



GROUP INTERNAL AUDIT'S CHARTER

This Charter sets out the mandate, approach, responsibility and authority of Group Internal Audit ("GIA"). It has been informed by the mandatory elements of The Chartered Institute of Internal Auditors' ("IIA") International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the International Standards for the Professional Practice of Internal Auditing ("Standards") and the IIA's Guidance on Effective Internal Audit in Financial Services ("the Code").

GIA's Mandate

GIA is an independent function whose primary role is to help the Board and Executive Management to protect the assets, reputation and sustainability of the Group.

GIA does this by risk assessing the organisation and its activities (including outsourced activities and all legal entities). This assessment, together with audits required (or expected) by regulators, allows GIA to formulate and execute an annual plan of audit and review activity (the "Plan") to form an opinion on the control environment and management's control approach. GIA does not have to cover all scope areas every year. The Plan is reviewed on a periodic basis to assess the impact of changing risks, with any significant changes to the Plan discussed and reviewed with senior management and approved by the Audit Committee.

The scope of GIA activities encompasses, but is not limited to, objective examinations of evidence for providing independent assessments on the adequacy and effectiveness of risk management, control and governance processes for the Group. GIA also performs reviews at the specific request of regulators, senior management or the Audit Committee. GIA assesses if key risks have been identified, governed in line with the established risk management processes (including risk appetite) and reported by senior management and/or the Risk function to Committees and Executive Management. GIA considers business strategy, policies and procedures as well as the Group's key priorities as part of this evaluation. It also considers whether the outcomes achieved, and the way business is conducted is in line with the objectives, risk appetite and valued behaviours of the organisation.

In line with the Group's valued behaviours ("Do the right thing", "Never settle" and "Better together"), GIA has also included culture considerations and indicators in its work, and specifically how the observed behaviours may impact the risk and control environment.

There is no aspect of the organisation which GIA is restricted from looking at as it delivers on its mandate. GIA's scope includes information presented to the Board for strategic

GROUP INTERNAL AUDIT'S CHARTER

decision making, including a review of significant business process changes, key corporate events, new products and services, acquisitions and divestments.

Audit Approach

GIA represents the third line of defence and provides independent assurance on the effectiveness of controls that support the first line's risk management of business activities and the control processes maintained by the second line. GIA works with the Group's other control functions, such as Finance, Risk and Compliance, but does not place unqualified reliance on their work.

The audit programme includes obtaining an understanding of the processes and systems under audit review, evaluating the design of controls, and testing the operating effectiveness and outcomes of key controls. In its approach, GIA evaluates the potential for the occurrence of fraud and how the organisation manages fraud risk. Additionally, GIA will consider management's control approach and whether the Group's actions achieve fair outcomes for clients, investors, our reputation and the markets in which we operate. A defined audit methodology is maintained by GIA. This is determined and refined in accordance with industry best practice from the IIA Standards and the Code, as recognised by regulators and statutory auditors.

GIA's core assurance work is audits and the main output of an audit is a graded report with an opinion on the control environment and, where applicable, management's control approach. GIA performs other types of review work including control and special reviews as well as continuous risk assessment activities to keep abreast of changing risks. GIA may issue an ungraded audit report, subject to approval by the GIA Chief Operating Officer or Group Head, Internal Audit.

Working with senior management, GIA supports long term improvements in the Group's control environment and tracks that sustainable corrective action plans are effectively implemented.

Authority and Independence

To ensure independence, GIA will remain free from interference by any element in the Group, including in matters of audit selection, scope, procedures, frequency, timing or report content. The following safeguards are in place:

1. The Audit Committee approves GIA's budget and resourcing, which are presented by the Group Head, Internal Audit;
2. The Audit Committee recommends the appointment and removal of the Group Head, Internal Audit;
3. The Remuneration Committee (of which all members are independent Non-Executive Directors) sets the remuneration of the Group Head, Internal Audit;

GROUP INTERNAL AUDIT'S CHARTER

4. The Group Head, Internal Audit reports to the Chairman of the Audit Committee and administratively to the Group Chief Executive, which ensures that GIA has the necessary independence, as well as authority, to exercise judgement, express opinions and make recommendations;
5. Internal auditors have no direct operational responsibility or authority over any of the activities they review. Accordingly, they do not develop or install systems or procedures, prepare records, or engage in any other activity which would normally be audited. In exceptional cases, GIA may second staff to other areas of the Bank. GIA's methodology contains procedures for handling actual or perceived conflicts of interest which includes performing an assessment to identify potential conflicts and implementing a 12-month cooling-off period for secondees returning to GIA during which secondees must not audit areas to which they were seconded; and
6. GIA may initiate direct communication with any member of staff, examine any activity or entity of the Group and has full and unconditional access to any records, files, data and physical properties of the Group. This includes access to management information systems and records, as well as the agendas, papers and minutes of all committees and forums. Furthermore, GIA has the right to attend and observe all executive committees and management meetings and any other management decision making forums across the Group.

The Group Head, Internal Audit will confirm to the Audit Committee, at least annually, the organisational independence of the internal audit activity. If the Group Head, Internal Audit determines that independence or objectivity may be impaired in fact or appearance, the details of impairment will be disclosed to the Audit Committee or the appropriate parties.

Reporting

GIA reports the results of its work at multiple levels within the organisation on a regular basis. The key reporting from GIA is as follows:

Audit Committee

- All control environment "Fails" or management control approach "Weak" reports;
- All audit issues that are rated Group Very High and High Risk; and issues deemed significant to the Group by Group Head, Internal Audit;
- A summary of the Management Control Approach ("MCA") scorecard results at a Group level and by Management Team member;
- Analysis of themes and trends emerging from GIA's work, and their impact on the organisation's risk profile;

GROUP INTERNAL AUDIT'S CHARTER

- An independent view of management's reporting on the risk management of the organisation, including management's remediation plans, and highlighting significant audit issues that are overdue for resolution;
- The people and functional strategy for GIA, including purpose, mandate and priorities;
- The performance of the Plan and any significant changes to it;
- Resourcing and budget;
- Any management responses to risk that may be unacceptable to the organisation; and
- The results of the quality assurance programme at least annually.

Other Board Committees

- GIA provides tailored reporting on the results of its work to the Brand, Values, and Conduct Committee ("BVCC"), Board Risk Committee ("BRC") and Board Financial Crime Risk Committee ("BFCRC") on the risk areas under their responsibility.

In addition to the reporting above, GIA reports the results of its work to senior management as well as to risk committees. A scorecard by each Management Team member on MCA and the control environment is provided quarterly.

People and Valued Behaviours

The Group Head, Internal Audit is responsible for assessing the skillset, resources and budget for GIA and presenting this to the Audit Committee. To enable audit work to be completed to a high standard, GIA monitors that its staff have an adequate mix of risk, business and professional audit skills to execute the Plan, and to provide independent and effective challenge to senior management. Where necessary, specialist co-source may be engaged to support the Plan.

All staff in GIA must exhibit the highest level of professional objectivity in gathering, evaluating and communicating information about the activity or process being examined. They must make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments. GIA will adhere to the Definition of Internal Auditing, the Core Principles for the Professional Practice of Internal Auditing, Code of Ethics and the Standards for the Professional Practice of Internal Auditing that are published by the IIA. It is expected that all members of GIA strive to operate as role models for the Group's valued behaviours. GIA methodology has defined "Habits of a Human Auditor" which are aligned to the Group's valued behaviours and communicated across the function.

GROUP INTERNAL AUDIT'S CHARTER

Through the Guest Auditor Programme, as well as short-term secondments and longer-term rotations into and out of the function, GIA plays a role in supporting the development of the Group's future leaders.

Quality Assurance and Improvement Programme

GIA will maintain a quality assurance and improvement programme which assesses the efficiency and effectiveness of GIA activities and identifies opportunities for improvement. This programme, overseen by the Group Head, Internal Audit, will include an evaluation of GIA's conformance with the Standards and the application of the IIA's Code of Ethics. The Head of Quality Assurance will provide an independent report on the results of its work to the Audit Committee on at least an annual basis.

The Audit Committee is responsible for evaluating the performance of GIA on a regular basis. Key performance indicators for GIA are tracked and included in a balanced scorecard. GIA is also subject to an external assessment at least every five years by an outside team of independent reviewers. This assessment will include the review of GIA's conformance with the mandatory elements of the IIA International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards and the Definition of Internal Auditing. The assessment also includes a review of the efficiency and effectiveness of the internal audit activity in carrying out this Charter and meeting the expectations of stakeholders.

Responsibility

The Group Head, Internal Audit is responsible for:

- Ensuring that the contents of this Charter are implemented within GIA and for establishing a process to ensure that GIA is performing in accordance with its Charter, standards and practices; and
- Reviewing the Charter and presenting it to the Audit Committee for approval at least annually.