



## **GROUP POLICY**

---

# **Risk Management**

**Version 1.5**





<b>1. Overview</b>	<b>4</b>
1.1. Introduction	4
1.2. Purpose	4
1.3. Core Principles	5
1.4. Application	5
1.5. Industry Guidance	5
1.6. Policy Risks	6
<b>2. Risk Governance</b>	<b>8</b>
2.1. Structure	8
2.2. Roles and Responsibilities	8
2.3. Risk Reporting	8
<b>3. Risk Strategy</b>	<b>10</b>
3.1. Strategic Objectives	10
3.2. Risk Appetite	10
3.3. Policy Exceptions	11
<b>4. Risk Management Framework</b>	<b>12</b>
4.1. Post Office Risk Management Framework	12
4.2. Risk Articulation	12
4.3. Risk Hierarchy and Classification	13
4.4. Risk Ownership	13
4.5. Harm Table and Control Effectiveness	13
4.6. Governance, Risk & Compliance (GRC) tool	13
<b>5. Policy Framework and Minimum Control Standards</b>	<b>14</b>
5.1. Policy Framework	14
5.2. Who must comply?	14
5.3. Minimum Control Standards	16
<b>6. Where to go for help</b>	<b>20</b>
6.1. Additional Policies	20
6.2. How to raise a concern	20
6.3. Who to contact for more information?	20
<b>7. Governance</b>	<b>21</b>

Post Office Limited - Document Classification: INTERNAL

7.1. Governance Responsibilities .....	21
7.2. Tools .....	21
7.3. Definitions.....	21
<b>8. Document Control .....</b>	<b>23</b>
8.1. Document Control Record .....	23
8.2. Oversight Committee.....	23
8.3. Company Details.....	23
8.4. Appendix A: Risk Appetite scale .....	24
8.5. Appendix B: HARM table .....	25

---

# 1. Overview

---

## 1.1. Introduction

The Chief Finance Officer has overall accountability to the Board of Directors to ensure that the Post Office actively monitors and strengthens its approach to risk management and promotes a consistent risk-intelligent culture.

Post Office must balance the need to provide essential services to our customers whilst maintaining and enhancing profitability, but also ensuring a strong commercial proposition for Postmasters within our network. Post Office is, and will continue to be, exposed to many sources of risk as a result of its various activities, external environment in which it operates and greater scrutiny from regulators, legislators and Government.

Failure to effectively manage risks will adversely impact Post Office's ability to deliver its business strategy, will undermine the protection and preservation of its reputation and brand, and the delivery of consistent, high-quality services.

In doing so, Post Office acknowledges that risk exists in everything it does. So, everyone in the organisation has a duty of care to manage these risks. However, risk management is as much about exploiting opportunities as it is about managing threats. Given this, Post Office will inevitably take a certain amount of risk in order to achieve its strategic objectives.

This Policy (with its clear principles and mandatory minimum control standards) is an important reference document in managing risks efficiently and effectively.

## 1.2. Purpose

The Policy has been established to set the minimum operating standards relating to enterprise risk management throughout Post Office.<sup>1</sup> It 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, employees and other stakeholders.

This Policy is organised around three areas:

- **Risk Governance:** This focuses on how Post Office risk management activity is organised. It describes (i) the relevant Committees (and their respective roles with regard to risk and how they interact) and (ii) the '3 lines of defence' risk management model (and where accountability and responsibility are placed within it);
- **Risk Strategy:** This focuses on Post Office's overall approach to risk management. It describes how risk management activities are aligned to the Post Office's strategic objectives, the level of risk exposure (appetite) that is acceptable and policy exceptions; and,
- **Risk Management Framework:** This defines the risk management activities that must be undertaken, how they will be undertaken and their frequency.

The Policy also outlines the minimum control standards that apply to each of these areas.

It is supported by a set of Guidelines which provides additional detail and practical guidance for the business to support the consistent and robust identification and management of risk and opportunities across the organisation. It is also underpinned by a corporate Governance, Risk and Compliance (GRC) tool<sup>2</sup>.

This Policy, the Guidelines and the supporting material are accessible on Post Office's Central Risk intranet site (<https://poluk.sharepoint.com/sites/Risks>).

---

<sup>1</sup> In this Policy "Post Office" means Post Office Limited and any wholly owned subsidiary.

<sup>2</sup> ServiceNow Advanced Risk Management and Policy & Compliance modules



### 1.3. Core Principles

The Post Office Risk Policy principles are based on ISO:31000 (Risk Management – Principles and Guidelines).<sup>3</sup> They also have regard to the UK Corporate Governance Code (Guidance on Risk Management, Internal Control and Related Financial and Business Reporting).<sup>4</sup> There are 7 principles:

- Risk management is fundamental to how Post Office is directed, managed and controlled at all levels;
- Risk management must be embedded in all Post Office activities. Its underlying risk culture and approach is key to effective decision making;
- Risks identified must be recorded on the corporate GRC tool and should continually be assessed, monitored, managed and reported at an individual and aggregate level;
- Risks will be considered for escalation to GE, RCC and ARC if they impact delivery of strategic priorities;
- Risk management processes must be aligned and integrated with the delivery of the Post Office's strategy and in such a way that supports an enterprise wide approach;
- Risk management must follow a consistent, transparent and auditable methodology and proactively recognise external factors, opportunities, and uncertainties;
- Risk reporting must allow for the effective review, challenge and monitoring of risk exposure against Post Office's approved risk appetite; and,
- Risk Governance must adhere to the industry standard '3 lines of defence' model to ensure clear accountability and appropriate segregation of duties.

### 1.4. Application

The Policy is applicable to areas within Post Office Ltd and its subsidiaries<sup>5</sup> and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the various Risk Appetites.

Post Office Management Services Limited is required to have a separate risk governance framework as part of its FCA authorisation, but their policy and approach will be aligned to the risk requirements of Post Office Limited and will continue to comply with the principles of this Group Risk Policy.

### 1.5. Industry Guidance

This Policy is aligned with the following industry standards and guidance:

**The Committee of Sponsoring Organizations of the Treadway Commission (COSO):** A joint initiative of five professional organisations seeking to improve performance by developing leadership that enhances internal control, risk management, governance and fraud deterrence.

**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 Standardization.

---

<sup>3</sup> ISO 31000 is a family of standards relating to risk management codified by the International Organization for Standardization .

<sup>4</sup> The UK Corporate Governance code, (formerly known as the Combined Code) is 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.

<sup>5</sup> Post Office Limited is wholly owned by the Department for Business, Energy and Industrial Strategy (BEIS). Its business consists of the core products and services provided by Post Office Group (mails, government services (including identity & licences) and retail), as well as selling the services of Group Companies, Post Office Insurance and Payzone Bill Payments Limited.



**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.

## 1.6. Policy Risks

### Risk Governance

- Due to the lack of engagement between the GE members and Central Risk Team, there is a risk that the Group Executive (GE) is unable to fulfil its responsibility of having an understanding of risks facing Post Office (including new and emerging risks), which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.
- Due to capacity and resourcing within the Central Risk Team, there is a risk that the RCC, ARC and Board are unable to fulfil their responsibilities of providing oversight, challenge and approve the direction of risks facing Post Office (including new and emerging risks), which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.

### Risk Strategy

- Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1st line do not refer to the Post Office Risk Appetite, where approved, when completing the risk assessments, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.
- Due to capacity and resourcing within the Central Risk Team, there is a risk that the Risk Appetite statements are not periodically reviewed and approved by ARC, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.
- Because the risk management knowledge and culture are not consistent across the business, there is risk that the risks outside Appetite are not periodically monitored by the GE, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.
- Due to failure of the business to identify and mitigate risk at an early stage, there is a risk that the business departs from an approved Policy, which may result in Post Office failing to achieve its strategic objectives and leading to reputational damage, regulatory breach, financial loss and/or customer impact.
- Because the knowledge and culture of the policy exception process is not consistent across the business, there is a risk that the Post Office Policy Exceptions are not reviewed, updated and managed to closure, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.
- Due to capacity and resourcing within the Central Risk Team, there is a risk that the GE is unable to fulfil its responsibility of having visibility on the open Post Office Policy Exceptions, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.

### Risk Management Framework

- Because the risk management knowledge and culture are not consistent across the business, there is a risk that the GE and Post Office 1st line fail to proactively identify, assess, own and manage their risks and/or maintain their associated internal control measures, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.
- Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1st line fail to articulate their risks in terms of their cause(s), the risk event itself and their impact, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.
- Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1st line fail to proactively monitor, action and update the treatment of risks,



which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.

- Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1st line overstate the effectiveness of controls, thereby understating the residual risk likelihood and impact, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.
- Due to capacity and resourcing within the Central Risk Team, there is a risk that Post Office HARM table and Group Risk Management Policy are not reviewed to ensure changes to Post Office strategic objectives and the external risk landscape are reflected. This may result in Post Office failing to achieve its strategic objectives and/or leading to reputational damage, regulatory breach, financial loss and/or customer impact.
- Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1st line fail to score their risks in accordance with the Post Office HARM table, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.
- Due to capacity within the Central risk team and business priorities, there is a risk that Post Office 1st line are insufficiently trained on risk management and operation of the corporate GRC tool, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.



## 2. Risk Governance

Post Office's Risk Governance focuses on how Post Office risk management activity is organised.

### 2.1. Structure

The Post Office risk management structure consists of the:

- **Board**<sup>6</sup>, informed and advised by the Audit, Risk & Compliance Committee (ARC). They have overall accountability for the assessment and management of risk, taking a strategic view of the risks faced by Post Office;
- **ARC**<sup>7</sup>: They support the Board in its assessment and management of risks. The ARC reviews Post Office's risk policy, risk appetite and attitude to risk to ensure these are appropriately defined and communicated so that parameters and expectations are understood;  
**Group Executive (GE)**<sup>8</sup>: The GE, led by the Chief Executive Officer, has operational responsibility for Post Office risk management and systems of internal control; and,
- **RCC**<sup>9</sup>: They support the Group Executive in fulfilling its responsibilities for the effective oversight of risk management, internal control and assurance, and compliance. The RCC reviews the information, plans and recommendations that are subsequently presented to the ARC.

### 2.2. Roles and Responsibilities

Post Office follows the industry standard '3 lines of defence' model with regard to risk management governance, compliance and oversight. This means:

- The **GE and their Business Units** perform the **1<sup>st</sup> line function**. They are accountable for identifying, assessing, owning and manage their risks. They are also accountable for the design, implementation and maintenance of the associated internal control measures;
- The **Central Risk** team perform the **2<sup>nd</sup> line function**. They oversee the corporate approach to risk management. This involves defining and implementing risk standards, policies, procedures and guidance. They also assist the 1<sup>st</sup> line function in the risk management activities in line with good practice as well as monitor compliance and effectiveness. Furthermore, they are accountable for reporting to the RCC, GE and ARC on Post Office risk performance, as well as advising on emerging risks and changing risk scenarios; and,
- **Internal Audit**, who operate independently of 1<sup>st</sup> and 2<sup>nd</sup> line functions, are the **3<sup>rd</sup> line**. They provide an independent evaluation of the adequacy and effectiveness of Post Office's control framework. An independent evaluation of risk management framework, and governance is undertaken by a 3<sup>rd</sup> party to ensure independence is maintained.

### 2.3. Risk Reporting

All Post Office risks must be monitored, reviewed and recorded regularly to determine whether, or not, the corporate risk profile has changed and to gain assurance that risks are managed effectively. Such regular (and incremental) reporting has several benefits including:

- ensuring responses are effective and efficient;
- building up knowledge to improve risk identification and analysis;
- providing a better link between risks and objectives, key dependencies, core processes and stakeholder expectations;

<sup>6</sup> 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.

<sup>7</sup> 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.

<sup>8</sup> The GE is a Committee of Post Office senior management responsible for day to day Post Office operational management.

<sup>9</sup> 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. 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.



- detecting and preparing for changes and trends in existing risks, including the extent to which risks are aligned with approved appetite;
- identifying and preparing for new and emerging risks; and,
- identifying good risk management practice, building on it and disseminating it to other parts of the organisation.

Post Office has in place a reporting cycle for Enterprise, Intermediate and Local risks (see section 4.3). Risk Dashboards are produced by the Central Risk team for each GE member. A Risk Update is submitted to every RCC and ARC bi-monthly. These reports include the latest position of enterprise, intermediate and local risks outside of appetite (including new and emerging risks). The data is taken directly from the Post Office's GRC tool<sup>10</sup> which provides a 'single source of truth'. Risks are escalated to the GE members through these dashboards.

A risk deep-dive occurs on a 6-monthly rotational cycle for each Business Area. It helps to identify and improve specific areas of risk and focuses on areas of key risks. However, all risks that are considered to have an impact on Post Office strategic objectives are also reported on a bi-monthly basis as per above paragraph.

For the Inquiry Programme, risks are managed through the Inquiry Steering Committee which meets fortnightly, and the papers include a risk and MI pack, with key risks called out for discussion at the start of each meeting. The reason for needing a separate regime for tracking and managing the risks within the Inquiry Programme is the confidentiality regime imposed by the Inquiry itself. This regime seeks to protect the Inquiry's confidential information by restricting access to that information to anyone that is not signed up to the confidentiality regime.

---

<sup>10</sup> For Post Office Insurance (POI), all risks at intermediate and local level are no longer recorded within the corporate GRC tool and managed independently by POI. POI provides POL with all key risks that are reported to the POI ARC, on a bi-monthly basis, in line with the RCC and ARC reporting timeline.

### 3. Risk Strategy

The Post Office's Risk Strategy focuses on Post Office's overall approach to risk management. This includes risk policy, guidelines, appetite and the techniques by which Post Office assess risks as well as the key priorities.

#### 3.1. Strategic Objectives

This Policy is focused on managing the risks and opportunities of Post Office associated with its strategic purpose of 'We're here, in person, for the people who rely on us'. Such focus increases the probability of success of achieving the strategic objectives.

#### 3.2. Risk Appetite<sup>11</sup>

Post Office has in place a series of risk appetite statements to:

- allow the Board, ARC, GE and RCC to understand the organisation's aggregated levels of risk to determine acceptability or not;
- provide further assurance that the strategic objectives will be secured and early warning where these are under threat;
- allow the business to focus limited resource to manage risks outside of risk appetite thresholds;
- support management in making decisions with an understanding of the degree to which the business is exposed to the consequences of a risk event;
- flex and adapt to the changing business environment; and,
- provide agreed tolerable risk levels, that Post office is willing to operate in given current funding constraints. However, all risks should be managed within the agreed risk appetite.

The Post Office's approach is based on industry-standard principles<sup>12</sup> namely:

- Scope: Risk appetite are primarily articulated at the enterprise risk level and guide/shape the management of linked intermediate and local risks;
- Complex: Risk appetites are complex given that excessive simplicity, while superficially attractive, is counter-productive;
- Measurable: Risk appetites are measurable so are based on relevant, accurate and readily available existing data;
- Flexible: Risk appetites are not single, fixed concepts. There will be different (and tailored) appetites for different enterprise risks; and,
- Manageable: The approach considers Post Office's risk management capability and the organisation's willingness and capacity for taking risks and level of maturity in managing them.

The ARC will approve all Risk Appetite Statements. They may also request, as necessary, the GE to support the articulation of additional Risk Appetite Statements as well as seek assurance Post Office is adhering to the approved Risk Appetite Statement thresholds.

The Post Office's '3 lines of defence' risk management oversee its Risk Appetite as follows:

1 <sup>st</sup> Line	GE	<ul style="list-style-type: none"> <li>• Effectively and clearly communicate goals and objectives, strategy, achievement metrics, and relevant time periods for pursuing the objectives related to developing risk appetite statements.</li> <li>• Set the Risk Appetite levels that ensure enough risk is being taken to ensure Post Office strategic objectives are met.</li> <li>• Secure Group consensus on statements and approach.</li> <li>• Commission revisions of Risk Appetite Statements as needed.</li> </ul>
	Individual Business Units and subsidiary Departments	<ul style="list-style-type: none"> <li>• Validate or raise concerns about the ongoing viability of existing Risk Appetite Statements approved by the GE /Board.</li> <li>• Monitor adherence to Risk Appetite Statements that apply to the Group.</li> </ul>

<sup>11</sup> Risk Appetite is the amount of overall risk an organisation is willing to pursue (or retain) to achieve the relevant strategic objective.

<sup>12</sup> Institute of Risk Management: Risk Appetite & Tolerance Guidance paper – 9/2011. Gartner: Ignition Guide to Drafting and Operationalizing Risk Appetite – 2/2020



2 <sup>nd</sup> Line	Central Risk	<ul style="list-style-type: none"><li>• Produce and implement Post Office Risk Management policy/standards procedures and guidance.</li><li>• Develop (in discussion with 1<sup>st</sup> Line) initial set of corporate Risk Appetite Statements.</li><li>• Oversee the corporate approach to risk management.</li><li>• Assist the 1<sup>st</sup> line function in the risk management activities in line with good practice as well as monitor compliance and effectiveness.</li><li>• Accountable for reporting to the GE, RCC, and ARC on Post Office risk performance, as well as advising on emerging risks and changing risk scenarios.</li></ul>
3 <sup>rd</sup> Line	Internal Audit	<ul style="list-style-type: none"><li>• Developing an annual audit plan based on identified risks and priorities.</li><li>• Conducting audits and reviews to examine and evaluate the adequacy and effectiveness of the frameworks of 1<sup>st</sup> line risk management, internal controls, processes and systems, and compliance with policies and regulations.</li><li>• Ensuring that corrective actions are taken in response to audit findings and monitoring their implementation.</li><li>• Report to RCC and ARC on its findings, particularly around areas of non-compliance.</li></ul>

Post Office assess risk appetite against a 5-tiered scale (8.4).

### 3.3. Policy Exceptions

A Policy Exception is required when the business wishes to operate outside of agreed policy and regulations.

Anyone in the business can request a Policy Exception. However, the Policy Exceptions should not be considered a normal part of business and it should only be raised when all other alternative options have been exhausted with discussions involving senior decision makers.

A Policy Exception Note (PEN) form needs to be completed by the Exception owner and approved by the GE member (or delegate GE-1) of the Business Area and the GE Policy Owner. Once approved, a copy of the PEN should be sent to the relevant Risk Business Partner (RBP).

For further information refer to the PEN form and "How to Guide" document [here](#) or contact your Business Unit Risk Business Partner.

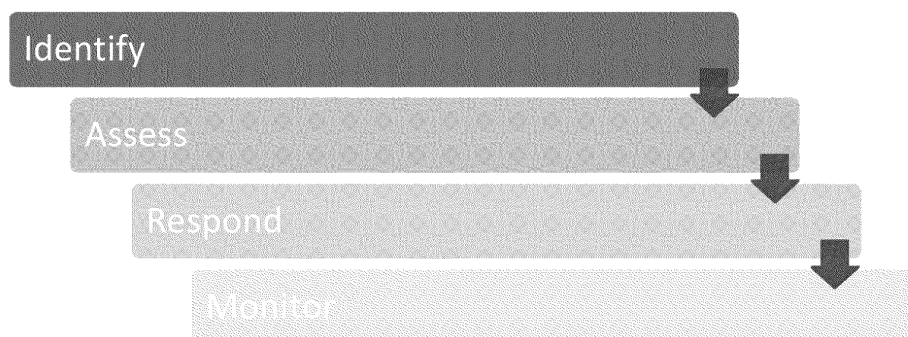
## 4. Risk Management Framework

---

The Post Office Risk Management Framework provides the standard for the management of risk to the organisation. This includes how risks are articulated, classified, evaluated as well as the risk management tools used.

### 4.1. Post Office Risk Management Framework

Post Office's risk management framework is designed so that the material risks throughout the business can be identified, assessed and effectively managed. This framework incorporates the following core elements:



**Figure 1. Post Office Risk Management Framework**

- **Identify:** Techniques by which Post Office identifies all the risks it faces be they existing, new or emerging. The Board, and those setting strategy and policy, should use horizon scanning and scenario planning collectively and collaboratively to identify and consider the nature of emerging risks, threats and trends;
- **Assess:** Whereby each risk is assessed in terms of its potential impact and likelihood for the inherent and residual risk score. A risk profile is produced providing a significance rating to each risk and therefore a tool for prioritising treatment efforts. Risk assessment also includes assessing the control effectiveness and ensuring control measures are in place;
- **Respond:** Implementation of actions to respond to risks including decisions on whether to tolerate, treat, transfer or terminate; and
- **Monitor:** This is focused on (a) reacting to early warning indicators of the need to make interventions, (b) reviewing emerging risks and opportunities, (c) reviewing whether risks owners are implementing the responses for which they are accountable and, (d) reporting on the success (or otherwise) of the interventions to date and whether additional activity is required.

### 4.2. Risk Articulation

All risks across the risk hierarchy must be expressed in terms of their cause(s), the risk event itself, and their impact:

- **Cause:** A cause is an element which alone or in combination with other causes has the potential to give rise to the risk. They are generally (but not exclusively) external;
- **Event:** An event is an articulation of the potential adverse or beneficial circumstances that could result from the cause – in effect the risk itself. Post Office risks should be classified (see section 4.3) against the Event not the Cause or the Impact; and,
- **Impact:** Impact is the outcome of a risk event materialising. Outcomes can be positive or negative. They can also be direct or indirect. It is also possible to express them qualitatively or quantitatively. They should be assessed using Post Office HARM table (see Appendix 8.5).



### 4.3. Risk Hierarchy and Classification

Post Office has a three-level risk hierarchy. These are:

- **Enterprise Risks:** The Post Office's key business risks are grouped into fourteen enterprise-level themes which mirror HM Government's approach to enterprise risk classification. These risks are Post Office-wide and so are of corporate importance. Each enterprise risk is owned by a single GE member. Central Risk provide an update on the management of these enterprise risks at each RCC and ARC;
- **Intermediate Risks:** These are sub-categories of an enterprise risk to which they are linked. They are often the key risks faced by individual business units; and,
- **Local Risks:** These are sub-categories of intermediate risks, to which they are linked. They are often more specific, local risks faced by individual subsidiary departments.

The Post Office risks have been categorised in a manner consistent with those advocated by HM Government's 'Orange Book'<sup>13</sup>.

### 4.4. Risk Ownership

Risks can be owned by any colleague within Post Office and its subsidiaries. Ownership of a risk is determined by the risk event itself and where the risk is classified under the risk hierarchy (see section 4.3). The Risk Owner is responsible and accountable for the management of the risks they own and for transferring ownership where the risk has:

- to be reallocated within the organisation due to internal restructure; or,
- has changed and it needs to be reassigned.

When a risk is transferred, the Risk Owner must provide the new owner with complete information about the risk to enable them to manage the risk appropriately. Risk ownership can only be transferred when a risk has been accepted by the new Risk Owner.

### 4.5. Harm Table and Control Effectiveness

Post Office assess each risk by demonstrating the relationship between the likelihood of the risk materialising (on a standard 1-5 scale) and the impact of the event should the risk materialise (again on a standard 1-5 scale) to provide an overall risk rating.

The Post Office corporate HARM table describes the impact/likelihood scales which must be applied. This is provided at Section 8.5.

Each active risk should have 2 ratings namely:

- **Inherent:** the level of risk before any control activities are applied; and,
- **Residual:** the latest level of risk considering the effectiveness of the controls currently in place.

and, where applicable, **Control Effectiveness** (i.e. Effective, Partially Effective and Not Effective). Refer to the Policy Guidelines for more details.

### 4.6. Governance, Risk & Compliance (GRC) tool

All Post Office risks (across all levels of the risks hierarchy) must be identified, analysed, evaluated, managed and recorded using the corporate GRC tool<sup>14</sup>. A SNOW Risk Management User Guide is available [here](#).

---

<sup>13</sup> HM Government: Management of Risk (Principles and Concepts) – May 2023

## 5. Policy Framework and Minimum Control Standards

---

### 5.1. Policy Framework

Post Office has established a suite of other Policies and standards on a risk sensitive approach which are subject to an annual review. These have been developed to comply with applicable legislation and regulation. These include but are not limited to:

- Anti-Bribery & Corruption Policy
- Business Continuity Management Policy
- Change Policy
- Code of Business Standards
- Financial Crime Policy
- Health and Safety Policy
- IT Disaster Recovery
- Treasury Policy
- Vulnerable Customer Policy
- Whistleblowing
- Internal Audit Charter
- Cyber Security Policy

### 5.2. Who must comply?

Compliance with the Risk Policy is mandatory for all Post Office employees<sup>15</sup> subsidiaries and applies wherever in the world the business is undertaken.

Where material non-compliance is identified the matter must be referred to the Policy Owner (the Director of Internal Audit and Risk Management) and Sponsor (the Chief Finance Officer). 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 or negligence, this may be treated as a disciplinary offence.

---

<sup>15</sup> 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.





### 5.3. 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. preventative, detective and corrective) which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

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

Risk Area	Description of Risk	Minimum Control Standards	Who is Responsible	When
<b>Risk Management Framework</b> (Risk Management Process)	Because the risk management knowledge and culture are not consistent across the business, there is a risk that the GE and Post Office 1 <sup>st</sup> line fail to proactively identify, assess, own and manage their risks and/or maintain their associated internal control measures, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Preventative control:</b> A periodic risk assessment is performed within the corporate GRC tool by the Post Office Risk Owners, to ensure Inherent/Residual score are assessed. For Post Office Insurance, risk assessments are managed independently via Powers Apps.	Risk Owners	Bi-annual /Ad hoc
	Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1 <sup>st</sup> line fail to articulate their risks in terms of their cause(s), the risk event itself and their impact, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Preventative control:</b> Articulation of risks in terms of their cause(s), the risk event itself, their impact and classification of risks against the event is ensured by the Post Office Risk Owners, as reflected in the corporate GRC tool.	Risk Owners	Ad-hoc
	Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1 <sup>st</sup> line fail to proactively monitor, action and update the treatment of risks, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Detective control:</b> Post Office Risk Owners monitor that all risks have an effective risk response (i.e. mitigate, accept, transfer or terminate). They must ensure the appropriate actions to treat the risk against the relevant risk response are reflected in the corporate GRC tool.	Risk Owners	Ad hoc
	Because the risk management knowledge and culture are not consistent across the business, there is a risk that the GE and Post Office 1 <sup>st</sup> line fail to proactively identify, assess own and manage their risks and/or maintain their associated internal control measures, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Detective control:</b> Central Risk Team through their a) 2 <sup>nd</sup> line assurance activity, assess the effectiveness of risk description (10% risk sample check across the portfolio) as evidenced in the Risk Assurance Report; b) deep dive for enterprise and intermediate risks, assess the effectiveness of the risk score and responses completed by the 1 <sup>st</sup> line, as evidenced in the GE Risk Dashboards.	Central Risk	Bi-Annual (Risk Assurance Report)/Bi-monthly (GE Risk Dashboards)



Post Office Limited - Document Classification: INTERNAL

Risk Area	Description of Risk	Minimum Control Standards	Who is Responsible	When
<b>Risk Management Framework</b> (Risk Management Process)	Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1 <sup>st</sup> line fail to articulate their risks in terms of their cause(s), the risk event itself and their impact, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.			
	Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1 <sup>st</sup> line fail to proactively monitor, action and update the treatment of risks, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.			
	Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1 <sup>st</sup> line overstate the effectiveness of controls, thereby understating the residual risk likelihood and impact, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Detective control:</b> Internal Audit through their annual audit programme assess the effectiveness of controls and report controls that are not designed or operating effectively to mitigate the risk.	Internal Audit	Ad-hoc
<b>Risk Management Framework</b> (Harm Table and Group Risk Management Policy)	Due to capacity and resourcing within the Central Risk Team, there is a risk that Post Office HARM table and Group Risk Management Policy are not reviewed to ensure changes to Post Office strategic objectives and the external risk landscape are reflected. This may result in Post Office failing to achieve its strategic objectives and/or leading to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Preventative control:</b> Post Office HARM Table and Group Risk Management Policy are reviewed by Central Risk and submitted for approval to ARC.	Central Risk ARC	Annually
	Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1 <sup>st</sup> line fail to score their risks in accordance with the Post Office HARM table, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Preventative control:</b> The inherent and residual risk rating are scored by the Post Office Risk Owners against the Post Office HARM table, as reflected in the corporate GRC tool.	Risk Owners	Ad-hoc

Risk Area	Description of Risk	Minimum Control Standards	Who is Responsible	When
<b>Risk Management Framework</b> (Risk Training)	Due to capacity within the Central risk team and business priorities, there is a risk that Post Office 1 <sup>st</sup> line are insufficiently trained on risk management and operation of the corporate GRC tool, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Preventative control:</b> One to one training is undertaken by Central Risk Business Partners with all new Post Office Risk Owners, following the allocation of corporate GRC tool licences by the 1 <sup>st</sup> line to ensure they are able to manage their risks within the tool. Central Risk provide corporate GRC tool user guide for all Risk Owners available in the Central Risk Team intranet.	Central Risk Business Partners	Ad-hoc
<b>Risk Governance</b> (Risk Reporting)	Due to the lack of engagement between the GE members and Central Risk Team, there is a risk that the Group Executive (GE) is unable to fulfil its responsibility of having an understanding of risks facing Post Office (including new and emerging risks), which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Detective control:</b> An Intermediate GE Risk Dashboard is provided on an agreed cycle with the GE members by the Central Risk Business Partners. The GE Risk Dashboard provides an overview of the enterprise and intermediate risks, their risk appetite position (whether outside or inside appetite) and agreement of key risks (with GE member), which may be included within the RCC/ARC report.	Central Risk Business Partners	Bi-monthly
	Due to capacity and resourcing within the Central Risk Team, there is a risk that the RCC, ARC and Board are unable to fulfil their responsibilities of providing oversight, challenge and approve the direction of risks facing Post Office (including new and emerging risks), which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact	<b>Detective control:</b> Head of Risk produces and submits to RCC and ARC a Risk Update showing the latest position of the group key enterprise and key intermediate risks (including new and emerging risks), as reflected in the corporate GRC tool.	Head of Risk	Bi-monthly
<b>Risk Strategy</b> (Risk Appetite)	Because the risk management knowledge and culture are not consistent across the business, there is a risk that Post Office 1 <sup>st</sup> line do not refer to the Post Office Risk Appetite, where approved, when completing the risk assessments, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact	<b>Preventative control:</b> Risk appetite is assessed by the Post Office Risk Owners against a 5-tiered scale, including open, flexible, neutral, cautious and averse risk appetite scale, as reflected in Post Office Risk Appetite Statements.	Risk Owners	Ad-hoc
	Due to capacity and resourcing within the Central Risk Team, there is a risk that the Risk Appetite statements are not periodically reviewed and approved by ARC, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Detective control:</b> Group Executive review Risk Appetite Statements supported by Central Risk. Risk Appetite Statements are approved by ARC.	Group Executive Central Risk Board/ARC	Bi-Annually or when changes to strategic objectives are required

Post Office Limited - Document Classification: INTERNAL

Risk Area	Description of Risk	Minimum Control Standards	Who is Responsible	When
	Because the risk management knowledge and culture are not consistent across the business, there is a risk that the risks outside Appetite are not periodically monitored by the GE, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Detective control:</b> Group Executive and Business Units monitor risks outside approved Risk Appetite Statements that apply to the Post Office Group within the GRC tool. Areas of non-compliance to Group Executive and Board/ARC are escalated by Central Risk.	Group Executive and Business Units Central Risk	Ad-hoc
<b>Risk Strategy</b> (Policy Exceptions)	Due to failure of the business to identify and mitigate risk at an early stage, there is a risk that the business departs from an approved Policy, which may result in Post Office failing to achieve its strategic objectives and leading to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Preventative control:</b> A Policy Exception Note (PEN) is completed by the 1 <sup>st</sup> line when the business is not compliant with a Post Office Policy. The PEN is approved by the GE member (or delegated GE-1) of the Business Area and GE Policy Owner. Once approved, a copy of the PEN and the approval emails are attached to the risk record by the risk owner (risk lead/risk champion) in ServiceNow GRC.	Risk Owners	Ad-hoc
<b>Risk Strategy</b> (Policy Exceptions)	Because the knowledge and culture of the policy exception process is not consistent across the business, there is a risk that the Post Office Policy Exceptions are not reviewed, updated and managed to closure, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact,	<b>Preventative control:</b> Post Office Risk Owner is responsible to ensure that the mitigation actions for the policy exception are achieved within the agreed timeline. This is completed for the duration of the open policy exception and evidenced in the activity journal or mitigation plan within the corporate GRC tool.	Risk Owner	Ad-hoc
	Due to capacity and resourcing within the Central Risk Ream, there is a risk that the GE is unable to fulfil its responsibility of having visibility on the open Post Office Policy Exceptions, which may result in failure to achieve strategic objectives, lead to reputational damage, regulatory breach, financial loss and/or customer impact.	<b>Detective control:</b> Central Risk Business Partners report on all Policy Exception Notes to the GE, RCC and ARC, as reflected in the "GE Risk Dashboard".	Central Risk Business Partners	Bi-monthly



## 6. Where to go for help

---

### 6.1. Additional Policies

This Policy is one of a set of policies. The full set of policies can be found on the SharePoint Hub under Policies.

### 6.2. 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, staff may:

- Discuss the matter fully with their Line Manager; or,
- A senior member of the HR Team, or
- Direct to the Whistleblowing Manager ( [redacted] GRO ), or
- Contacting the “Speak Up” line, a confidential reporting service which is run by an independent company Convercent (Tel: ( [redacted] GRO ) / Secure on-line portal: [redacted] GRO )

### 6.3. 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 the Director of Internal Audit and Risk Management.

## 7. Governance

---

### 7.1. Governance Responsibilities

The Policy sponsor takes responsibility at GE level for policies covering their areas.

The Policy Owner is the Director of Internal Audit and Risk Management who is responsible for ensuring that the content is up to date and is capable of being executed. As part of the review process, they need to ensure that the minimum controls articulated in the policy are working or to identify any gaps and provide an action plan for remediation.

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

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

### 7.2. Tools

ServiceNow GRC (Advanced Risk Management & Policy and Compliance modules).

GRC provides Post Office with a structured approach to managing its overall approach to governance, enterprise risk management and regulatory compliance to secure achievement of its overall strategic objectives:

- **Governance and Compliance:** This ensures the Post Office's governance framework, including policies, laws and regulations, and best practices are in one place in one system, and mapped to associated controls. It provides for the identification of relevant business, risk and IT owners (and systems).
- **Risk Management:** This identifies and manages existing risks in a single place as well as collect information about emerging risks, and the accuracy of the associated controls.
- **Implement real-time monitoring:** This identifies non-compliant controls and monitors high-risk areas.
- **Vendor Assessment:** This assesses vendor risk and provides the ability to manage and assess vendors in a consolidated manner.
- **Reporting:** GRC supports the Post Office in providing both qualitative and quantitative assessment scores, informed by service performance data allowing us to more accurately gauge our risk exposure in real time.

### 7.3. Definitions

**Appetite:** This is the level of risk that the Group is prepared to accept or pursue or before action is deemed necessary to reduce it.

**Control:** This is any action taken to reduce the likelihood and/or magnitude of a risk.

**Policy Exception:** There are on occasion exceptional situations where Post Office may need to operate outside of policy. In these circumstances the business can choose to accept this risk and formally request a policy exception.

**Governance:** This is the system by which organisations are directed and controlled. It defines accountabilities, relationships and responsibilities in the organisation as well as determine the rules and procedures and monitors performance.

**Impact:** This is the estimated result including financial, operational and reputational that would be realised if a risk event would occur.

**Likelihood:** This is the evaluation or judgement regarding the chances of the risk materialising. Likelihood is also called 'probability' or 'frequency'.

**Risk:** Risk is defined as the effect of uncertainty on the Post Office achieving its strategic objectives. That effect may be positive, negative or a deviation from the expected. Risks are described in terms of causes, potential events and their consequences.

**Risk Management:** This is the co-ordinated activities designed and operated to manage risk and exercise internal control within an organisation.



## 8. Document Control

### 8.1. Document Control Record

SUMMARY			
GE Policy Sponsor	Standard Owner	Standard Implementer	Standard Approver
AI Cameron (CFO)	Johann Appel (Direct of Internal Audit and Risk Management)	Central Risk	ARC/Board
Version	Document Review Period	Policy – effective date	Policy location
1.5	Annual	1/2024	Group Policy SharePoint Hub Central Risk Intranet site

REVISION HISTORY			
Version	Date	Changes	Updated by
1.0	11/2019	Reviewed and refreshed to reflect new Group Head of Risk position and ensure Business hold accountabilities for identification and management of their risks	Jenny Ellwood
1.1	11/2020	Annual Review and minor amends	Mark Baldock
1.2	11/2021	Annual Review and minor amends (incorporation into new Policy template)	Mark Baldock
1.3	3/2022	Incorporation of revised HARM table (Section 7.5)	Mark Baldock
1.4	10/2022	Annual Review and amends	Roberta Zavaglia Audrey Cahill
1.5	10/2023	Annual Review and amends	Roberta Zavaglia Audrey Cahill

### 8.2. Oversight Committee

Committee	Date Approved
POL R&CC	10/11/23
POL ARC	27/11/23
Board	30/01/23

**Next Policy Annual Review Date: RCC & ARC (November 2024), Board (November 2024)**

### 8.3. 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.

Payzone Bill Payment Limited is a limited company registered in England and Wales under company number:11310918. VAT registration number GB 172 6705 02. Registered office: Finsbury Dials, 20 Finsbury Street, London, England EC2Y 9AQ

## 8.4. Appendix A: Risk Appetite scale

	Appetite rating	Impact/Likelihood Rating span	Risk taking philosophy	Tolerance for Uncertainty <sup>16</sup>	Decision choice <sup>17</sup>	Prioritisation of Strategic Objective <sup>18</sup>
	Open		Will take risks and <b>accept the possibility of failure</b>	Will <b>accept the possibility of failure</b>	Will choose the <b>option with the highest return</b>	<b>Will accept risks could materialise</b> and the achievement of (some) strategic objectives could be compromised
	Flexible	16-20	Will <b>take justified risks</b>	Will choose the option which has <b>some degree of risk</b>	Will accept risks materialising subject to being <b>able to proactively manage their adverse impact</b>	<b>Will accept (under certain conditions) risks could materialise</b> the achievement of (some) strategic objectives could be compromised
	Neutral	11-15	<b>Prefers, on balance, safe delivery to risk taking</b>	Will <b>accept, on balance, risks</b> could materialise	Will accept risks could materialise but only if <b>adverse impact is limited and heavily outweighed by benefits</b>	Would <b>prefer ideally not to accept</b> risks materialising if this meant the achievement of (some) strategic objectives could be compromised
	Cautious	6-10	Will take a <b>conservative approach to risks</b>	Will <b>accept some risks</b> could materialise	Will accept some risks materialising but only if activity is essential and the <b>possibility and extent of failure is limited</b>	Would be <b>somewhat reluctant</b> to accept risks materialising if this meant the achievement of (some) strategic objectives would be compromised
	Averse	1-5	Will <b>avoid nearly all risks</b> where at all possible	Has an <b>extremely low appetite for any risks</b> to materialise	Will always select the option with the <b>lowest risk</b>	Would be <b>extremely reluctant</b> to accept risks materialising if this meant the achievement of (some) strategic objectives would be compromised

<sup>16</sup> **Tolerance for uncertainty:** How willing is Post Office to accept uncertain outcomes? This illustrates the Board's appetite to trade off certainty to achieve a given objective. A low rating demonstrates the Board's need for certain outcomes, while a high rating shows the Board will pursue an objective even with an uncertain outcome.

<sup>17</sup> **Decision choice:** When faced with multiple decision options, how is Post Office willing to select a decision that puts a strategic objective at risk? This question assesses the Board's acceptance that a given choice may lead to failure to meet a strategic objective. A Board who are averse will only choose options that pose a minimal threat to the strategic objective's achievement. A Board open to this risk are willing to trade off the possibility of failure for a high-risk, high-reward decision.

<sup>18</sup> **Prioritisation of strategic objective:** How willing is Post Office willing to trade off this specific objective against achievement of other objectives? This demonstrates the Board's willingness to pursue achievement of a given strategic objective over achievement of another. A Board who are averse to this would never trade off completing the objective in question for failure of other objectives. A Board which is open would be willing to accept this trade-off.



## 8.5. Appendix B: HARM table

## (i) IMPACT SCALE

IMPACT: THE IMPACT OF THE RISK MATERIALISING COULD BE ONE (OR MORE) OF THE FOLLOWING ...	SCORE	RATING	STRATEGIC/FINANCIAL IMPACT ON POST OFFICE GROUP	OPERATIONAL IMPACT ON POST OFFICE GROUP	REPUTATION/LEGAL IMPACT ON POST OFFICE GROUP	IMPACT ON OUR POSTMASTERS & STRATEGIC PARTNERS	IMPACT ON OUR CUSTOMERS
	5	CRITICAL (VERY HIGH)	<ul style="list-style-type: none"> <li>Post Office unable to achieve one/or more of its strategic objectives</li> <li>Critical weakening of Post Office commercial profitability and/or ability to grow</li> <li>Impact to Revenue ≥£5M</li> </ul>	<ul style="list-style-type: none"> <li>Post Office capacity to respond exceeded</li> <li>Immediate Board/GE involvement required</li> <li>Critical lack of people resources availability and/or skills</li> <li><b>Projected =&gt; 5 days</b> total loss of front office/back office corporate IT service</li> <li><b>Projected =&gt;10% reduction</b> in approved number of Branch locations</li> <li><b>Projected =&gt;20% reduction</b> in profiled levels of Branch footfall &amp; transactions</li> </ul>	<ul style="list-style-type: none"> <li>Protracted negative references in Parliament, national publications, social media and websites</li> <li>Post Office's product(s) and/or service(s) quality is compromised across the digital/physical market(s) and in all UK regions</li> <li>Post Office activity attracts critical levels of fines and prosecutions and/or multiple litigations and/or regulatory censure</li> <li>Critical long-term damage to Post Office Brand</li> </ul>	<ul style="list-style-type: none"> <li>Critical weakening in relationship between Post Office and Postmasters</li> <li>Critical weakening of Postmaster community's commercial profitability and ability to grow</li> <li><b>Projected =&gt;10%</b> reduction in remuneration or increase in costs impacting <b>=&gt;50%</b> of Network</li> <li>Network service disruption of key branch locations <b>=&gt;5 days</b> and/ or impacting <b>=&gt;50%</b> of Network</li> </ul>	<ul style="list-style-type: none"> <li><b>Projected (&gt;30%)</b> increase, over agreed baseline, in number of customer complaints received over quality of products and/or services</li> <li><b>Projected [&lt;89%]</b> customer satisfaction score secured over quality of products and/or services</li> <li><b>Projected [&gt;1m]</b> of online customer sessions impacted by not being able to access our digital platform</li> </ul>
	4	MAJOR (HIGH)	<ul style="list-style-type: none"> <li>Major impact on Post Office ability to achieve one/or more of its strategic objectives</li> <li>Major (but not critical) impact on Post Office commercial profitability and/or ability to grow</li> <li>Impact to Revenue between £2M and £4.9M</li> </ul>	<ul style="list-style-type: none"> <li>Post Office experience major adverse impact throughout organisation</li> <li>GE proactive involvement required</li> <li>Major lack of people resources availability and/or skills</li> <li><b>Projected 3-4 days</b> total loss of front office/back office corporate IT</li> <li><b>Projected 5-9% reduction</b> in approved number of Branch locations</li> <li><b>Projected 15-19% reduction</b> in profiled levels of Branch footfall &amp; transactions</li> </ul>	<ul style="list-style-type: none"> <li>Sporadic negative references in national publications, social media and external websites</li> <li>Post Office's product(s) and/or service(s) quality is compromised across the digital/physical market(s) and in majority (but not all) UK regions</li> <li>Post Office activity attracts major levels of fines and prosecutions and/or multiple litigations and/or regulatory censure</li> <li>Major medium to long-term damage to Post Office Brand</li> </ul>	<ul style="list-style-type: none"> <li>Major weakening in relationship between Post Office and Postmasters</li> <li>Major weakening of Postmaster community's commercial profitability and ability to grow</li> <li><b>Projected =&gt;5%</b> reduction in remuneration or increase in costs impacting <b>=&gt;50%</b> of Network <b>OR Projected =&gt;10%</b> reduction in remuneration or increase in costs impacting <b>=&gt;25%</b> of Network</li> <li>Network service disruption of key branch locations between <b>3-4 days</b> and/or impacting between <b>25%- 49%</b> of Network</li> </ul>	<ul style="list-style-type: none"> <li><b>Projected (21-30%)</b> increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services</li> <li><b>Projected [90-93%]</b> customer satisfaction score secured over quality of products and/or services</li> <li><b>Projected (600k-1m)</b> of online customers impacted by not being able to access our digital platforms</li> </ul>
	3	SIGNIFICANT	<ul style="list-style-type: none"> <li>Significant impact on Post Office ability to achieve one/or more of its strategic objectives</li> <li>Significant (but not major) impact on Post Office commercial profitability and/or ability to grow</li> <li>Impact to Revenue between £1M and £1.9M</li> </ul>	<ul style="list-style-type: none"> <li>Post Office experience significant adverse impact in multiple (but not all) parts of the organisation</li> <li>Substantial specific business/departmental management intervention required</li> <li>Significant lack of people resources availability and/or skills</li> <li><b>Projected 1-2 days</b> total loss of front office/back office corporate IT service</li> <li><b>Projected 3-4% reduction</b> in approved number of Branch locations</li> <li><b>Projected 11-14% reduction</b> in profiled levels of Branch footfall &amp; transactions</li> </ul>	<ul style="list-style-type: none"> <li>Negative references in regional publications, social media and external websites</li> <li>Post Office's product(s) and/or service(s) is compromised but relatively restricted across the digital/physical market(s) and/or isolated to particular UK region</li> <li>Post Office activities result in breach of regulation which requires internal investigation and/or regulatory disclosure</li> <li>Significant medium to long-term damage to Post Office Group's Brand</li> </ul>	<ul style="list-style-type: none"> <li>Significant weakening in the relationship between Post Office and Postmasters</li> <li>Significant weakening of Postmaster community's commercial profitability and ability to grow</li> <li><b>Projected =&gt;5%</b> reduction in remuneration or increase in costs impacting <b>=&gt;25%</b> of network <b>OR Projected =&gt;10%</b> reduction in remuneration or increase in costs impacting <b>15%-24%</b> of Network</li> <li>Network service disruption of key branch locations between <b>1-2 days</b> and/or impacting between <b>15%-25%</b> of Network.</li> </ul>	<ul style="list-style-type: none"> <li><b>Projected (11-20%)</b> increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services</li> <li><b>Projected [94-96%]</b> customer satisfaction score secured over quality of products and/or services</li> <li><b>Projected (200k-600k)</b> of online customers impacted by not being able to access our digital platforms</li> </ul>
	2	MODERATE (LOW)	<ul style="list-style-type: none"> <li>Moderate impact on Post Office Group's ability to achieve one/or more of its strategic objectives</li> <li>Moderate (but not minor) impact on Post Office commercial profitability and/or ability to grow</li> <li>Impact to Revenue between £500k and £999k</li> </ul>	<ul style="list-style-type: none"> <li>Post Office experience material adverse impact in single area of the organisation</li> <li>Departmental management intervention required</li> <li>Moderate lack of people resources availability and/or skills</li> <li><b>Projected 1-day</b> total loss of front office/back office corporate IT service</li> <li><b>Projected 1-2% reduction</b> in approved number of Branch locations</li> <li><b>Projected 6-10% reduction</b> in profiled levels of Branch footfall &amp; transactions</li> </ul>	<ul style="list-style-type: none"> <li>Negative references in local publications</li> <li>Post Office's product(s) and/or service(s) is compromised but not yet available across the digital and/or physical market(s)</li> <li>Post Office activities result in moderate legal issue and relatively immaterial non-compliance and/or regulatory breach which is relatively easily resolved internally</li> </ul>	<ul style="list-style-type: none"> <li>Moderate weakening in relationship between Post Office and Postmasters</li> <li>Moderate weakening of Postmaster community's commercial profitability and ability to grow</li> <li><b>Projected =&gt;5%</b> reduction in remuneration or increase in costs impacting <b>6%-9%</b> of Network</li> <li>Network service disruption of key branch locations <b>&lt;=1 day</b> and/or impacting between <b>10%-14%</b> of Network</li> </ul>	<ul style="list-style-type: none"> <li><b>Projected (5-10%)</b> increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services</li> <li><b>Projected [97-98%]</b> customer satisfaction score secured over quality of products and/or services</li> <li><b>Projected (100-200k)</b> of online customers impacted by not being able to access our digital platforms</li> </ul>
	1	MINOR (VERY LOW)	<ul style="list-style-type: none"> <li>Little impact on Post Office ability to achieve one/or more of its strategic objectives</li> <li>Insignificant impact on Post Office commercial profitability and/or ability to grow</li> <li>Impact to Revenue &lt;£500k</li> </ul>	<ul style="list-style-type: none"> <li>Post Office experience no measurable adverse impact to the business</li> <li>Local management/staff manage the problem without escalation</li> <li>Minor lack of people resources availability and/or skills</li> <li><b>Projected &lt;1 day</b> total loss of front office/back office corporate IT service</li> <li><b>Projected &lt;1% reduction</b> in approved number of Branch locations</li> <li><b>Projected 1-5% reduction</b> in profiled levels of Branch footfall &amp; transactions.</li> </ul>	<ul style="list-style-type: none"> <li>Little media coverage</li> <li>No issue with the quality of Post Office's product (s) and/or service(s)</li> <li>Post Office activities result in low-level legal issue which is easily resolved internally</li> </ul>	<ul style="list-style-type: none"> <li>Insignificant weakening in the relationship between Post Office and Postmasters</li> <li>Insignificant weakening of Postmaster community's commercial profitability and ability to grow</li> <li><b>Projected =&gt;5%</b> reduction in remuneration or increase in costs impacting <b>=&lt;5%</b> of Network.</li> <li>Network service disruption of key branch locations <b>&lt;1 day</b> and/or impacting between <b>5%-9%</b> of Network.</li> </ul>	<ul style="list-style-type: none"> <li><b>Projected (&lt;5%)</b> increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services</li> <li><b>Projected [=&gt;99%]</b> customer satisfaction score secured over quality of products and/or services</li> <li><b>Projected (&lt;100k)</b> of online customers impacted by not being able to access our digital platforms</li> </ul>



(ii) **LIKELIHOOD SCALE**

	SCORE	RATING	DESCRIPTION
<b>LIKELIHOOD: THE LIKELIHOOD OF RISK MATERIALISING ...</b>	5	<b>ALMOST CERTAIN/VERY HIGH</b>	<ul style="list-style-type: none"> <li>• Risk almost certain to materialise unless action taken</li> <li>• Risk could be expected to materialise</li> </ul>
	4	<b>LIKELY/HIGH</b>	<ul style="list-style-type: none"> <li>• Risk likely to materialise frequently if events follow normal patterns and mitigating action is not taken.</li> <li>• Risk could be expected to materialise</li> </ul>
	3	<b>POSSIBLE/MODERATE</b>	<ul style="list-style-type: none"> <li>• Risk unlikely to materialise but it is possible</li> <li>• Risk could be expected to materialise infrequently/irregularly/sporadically</li> </ul>
	2	<b>UNLIKELY/LOW</b>	<ul style="list-style-type: none"> <li>• Risk very unlikely to materialise</li> <li>• Risk could materialise intermittently</li> </ul>
	1	<b>RARE/VERY LOW</b>	<ul style="list-style-type: none"> <li>• A remote likelihood that risk would materialise</li> <li>• Almost inconceivable that risk would occur</li> </ul>