Group Internal Audit Charter

Terms of Reference

Approved by the Group Audit Committee | 18 September 2024

Bank of Ireland Information Classification Green

Bank of Ireland

Group Internal Audit Charter

1. Purpose

As the third line of defence within the Group's Risk Management Framework[1], Group Internal Audit (GIA) provides independent, timely, objective, and reasonable assurance to its key stakeholders on the effectiveness of the Group's risk management, governance and internal control. GIA's purpose is to **'Help Make Bank of Ireland Better'**. To achieve this, we strive to protect the Group, it's customers and stakeholders and strengthen the Group's ability to create, protect and sustain value, by providing risk-based and objective assurance, insight and foresight. GIA seeks to contribute to the enhancement of risk management, including proactive identification of issues and risk exposures. GIA promotes sustainable remediation of identified issues and sharing of lessons learned, for the on-going benefit of the Group, its customers, and key stakeholders.

2. Mandate

Authority

The internal audit function's authority is created by its direct reporting relationship to the Group Audit Committee (GAC). Such authority allows for unrestricted access to the GAC.

The GAC grants the internal audit function the mandate to provide the audit committees, risk committees and senior management with objective assurance, insight, and foresight. The scope of the mandate covers all of the Group's activities, including services provided by third parties, subject to the right to audit. Assurance activities will be risk-based to focus on the material risk types arising from the Group's activities, together with any regulatory mandated audits.

The GAC:

- Authorises GIA to have unrestricted access to all of the Group's functions, records, assets, property and personnel necessary for the discharge of GIA's responsibilities (see Section 3); and
- Approves the GIA budget and resource plan to allow for GIA to carry out its responsibilities effectively.

Role

The role of GIA is to understand the Group's risk types and to evaluate the adequacy and effectiveness of the systems of risk management, governance and internal control, within first and second lines of defence. This includes assessing adherence to the risk management activities and requirements outlined in the Risk Management Framework and risk policies. This enables GIA to provide reasonable assurance to the GAC of the Board of Bank of Ireland Group plc, the Court Audit Committee (CAC) of the Court of Directors of the Bank[2], the Board Risk Committee, Court Risk Committee, subsidiary audit and risk committees as relevant, management and other interested parties (including regulators/supervisors, and external auditors), on how effective the Group's principal risk types are being identified, assessed, monitored, managed and reported.

At least annually, GIA provides an update to the Board on the Group's overall control environment[3] and risk management framework maturity. The quality of enterprise insight conveyed via these overall opinions represent the most prominent mechanism through which GIA delivers its purpose to Bank of Ireland and form the basis of all supporting plans and activities. GIA utilises a range of products and approaches, with a focus on agility, to ensure these opinions are up to date and comprehensive to enable the Board and management to make informed and timely decisions.

GIA's role in the provision of independent assurance operates on the basis that management has primary accountability for effective risk management and control, including the management of fraud risk.

While maintaining its independence, GIA can also provide Advisory Services which are capped and managed at five per cent of available time.

Independence and Objectivity

GIA's independence is protected by the authority vested in it by the GAC and all GIA activities shall remain free from undue influence by management or other restrictions. GIA staff are required to have and maintain an impartial, unbiased attitude and avoid any conflict of interest. A GIA Code of Ethics is in place to limit impairment to independence and objectivity. When GIA staff become aware of an impairment that may affect their objectivity, a disclosure of impairment is made to the assignment supervisor or the Group Chief Internal Auditor (GCIA).

The GCIA manages the internal audit function and has a primary (functional) reporting line to the Chair of the GAC, as well as a secondary (administrative) reporting line to the Group CEO. The GAC is responsible for approving the GIA risk-based assurance plan, the supporting annual budget, and resource plan. The GAC also approves the performance appraisal and remuneration of the GCIA, subject to the determination of the Group Remuneration Committee. Any changes must be discussed with the Chair of the GAC prior to implementation. GAC are also responsible for the appointment, replacement or dismissal of the GCIA.

Additionally, where the GCIA has roles and or responsibilities that fall outside of internal auditing, safeguards are in place to provide measured separation of the dual roles. The GCIA refrains from reviewing or approving any internal audit assurance report for non-internal audit functions over which the GCIA has management responsibilities. i.e. Speak-up and Sensitive Investigations. A GIA guidance document is in place that requires an independent party outside the internal audit function to oversee assurance of these activities.

As independence is essential in ensuring the effectiveness of the internal audit function, internal auditors cannot themselves develop or implement systems or procedures or controls or engage in any other activity they normally would be expected to review. In addition, internal auditors are precluded from auditing specific operations that they had previously been responsible for, or directly involved in, for a minimum period of 1 year[4].

[1] The Risk Management Framework is a document owned by the Group Chief Risk Officer that sets out Bank of Ireland's group wide approach to risk management.

[2] The duties of the GAC extend to the Company and the Group as a whole, while the duties of the CAC extend to the GovCo Group as a whole, subject, where appropriate, to the authority of the GAC. The GovCo Group consists of the 'Bank' and its subsidiaries.

[3] Control Environment is the collection of frameworks, policies, controls and governance structures that provide the basis for carrying out internal control across the Group.

[4] GIA have prescribed controls in place to prevent such conflicts arising. Where co-sourcing or outsourcing is used, to avoid possible conflicts of interest, the co-source / outsource partner must ensure that a sufficient 'cooling-off' period (minimum of 1 year) has elapsed if the co-source / outsource partner carried out work in the area being reviewed in the Group.

Independence will not be compromised where GIA personnel attend steering committees or workshops if GIA is satisfied that no conflict arises between GIA's role on the committee/workshop and as an independent assurance provider. In agreement with GIA, the Terms of Reference of such committees should clearly stipulate the role of GIA in attendance. Additionally, GIA guidance on advisory services is in place to limit impairment to independence and objectivity.

The GCIA provides an annual attestation of independence to the GAC, CAC and subsidiary audit committees, as relevant. In the event of any conflict or impairment of independence arising, the GCIA will inform the Chair of the GAC/CAC and the subsidiary audit committees as relevant, at the earliest possible opportunity.

GIA governs itself by adherence to the Global Internal Audit Standards, including the principles of Ethics and Professionalism (Integrity, Objectivity, Competency, Due Professional Care, and Confidentiality).

Responsibilities

The GCIA is accountable to the GAC, CAC and subsidiary audit committees, as relevant, for GIA's programme of assurance activities, including the reporting of overall findings and any areas of concern resulting from such assurance activities.

GIA's assurance activities include a number of undertakings (on a risk-based approach where appropriate):

- reviewing and assessing the governance, risk management and internal control of the Group, including the risk and control culture;
- reviewing and assessing the specific risk management activities outlined in the Risk Management Framework: Risk Identification and Assessment, Risk Appetite, Risk Policies, Stress Testing and Scenario Analysis, and Risk Monitoring and Reporting;
- reviewing the effectiveness of the Group's management of the Principal Risk Types (Level 1) and Operational Sub Risk Types (Level 2) as defined in the Risk Management Framework;
- assessing and providing opinion on the Group's control environment and risk management framework maturity on an enterprise-wide level;
- reviewing and assessing key management information used for strategic and operational decision making;
- responding to regulator/supervisor requests, including those in relation to review of remedial actions; and
- evaluating specific operations at the request of GAC or management, as appropriate.

GIA is not relieved of responsibility to review areas of the Group that are subject to review by other Group functions or control self-assessment processes, but must assess the extent to which it can rely on the work of others in planning its assurance activities.

The GCIA will ensure that internal auditors:

- Conform with the Global Internal Audit Standards, including the principles of Ethics and Professionalism (Integrity, Objectivity, Competency, Due Professional Care, and Confidentiality);
- Understand, respect, meet, and contribute to the legitimate and ethical expectations of BOI Group[5];
- Are able to recognise conduct that is contrary to expectations and report organisational behaviour that is inconsistent with the Group's ethical expectations, as described in applicable policies and procedures;
- Have a work environment where internal auditors feel supported when expressing legitimate, evidence-based engagement results, whether favourable or unfavourable; and
- Adhere to established methodologies designed to guide the internal audit function.

The GCIA will ensure adherence to any applicable regulatory guidance and market conduct standards. For example, the Central Bank of Ireland's Individual Accountability Framework ('IAF') includes its own conduct standards which applies to GIA staff within controlled function roles.

Changes to the Mandate and Charter

The GCIA will consider any changes to the Mandate or other aspects to the GIA Charter at least annually or earlier in the event of a significant change to BOI Group or to the Global Internal Audit Standards. Proposed changes will be presented to the GAC for approval.

3. Access

GIA staff have unrestricted access to all of the Group's functions, records, assets, property and personnel necessary for the discharge of GIA's responsibilities. In addition, the GCIA has direct access to the Governor, the Group Chief Executive, and the Chairs of the GAC/CAC and subsidiary audit committees, as required.

This right of access extends to organisations that carry out outsourced functions on behalf of the Group and extends to businesses in which the Group has a substantial interest, subject to the Group's contractual right to audit. Any proposed exceptions to GIA's right of access must be approved by the GAC.

4. Reporting

The outcome of each assignment will be formally reported to the head of the relevant business unit and other parties, as appropriate. Assignments are required to be objective, timely, risk focused, and seek to add value.

GIA will follow up and report on the status of management actions to implement appropriate solutions to issues identified by GIA during its assurance activities. GIA reports on the status of all open and overdue issues to the GAC, CAC and subsidiary audit committees, and CEO as relevant.

GIA will meet with the Group's regulators/supervisors periodically and provide them with updates of the findings from completed assignments.

The GCIA will meet formally with the Group Chief Executive Officer on a quarterly basis, or more frequently where necessary. Likewise, the GCIA or delegate will meet with members of the Group Executive Committee on a quarterly basis, or more frequently where necessary. The GCIA, or nominated representative, is an attendee at GAC/CAC

[5] Per the Individuality Accountability Framework (IAF), GIA staff are required to contribute to the legitimate interests to BOI Group and its conduct to staff and its customers while performing their daily activities.

meetings, subsidiary audit and risk committee meetings, Board Risk Committee, Court Risk Committee and Executive Risk Committee (ERC) meetings. In addition, the GCIA is an independent attendee at Group Executive Committee meetings and has the right to attend any other Group committees or governance fora.

The GCIA will present formal updates to the GAC/CAC on at least six occasions per annum including updates on GIA's performance metrics as agreed by the GAC. The GCIA will update the Board Risk Committee, Court Risk Committee and subsidiary audit and risk committees as required. At least once per year, the GCIA will meet the GAC/CAC and subsidiary audit committees, without the presence of management. In addition, the GCIA will meet with the Chair of the GAC/CAC on a regular basis and additionally, with the chairs of subsidiary audit committees, as required.

In accordance with the Terms of Reference of the GAC and CAC, the GCIA may, if necessary, request the Secretary of the GAC and CAC to convene a meeting of the committee.

5. Planning

GIA's planned assurance activities are developed by assessing and prioritising the Group's higher risk areas. This is informed by a review of the Group's objectives, priorities, risks and challenges, and discussions with management, as well as members of the GAC/CAC and subsidiary audit committees, as relevant. The GIA Assurance Plan is approved by the CAC, subject to approval of the GAC, and relevant elements of the plan are provided to subsidiary audit committees for their approval, as relevant. The plan is flexible and subject to ongoing review to ensure the focus remains on areas of higher risk. The GCIA will communicate the impact of resource limitations and significant interim changes to senior management, the Board, the GAC, CAC and subsidiary audit committees, as relevant. Any material amendment to the plan requires the approval of the CAC, subject to approval of the GAC and subsidiary audit committees, as relevant.

6. Quality Assurance and Improvement Programme

GIA maintain a quality assurance and improvement program (QAIP) that covers all aspects of the internal audit function, including the internal audit function's conformance with the Global Internal Audit Standards. The QAIP is structured around four key elements: Methodology; Ongoing Monitoring of Performance; Quality Assurance Assessments; and Periodic External Assessments. On an ongoing basis, GIA's audit methodology is reviewed and aligned with the Institute of Internal Auditors' International Professional Practices Framework, which are the Global Internal Audit Standards and Topical Requirements ('IIA Standards') and the UK Chartered Institute of Internal Auditors' Internal Audit Code of Practice. GIA's audit methodology is also periodically reviewed in light of new developments and evolving industry practice. The QAIP includes a Quality Assurance (QA) programme that allows for both internal and external QA reviews and is aimed at ensuring adherence to audit methodology and the continuous improvement of GIA's assurance activities. Findings of the QA review programme are shared with the GAC, CAC and subsidiary audit committees on an annual basis as part of the QAIP update, and include an overview of QA results, key lessons learned, and actions taken to address them.

The GCIA will report annually to the GAC, CAC and subsidiary audit committees regarding the internal audit function's conformance with the IIA Standards. The GCIA will periodically discuss the mandatory aspects of the standards and the extent of the commitment to them with senior management, the GAC/CAC and subsidiary audit committees, as relevant. In the event that the GCIA is unable to conform with a mandatory requirement, alternative actions to achieve the related principle will be agreed and communicated as part of the annual QAIP update.

GIA seeks to ensure that staff have the required capability to meet the requirements of its Charter but, if a gap in the specific skills or expertise required for an assignment is identified, GIA will consider the option of co-sourcing or outsourcing.

In line with IIA standards, independent effectiveness reviews of GIA will be commissioned by the GAC at least every 5 years.

7. Integrity and Confidentiality

GIA staff are required to operate to the highest standards of integrity.

All information obtained or received by GIA staff in the course of duty or otherwise will be treated in accordance with the relevant risk policies and standards e.g. Information Security and Cyber Risk, Data Risk and Data Privacy Risk.

8. GCIA's Obligations under the Central Bank (Supervision and Enforcement) Act, 2013

Section 38(2) – Protected Disclosures specifies that a person appointed to perform a pre-approval controlled function, such as the GCIA, shall, as soon as it is practicable to do so, disclose to the Central Bank of Ireland (CBoI), information relating to one or more of the matters specified in The Act (Section 38), subsection (1)(a) to (d) which he or she believes will be of material assistance to the Bank:

(a) that an offence under any provision of financial services legislation may have been or may be being committed;

(b) that a prescribed contravention may have been or may be being committed;

(c) that any other provision of financial services legislation may have been or may be being contravened;

(d) that evidence of any matter which comes within paragraph (a), (b) or (c) has been, is being or is likely to be deliberately concealed or destroyed.

Should this occur, the following steps will be taken by the GCIA:

(i) the GCIA will establish if the matter has been/will be disclosed by management to the CBoI within a reasonable timeframe;

(ii) if the GCIA is not satisfied with step 1, the matter will be raised with the Chief Compliance Officer/Group Chief Risk Officer;

(iii) if the GCIA is not satisfied that the reporting obligations will be met on foot of step 2, the matter will be raised with the Group CEO;

(iv) if the GCIA is not satisfied that the reporting obligations will be met on foot of step 3, the matter will be raised with the Chair of the GAC; and

(v) if the GCIA is not satisfied that the reporting obligations will be met on foot of step 4, the matter will be raised with the relevant contact in the CBoI.

Bank of Ireland is regulated by the Central Bank of Ireland.

Bank of Ireland