POL00447894

Risk Management Policy Guidelines

Version – V1.2

POL00447894

POL00447894

1. Introduction

The commercially competitive and highly regulated environment, together with operational complexity, exposes the Post Office to a number of risks.

Each year the Post Office Board begins its planning period with a set of strategic options balanced against a wallet of finite resource and funding. Each of these options carries with it a profile of varying risks, therefore a robust and effective Risk Policy and Guidelines are designed to assist the Board with a pragmatic assessment of competing strategy options versus the Post Office financial resources.

We define risk as anything that can adversely affect our ability to meet the Post Office's strategic objectives, maintain its reputation and comply with regulatory standards. We seek to understand and harness risk in the pursuit of our objectives and aim to operate within an acceptable level of risk taking, with an effective risk management process.

1.1. Scope of the Guidelines

The Policy Guidelines aims to:

- Enable the effective identification, measurement, monitoring and management of risks that may have an impact on the achievement of our strategic ambitions, create reputational damage or a regulatory breach;
- Ensure that risk taking activities are aligned with risk appetite where approved;
- Ensure compliance with applicable legislative and regulatory requirements;
- Support the business to monitor material changes to the risk profile;
- Support the Central Risk Team to provide a consistent level of oversight, challenge and assurance to the Board.

It describes:

- Risk culture and leadership;
- Governance and oversight of risk management activities;
- Accountability for risk management;
- Our risk strategy, including risk appetite and policy exceptions;
- Risk management framework used to identify, assess and manage risks.
- Categorisation of risk.

POL00447894

2. Risk Governance

2.1. Risk Management Culture

Risk culture is the set of acceptable behaviours, discussions, decisions and attitudes toward taking and managing risk, encouraged by the tone from the top. Such attitudes and behaviours comprise, but are not limited to, timely, transparent and honest communication, a common purpose, values and ethics and the active promotion of learning and continuous development. The board has a responsibility to establish, communicate and put into effect a risk culture that aligns with the strategy and objectives of the business and thereby supports the embedding of its risk management and processes.

We have a risk culture that ensures colleagues understand that they are accountable for the risks they take and that the needs of customers are paramount. It is the responsibility of every colleague to be aware of and understand risk and risk management, and how this should apply to their day to day activity.

Achieving a good risk aware culture is ensured by establishing an appropriate risk principles and process.

2.2. Risk Management Structure (3LOD)

The structure of risk management at Post Office is based on the three lines of defence (3LOD) model as its primary means to demonstrate a structured approach to governance, compliance and oversight. The three lines of defence model provides a simple and effective way to help delegate and coordinate risk management roles and responsibilities within and across the organisation. Refer to Appendix 5.1 for three line of defence structure.

POL00447894

2.3. Risk Management Roles and Responsibilities

Implementing risk management requires appropriate delegation of authorities, as well as clear accountabilities, and responsibilities at each organisational level.

The **Post Office Board** through its Audit, Risk & Compliance Committee (ARC) has responsibility to review the overall risk management and strategy.

The **Accountable Officer (or CEO)** set the tone at the top for risk management throughout the business and establishes governance arrangements at Post Office.

The **General Executive (GE)** has day to day responsibility for the systems of internal control, including risk management.

The **Risk and Compliance Committee (RCC)** reviews the effectiveness of the Risk Policy and management of principal risks.

The **Central Risk Team** oversee the corporate approach to risk management. This involves defining and implementing risk standards, policies, procedures and guidance. They also assist the 1st line function in the risk management activities in line with good practice as well as monitor compliance and effectiveness.

All **colleagues, contractors and Postmasters** should be risk aware.

Refer to Appendix 5.2 for Roles and Responsibilities and 5.3 for RACI (Responsible, Accountable, Consulted and Informed) Model.

2.4. Risk Reporting

Risk reporting allows for the effective review, challenge and monitoring of risk exposure against Post Office's approved risk appetites. 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;
- detecting and preparing for changes and trends in existing risks, including the extent to which risks are aligned with approved appetite and tolerance levels;
- 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.

A corporate Governance, Risk & Compliance (GRC) software tool (i.e. ServiceNow GRC Risk Management) supports the Post Office in providing risk performance data allowing us to more accurately gauge our risk exposure in real time.

In addition to this, the Central Risk Team provide appropriate and timely reporting (every 2 months) to GE members, RCC and ARC, such as:

- Risk "Dashboard" showing the latest position of their Enterprise and Intermediate risks outside of appetite (including new and emerging risks) to GE members;

- Risk Update to RCC and ARC showing the latest position of the group key intermediate and local risks outside appetite (including new and emerging risks).

Risks are escalated to the GE members through these Dashboards.

POL00447894

3. Risk Strategy

3.1. Risk Appetite

Risk appetite is agreed by the Board and is the extent to which Post Office will accept that a risk might happen in pursuit of day to day businesses activites. It therefore defines the boundaries of activity and levels of exposure that we are willing and able to tolerate. It provides agreed tolerable risk levels, that Post office is willing to operate in given current funding constraints. The application of risk management practices cannot, and will not eliminate all risk exposure.

Board risk appetite statements by Principal risk were initially approved by Board in 2015/16 and are currenly under review. From this review, risk appetite statements were updated and approved in 2021 for Legal and Operational, in 2022 for Technology and in 2023 for People, Commercial, Governance and Financial. Refer to our Central Risk Team intranet Risk Appetite (sharepoint.com) for all refreshed appetite statements.

3.2. 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 you should only raise 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). The approved PEN and approval email from the Policy Owner and GE member (or delegate GE-1) needs to be attached to the new risk record in ServiceNow GRC tool.

For further information refer to the PEN form and "How to Guide" document or contact your Business Unit Risk Business Partner.

POL00447894

4. Risk Management Framework

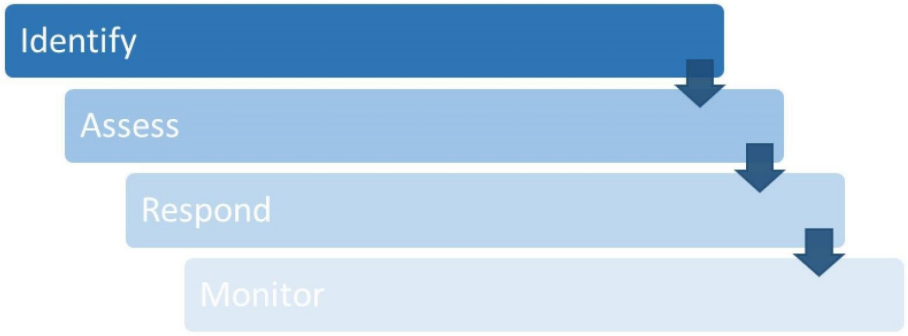
4.1. Overview

Effective risk management helps us to ensure that our products and processes are fit for purpose. Customers, shareholders and regulators require Post Office to have effective processes to identify, manage, monitor and report the risks it is all might be exposed to.

We are committed to working with all colleagues to make risk management a core process that is an integral part of business activities. The benefits of managing our risk includes:

- Supporting the achievement of our trading profit target;
- Supporting good customer outcomes;
- Compliance with legal and regulatory frameworks;
- Management of external impacts and change;
- Improving decision making, planning and prioritisation;
- Supporting cost efficiency;
- Exploiting opportunities and encourages innovation.

The Risk Management Framework, shown below, is the means by which the business will effectively manage risk. This Framework ensures that risks are identified and managed effectively across the business. To demonstrate this, Post Office risks are recorded and managed within the ServiceNow GRC Risk Management tool. A SNOW Risk Management User Guide is available here.



4.2. Identify

Risk identification is vital to the success of the Risk Management Process. It is:

- An ongoing activity, with individual risks and the impact and/or likelihood of risks materialising changing regularly;
- The process of determining what risks might prevent us from delivering our objectives.

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.

POL00447894

Risks are identified from a number of sources including:

- Changes to the operating environment, periodic horizon scanning and review of external environment;
- Planning (at strategic, group and operational levels);
- Monitoring of assurance activity;
- Monitoring of performance;
- Existing forums (Board, ARC, RCC, GE, audit team and project / programme meetings) where risk is a standing agenda item;
- External risk workshops or conferences attended by Central Risk Team and colleagues;
- Indicators of emerging risks;
- Internal / external audit;
- Incidents management.

Risk Hierarchy and Classification

Post Office has a risk hierarchy which involves three tiers of risk: enterprise, intermediate and local (enterprise risks are Post Office's key business risks, intermediate risks are sub-categories of an enterprise risk to which they are linked and local risks are generally sub-categories of intermediate risks, to which they are linked). These are linked into fourteen risk themes which mirror HM Government's approach to enterprise risk classification. Refer to Appendix 5.4 for Risk Hierarchy and 5.5 for Risk Classification.

Risk Ownership

All risks, once identified, must be assigned a risk owner with a ServiceNow GRC Risk Management license and sufficient authority and responsibility for ensuring the risk is managed and monitored. The risk owner may not always be the action owner responsible for mitigating actions.

Accountability helps to ensure that 'ownership' of the risk is recognised and the appropriate management resource allocated.

Normally the Enterprise risks are owned by GE members, Intermediate risks by GE, GE-1 or GE-2 and Local Risks by Business team level.

Risk Articulation

All risks across the risk hierarchy are defined by their cause(s), the risk event itself, and their impact, in line with the Bow Tie Methodology (see picture below):

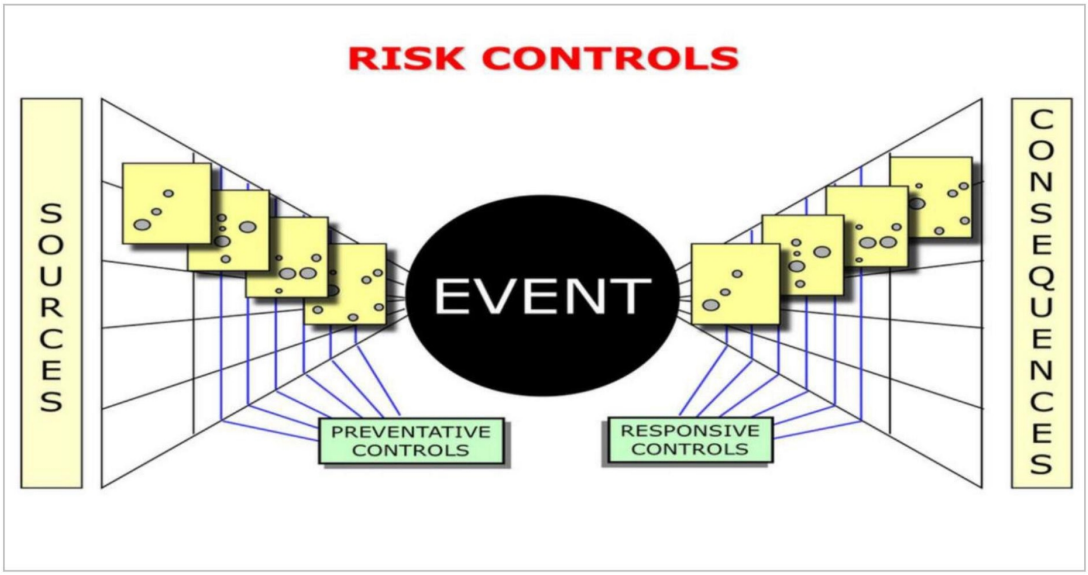
- Cause: A cause is an element which alone or in combination with other causes has the potential to give rise to the risk. They are normally (but not exclusively) external;
- Event: An event is an articulation of the potential adverse or beneficial circumstances that could result from the cause – in effect the risk itself. A risk may have multiple causes and consequences and can affect multiple business objectives. Post Office risks are classified against the Event not the Cause or the Impact; and,
- Consequences/Impact: Consequences are 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. Refer to our Central Risk Team intranet here for the HARM Table.

POL00447894

Bow Tie Methodology

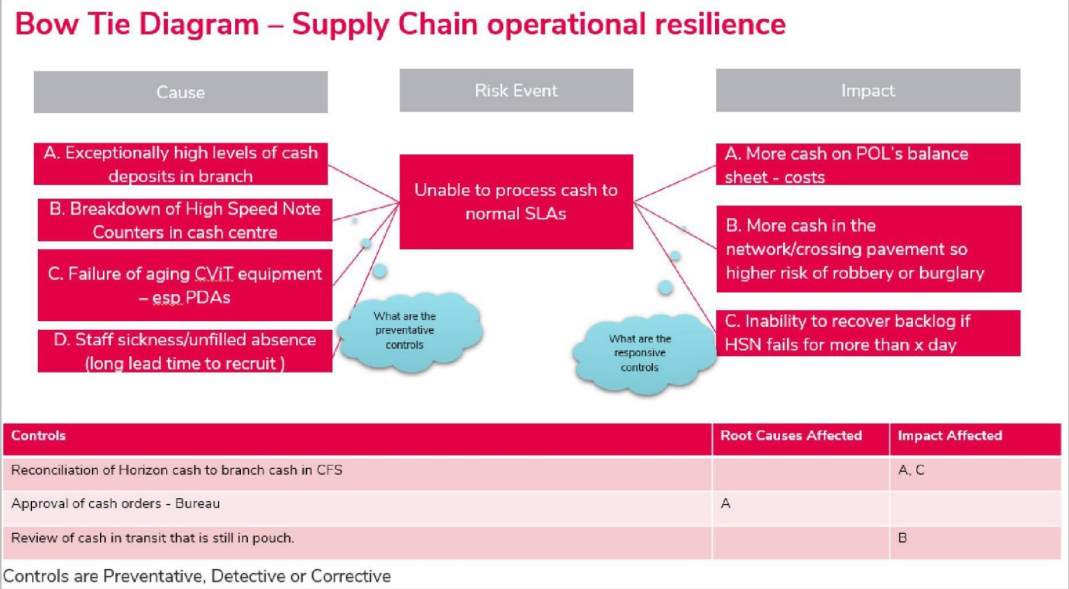
The Bow-Tie Diagram below illustrates the connections between risk events, their root causes and consequences/impact by:

- Visualising a summary of plausible consequences that could exist around a certain event.
- Displaying what control measures an organization can take to control those consequences



Examples of risks articulated in line with the Bow Tie diagram are showed below:

Example 1

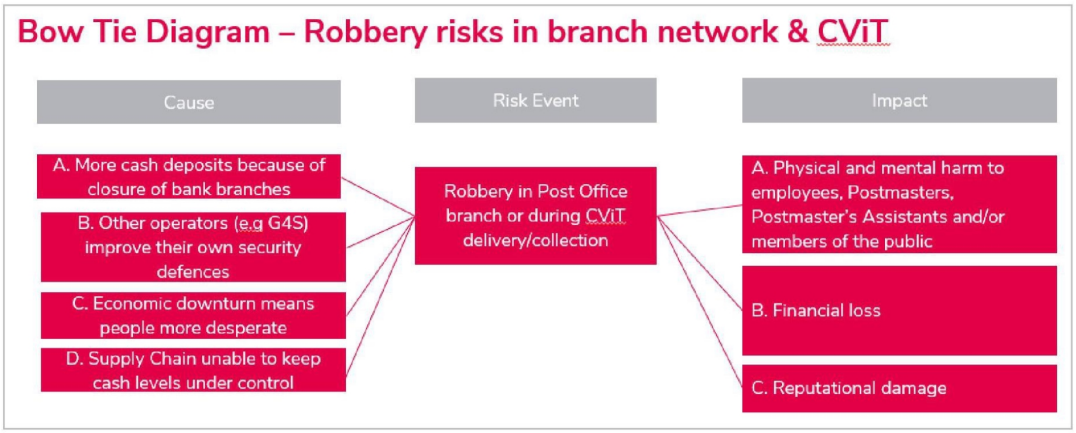


Controls	Root Causes Affected	Impact Affected
Reconciliation of Horizon cash to branch cash in CFS		A, C
Approval of cash orders - Bureau	A	
Review of cash in transit that is still in pouch.		B

Controls are Preventative, Detective or Corrective

POL00447894

Example 2



4.3. Assess

Once a risk is identified it is evaluated and assessed. Risk evaluation helps to determine the severity of the risk faced by the likelihood of it materialising, together with the severity of the impact. The result of this evaluation gives a score which feeds into an overall risk profile.

The measurement of risk is based primarily on a traditional *impact v likelihood* approach using a 5 x 5 HARM Table matrix, as summarised below:

- Impact and likelihood are multiplied to give an overall score.
- The overall scoring can range from 1 to 25, with higher scores indicating a greater level of exposure.
- Measuring risks at Post Office is a qualitative process with individual views on the likelihood and impact on the business, which will vary.

The result of the risk evaluation is used to produce a risk profile which gives a risk rating to each risk and therefore provides a tool for prioritising treatment. This also ranks each identified risk to give a view of its relative importance.

Each active risk should have 2 ratings namely:

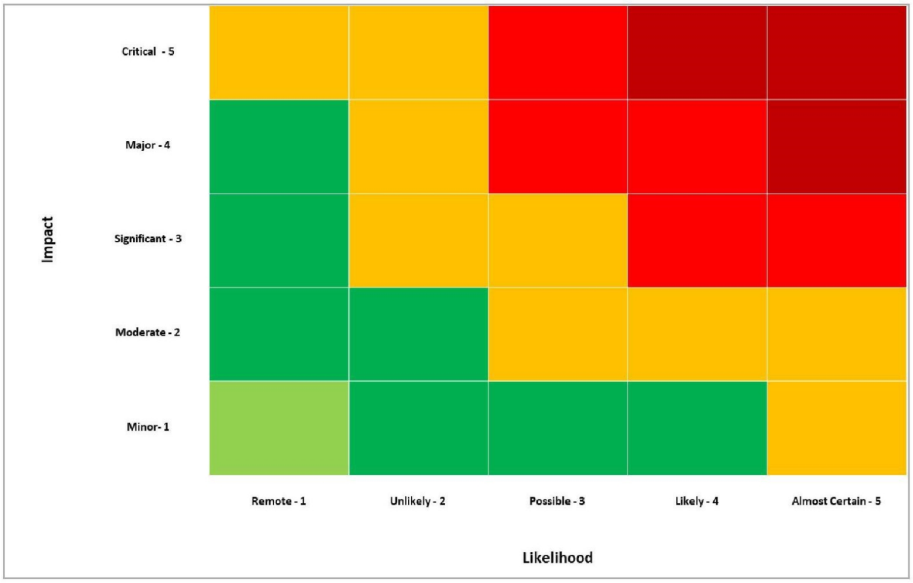
- Inherent: the level of risk before any control activities are applied;
- Residual: the latest level of risk considering the effectiveness of the controls currently in place.

And, where applicable, Control Effectiveness:

Effectiveness	**Performance**
Effective	The control(s) significantly reduces the risk, bringing the residual risk within appetite
Partially Effective	The control(s) has some impact on reducing the risk
Ineffective	The control(s) does not adequately address the risk

POL00447894

Risk Heatmap



4.4. Respond

Respond is the implementation of actions to respond to risks including decisions on whether to tolerate, treat, transfer or terminate. The risk score creates a decision point in which we decide how to respond, as follows:

Risk Response	Description
Accept **(Tolerate/Retain)**	The exposure may be tolerable without any further action being taken. Even if it is not tolerable, the ability to do anything about some risks may be limited, or the costs of taking any action may be disproportionate to the potential benefit gained.
Mitigate **(Treat/Control/Reduce)**	By far the greater number of risks will be addressed in this way. The purpose of treatment is that, whilst continuing within Post Office with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level.
Transfer	Transferring a risk by means of an insurance policy (e.g. a cyber risk might be transferred because we have an insurance policy)
Avoid **(Terminate/Eliminate)**	Some risks will only be treatable or containable to acceptable levels, by terminating the activity. In these circumstances, appropriate responses will be elimination of the risk by stopping the process or activity, substituting an alternative process or outsourcing the activity that is associated with the risk (e.g., you can decide to ban the usage of laptops outside of the company premises if the risk of unauthorized access to those laptops is too high – because, e.g., such hacks could halt the complete IT infrastructure you are using)

POL00447894

4.5. Monitor

The risk information within the ServiceNow GRC Risk Management is used to develop the main source of risk reporting for use by management and, where applicable by both Internal and External Audit requests.

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.

Information should be updated regularly to ensure accurate and up to date information is available for reporting purposes.

In addition to this, in accordance with the Companies Act 2006, the Annual Report and Accounts include statements on the key risks and uncertainties facing the business together with the high level remediation activities. This work is informed by year end processes, which includes a review of Enterprise Risks and the Executive Declaration process which enables GE to consider (and attest annually) if any additional disclosures are required.

Escalation

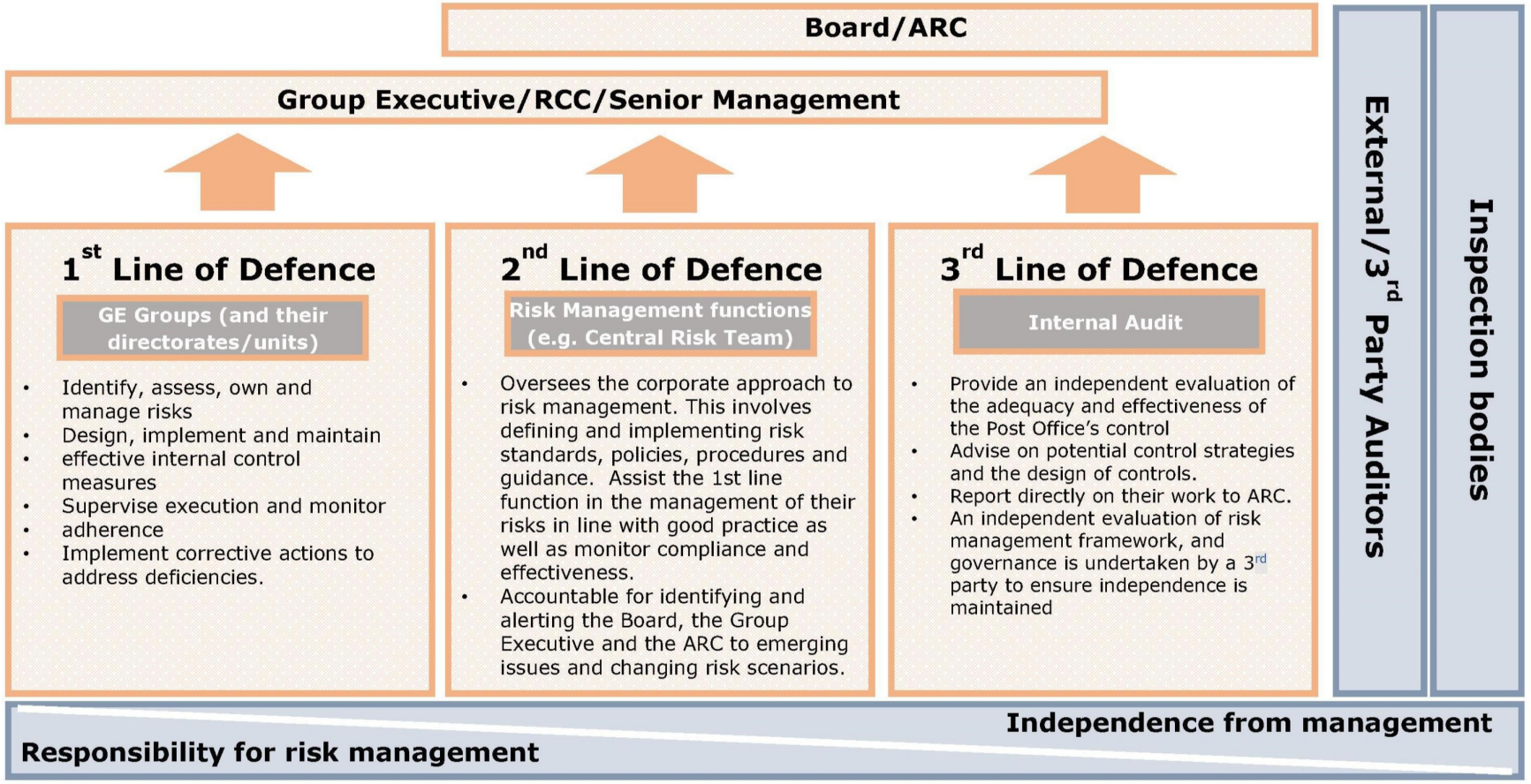
This is the process which ensures that risks are escalated, as required. This is critical to ensuring appropriate decisions and actions are taken to respond appropriately to a particular risk. It is the responsibility of the individual risk owner to raise risks which they believe have a material impact to Post Office/outside appetite and/or tolerance. Such risks should be escalated through the business hierarchy that the risk exists.

This should ensure that (a) appropriate decisions and actions are taken to respond appropriately to a particular risk, (b) different areas of professional expertise and views are appropriately considered in the management of risks, and (c) sufficient information and evidence to facilitate risk oversight and decision making are provided.

POL00447894

5. Appendix

5.1. Three Line of Defence Structure



POL00447894

5.2. Roles and Responsibilities

Level	Roles and Responsibilities
Board	• Set the tone at the top for risk management throughout the business and establishes governance arrangements. • Ensure that a framework of systems processes for effective risk management and internal control are in place and functioning appropriately. • Consider information on the operation of risk management arrangements via papers to the Audit, Risk and Compliance Committee, Accountable Officer and through the annual assurances for the completion of the annual report and accounts. • Assure itself that the business identifies and effectively manages any risks that could affect the achievement of the strategy. • Defines the overall risk appetite. • Monitor the risk profile. • Monitor and act on escalated risks.
Audit, Risk and Compliance Committee (ARC)	• Review the Risk Policy, Risk Appetite and attitude to risk to ensure these are appropriately defined and communicated. • Review the Post Office's overall risk position and periodically invite management to outline risk management strategy and status within their specific business units. • Review management's assessment of the degree of risk the Post Office prudently incurs in achieving a reasonable balance between the cost of managing risk and control systems and the benefits derived. • Review areas of specific risk as highlighted by management, including enterprise and intermediate risk. • Monitor the Risk and Compliance Committee activities and receive summary reports as appropriate. • Approve the Risk Policy and Risk Appetite for the business.
Risk and Compliance Committee (RCC)	• Review the effectiveness of the Risk Policy and maintain oversight of the development and implementation of the components. • Maintain oversight of the current risk exposures of Post Office and advice on future risk strategy. • Review the identification and effective management of current key risks, identified mitigating actions and emerging risks. • Receive and review risk reports from Sub-Committees. • Consider and review the adequacy of internal controls and make recommendations for the improvement. • Monitor the implementation of key recommendations and management action plans. • Review the adequacy of policy governance and recommend changes.
Accountable Officer	• Specific personal responsibility for signing the annual accounts, including the Accountable Officer's Governance Statement.
General Executive	• Implement risk management and its assurance mechanisms. • Contribute to and review of the Enterprise and Intermediate and local risks outside of appetite, where approved.
Non-Executive Directors	• Provide independent and objective scrutiny of the risk management structure and processes.

POL00447894

Level	Roles and Responsibilities
Director of Internal Audit and Risk Management	• Agrees on the information to be reported to Board Committees. • Ensure appropriate risk governance arrangements are in place. • Owner of the Group Risk Management Policy and ensures it is implemented. • Owns and manages escalated risks as appropriate. • Ensure adequate resource within the Central Risk Team. • Attends the ARC and RCC.
Central Risk Team	• Oversee the corporate approach to risk management. • Assist the 1st line function in the risk management activities in line with good practice as well as monitor compliance and effectiveness • Enable risk identification including emerging risks. • Monitor risks assessment completion and mitigation plans. • Monitor compliance with risk appetite, where approved. • Provide independent challenge and review to monitor the status of risks and, where necessary, to escalate issues to GE/RCC/ARC. • Provide latest position of risks within the business through Risk report "Dashboard" to the GE and Risk Paper to the RCC and ARC. • Provide assurance to Board Committees and leadership over the effectiveness of risk management. • Develop plans to improve the management of risk. • Support the Policy Exception processes. • Develop and implement Risk Management Policy and Risk Management Guidelines. • Develop (in discussion with 1st line) Risk Appetite Statements. • Support the business in developing an appropriate risk culture including upskilling capability training. • Facilitate GE meetings / risk meetings/ workshops. • Provide training on ServiceNow GRC Risk Management tool. • Develop and update ServiceNow GRC Risk Management tool training materials. • Ensure ServiceNow GRC Risk Management tool works properly and raise issues where necessary.
Risk Owners	• Support the implementation of the Risk Policy and Risk Management Guidelines. • Identify new risks including emerging risks. • Perform risk assessments and update mitigation plans on ServiceNow GRC Risk Management tool according to the risk assessment release schedule. • Seek Central Risk Team support and escalate if required. • Should be Post Office permanent employee. • Raise and manage Policy Exceptions.
New starters	• Follow the Risk Management Policy and Risk Management Guidelines and understand the part they play. • Be risk aware, identify / report on potential risks and minimise. • Participate in any training sessions or workshops as required. • Carry out any agreed control measures and duties as instructed.
Compliance	• Provide the business with up-to-date regulatory requirements. • Support compliance with regulations and best practice.
Internal Audit	• Internal Audit work is undertaken on major risks faced by the business and effectiveness of associated controls.

POL00447894

Level	Roles and Responsibilities
	• Provide independent, objective assurance on the effectiveness of the systems of internal control. • An independent evaluation of risk management framework and governance is undertaken by a 3rd party to ensure independence is maintained. • Provide recommendations for improvement where necessary.

POL00447894

5.3. Post Office Risk Management Overview – RACI Model

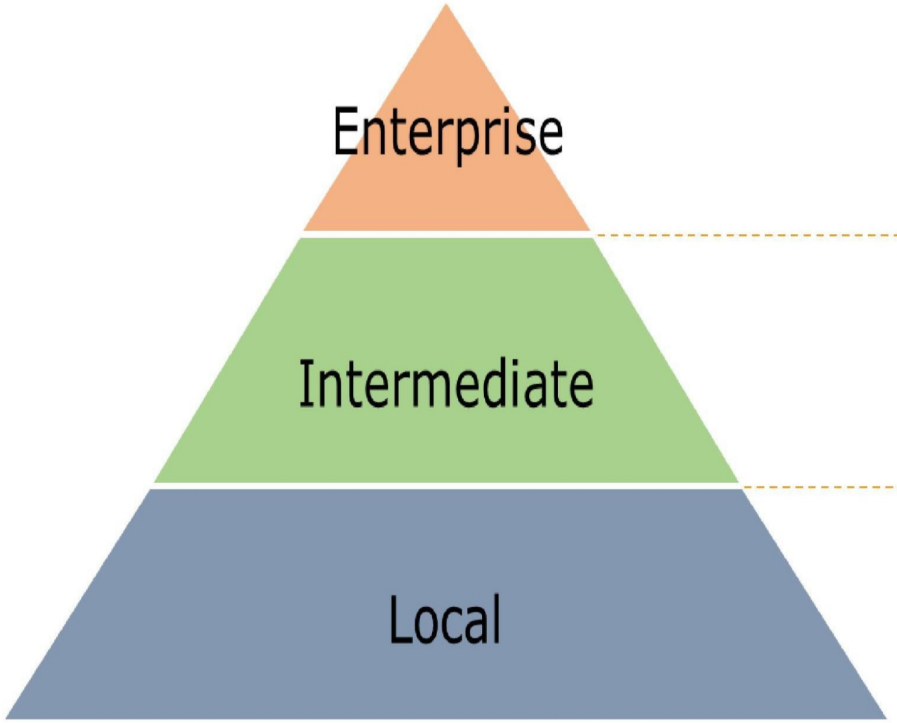
Activity	Board/ ARC[1]	RCC[2]	Entity/Department Owner	Risk Owner	Control Owner	Risk Response Owner	Central Risk Team
Sign off Risk policy and risk standards	A	C	I				C
Implement Risk policy and risk standards	R	C	R	R	R	R	A
Set Risk Appetite	A	C	R	C	I	I	C
Identify Risks	A	R	A	A	A	A	A
Assess Risks			A	R	I	I	C
Assess controls			A	A	R	I	I
Respond to Risks			A	A	I	R	I
Update Mitigation Plan			A	A	I	R	I
Monitor corporate approach to risk management	A	R	C	C	I	I	R
Assist the risk management in line with best practice			A	C	I	I	R
Report Post Office Risk Profile	I	I	A	C	I	I	R

[1]*ARC: Audit, Risk & Compliance Committee*
[2]*RCC: Risk and Compliance Committee*

R	Responsible	Who is assigned to do the work
A	Accountable	Who makes the final decision and has the ultimate ownership
C	Consulted	Who must be consulted before a decision is taken
I	Informed	Who must be informed that a decision or action has been taken

POL00447894

5.4. Risk Hierarchy



Enterprise Risks are Post Office's key business risks. These risks are Post Office-wide and so are of corporate importance.
Each enterprise risk is owned by a relevant GE member. Central Risk provide an update on the management of these enterprise risks at each RCC and ARC.

Intermediate Risks are sub-categories of an enterprise risk to which they are linked. They are often the key risks faced by individual business units.

Local Risks are generally sub-categories of intermediate risks, to which they are linked. They are often more specific, local risks faced by the departments within individual business units.

POL00447894

5.5. Risk Classification

Risk Category	Description
Change	Risks around Post Office change programmes/projects are not aligned to Strategic Purpose, are ineffectively governed and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.
Commercial	Risks around weaknesses in the Post Office management of commercial partnerships, supply chains and contractual requirements, insufficient product/service development, unattractive products/services and wider adverse trading performance.
Financial	Risks around Post Office not managing finances and tax liabilities effectively, levels of unsustainable borrowing, insufficient liquidity, unsustainable levels of borrowing, loss of revenue, inadequate investment and insufficient funding.
Governance	Risks around Post Office having an ineffective corporate structure, unclear plans, competing priorities, opaque accountability, inadequate oversight of corporate performance and untimely and ineffective decision-making.
Health & Safety	Risks around Post Office facing a challenging external H&S environment and having an inadequate internal H&S environment and ineffective internal H&S working practices
Information	Risks around Post Office capturing data ineffectively, not exploiting it adequately and suffering from material data inaccuracy.
Legal & Regulatory	Risks around Post Office having an ineffective corporate and compliance & control environment, ineffectively managing its contract & transaction management obligations, being non-compliant with its statutory & regulatory requirements (including Employment Law and Pension obligations), encountering adversarial Disputes & Litigation and misuse of its Intellectual Property & Brand.
Marketplace & Brand	Risks around Post Office being unable to compete in the market place, unable to undertake sufficient market research, experiencing volatile consumer demands and suffering from a tarnished Brand.
Operational	Risks around Post Office being unable to focus on postmaster or customer needs or deliver a high quality customer experience, because of insufficient operational capacity, inadequate capability, ineffective business processes and inadequate Business Continuity/Disaster Recovery arrangements.
People	Risks around Post Office having a sub-optimal business culture, ineffective on-boarding arrangements, unsatisfactory retention levels, insufficient L&D, inadequate Work-Life balance, inadequate rewards and recognition, ineffective Knowledge Transfer/corporate memory arrangements and adversarial Industrial Relations.

POL00447894

Risk Category	Description
Reputation	Risks around Post Office having an adverse environmental impact, suffering from ethical violations, inadequate Corporate Social Responsibility and a damaged reputation and loss of trust.
Security	Risks around Post Office having inadequate and ineffective Cyber and Security arrangements.
Strategy	Risks around Post Office's Strategic Purpose (including M&A and divestments) being poorly designed or unaligned with wider macro-economic environment, unable to be delivered by current capabilities and mechanisms and not fully supported by key external stakeholders.
Technology	Risks around Post Office IT services being unsatisfactory, IT performance ineffective, IT Infrastructure and products/services inadequate, IT processes deficient and IT development insufficient.

POL00447894

5.6. Risk Taxonomy

#	Name	Description
1	Control effectiveness	Assessment of the quality of controls used to minimize the inherent risks of the Post Office.
2	Control environment	Attitude, awareness, and culture of the Post Office regarding risk management and/or internal control.
3	Control	Actions to reduce the likelihood and/or magnitude of a risk.
4	Governance	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.
5	HARM table	Description of parameters for assessing risks.
6	Impact	Effect on the Post Office's financial, infrastructure and reputation position when a risk materialises.
7	Inherent risk	Level of risk before any control activities are applied. Sometimes referred to as Gross risk.
8	Likelihood	Evaluation or judgement regarding the chances of the risk materialising, sometimes established as a 'probability' or 'frequency'.
9	Residual risk	Existing level of risk taking into account the controls already in place. Sometimes referred to as Net risk or Current risk.
10	Risk management process	Co-ordinated range of activities that deliver management and control of risks within Post Office.
11	Risk Response	Implementation of actions to respond to risks including decisions on whether to tolerate, treat, transfer or terminate
12	Risk	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.
13	Risk appetite	The amount of and type of risk that the Post Office is willing to pursue or retain.
14	Stakeholders	Persons or groups of people with an interest in the activities of the Post Office.
15	Terminate	Response that is appropriate when the level is not acceptable to the Post Office, also referred to as Avoid or Eliminate.
16	Tolerate	Response that is appropriate when the level of risk is acceptable to the Post Office, also referred to as Accept or Retain.
17	Transfer	Response for risks that the Post Office wishes to transfer to another party, usually by means of insurance or contractual transfer.
18	Treat	Response for risks that the Post Office believes can be further treated by the introduction of cost-effective (corrective) controls, also referred to as Control or Reduce.

POL00447894

5.7. Version History

Date	Version	Updated by	Change Details
October 2022	1.0	Roberta Zavaglia/Audrey Cahill	Annual review and amends
October 2023	1.0	Roberta Zavaglia	Annual review and amends