

Group policy

Enterprise Risk Management

Version 1.0 | Public | March 2025



Contents

1	Overview	3
1.1	Introduction	3
1.2	Purpose	3
1.3	Who Must Comply	4
1.4	Core Principles	4
1.5	Policy Framework	7
2	Where to go for help	8
2.1	Reporting Non-Compliance	8
2.2	Reporting a Concern – How to ‘Speak Up’	8
3	Document control	9
3.1	Document control record	9
3.2	Policy Approval	9
	Appendices	10
	Risk Appetite Categories and Level of Appetite	10
	Risk Appetite Scale	10
	Risk Impact Table	11
	Definitions	12
	Applicable Regulation and Legislation	13
	Governance Responsibilities	14

1 Overview

1.1 Introduction

The Chief Financial Officer has overall accountability to the Post Office Group¹ Board for the design and implementation of controls to prevent and manage the risks associated with Enterprise Risk Management (ERM) policy/framework. It is the responsibility of management to ensure that risks are understood and appropriately managed in accordance with this policy.

Taking and managing appropriate levels of risk is an integral part of all the Company's activities. Risk management, performed rigorously and comprehensively, creates stability by strengthening internal controls, and directly contributes to the achievements of the organisations strategic objectives and to balance the needs of shareholders, postmasters, employees, customers, regulators and other stakeholders.

1.2 Purpose

The purpose of this policy is to ensure the Company maintains a consistent and proportionate risk management process that demonstrates the following:

Effective Corporate Governance: This policy demonstrates how the Company applies a consistent approach to risk management to support the Company's governance responsibilities for responsible risk-taking, which serves the best interest of its key stakeholders (shareholders, postmasters, employees, customers, regulators and other stakeholders).

Effective Risk Management: This policy demonstrates how the Company incorporates a consistent approach to risk management into the culture and strategic planning processes of the Company that supports decision making and resource allocation at both an operational and strategic level. This is achieved by the policy aiming to:

- Ensure that current and emerging risk are identified and understood.
- Ensure appropriate mitigation activities / controls are implemented to manage key risks.
- Establish a transparent approach to reporting risk across the Company through open communication and monitoring of key risks.

The policy is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across Post Office. Compliance with these policies supports the Post Office in meeting its business objectives and to balance the needs of shareholders, postmasters, employees, customers, regulators and other stakeholders.

¹ In this Policy "Post Office" and "Group" means Post Office Limited and its wholly owned subsidiary, Post Office Management Services Limited.

1.3 Who Must Comply

Compliance with this policy is mandatory for all Post Office Limited employees² and applies wherever in the world the Group's business is undertaken.

Where the Post Office holds a supplier relationship with a third party, and it is appropriate for the supplier to adhere to this policy then provisions should be included within their contracts to reflect this along with their own equivalent Policy.

1.4 Core Principles

Post Office's risk management, reporting structures and governance is designed to ensure adherence to the requirements of the UK Corporate Governance Code. The key aspects are summarised below:

Board, is responsible for:

- Ensuring that ERM is used to help inform, develop and achieve the strategic objectives of the Company.
- Setting the risk appetite levels.
- Understanding the nature and magnitude of high-level risks (Enterprise Risk) to which the Company is exposed.
- Annually approving risk management policies to ensure the Company's risk exposures remain appropriate.

Chief Executive Officer (Group CEO), is responsible for:

- Ensuring all executive risk owners integrate ERM into the development of strategic plans and operational decisions.
- Reporting on the Company's risk profile to the Board of Directors and the Audit, Risk and Compliance Committee (ARC).

ARC, is responsible for:

- Reviewing management's assessment and assertions against high level risks (Enterprise Risk).
- Ensuring risk management processes are in place for the measurement, monitoring and reporting of the Company's high-level risks (Enterprise Risk).
- Agreeing the risk appetite levels.
- Annually reviewing risk management policies to ensure the Company's risk exposure remain appropriate.
- Reporting to the Board on risk exposure levels.

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, agency workers, volunteers, interns, and contractors.

Executive Management is responsible for:

- Reviewing emerging risks, prioritising identified risks, approving risk treatments and ensuring sufficient allocation of resources to implement risk treatments.
- Reviewing the results of risk treatments and updating the Enterprise and Intermediate risk in preparation for ARC reporting, especially for risk outside of extended appetite.
- Ensuring ERM is integral to strategic goal setting and decision making.
- Ensure the implementation sound risk management practices and positive risk culture in all Company's activities.

Risk and Compliance Committee (RCC) is responsible for:

- Identifying emerging high-level risks, prioritising mitigations for identified high-level risks, approving risk treatments and ensuring sufficient resources allocated to implement risk treatments.
- Monitoring the results of risk treatments, reviewing and updating the Enterprise and Intermediate risk registers in preparation of ARC reporting.
- Ensuring that the ERM Policy and Process documentation are maintained and that the ERM process is performed by all Functions.
- Reviewing, monitoring and approving risk sitting outside of risk appetite.
- Reporting to Executive and ARC on risk exposure.

Group Risk and Assurance (GRA), are responsible for:

- Facilitating the implementation of the ERM Policy and Process by Risk Owners and Executive Management.
- Developing the Company's ERM Framework, in line with industry best practice, to efficiently and effectively identify, assess and mitigate risks.
- Facilitate Risk reporting to Executive and ARC.

Risk Owners, are responsible for:

- Ensuring the ERM process is followed including regular horizon scanning for new and emerging risks and updating the Intermediate Risk and Control Registers.
- Implement risk treatments to bring Intermediate Risk within risk appetite.
- Ensuring controls are designed appropriately and remain fit for purpose.
- Advising their Executive of any risk that cannot be managed within risk appetite and where appropriate, ensuring a formal risk acceptance is approved.

Reporting

GRA (via challenge and review from the RCC) will on a periodical basis submit a report to ARC. The report should provide appropriate information on the following:

- Nature and magnitude of Enterprise Risks.
- Metrics in place to review and support risk assessments.
- For Enterprise Risk outside of extended risk appetite, managements plans to remediate.
- Trends in high-risk areas and changes to risk management activities.

- Emerging risks.
- Material risks that have been risk accepted by Management.
- Exceptions to the Company's ERM policy.

The ARC will report to the Board on its review of risk management activities.

Strategic Outcomes

This Policy is focused on managing the risks of Post Office associated with its strategic outcomes: 'Strengthen the Commercial proposition', 'Ensure the Network is fit for purpose', 'Transform technology and data', 'Deliver a new operating model' and 'Reset relationships with Postmasters'.

Such focus increases the probability of success of achieving the strategic outcomes.

Risk Appetite and Extended Risk Appetite

- Risk Appetite refers to the amount of risk Post Office is willing to operate within, in order to achieve its strategic objectives.
- Extended Risk Appetite is the maximum risk the Company is willing to take, usually for a limited period of time before mitigations are required to reduce the level of risk back to Risk Appetite. Alternatively, risks are escalated for risk acceptance where the Company believes that the risk will continue to remain outside of extended risk appetite despite implementing all mitigations within its authority.

The Board will agree the risk appetite and extended risk appetite levels for each category of risk as part of the annual review of the ERM Policy. Risk appetite approval refers to a formalised statement that outlines the willingness to accept risk in pursuit of its objectives, guiding how risks are managed effectively. (**Appendix 1**). Risk appetite statements include a risk appetite scale which has several acceptance levels, ranging from avoidance of risk, through to taking justified risk (**Appendix 2**). The level of risk we are willing to accommodate will vary depending on individual risk scenarios. Risk appetite can and will change over time, sometimes rapidly as economic and business environment conditions change, and therefore the statements are evolving.

We rigorously identify and assess risks, agree our appetite for those risks, and then manage them accordingly. When assessing risks and deciding on the appropriate response we consider the potential impacts and harms these risks could have on our key stakeholders (shareholders, postmasters, employees, customers, regulators etc.).

Risk Management and Control Framework

The risk management and control framework are a combination of processes by which the Group identifies, assesses, measures, manages and monitors the risks that may impact the successful delivery of its strategic objectives and its ability to meet obligations towards key stakeholders (shareholders, postmasters, employees, customers, regulators, etc.). Based upon our risk appetite, the risks identified are either accepted or appropriate actions are taken to mitigate them. Risk assessment is guided by the risk impact table (**Appendix 3**), which offers the risk owner clear measurement criteria to evaluate the impact of their risk.

The ERM framework incorporates the following core elements:

Identify

- Recorded by each business function
- Risk mapping to identify new or emerging themes

Assess

- Determining the likelihood of the identified risk
- Evaluating the potential impact

Respond

- Agreeing proportionate actions to manage the identified risks
- Identifying existing controls

Monitor

- Review the effectiveness of controls
- Maintaining continued oversight and tracking

All Post Office risks (across all levels of the risks hierarchy – Enterprise, Intermediate and Local) must be identified, analysed, evaluated, managed and recorded.

1.5 Policy Framework

The Group Enterprise Risk Management Policy (the “Policy”) is reviewed and updated annually (or more frequently as necessary) to ensure ongoing relevance and compliance with regulatory or legislative changes and to reflect any lessons learned from both internal and external events.

This policy is classified as a Group Key Policy. It is therefore subject to annual review and endorsement at the Risk and Compliance Committee (R&CC), the Audit, Risk and Compliance Committee (ARC) and Board where appropriate. Thereafter, it is adopted by Post Office Limited and its wholly owned subsidiary³.

³ This refers to Post Office Management Services Limited, which is an FCA regulated principal.

2 Where to go for help

2.1 Reporting Non-Compliance

Where non-compliance is identified, the matter must be referred to the Policy Owner, which is the Group Director of Assurance and Risk. Where required, any investigations will be carried out in accordance with the Investigations Policy.

Where it is identified that an instance of non-compliance is caused through wilful disregard and / or negligence, this may be treated as a disciplinary matter.

2.2 Reporting a Concern – How to ‘Speak Up’

Post Office strive to foster an environment where everyone feels comfortable speaking up. Post Office encourages anyone to raise concerns about wrongdoing, illegal activities, or unethical behaviour.

Information and contact details:

Confidential reporting Speak Up service:

- Telephone Number: 0800 041 8159
- <http://speakup.postoffice.co.uk/> which is a secure on-line web portal
- Via email: speakup@postoffice.co.uk



3 Document control

3.1 Document control record

Summary

Version	Document review period	Policy – effective date	Policy location
1.0	Annual	March 2025	https://corporate.postoffice.co.uk/en/governance/our-structure/useful-corporate-information/


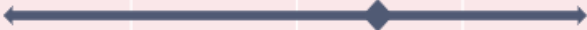







3.2 Policy Approval

Committee	Date approved
POL R&CC	10/03/25
POL ARC	25/03/25
BOARD	15/04/25

Next policy annual review date: March 2026

Appendices

Risk Appetite Categories and Level of Appetite

Category	AVERSE	MINIMAL	CAUTIOUS	FLEXIBLE	OPEN
Data & Information Management (cyber)					
Business Change & Transformation (project/programme)					
Strategy					
Financial					
Operations					
People *					
Legal & Regulatory					
Reputation					
Commercial					



Risk Appetite



Extended Risk Appetite

* Includes postmasters

Risk Appetite Scale

Rating	AVERSE	MINIMAL	CAUTIOUS	FLEXIBLE	OPEN
Philosophy	"Sacred" Avoidance of risk is a core objective	Extremely conservative	Preference for safe delivery	Will take strongly justified risks	Will take justified risks
Tolerance for uncertainty	Extremely low	Low	Limited	Expect some	Fully anticipated
Choice when faced with multiple options	Will select the lowest risk option, always	Will accept only if essential, and limited possibility/extend of failure	Will accept if limited and heavily out-weighted by benefits	Will choose to put a risk, but will manage impact	Will choose option with highest return: accept possibility of failure
Trade-off against achievement of other objectives	Never	With extreme reluctance	Prefer to avoid	Willing under the right conditions	Willing

Risk Impact Table

(i) IMPACT SCALE

Impact	Strategic Execution	Financial ¹	Commercial ¹	Operations/Service Disruption	People / Health and Safety ¹	Legal and Regulatory ¹	Reputation ²
Minor (1)	<ul style="list-style-type: none"> No impact on programme RAG status 	<ul style="list-style-type: none"> Impact on operating cost of <€100k Fraudulent activity resulting in a loss of <€1k 	<ul style="list-style-type: none"> No or immaterial impact on sales No or immaterial impact on Postmaster Remuneration 	<ul style="list-style-type: none"> No disruption to customer facing operations & services No Internal disruptions including PM Journeys 	<ul style="list-style-type: none"> No injuries or minor first-aid cases. Increase in employee turnover <1% Increase in Absence rates <1% 	<ul style="list-style-type: none"> No breach in law or regulations No public censure 	<ul style="list-style-type: none"> Minor negative stakeholder reaction
Moderate (2)	<ul style="list-style-type: none"> Programme RED RAG status <2 	<ul style="list-style-type: none"> Impact on operating cost of €100k – €250k Fraudulent activity resulting in a loss of €1k – €50k 	<ul style="list-style-type: none"> Moderate impact on sales £1M – £3M (0.1% - 0.3% of sales) Moderate impact on Postmaster remuneration <€2M (<0.4% of Postmaster Remuneration) 	<ul style="list-style-type: none"> Moderate disruption to customer facing operations & services <1 hour Moderate disruption to internal systems including PM journeys <1 hour 	<ul style="list-style-type: none"> Injuries requiring hospitalisation/period off work Potential H&S fine and employee compensation <€250k Increase in employee turnover <5% Increase in absence rates <3% 	<ul style="list-style-type: none"> Technical breach in law or regulations Public censure / fine < €250k 	<ul style="list-style-type: none"> Moderate negative stakeholder reaction (<24hrs) Moderate impact on reputation or organisation and stakeholders
Major (3)	<ul style="list-style-type: none"> Programme RED RAG status 2 - 5 	<ul style="list-style-type: none"> Impact on operating cost of €250k – €500k Fraudulent activity resulting in a loss of €50k – €500k 	<ul style="list-style-type: none"> Major impact on sales £3M – £10M (0.3% - 1% of sales) Major impact on Postmaster remuneration £2M – £5M (0.4% - 1% of Postmaster Remuneration) 	<ul style="list-style-type: none"> Major disruption to customer facing operations & services 1 – 2 hours Major disruption to internal systems including postmaster journeys 1 – 2 hours 	<ul style="list-style-type: none"> Injuries requiring hospitalisation (>1 day)/period off work Potential H&S fine and employee compensation £250k – €500k Increase in employee turnover <10% Increase in absence rates <5% Potential for operational disruption <3 days 	<ul style="list-style-type: none"> Major breach in law or regulations Public censure / fine £250k – €500k 	<ul style="list-style-type: none"> Major negative stakeholder reaction <3 days Increasing concerns notable with key stakeholders
Significant (4)	<ul style="list-style-type: none"> Programme RED RAG status 5 – 10; requiring critical adjustments otherwise strategy invalid Organisation still commercially and operationally viable 	<ul style="list-style-type: none"> Impact on Operating cost of €500k – €750k Fraudulent activity resulting in a loss of €500k – €750k 	<ul style="list-style-type: none"> Significant impact on sales £10M – £20M (1% to 2% of sales) Significant impact on Postmaster remuneration £5M – £10M (1% - 2% of Postmaster Remuneration) 	<ul style="list-style-type: none"> Significant disruption to customer facing operations & services >2 hours Significant disruption to internal systems including PM journeys >2 hours 	<ul style="list-style-type: none"> Fatality or severe life changing injury(s) Potential H&S fine and employee compensation £500k – €750k Increase in employee turnover <15% Increase in absence rates <7% Potential for operational disruption <6 days 	<ul style="list-style-type: none"> Significant breach in law or regulations Public censure / fine £500k – €750k 	<ul style="list-style-type: none"> Long running negative stakeholder reaction < 1 week Requires significant management and involvement of key stakeholders Significant loss of trust with key stakeholders
Critical (5)	<ul style="list-style-type: none"> Programme RED RAG status >10; requiring critical adjustments otherwise strategy invalid Threatens the commercial and operational viability of the organisation 	<ul style="list-style-type: none"> Impacted on Operating cost of >€750k Fraudulent activity resulting in a loss of >€750k 	<ul style="list-style-type: none"> Critical impact on sales >€20M (>2% of sales) Critical impact on Postmaster remuneration >€10M (>2% of Postmaster Remuneration) 	<ul style="list-style-type: none"> Critical disruption to customer facing operations & services >12 hours Critical disruption to internal systems including PM journeys >12 hours 	<ul style="list-style-type: none"> Fatalities or multiple severe life changing injuries requiring hospitalisation Potential H&S fine and employee compensation >€750k Increase in employee turnover >15% Increase in absence rates >7% Potential for operational disruption >6 days 	<ul style="list-style-type: none"> Critical breach in law or regulations Public censure / fine > €750k 	<ul style="list-style-type: none"> Prolonged negative stakeholder reaction > 1 week Requires significant management and involvement of key stakeholders Loss of credibility / Trust with key stakeholders

¹ All figures are annualised impacts, unless a risk is considered a one-off exposure, for instance a regulatory fine.

² Stakeholders include Shareholder, Postmasters, Media, Regulators, Customers, Clients, Partners, Suppliers etc.

(ii) LIKELIHOOD SCALE

	Options
1	Very unlikely <1% (once in every 100 years) Rare, may occur in exceptional circumstances, no or little experience of similar event
2	Unlikely 1% - 10% (once in every 10 years) Might occur at some point.
3	Possible 10% to 20% (once in every 5 years) Could reasonably occur.
4	Likely 20% - 50% (once in every 2 years) Will probably occur.
5	Very likely >50% (every year) High expectation it will occur, almost certain

Definitions

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, agency workers, volunteers, interns, and contractors.

Board: The Board is collectively responsible for setting Post Office’s strategic direction and primary business objectives. It establishes a robust governance framework and ensures that the Company has financial and human resources required to achieve its agreed objectives. It is chaired by a non-Executive Director.

Audit Risk Committee (ARC): The ARC is a Committee of the Board from which it derives its authority. It provides oversight of Post Office’s Group’s risk management systems, operational controls and key systems, including monitoring exposures to the Group Risk Appetite.

Executive Group: The Executive Group comprises the most senior members of the Leadership Team under the authority of the Group Chief Executive Officer. It assists the Group Chief Executive Officer in the performance of his or her duties for the day-to-day running of the business of the Company.

Risk Compliance Committee (RCC): The RCC is a standing committee of the Executive Group. 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. 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.

Subsidiary: This refers to Post Office Management Services Limited, which is an FCA regulated principal.

Enterprise Risk: If the risk materialised the business could not operate – owned by Executive Team.

Intermediate Risk: These are sub-risks linked to enterprise risk. The key risks faced by individual business units; key processes that could destabilise the business, trending thematic at a local level – risk owned by Senior leaders/leadership members.

Local Risk: These are sub-risks linked to intermediate risks. Often more specific, local risks faced by individual subsidiary departments.

Applicable Regulation and Legislation

The policy is aligned with the following industry standards and guidance:

COSO Enterprise Risk Management–Integrated Framework (2017): Addresses the evolution of enterprise risk management and the need for organisations to improve their approach to managing risk to meet the demands of an evolving business environment.

COSO Internal Control – Integrated Framework (2013): An Integrated Framework which helps organisations design and implement internal control.

ISO 31000: A family of standards relating to risk management codified by the International Organization for Standardisation.

The UK Corporate Governance code (formerly known as the Combined Code): Part of UK company law with a set of principles of good corporate governance aimed at companies listed on the London Stock Exchange. It is overseen by the Financial Reporting Council.

The UK Government Orange book: Management of Risk - Principles and Concepts builds on the original Orange Book to help improve risk management further and to embed this as a routine part of how the UK Government manage risk.

Governance Responsibilities

The Policy Sponsor responsible for overseeing this Policy is the Chief Financial Officer. The Policy Owner is the Group Director of Assurance and Risk who is responsible for ensuring that the content is up to date and is capable of being executed. The Group Director of Assurance and Risk is also responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee as required.

The Audit, Risk and Compliance Committee is responsible for approving the Policy and overseeing compliance.

Additionally, the Policy Owner will ensure that the policy is implemented in practice and will inform the owners of other impacted policies where new or significant changes are made to this policy.

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718, respectively. Registered Office: 100 Wood Street, London, EC2V 7ER

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.