. ***Our work is insightful, proactive, and future-focused***
10. ***We promote organisational improvement***

1.4. Application

This Charter covers all activities undertaken by Internal Audit within Post Office Ltd[1] and its subsidiaries.

In exceptional circumstances, where risk sits outside of Post Office Limited's accepted Risk Appetite, a Risk Exception can be granted. For further information in relation to the risk exception process please contact the Risk & Assurance team. GRO

[1] In this Policy "Post Office" and "Group" mean Post Office Limited and any wholly owned subsidiary that formally adopts this policy

POL00447840

Further information in relation to the risk exception process can be found here.

1.5. The Risk

Post Office operates the Three Lines of Defence model in its overall arrangements for managing risks and controls. Internal Audit forms the third line of defence by providing independent assurance over the activities of the first and second lines. Failure to formally agree the position and governance structure of the internal audit function may undermine its ability to provide robust assurance the Board, ARC and Senior Management.

1.6. Professional Standards and Industry Guidance

The work of Internal Audit adheres to the Chartered Institute of Internal Auditors' (CIIA) International Standards for the Professional Practice of Internal Auditing and the International Professional Practice Framework. The COSO (Committee of Sponsoring Organisations of the Treadway Commission) Framework is used as a basis for evaluation of internal controls.

Internal Audit also considers the CIIA's Practice Advisories, Practice Guides, and Position Papers as applicable to guide its work. In addition, Internal Audit adheres to Group policies and its own methodology.

POL00447840

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which Post Office will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that Post Office are willing and able to tolerate.

Post Office have a five scale approach to risk appetite, Averse, Cautious, Neutral, Flexible and Open.

Internal Audit will consider the risk appetite of the relevant business unit when planning, testing and reporting each audit review, in order to assess if controls are designed and operating effectively to manage risks to within the adopted risk appetite.

Post Office acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required. (See section 1.4 for further details)

2.2. Policy Framework

This Charter is a stand-alone policy that is supported by the Internal Audit Methodology document. Internal Audit will, in the first instance, consider policies in use across the business as a baseline for minimum operating standards in areas of review

2.3. Who must comply?

Compliance with this Policy is mandatory for all employees[2] of the Internal Audit function and the wider Post Office Group, as well as staff provided through co-source arrangements.

The access authority granted under this Charter applies to all functions, records, property and personnel at all management levels including the external auditors and contractors insofar as it applies to approved audits, reviews and investigations. Failure to allow or provide access as described will be escalated to the audit sponsor and may result in a limitation of scope reported to the ARC.

Where material non-compliance is identified the matter must be referred to the Policy Owner and Sponsor. Where required, any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that that an instance of non-compliance is caused through wilful disregard or negligence, this may be treated as a disciplinary offence.

The next page sets out the minimum control standards that the Post Office has implemented to control these risks.

---

[2] In this policy "employee" and "staff" means all persons working for the Group or on our behalf in any capacity including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, and contractors.

POL00447840

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks, so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventative which are required to en sure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets the relationships between identified risk and the required minimum control standards.

Risk area	*Description of Risk*	*Minimum Control Standards*	*Frequency*	*Control owner*
Compliance with Charter	*Internal Audit team fail to meet standards described in the Charter due to limitations of:* *a) skills and knowledge*	• *All permanent employees hold a professional qualification relating to audit (such as ACA, CIIA, CIPFA, CIMA, CISA). Membership of these bodies requires a commitment to abide by high standards of professional conduct.*	*Onboarding*	*Director of Internal Audit & Risk*
		• *All individuals provided under the co-source agreement are assessed for, inter alia, an appropriate of level of skill and knowledge to carry out the assignment.*	*Before each assignment*	*Lead Auditor*
		• *All other individuals (secondees, interns, guest auditors etc) are briefed and supervised by a named senior member of the team and overseen by the Director of Internal Audit & Risk.*	*Per engagement*	*Director of Internal Audit & Risk*

POL00447840

Risk area	*Description of Risk*	*Minimum Control Standards*	*Frequency*	*Control owner*
		• *Compliance with standards is considered as part of the annual performance appraisal process.*	*Annual*	*Director of Internal Audit & Risk*
	b) processes and procedures	• *All audits are planned, executed and reported in line with an industry standard internal audit methodology. This is reviewed at least annually against processional standards.*	*Annual*	*Director of Internal Audit & Risk*
	c) independence	• *A running total of co-source audit vs non-audit spend is maintained. All non-audit spend exceeding 80% of the annual IA budget requires ARC approval.* • *The Lead Auditor considers the previous involvement of individuals for possible conflicts.* • *Off-plan requests by the business are assessed for possible current or future independence compromise and approved before the assignment is accepted.*	*Event driven* *Before each assignment* *Event driven*	*Director of Internal Audit & Risk* *Lead Auditor* *Director of Internal Audit & Risk*
	d) budget	• *The budget is based on the proposed annual plan and is approved by the ARC. The Director of Internal Audit & Risk confirms that the function is adequately resourced to carry out its obligations.*	*Annual*	*Director of Internal Audit & Risk*

POL00447840

3. Internal Audit Charter

3.1. The Internal Audit Function

Internal Audit is an independent review function set up within the Post Office organisation as a service to the Board and all levels of management. The Director of Internal Audit & Risk is responsible for assuring the effectiveness of the design and operation of risk management and internal control frameworks throughout the organisation's activities.

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal control, and governance processes.[3]

3.2. Objectives of Internal Audit

- ***Provide the Board with independent and objective assurance over Post Office Group's controls.***
- ***Provide assurance that Post Office processes for identifying, assessing and managing risks are effectively deployed.***
- ***To help management improve their decision making processes, controls and operations through risk and control advice and support.***

3.3. Role and Scope

The role of Internal Audit is to understand the key risks of the organisation and to examine and evaluate the adequacy and effectiveness of the frameworks of risk management and internal control as operated by the organisation.

Internal Audit, will therefore review, appraise, evidence and report on:

a) The adequacy and effectiveness of the frameworks of:
- ***Operational control across the organisation (for example controls over cash processes and outsourced services).***
- ***Financial control.***
- ***Management control.***
- ***Information Security (for example cyber security controls).***

b) The integrity of processes and systems, including those under development, to ensure that controls offer adequate protection against error, fraud and loss.

c) Company policies, standards and procedures, including their effectiveness and appropriateness.

---

[3] Definition of Internal Auditing – Global Institute of Internal Auditors Inc

POL00447840

d) National and International legislation where applicable are effectively recognised and acted upon by the company.
e) The operation of the organisation's corporate governance and risk governance arrangements.
f) Significant aspects of the organisation's activity including major projects and change programmes, and as directed by the ARC.
g) Effectiveness of the organisation's fraud management processes:

- *Management remain responsible for establishing and maintaining systems for the prevention of fraud and theft. However, the internal audit department may be requested to assist in the investigation of significant suspected fraudulent activities and will notify the ARC of the results.*
- *Where regular audit work may reveal fraud risk or actual fraud and irregularities, this will be reported to management, the Risk and Compliance Committee (RCC) and to the ARC.*

h) Other key stakeholders:

The Internal Audit team will liaise, as appropriate, with other providers of assurance including second line of defence functions (including Group Central Risk team), external audit, other external assurance providers (e.g. Bank of England) and assurance providers of partner organisations (e.g. Bank of Ireland).

3.4. Matters specific to Post Office Insurance

POL has agreed with Post Office Insurance (POI) to provide a designated member of the internal audit team (the Auditor) to fulfil the role of an internal audit function for an authorised insurance intermediary, in accordance with the Financial Conduct Authority and the Chartered Institute of Internal Auditors' guidelines and requirements.

All audit work will be carried out as described in the Group Internal Audit Charter. However, the Auditor will report and be accountable to the POI ARC on all POI related matters.

References in the Charter to the 'Group Executive' or 'GE member' should be substituted for 'member(s) of the Executive Committee' in regard to POI. References to the Internal Auditor include the Director of Internal Audit & Risk (or their representative) and the Internal Audit co-source provider.

In addition, it should be noted that POI has its own independent second line risk and compliance function that operates independently of the Group.

POL00447840

3.5. Independence

The internal audit activity, in accordance with CIIA Standard 1100, must be independent in fact and appearance, and internal auditors must be objective in performing their work. Independence is the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. Objectivity requires that internal auditors do not subordinate their judgement on audit matters to others. Threats to independence and objectivity must be managed at the individual auditor, engagement, functional, and organisational levels.

Independence and objectivity is protected in the following ways:

i. Internal Audit has direct and unrestricted access to senior management, the Board and the ARC members.

The Director of Internal Audit & Risk reports functionally to the Chair of the Audit, Risk and Compliance Committee (ARC) who is a Non-Executive Director of the Board, and administratively on a day to day basis to the Group Chief Finance Officer. The Director of Internal Audit & Risk has access to the Board Chairman, Non-Executive Directors and the CEO. The Internal Audit staff report to the Director of Internal Audit & Risk.

ii. Independence and objectivity are assessed before each assignment.

Per the Internal Audit Methodology, the lead auditor is required to assess the independence and objectivity of the audit team (including co-source members) for each assignment undertaken. Consideration is given to:

- ***individuals' previous roles within Post Office, its partners and key suppliers;***
- ***the nature and extent of non-core audit support previously provided to the business, for example attendance (as observers) at steering committees or review of policy and process changes.***

iii. Co-source provider spend on non-IA activity is controlled

A threshold for non-Internal Audit services undertaken by the co-source providers (currently Deloitte and Mazars) is set at 80% of the annual internal audit budget. The ARC must approve any significant work that will result in the threshold being exceeded, to ensure the service remains appropriately independent.

The Director of Internal Audit & Risk will confirm to the ARC, at least annually, the organisational independence of the internal audit activity. If the Director of Internal Audit & Risk determines that independence or objectivity may be impaired in fact or appearance, the details of impairment will be disclosed to the ARC or the appropriate parties.

3.6. Access and Authority

- ***The Post Office Internal Audit team have unrestricted access to all functions, records, property and personnel at all management levels including the external auditors and contractors insofar as it applies to authorised audits, reviews and investigations.***
- ***All members of the Internal Audit team will abide by company and professional standards with regards to confidentiality. Audit files and evidence will be appropriately secured.***

POL00447840

- *Where information is of particular sensitivity, management may request that access to the information be restricted to the Director of Internal Audit & Risk only.*
- *If required access has not been forthcoming and following due process remains as such and this has a significant restriction on the effective completion of an audit, the limitation should be reported. Effort to resolve the situation should be undertaken and only after these steps should such limitations be reported to the Audit, Risk and Compliance Committee (ARC).*

3.7. Reporting on Activity

- *The findings on engagements shall be cleared upwards through line management and to the appropriate GE member. Reports will be summarised for the RCC and ARC, who may request access to the full reports. Reports will also be provided to the CEO, CFO and other stakeholders as appropriate.*
- *Formal reports will be classified as confidential. Access to final reports by individuals not directly associated with the audit, shall be approved by the Director of Internal Audit & Risk and the owning GE member.*
- *A follow-up process will be implemented to track progress with agreed audit actions. The results of follow-ups, including the implementation rate of recommendations and overdue audit actions will be reported to the ARC on a periodic basis.*

3.8. Audit Plan

To develop the risk-based annual audit plan, the Director of Internal Audit & Risk consults with senior management and the board and obtains an understanding of the organisation's strategies, key business objectives, associated risks and risk management processes. The Director of Internal Audit & Risk must review and adjust the plan, as necessary, in response to changes in the organisation's business, risks, operations, programmes, systems, and controls.

- *The Director of Internal Audit & Risk will submit a rolling risk based plan for approval by the ARC, review progress against plan with the ARC quarterly and where necessary amend the plan to reflect changing risk priorities.*
- *The plan will project a maximum of six to twelve months into the future although some areas will require annual review.*
- *The plan will also be made available to the Board and the GE and be flexible to requests from the business that arise during the year.*
- *Audits will generally be planned alongside management and announced, but at times visits, checks and investigations may be unannounced to the business area concerned. This includes all aspects of the group including head office functions.*

3.9. Management Requests

Management may make requests for audits or reviews through the year:

- *Requests will be evaluated in terms of risks and an effort will be made to address these requests wherever possible.*

POL00447840

- *Other than short assignments, the ARC should be informed of proposed changes to the plan especially where this will impact delivery or delay start of currently planned work.*
- *The Chair of the ARC and the Director of Internal Audit & Risk will discuss significant changes to the plan and agree steps with the business.*

3.10. Audit Committee Liaison

- *The Director of Internal Audit & Risk should meet with the Chair of the ARC outside of regular audit meetings, without the presence of management at least twice a year.*
- *The Director of Internal Audit & Risk may meet with any other members of the ARC and with the external audit partner outside of ARC committee meetings.*
- *All members of the committee may request a meeting with the Director of Internal Audit & Risk to discuss risk, control and audit matters.*
- *The Director of Internal Audit & Risk will provide support and guidance where requested to help the ARC committee members discharge their duties.*

3.11. Staffing and Resource

- *The Director of Internal Audit & Risk shall ensure that the department is sufficiently resourced to carry out its duties in terms of professional competency, business knowledge and awareness and technical proficiency. An annual attestation to this effect will be made to the ARC. Additional technical training needed to ensure an audit can be effectively conducted should be arranged.*
- *Specific audit tools to improve efficiency and effectiveness of audits (such as for extraction and analysis of large quantities of data) will be identified and obtained where appropriate.*
- *In coordinating activities, the Director of Internal Audit & Risk may rely on the work of other assurance and consulting service providers. In such instances, the competency, objectivity and due professional care of the assurance and consulting service providers will be considered. The Director of Internal Audit & Risk will obtain a clear understanding of the scope, objectives and results of the work performed by other providers of assurance and consulting services. Where reliance is placed on the work of others, the Director of Internal Audit & Risk is still accountable and responsible for ensuring adequate support for conclusions and opinions reached by the internal audit activity.*
- *In accordance with International Standards of Internal Auditing, the department should not undertake audit work where it does not feel it is sufficiently skilled to do so. In which case, specialised services or staff from either within the organisation or external to it should be considered and sought.*

3.12. Advice and support

Internal Audit should not be required to:

- ***Perform operational duties.***
- ***Operate controls, other than those within the department.***
- ***Approve accounting transactions outside of the department.***

POL00447840

- ***Implement controls that are the responsibility of management.***

It is within normal accepted practice and International Internal Auditing Standards for Internal Audit to be requested to assist in a facilitative or consulting nature. Where this falls within the general remit of advising on risk and control this will be considered part of the service offering, with regard to resources available and time required.

Where it is agreed as appropriate for a member of the Internal Audit team to provide significant input to an activity or project that is beyond the normal remit, which means they should be temporarily seconded to another department or team, then the following measures will apply:

- ***The request will be approved jointly by the Director of Internal Audit & Risk and the Chair of the ARC.***
- ***The resource impact on the approved audit plan should be approved by the ARC who will either approve the reduction in scope to the audit plan or request the Board to approve temporary resource to address the shortfall.***
- ***The work conducted by the seconded member will be the responsibility of the receiving manager, not the Director of Internal Audit & Risk. The work will not be defined as internal audit work.***

3.13. Standards of Audit Practice

The Director of Internal Audit & Risk will implement an audit approach that incorporates the mandatory elements of the CIIA's International Professional Practices Framework (IPPF), being:

- ***Definition of Internal Auditing,***
- ***Code of Ethics, and***
- ***International Standards for the Professional Practice of Internal Auditing (including interpretations and glossary).***

In addition, the approach will be aligned with further Recommended Guidance within the IPPF insofar as it furthers the objectives of the Internal Audit function.

POL00447840

3.14. Approvals

GRO

Director of Internal Audit & Risk — Dated: 21 June 2023

Chief Executive Officer — Dated: _____

Group Chief Finance Officer — Dated: _____

Chair of Audit, Risk and Compliance Committee — Dated: _____

POL00447840

4. Where to go for help

4.1. How to raise a concern

Any Post Office employee who suspects that there is a breach in this Policy should report this without any undue delay.

Post Office employees can raise concerns via:

- ***Your line manager***
- ***A senior member of the HR Team***
- ***Contacting the "Speak Up" line, a confidential reporting service which is run by an independent company, Convercent:***
  - ***Telephone Number:*** GRO
  - GRO ***which is a secure on-line web portal***
- ***Direct to the Whistleblowing Manager*** GRO

4.2. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact Johann Appel GRO

GRO

POL00447840

5. Governance

5.1. Governance Responsibilities

The Policy Sponsor, responsible for overseeing this Policy, is the Group Chief Finance Officer of Post Office Limited.

The Policy Owner is the Director of Internal Audit & Risk, who is responsible for ensuring that the content is up to date and is capable of being executed.

Additionally, the Director of Internal Audit & Risk is responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee as required.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Post Office risk appetite.

POL00447840

6. Control

6.1. Document Control Record

SUMMARY			
GE Policy Sponsor	**Standard Owner**	**Policy Author**	**Standard Approver**
Al Cameron	*Johann Appel*	*Johann Appel*	*RCC/ARC*
Version	**Document Review Period**	**Policy – effective date**	**Policy location**
V0.2	*2023*	*May 2023*	*Key policies (sharepoint.com)*

REVISION HISTORY			
Version	**Date**	**Changes**	**Updated by**
V0. 1	*May 2021*	*Adopting standard group policy format, adding minimum control standards, independence policy and IA principles*	*Charlotte Webster*
V0. 2	*May 2023*	*Minor updates such as job titles. Policy moved to new internal policy template.*	*Johann Appel*

6.2. Oversight Committee: Risk and Compliance Committee / Audit and Risk Committee

Committee	Date Approved
POL R&CC	**09/05/23**
POL ARC	**16/05/23**

Next Policy Annual Review Date: May 2025

POL00447840

6.3. Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.