POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	DRAFT Internal Control Framework	**Meeting Date:**	26th September 2022
Author:	Anshu Mathur Interim Group Compliance Director Rebecca Barker, Deputy Head of Risk	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Discussion

This paper provides an overview of the work undertaken to develop a DRAFT POL Control Framework. This has been presented and discussed at the Risk and Compliance Committee on 13 September 2022, who agreed to the principles and concepts of the Framework. This has also been distributed to the GE on 14 September 2022.

Given the cost challenges, this DRAFT framework was approved as a direction of travel, against which POL can make incremental steps towards control maturity ie the committee agreed not to associate this with any formal outcomes or timetable.

It was recognised that the principles of the DRAFT Control Framework are being applied within the assurance approach for 'Historical Matters', Technology Change, Whistleblowing and Investigations.

Executive Summary

A Control Framework provides the Business with a clear and consistent approach against which its control environment can be maintained but more importantly also measured, monitored, and demonstrated.

The Draft POL Control Framework provides this clarity and sets out the standards and key building blocks of what constitutes a robust control environment, namely:

- <u>Control Continuum</u> - A scale against which the business can self-assess their control environment maturity and direction of travel (to be set by the Board).
- <u>Three lines of defence</u> – Clarifying the roles and responsibilities between the first line, second line and third line of defence, so that no ambiguity exists and we have a proportionate assurance model or target operating model that is doable for POL.
- <u>Coverage / Adequacy</u> of controls to manage business risk – Clear guidance on what and how a Business function environment should be created to ensure adequate coverage and identification of business risks and related controls.
- <u>Assurance of controls effectiveness</u> – A defined model against which Controls will be sampled for checking against evidence, to ensure POL has a continuous assurance in place which the RCC, GE and ARC understand and can rely on.

  More importantly, this should then be the genesis for the creation of integrated assurance plans to ensure POL coverage of key risk (actual/emerging) and their remediation is being assessed and monitored.
- <u>POL Compliance Dashboard</u> – A formalised dashboard to measure the state and direction of travel of POL control environment.

POL00447843

The DRAFT POL Control Framework has been developed in manner in which it provides clear guidance, yet is not prescriptive, hence allowing the Business Functions the sufficient flexibility to ensure they can adopt and or choose their approach to demonstrate adherence to the standards. Given POL's cost challenge this is imperative.

It also recognises and will leverage the risk and control work already performed and being monitored via SNOW.

In creating this DRAFT Framework we have sought guidance and input from Finance, LCG, Group Risks, and Technology. Their contributions and constructive challenges have been invaluable.

Next steps

1. Continue to embed the principles with Tech Change, Whistleblowing and Investigations.
2. Begin to apply the principles of the framework across the organisation, where capacity exists, in a light touch manner leveraging existing resources and risk/control activities undertaken.

DRAFT - POL Control Framework

1. Purpose

This document provides the minimum standards and associated guidance for POL to ensure an appropriate control environment exists and is maintained. This Framework provides guidance on the key building blocks of a control environment and clarifies the roles and responsibilities across the three lines of defence. .

As risks and associated controls are a key underpin, this Control Framework is fully aligned to the Group Risk policy, and is intended to support POL to operate within agreed risk appetites and tolerances set by the Board.

Implementing the Control Framework will also facilitate the timely and proactive identification of issues and or exceptions, risk trends, and themes to ensure these are appropriately monitored, discussed and challenged at various governance forums such as the Risk Compliance Committee and Audit & Risk Committee.

This framework is aligned with the COSO framework to ensure POL can develop a strong, effective internal control system and will also ensure POL can comply with the provisions of UK Sox.

2. Authority and Responsibility

POL Control Framework is owned by the Group General Counsel under the delegated authority of the Board. Executive Management (and their Functions) are responsible for working within this framework and maintaining sufficient processes, systems and evidence to demonstrate compliance. (**Please refer to Appendix A for the GRC Framework**)

3. Control Environment Maturity Continuum – Our desired end state

It is the strategic objective of the PO to operate under a stable and appropriate control environment to ensure key risks at an enterprise, intermediate and local levels are being proactively managed and monitored. A standard control environment maturity continuum scale is provided below:

Undeveloped/ Unreliable	Informal	Established/ Standardised	Integrated/Monitored	Optimised
Piecemeal and ad-hoc control environment with limited assurance and oversight. Driven by issues and incidents and or regulatory /legislation.	Risk & Control Framework, Policies and Procedures are designed and in place. Risk / Control universe not mapped to organisational design and or activities. Controls are not adequately documented; controls mostly dependent on people No formal training or communication of control activities	Risk and Control activities are designed and embedded. Risk and Control universe is mapped and maintained. Use of GRC tool is embedded. 3 LoD exists in parts and lacks integration. Formalised controls training and communication.	Established risk and controls universe supported by periodic testing and assurance. Efficacy and reporting of controls driven by first line activity, with appropriate oversight from 2nd Line and 3rd Line of Defence. Integrated Assurance providing objective oversight on Control Environment. Limited use of automation.	A fully integrated control framework with real time monitoring by management with continuous improvement embedded by design

Whilst, PO current control environment maturity varies, our strategic operating target for 2025 should be to able to demonstrate a control maturity between **‘Established/Standardised’ and ‘Monitored’.**

For this to be achieved, every function within PO will need to be able to demonstrate in a standardised and consistent manner the following:

- **Integrated Assurance** - How and through what activities do Management gain assurance that their control environment is mature, and coverage of key risks and their associated controls remain effective to prevent significant issues / incidents that may cause reputational, financial, commercial and or operational damage to the PO.

  This Framework defines and explains the PO ‘Three lines of defence’ model to ensure the business embeds a robust, efficient and integrated assurance approach within which the roles and responsibilities of the first line, second line and third line are clear and understood. Please refer to **Section 4** below.

- **Adequate Coverage** - A key requirement of a mature control environment is to be able to demonstrate key risks and associated controls and how these provide adequate coverage over **all** key activities, related processes and procedures ie POL universe.

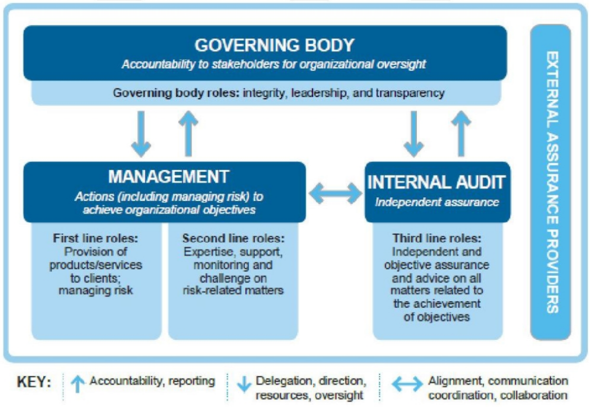
  Please refer to **Section 5** below, which provides guidance on how Management should create, and then maintain their universe, and associated risks and controls.

4. Three Lines of Defence Model

The IIA Three Lines of Defence (3LoD) model ensures clarity and a structured approach for the overall management of risk and exercising control within an organisation, thus minimising gaps in risk management and unnecessary duplication of risk coverage and or assurance activities.

The 3LoD model is recognised as best practice for risk and control management, and accordingly is the basis for POL Control Framework.

The Institute of Internal Auditors’ Three Lines Model is provided below:


GOVERNING BODY
Accountability to stakeholders for organizational oversight
Governing body roles: integrity, leadership, and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
INTERNAL AUDIT
Independent assurance
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication coordination, collaboration

- **First line of defence** - Functions that **own and manage risks & controls**
- **Second line of defence** - Functions that **monitor / oversee** or who specialise in compliance or the management of risk
- **Third line of defence** - Functions that provide **independent assurance**

The table below operationalises the above IIA model to how the three lines of defence should operate and be embedded within POL. This clarifies the activities and roles/responsibilities between the first, second and third lines of defence.

Three Lines of Defence – Roles and Responsibilities

First Line *Functions that own and manage risks*		***Second Line*** *Functions that monitor / oversee or who specialise in compliance or the management of risk*	**Third Line** *Functions that provide independent assurance*
Business Process Operators:	***Functional Compliance Leads***	***Group Compliance & Group Risk***	***Group Internal Audit***
• **Accountable** for executing business controls and embedding the POL Control Framework • Maintain required **evidence** of control execution • **Develop and execute** mitigations for control failures • **Support** Compliance Review and or Deep dives	• **Responsible** for embedding POL Control Framework within Functions • **Ensure** risk and control approach / methodology align with Group Risk Policies • **Continue reassessing** controls and processes on ongoing basis • **Perform** and **support** control testing, monitoring • **Perform** functional deep dives and RCA's • **Coordinate** and monitor mitigation plans for failures • **Identify** emerging trends. • **Report** to Group Compliance on CSA outcomes and progress against remediations plans • **Report** overall status via monthly Functional dashboards	• **Lead and Support** the embedding of POL Control Framework and Group Risk Framework and policies. • **Provide** guidance on CSA Testing and Methodologies • **Perform** Functional CSA where no dedicated Functional Risk & Compliance lead role • **Perform** quality reviews/tests on functional CSA outcomes • **Consolidate** functional dashboards reports into one central Group dashboard • **Monitor** progress against mitigation plans for control failures • **Perform** investigations and compliance reviews if requested by Group legal Counsel, GE and RCC • **Identify and report** emerging trends and risks. • **Report** status of Control Environment to RCC/ARC focussing on non-compliance • **Report status of Risk Exposure to RCC/ARC**	• **Provide** objective and independent assurance on the adequacy and effectiveness of the risk management and control, making recommendation for improvement. • **Report** to RCC/ARC on its findings, particularly around areas of non-compliance.
• Defined ownership for risk and controls. • Risk and Controls subject to regular review and monitoring at GE Leadership Team • Operate within Board set risk appetite and tolerances to deliver strategic objectives • Escalate to Second line concerns for viability of existing risk appetite • Up to date Risk and Control Universe: • Issues and incidents • People, Process & system changes • CSA failures • Adequate repository of risk, and evidence of control execution. • Support second and third line assurance reviews and or investigations • Inform Functional Compliance & Risk Leads of material changes to People, Process and systems.	• Appointed Functional Risk & Compliance Leads. • Maintain oversight of changes to people, process and systems to assure efficacy of risk and control environment • Support Functional or Execute 'Control Self Assessments' (CSA): • Ensure appropriate CSA coverage and frequency • CSA failures are tracked and monitored till remediation • Update Control Dashboard - Key risk indicators, KPI's, CSA results, Issues / incidents / Root causes etc to demonstrate state of control environment and related trends / themes or emerging risks. • Perform investigations and Reviews.	• Train/assess Functional Compliance leads • Provide assurance of First line compliance with standards: • Risk and control Universe • Risk Assessments and Coverage • Control efficacy • CSA • Perform entity and intermediate risks and policy compliance reviews • Ensure risks appetites and tolerances are adhered to. • Identifying Entity level trends and emerging issues and risks • Assess and report PO control environment maturity • Escalate areas of non-compliance to GE and Board/ARC • Deliver Compliance Programme across the PO. • Provide input and opinion on Risk Acceptances, for RCC consideration. • Monitor universe of REN	• **Unrestricted** access to all Company information, data, processes etc.

The effective implementation of the above model would provide a sound basis for assuring the GE, ARC and Board that POL is robustly managing their risk and maintaining an appropriate risk and control environment.

5. Control Universe

A) Universe – key activities and or processes

A key first step in assessing risks and controls is Management being able to demonstrate their understanding and coverage of their 'universe' of key activities and processes. An illustrative example of how management should document their universe and ensure adequate coverage can be found in **Appendix B.**

As several methods can be adopted to create, evidence and maintain a 'Universe', this framework does not prescribe how this should be done, however Management should be able to clearly demonstrate:

- How or what basis has their universe been created - Particularly to ensure appropriate coverage; a few examples of what an Universe can be based on are: organisational structures/design (CEO minus -3 or 4), (business units and support departments), service/product lines, customer journeys or touch points, regulatory or legal requirements etc.

- To what business activity and or process level is the universe mapped to
  For eg. The level of detail at which a universe can be based on, can range from an entity level (level 0 or 1) to a key stroke view (level 4/5). Usually a mid-range is preferable as this provides a good balance between capturing key activities vs too much detail.

- How the universe is maintained
  For eg. How are changes in process, activity and or org design managed and reflected in the universe i.e. change control, continuing assessment of risks & control etc.

- What assurance exists
  What assurance activities are undertaken to provide Management a view that their universe is complete, and reflects business activities and the associated inherent / residual risks profiles.

  In a mature control environment an integrated assurance plan would be created between the 3 LoD's.

Management's universe should also be the basis on which their Enterprise Risk Management and the PO Risk Framework is applied to measure, monitor, and report against Board set risk appetite/tolerance.

B) Identification of Controls

As mentioned above, Management are accountable for ensuring a robust control environment exists within POL which operates within Board agreed risks appetites and tolerance.

To discharge their accountability, Management should be able to demonstrate that their controls are not only identifiable but are also being managed in a diligent, consistent manner and can be mapped back to their risk.

To ensure an appropriate universe of controls exists to manage risk the following key principles should be applied in the identification of controls.

- Apply PO Risk management process in identifying, and measuring risks materiality. Please refer to **Appendix D** where the risk management process has been illustrated.
- Assess risk identified at an '<u>Inherent Level</u>' only ie assuming no controls exists.
- Document controls that manage the inherent risk.

  Controls documented should be SMART and not a process or procedure. Controls Identified and documented should be key controls (defined in **Section 6A**)
- Control owners are clearly identified.
- Processes and procedures capture the requirements to evidence and document controls.
- Ensure controls continue to remain effective through regular assessment. (refer to 6 below)
- Ensure controls are reflected in SNOW and can be linked and mapped to risk.

6. <u>Assessing control effectiveness</u>

As mentioned above it is Management accountability to ensure an appropriate control environment exists and is maintained. Whilst capturing key controls is an essential first step, their regular assessment, monitoring and embedding continuous learning from issues/incidents are equally important.

A) Definition of key controls

The POL Control Framework should be balanced and proportionate. The goal is not to reach absolute coverage or monitor or provide assurance on every activity or process within an organisation, as this would be untenable, inefficient and very challenging to embed, maintain and monitor.

Consequently, Management need to be aware of their **<u>key controls</u>** (derived from their universe refer to **Section 5** above). A control will be deemed key if it meets the following criteria:

- reduces or eliminates key risk or multiple risks
- ensures the delivery of key outcomes
- is appropriate to the risk appetite of the function
- protect some area of the business/expose a potential area of failure
- they are regularly tested or audited for effectiveness

The definition of **key risks** summarised below has been extracted from the PO Risk Policy 'Harm Table' (**Please refer to Appendix C**). A risk will deemed key if meets the following criteria:

- Impact delivery of strategic priorities
- Severely impact Commercial/Financial/Operational stability
- Lead to Postmaster/customer detriment and/or severe Reputational Damage

In the identification, and subsequent monitoring of **Key Controls**, management should ensure that the controls are designed in accordance to the principles stated in **Section 5B** above.

What benefits will we gain from risk and control mapping?

Efficiency – one control can mitigate any number of risks. Mapping controls to risks will identify duplication of effort across different teams, and allows new risks to be assessed against an existing menu of controls so mitigation doesn't start from scratch
Effectiveness – mapping risks to controls allows the business to understand the full impact of a control changing or failing
Assurance - Enables aggregated assurance to be developed, resulting in more insightful MI = better decision making at a higher level.
Completeness – all risks are connected to their mitigating control(s), giving clarity around how they are managed, and enabling those charged with oversight to identify gaps or weaknesses. Also, reduced or archived risks may mean that the associated controls can be reduced or stopped, which might translate into resource savings for the business.

B) First Line - Management Control Self-Assessments/Self Attestations (CSA)

The CSA's comprise periodic control testing, carried out by the Functional Teams under the guidance and supervision of the Functional Compliance Leads to ensure that controls are designed adequately and operate as designed. It focusses on the key controls mitigating the gross risks (inherent risks) to ensure POL compliance with its obligations rated significant, major and significant in line with PO Risk Policy.

The frequency of CSA should be determined by a combination of the gross impact of the risk, and the frequency of the controls operation. This will allow PO to deploy resources efficiently and effectively. In summary management should consider:

- Type of control – Manual/ System driven
- Frequency of control – daily, weekly, monthly, quarterly, etc
- Nature of risks being managed - PM detriment, Regulatory, H&S etc
- History of incidents and or issues

Please refer to **Appendix E** CSA Test Methodology

Sufficient evidence should be retained by Functional Teams/ Functional Compliance leads to substantiate the outcomes. The risks and key controls subject to CSA's should be regularly reviewed , at least quarterly, to ensure that all 'inherent risks are captured.

Changes to CSA can be driven by new, emerging, or evolving regulatory obligations, risks or control/processes. The Functional Compliance Leads will share the changes and rationale for changes to key controls and SA with the Group Compliance Team.

Where possible and appropriate Functional Teams should consider the identification of E2E controls and CSAs for risk that are cross functional.

Where control failures are identified, these should be appropriately reflected in SNOW (non-compliant), and the root causes should be investigated and remediated through to completion. The testing frequency of controls that fail a CSA should be increased to provide assurance that the root cause(s) are sustainably addressed.

To assess and regularly monitor the state of controls a Functional dashboard should be created, and shared with Group Compliance. The functional dashboard should comprise key risk indicators, KPI's, CSA results, issues / incidents / root causes etc to demonstrate state of control environment and related trends / themes or emerging risks. These Functional dashboards will be a key underpin to the creation / collation of the POL Group Compliance Dashboard (Please refer to **Appendix F**)

A CSA coverage plan should be prepared on an annual basis, and shared with Group Compliance and Group Risks.

C) Second Line Assurance – Group Compliance Team and Group Risk

The central compliance team will periodically review and or test the output of the Functional Compliance Teams to ensure quality of testing, and documentation is maintained.

The Group Compliance team can perform sample checks to objectively assure that appropriate evidence exists to demonstrate execution of the control and that Management are on plan to ensure adequate controls coverage for a period. This can also be achieved through the Group compliance/risk assurance plan.

The Group Compliance and Group Risk Teams, should annually create, deliver an integrated Compliance & Risk Coverage Programme. The programme should be created in consultation with the first line functional compliance leads, and the third line to ensure the following:

- Integrated Assurance - activities are aligned between the LoD ie avoiding duplication or significant gaps.
- Adequate, timely and appropriate assurance maintained on high risk areas.
- Reviews performed with first line to proactively remediate risks and design controls, if any gaps identified

These Compliance Coverage Programme will be approved and monitored by ARC on an annual basis.

The outputs of the compliance & risk coverage programme, along with the results of CSA's would be considered by Group Risk when assessing the management of associated.

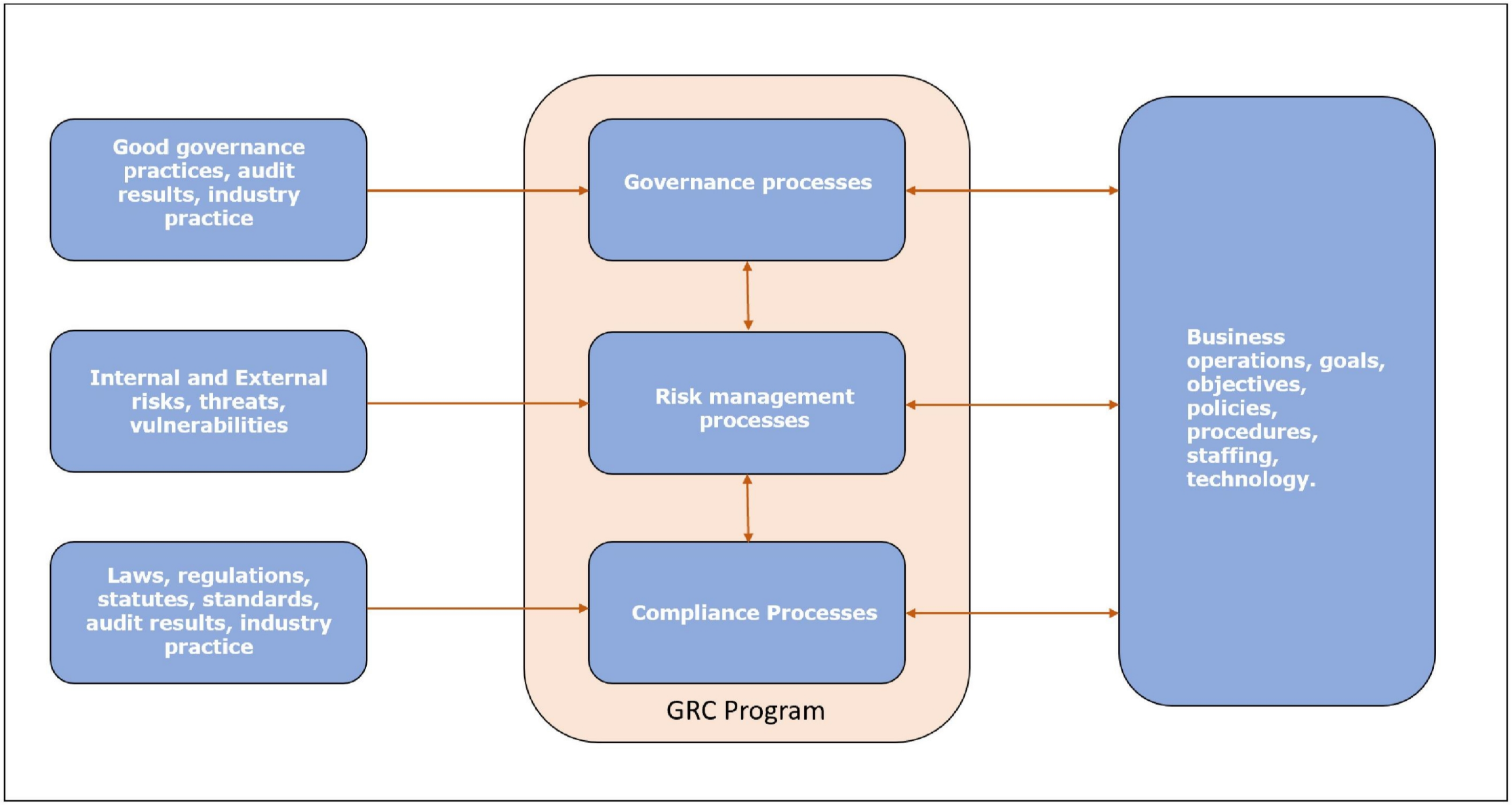
The Group Compliance Team will aggregate functional Compliance Dashboards and report to the GE and ARC on a monthly and quarterly basis respectively, to assess overall trends, themes (current and emerging) to monitor the health of PO Control Environment (Please refer to **Appendix F**).

D) **Third Line Assurance – Group Internal Audit**

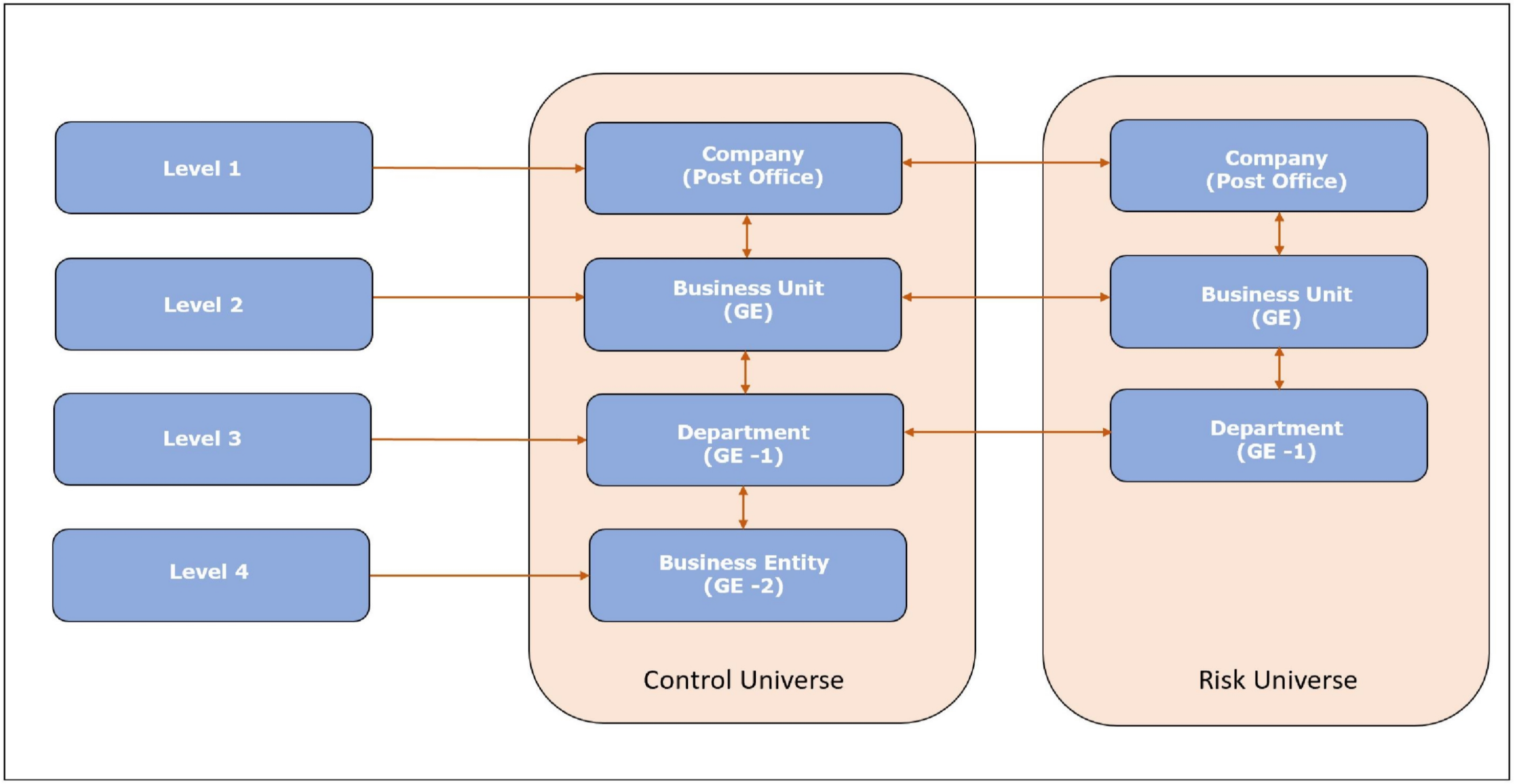
The role of Internal Audit is to understand the key risks of the organisation and to provide independent assurance to management and the Board over the adequacy and effectiveness of the frameworks of risk management and internal control operated by Post Office. This is done through an annual risk based audit programme as approved by the ARC. The programme will include an appraisal of the effectiveness of Second Line activities as well as in depth reviews of First Line activities.

Appendices DRAFT

Appendix A – Governance Risk & Compliance Framework


Good governance practices, audit results, industry practice
Internal and External risks, threats, vulnerabilities
Laws, regulations, statutes, standards, audit results, industry practice
Governance processes
Risk management processes
Compliance Processes
GRC Program
Business operations, goals, objectives, policies, procedures, staffing, technology.

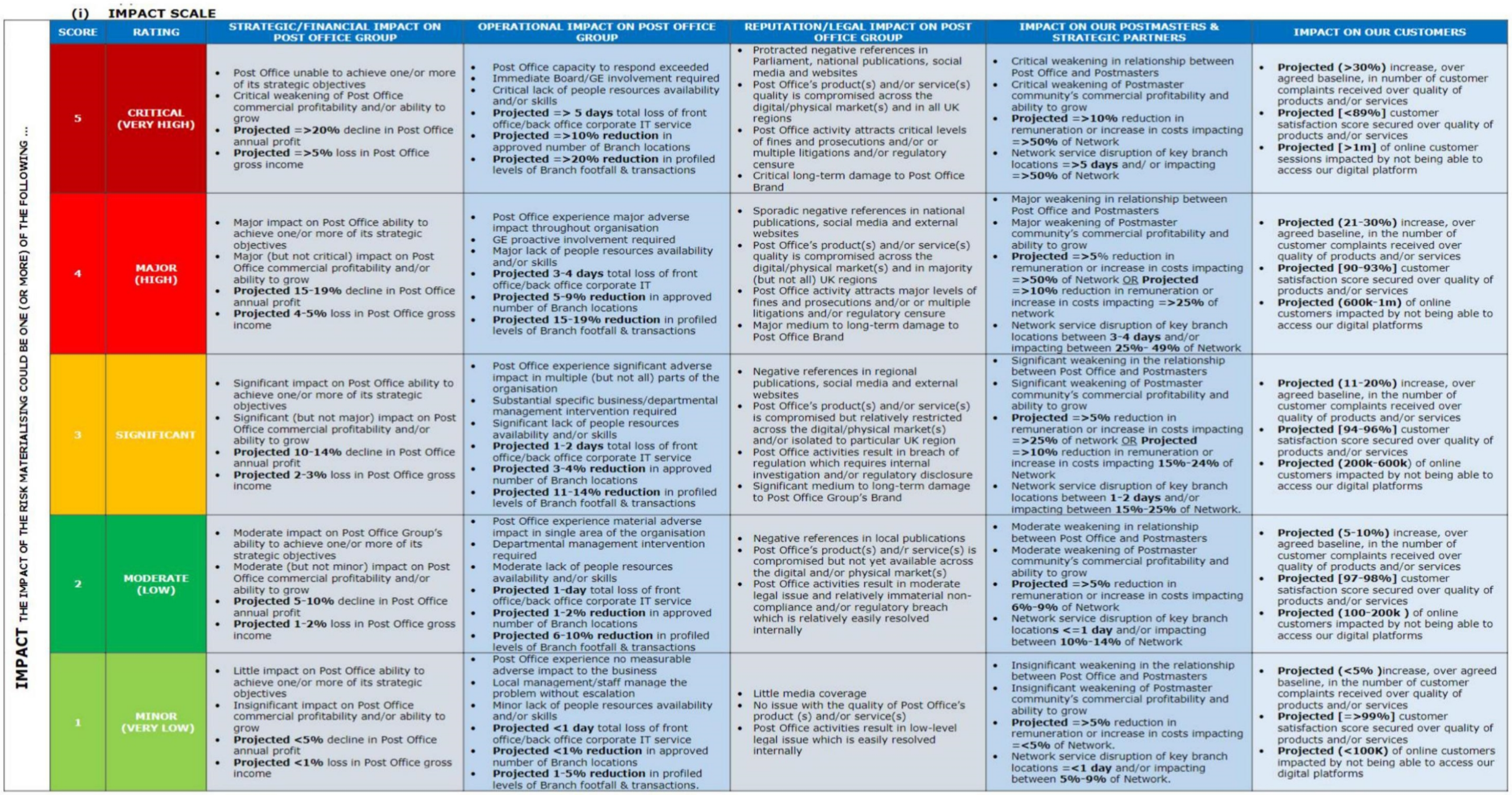
Appendix B – Control and Risk Universe DRAFT



POST OFFICE

Appendix C – Post Office Corporate Harm Table

DRAFT



(i) **IMPACT SCALE**

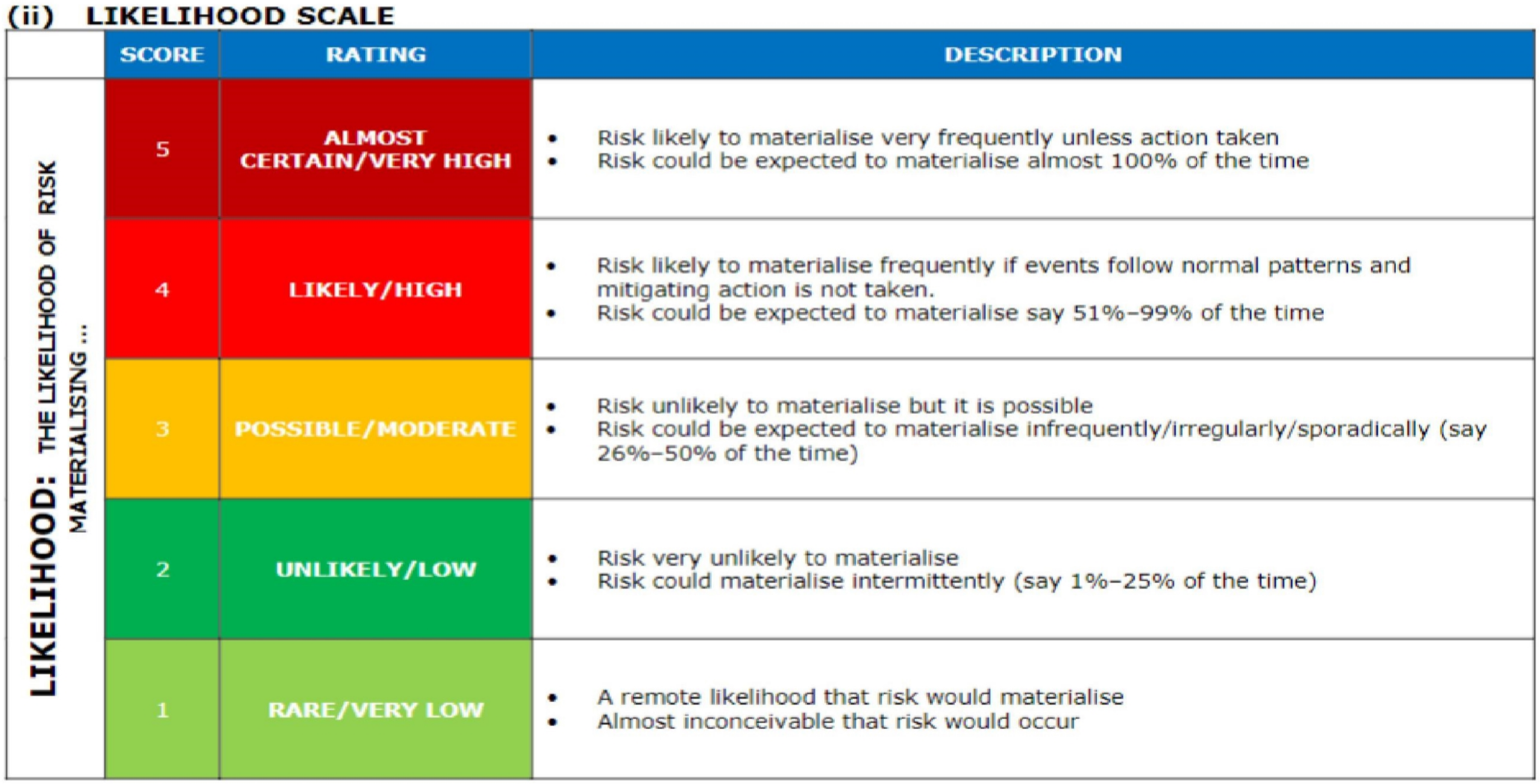
IMPACT THE IMPACT OF THE RISK MATERIALISING COULD BE ONE (OR MORE) OF THE FOLLOWING …

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)	• Post Office unable to achieve one/or more of its strategic objectives • Critical weakening of Post Office commercial profitability and/or ability to grow • **Projected =>20%** decline in Post Office annual profit • **Projected =>5%** loss in Post Office gross income	• Post Office capacity to respond exceeded • Immediate Board/GE involvement required • Critical lack of people resources availability and/or skills • **Projected => 5 days** total loss of front office/back office corporate IT service • **Projected =>10% reduction** in approved number of Branch locations • **Projected =>20% reduction** in profiled levels of Branch footfall & transactions	• Protracted negative references in Parliament, national publications, social media and websites • Post Office's product(s) and/or service(s) quality is compromised across the digital/physical market(s) and in all UK regions • Post Office activity attracts critical levels of fines and prosecutions and/or or multiple litigations and/or regulatory censure • Critical long-term damage to Post Office Brand	• Critical weakening in relationship between Post Office and Postmasters • Critical weakening of Postmaster community's commercial profitability and ability to grow • **Projected =>10%** reduction in remuneration or increase in costs impacting **=>50%** of Network • Network service disruption of key branch locations **=>5 days** and/ or impacting **=>50%** of Network	• **Projected (>30%)** increase, over agreed baseline, in number of customer complaints received over quality of products and/or services • **Projected [<89%]** customer satisfaction score secured over quality of products and/or services • **Projected [>1m]** of online customer sessions impacted by not being able to access our digital platform
4	MAJOR (HIGH)	• Major impact on Post Office ability to achieve one/or more of its strategic objectives • Major (but not critical) impact on Post Office commercial profitability and/or ability to grow • **Projected 15-19%** decline in Post Office annual profit • **Projected 4-5%** loss in Post Office gross income	• Post Office experience major adverse impact throughout organisation • GE proactive involvement required • Major lack of people resources availability and/or skills • **Projected 3-4 days** total loss of front office/back office corporate IT • **Projected 5-9% reduction** in approved number of Branch locations • **Projected 15-19% reduction** in profiled levels of Branch footfall & transactions	• Sporadic negative references in national publications, social media and external websites • 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 • Post Office activity attracts major levels of fines and prosecutions and/or or multiple litigations and/or regulatory censure • Major medium to long-term damage to Post Office Brand	• Major weakening in relationship between Post Office and Postmasters • Major weakening of Postmaster community's commercial profitability and ability to grow • **Projected =>5%** reduction in remuneration or increase in costs impacting **=>50%** of Network OR **Projected =>10%** reduction in remuneration or increase in costs impacting **=>25%** of network • Network service disruption of key branch locations between **3-4 days** and/or impacting between **25%- 49%** of Network	• **Projected (21-30%)** increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services • **Projected [90-93%]** customer satisfaction score secured over quality of products and/or services • **Projected (600k-1m)** of online customers impacted by not being able to access our digital platforms
3	SIGNIFICANT	• Significant impact on Post Office ability to achieve one/or more of its strategic objectives • Significant (but not major) impact on Post Office commercial profitability and/or ability to grow • **Projected 10-14%** decline in Post Office annual profit • **Projected 2-3%** loss in Post Office gross income	• Post Office experience significant adverse impact in multiple (but not all) parts of the organisation • Substantial specific business/departmental management intervention required • Significant lack of people resources availability and/or skills • **Projected 1-2 days** total loss of front office/back office corporate IT service • **Projected 3-4% reduction** in approved number of Branch locations • **Projected 11-14% reduction** in profiled levels of Branch footfall & transactions	• Negative references in regional publications, social media and external websites • 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 • Post Office activities result in breach of regulation which requires internal investigation and/or regulatory disclosure • Significant medium to long-term damage to Post Office Group's Brand	• Significant weakening in the relationship between Post Office and Postmasters • Significant weakening of Postmaster community's commercial profitability and ability to grow • **Projected =>5%** reduction in remuneration or increase in costs impacting **=>25%** of network OR **Projected =>10%** reduction in remuneration or increase in costs impacting **15%-24%** of Network • Network service disruption of key branch locations between **1-2 days** and/or impacting between **15%-25%** of Network.	• **Projected (11-20%)** increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services • **Projected [94-96%]** customer satisfaction score secured over quality of products and/or services • **Projected (200k-600k**) of online customers impacted by not being able to access our digital platforms
2	MODERATE (LOW)	• Moderate impact on Post Office Group's ability to achieve one/or more of its strategic objectives • Moderate (but not minor) impact on Post Office commercial profitability and/or ability to grow • **Projected 5-10%** decline in Post Office annual profit • **Projected 1-2%** loss in Post Office gross income	• Post Office experience material adverse impact in single area of the organisation • Departmental management intervention required • Moderate lack of people resources availability and/or skills • **Projected 1-day** total loss of front office/back office corporate IT service • **Projected 1-2% reduction** in approved number of Branch locations • **Projected 6-10% reduction** in profiled levels of Branch footfall & transactions	• Negative references in local publications • Post Office's product(s) and/r service(s) is compromised but not yet available across the digital and/or physical market(s) • Post Office activities result in moderate legal issue and relatively immaterial non-compliance and/or regulatory breach which is relatively easily resolved internally	• Moderate weakening in relationship between Post Office and Postmasters • Moderate weakening of Postmaster community's commercial profitability and ability to grow • **Projected =>5%** reduction in remuneration or increase in costs impacting **6%-9%** of Network • Network service disruption of key branch location**s <=1 day** and/or impacting between **10%-14%** of Network	• **Projected (5-10%)** increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services • **Projected [97-98%]** customer satisfaction score secured over quality of products and/or services • **Projected (100-200k)** of online customers impacted by not being able to access our digital platforms
1	MINOR (VERY LOW)	• Little impact on Post Office ability to achieve one/or more of its strategic objectives • Insignificant impact on Post Office commercial profitability and/or ability to grow • **Projected <5%** decline in Post Office annual profit • **Projected <1%** loss in Post Office gross income	• Post Office experience no measurable adverse impact to the business • Local management/staff manage the problem without escalation • Minor lack of people resources availability and/or skills • **Projected <1 day** total loss of front office/back office corporate IT service • **Projected <1% reduction** in approved number of Branch locations • **Projected 1-5% reduction** in profiled levels of Branch footfall & transactions.	• Little media coverage • No issue with the quality of Post Office's product (s) and/or service(s) • Post Office activities result in low-level legal issue which is easily resolved internally	• Insignificant weakening in the relationship between Post Office and Postmasters • Insignificant weakening of Postmaster community's commercial profitability and ability to grow • **Projected =>5%** reduction in remuneration or increase in costs impacting **=<5%** of Network. • Network service disruption of key branch locations **=<1 day** and/or impacting between **5%-9%** of Network.	• **Projected (<5%)**increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services • **Projected [=>99%]** customer satisfaction score secured over quality of products and/or services • **Projected (<100K)** of online customers impacted by not being able to access our digital platforms

POL00447843

Appendix C – Post Office Corporate Harm Table

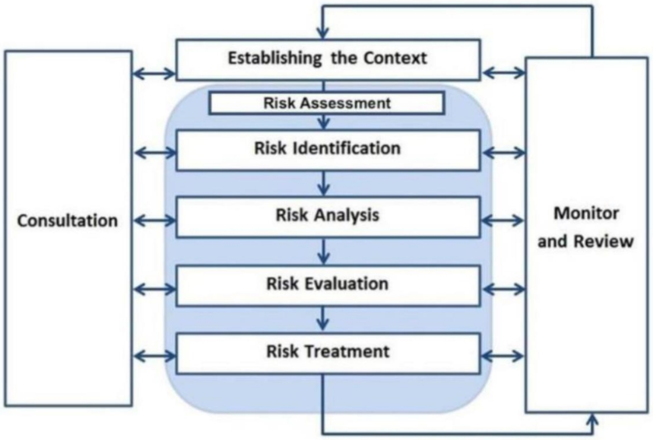
DRAFT



(ii) LIKELIHOOD SCALE

	SCORE	RATING	DESCRIPTION
LIKELIHOOD: THE LIKELIHOOD OF RISK MATERIALISING …	5	ALMOST CERTAIN/VERY HIGH	• Risk likely to materialise very frequently unless action taken • Risk could be expected to materialise almost 100% of the time
	4	LIKELY/HIGH	• Risk likely to materialise frequently if events follow normal patterns and mitigating action is not taken. • Risk could be expected to materialise say 51%–99% of the time
	3	POSSIBLE/MODERATE	• Risk unlikely to materialise but it is possible • Risk could be expected to materialise infrequently/irregularly/sporadically (say 26%–50% of the time)
	2	UNLIKELY/LOW	• Risk very unlikely to materialise • Risk could materialise intermittently (say 1%–25% of the time)
	1	RARE/VERY LOW	• A remote likelihood that risk would materialise • Almost inconceivable that risk would occur

Appendix D – Risk Management Process



Appendix E – Control Self-Assessment Sampling (CSA) Methodology

The table below provides the CSA frequency and sampling methodology:

Functional Compliance Team			
Control Frequency	**Testing Frequency**	**Minimum Sample Size**	**Sample Period**
Annual	Annual	1 (Annually - 1)	Prior 12 months
Quarterly	6 Monthly	1 (Annually - 2)	Prior 6 months
Monthly	Quarterly	1 (Annually - 3)	Prior 3 months
Weekly	Monthly	1 (Annually - 6)	Prior Month
Daily	Monthly	2 (Annually - 6)	Prior Month
Automated*	Annually	1 (Annually - 1)	Prior 12 Months
Ad-hoc	Obtain guidance from the Group Compliance Team for minimum sample size and frequency.		

*Automated controls are those that require no manual intervention and or monitoring.

Group Compliance and Group Risk can also perform sampling to ensure and assess Control Framework Standards and principles are being adhered to. The sample size may vary depending on issues/incidents and or breaches.

The direction of travel should be to reduce sampling checks by Group and replace with an integrated second line assurance plan. This will be contingent on Functional Compliance Teams being able to demonstrate that the POL CF has been embedded in a consistent manner. This transition would be ratified by the RCC.

Appendix F – Illustrative example of a POL Group Compliance Dashboard:

Area	Measure	Month	YTD	Prior Year End	Target	Explanation / Commentary
Cultures and behaviours	Tone from the top/Ways of Working (Are GE displaying the right behaviours, values and cultures)				> XX% or Score	This would be sourced from the people engagement score Will need to agree with GE which Questions this would be based on (Consider Metrics of REMCO)
	Training Completion %				95%	Sourced from L&D and metrics issued on a monthly basis Highlighting functional exceptions
Legal & Regulatory Issues and Incidents	Regulatory Breaches #				Reducing Trend	Sourced from Functional Dashboards Highlighting trends and thematic
	Remediations Overdue				0	All Regulatory Issues and Incidents should be tracked in Functions in which they are owned and there should be a remediation plan
Operational Issues and incidents	Issues and Incidents #				Reducing Trend	Sourced from Functional Dashboards Highlighting trends and thematic
	Repeats #				0	Focussing on RCA and efficacy of remediations (if in place)
	PM Detriment #				0 Reducing Trend	Identifying if any issues/incidents has led to or could have led to PM detriment
	Remediations Overdue				0	Sourced from Functional Dashboards
Policy Compliance and Breaches	Level of Non-compliance #					Sourced from Issues and incidents (ie may be an overlap) and from policy reviews
Technology Releases/Changes	P1 / P2 incidents #				Reducing Trend	Summarising RCA for P1 and P2's, and identifying RCA and trends/thematic
Overdue Internal Audit Management Actions	Overdue Actions # > 3 months				0 Reducing Trend	Sourced from Internal Audit, with exceptions highlighted if represent material risks
Overdue Group Compliance Management Actions	Overdue Actions # > 3 months				Reducing Trend	If and when Group Compliance have an integrated Assurance plan.
Control Self-Assessment – First Line Results	CSA due vs completed #/#				>95%	Sourced from Functional Dashboards
	Pass rate %				>95%	With failures summarised and tracked as exceptions
Control Self-Assessment – Group Compliance	Pass rate %				100%	This is the results of the Group Compliance sampling
Risk Management	Enterprise Risk - # OOT (# No remediation plan)		NA		Reducing Trend	Tracked from the GE and sourced from Group Risk. Expect to have OOT risk but then we should have remediations unless OOT has been accepted by Board
	Intermediate Risk - # OOT (# No remediation plan)		NA		Reducing Trend	Tracked from the GE and sourced from Group Risk
	Local Risk - # OOT (# No remediation plan)		NA		Reducing Trend	Probably not for this dashboard but should be part of GE Functional Dashboards.
Data Management Maturity	TBC					Not sure but I think may be needed once we have a Data Management Committee and aligned data maturity strategy and delivery plan
Status of Assurance on Historical matters	TBC					Again not sure but feel in the short term this may be needed to be monitored separately.

NB: Once agreed, this dashboard will be submitted to the GE on a monthly basis. The measures will be RAGed to ease identification of exceptions. Also if and when agreed we will need time to operationalise this to weed out any operational data issues and embed this efficiently across the functions and or Group.