Appendix 1 - NatWest Group Internal Audit Charter

The operation of Group Internal Audit (GIA) in NatWest Group (the Group) and its subsidiary companies is governed by the Group Internal Audit Charter, which is reviewed and approved annually by the Group Audit Committee (GAC).

1.A.1 OVERVIEW

GIA, as the third Line of Defence and in accordance with the Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF), is responsible for providing independent and objective assurance to the Group Board, its subsidiary legal entity boards and executive management on the adequacy and effectiveness of key internal controls, governance and the risk management in place to monitor, manage and mitigate the key risks to the Group and its subsidiary companies achieving their objectives.

1.A.2 REMIT, ROLE AND COVERAGE

GIA's remit is unrestricted and is overseen by the Group Chief Audit Executive (Group CAE).

In line with its role and responsibilities, GIA has a risk based coverage approach to provide sufficient assurance on the adequacy of the design and operational effectiveness of key internal controls, governance and risk management in place to monitor, manage and mitigate the key risks to the Group and its subsidiary companies.

The frequency and scope of audit coverage is determined from an on-going assessment of key risks to the Group and its subsidiary companies. Execution of the Audit Plan includes obtaining an understanding of the Group and its subsidiary companies' processes and systems. All engagements are performed in accordance with the IPPF and operationalised through GIA's audit methodology and procedures.

GIA responds to regulators' requests including providing assurance on specified areas and assessing progress on the Group and its subsidiary companies' remediation activities.

In addition, where appropriate, GIA provides advice to the Group and its subsidiary companies on the adequacy and effectiveness of key internal controls, governance and risk management.

1.A.3 RIGHTS AND AUTHORITY

GIA derives its authority from the Board through the GAC. The Group CAE is authorised by the GAC to have full and unrestricted access to any of the Group and its subsidiary companies' personnel, including senior management and the Board, physical records, data, IT systems, digital communications, locations and physical property for the purpose of GIA fulfilling its roles and responsibilities. The Group CAE is responsible for ensuring that this authority is exercised responsibly and that confidentiality is maintained over all information and records obtained.

The Group CAE also has:

- The right to be informed promptly of any major potential or actual control failures relevant to the Group and its subsidiary companies, including those identified by external auditors, regulators or other external parties.
- The right of attendance at any committees that the Group CAE, CAEs of subsidiary legal entities, Chief Auditors or regional Heads of Audit consider relevant or necessary.
- The right to be informed promptly of any major acquisition, re-organisation or disposal that may have a material impact on the risk management and control environment of the Group or its subsidiary companies.

The Group and its subsidiary companies make sure GIA has the appropriate level of access to third parties through the inclusion of agreed wording in contracts and service level agreements. All employees are requested to assist GIA in performing its role.

1.A.4 INDEPENDENCE

Reporting Lines

The Group CAE reports to the Chair of the GAC and has a secondary reporting line to the Group's Chief Executive (CEO) for administrative purposes only[1].

Oversight of Group CAE Performance

The GAC is responsible for the appointment and termination of employment of the Group CAE, subject to approval under the FCA / PRA Approved Persons' regime. The objectives and performance review of the Group CAE are determined by the Chair of the GAC with support from the CEO. The Chair of the GAC is responsible for approving the remuneration of the Group CAE, with support from the CEO, and for recommending the remuneration of the Group CAE to the Group Performance and Remuneration Committee.

Independence, Objectivity and Conflicts

GIA executes its duties freely and objectively in accordance with the IIA's Code of Ethics and Standards on independence and objectivity. IA does not:

- Set the risk appetite for the Group or its subsidiary companies.
- Impose risk management processes.
- Replace management's quality assurance activities or the challenge and testing activities of the second Line of Defence.
- Take decisions on risk mitigation, including designing action plans and risk acceptance.
- Implement risk mitigation actions on behalf of management.
- Take responsibility for risk management.

GIA avoids or manages any conflicts of interest and the Group CAE reports to GAC, at least annually, on the organisational independence of the function.

GIA does not have direct operational responsibility or authority over any of the areas audited and individuals only audit areas of previous responsibility in line with the GIA Conflicts Policy.

GIA does not implement internal controls, develop procedures, install systems, prepare records or engage in any other similar activity that may impair or be seen to impair its judgement.

1.A.5 PROFESSIONAL PRACTICES

GIA complies with the IIA's IPPF, which comprises mandatory guidance on Core Principles, the Code of Ethics, Standards and the Definition of internal auditing. In addition, GIA adheres to all applicable jurisdictional internal audit specific requirements and relevant Group policies and procedures. GIA is required to comply with the following ten Core Principles:

- Demonstrate integrity.
- Demonstrate competence and due professional care.
- Be objective and free from undue influence (independent).
- Align with the strategies, objectives, and risks of the organisation.
- Be appropriately positioned and adequately resourced.
- Demonstrate quality and continuous improvement.
- Communicate effectively.
- Provide risk-based assurance.
- Be insightful, proactive, and future-focused.
- Promote organisational improvement.

GIA maintains dialogue with key regulators and professional and industry bodies, including the IIA and CIIA, to ensure operating processes and standards are aligned to current thinking and guidance.

[1] Illustrative examples of this include approval of travel and expenses, approval of systems' access/permissions, approval of personal account dealing requests and approval of annual leave requests.

1.A.6 RESOURCES

The Group CAE is responsible for making sure GIA is sufficiently resourced, both in terms of capacity and capability and has access to the resources and expertise necessary to undertake work across the Group and its subsidiary companies, including specialist areas.

GIA operates an environment of continuous professional development, to ensure skills and knowledge are maintained and developed, including supporting Professional Certifications and Qualifications.

1.A.7 INTERACTION WITH THE GAC

GIA interacts with the GAC to support it in discharging its oversight responsibilities in respect of GIA:

- To review the Internal Audit Charter.
- To approve GIA's annual Audit Plan and budget, with reference to the appropriateness of proposed risk coverage and to receive updates on progress.
- To monitor and review, at least annually, the effectiveness of GIA.
- To receive and review a summary of Quality Assurance results.
- To assess and confirm the independence of the GIA function.
- To receive and review GIA's periodic Opinion, which reports on the overall adequacy and effectiveness of key internal controls, governance and risk management; issues identified and the adequacy of management's remediation activity.

1.A.8 SUBSIDIARY AND BRANCH IA

The CAEs of subsidiary legal entities have a reporting line into the Chair of the relevant Audit Committee, in addition to a functional reporting line into the Group CAE.

Regional Heads of Audit have a functional reporting line into the Group CAE, in addition to any statutory or regulatory required reporting line within the branch's governance structure.

1.A.9 RELIANCE ON THE WORK OF OTHERS

GIA may place reliance on the work of other functions within the Group and its subsidiary companies after performing a review to confirm that the IIA requirements for assurance providers have been met. Exceptionally and with the approval of the Group CAE, GIA may also place reliance on other assurance providers external to the Group and its subsidiary companies.

1.A.10 QUALITY ASSURANCE AND IMPROVEMENT

GIA develops and maintains a quality assurance and improvement programme (QAIP) that covers all aspects of GIA activity. The QAIP is performed by individuals who are independent of the delivery of the Audit Plan and who have sufficient knowledge of internal audit practices and the IPPF. A summary of the quality assurance results is reported to the GAC at least annually by the Group CAE or the Head of Practices and Strategy.

The GAC will commission an independent external quality assessment review of GIA at least every five years in line with IIA Standards.

Approved by:

Group Audit Committee (GAC)

Date: 13 December 2021