

INTERNAL AUDIT CHARTER

1. INTRODUCTION

- 1.1 The Board of Directors of CYBG PLC, Clydesdale Bank (CB) PLC and Virgin Money (VM) PLC (collectively, the CYBG Board) has ultimate responsibility for monitoring and overseeing senior management's establishment and maintenance of an adequate, effective and efficient governance, risk management and internal control framework (GRCF). The Board has appointed and authorised the CYBG/CB¹ and VM Boards' Audit Committees (BACs) to assist them in effectively discharging these responsibilities for the whole Group/CB and for VM respectively. Separate VM corporate governance arrangements will be in place for at least as long as separate banking licences exist.
- 1.2 The Board has established CYBG Internal Audit (IA) as a key component of the GRCF.
- 1.3 This IA Charter sets out the purpose, scope, activities and responsibilities of the IA function, along with the organisational framework within which it operates. It is approved by the BACs and should be read in conjunction with the BAC Charters.
- 1.4 IA adopts the definition of internal audit as defined by the Institute of Internal Auditors (IIA)². IA's role as third line of defence is to provide assurance to the Board that the significant inherent risks in the organisation are addressed by an adequate and effective GRCF through the first and second lines of defence.
- 1.5 The assurance output can be used by the Board and management in the discharge of their responsibilities.

2. PURPOSE AND OBJECTIVES

- 2.1 IA supports the Board in executing its duty to safeguard CYBG by protecting and strengthening its assets, reputation and sustainability. Through its functional reporting line to the Chairs of the separate CYBG/CB and VM BACs, IA fulfils its oversight and assurance objectives through:
 - a) Assessing whether all significant risks have been identified and appropriately reported by management and the Risk function to the Board and Executive Management;
 - b) Conducting such internal audit work as is necessary to provide independent assurance that these risks are adequately controlled, including business as usual and change activity;
 - c) Coordinating with other assurance providers to optimise assurance coverage and outputs;
 - d) Gauging and reporting on the risk and control culture, by assessing management risk awareness through individual and thematic reviews;
 - e) Identifying improvements required to the GRCF;
 - f) Helping ensure agreed business actions are implemented sustainably; and
 - g) Supporting investigations arising from whistleblowing disclosures as requested and providing periodic assurance over the whistleblowing framework.

3. ROLE AND RESPONSIBILITIES

- 3.1 The CYBG/CB and VM BACs review and oversee the activities of IA and assess the overall effectiveness of the function. IA must adhere to the BAC duties and responsibilities regarding the IA function as described in the BAC Charters.
- 3.2 The Group Director Internal Audit (GDIA) is responsible for:
 - a) Establishing an IA strategy and directing IA policies, procedures and standards in line with IIA Standards, Codes & Practices and IA Methodology;
 - b) Establishing and maintaining an IA team with the skills and experience commensurate with the risks of the organisation (internally within the organisation or externally through the use of specialist resources);
 - c) Providing the BACs with a regular assessment of the skills required to conduct the work needed and whether the IA budget is sufficient to allow the function to recruit and retain staff with the expertise and experience necessary;
 - d) Preparing and regularly reviewing the scope of the annual IA Plan, outlining coverage of key risk and strategic areas;

¹ CYBG and Clydesdale Bank Plc BACs are required for respective regulatory purposes (CYBG - Corporate Governance & Listing Rules and CB Plc - FCA/PRA). This Charter ensures alignment to both.

² Institute of Internal Auditors UK defines IA as "an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations".

- e) Preparing periodic IA opinion on the adequacy and effectiveness of the governance, risk management and internal control environment including annual internal attestations of compliance with regulatory requirements (where necessary), and other relevant matters;
 - f) Meeting privately, on at least an annual basis, with the BACs without management present;
 - g) Reporting to the BACs on the operations of IA, the delivery of IA Plan, and the profile of audit issues raised across the organisation;
 - h) Adherence to IA quality assurance programme, the results of assessments will be presented to the BACs at least annually; and
 - i) Arranging for an independent and objective external assessment of the IA function at appropriate intervals which will not exceed 5 years. As the CYBG/CB and VM BACs should regularly monitor, review and assess the effectiveness of the IA function, the CYBG/CB and VM BAC Chairs will oversee and approve the appointment process for the independent assessor.
- 3.3 IA will provide assurance over the Whistleblower policy and framework, which are managed by Regulatory & Compliance Risk team. Where required and appropriate IA will conduct and support specific investigations.
- 3.4 The BACs are responsible for approving the IA annual audit plans and financial budget and disclosing in the annual report whether it is satisfied that IA is effective and has sufficient resources and skillsets.

4. SCOPE

- 4.1 CYBG has adopted a three lines of defence governance. As the third line of defence, the scope of IA's work considers all CYBG legal entities and brands, first and second line activities and Business Units, and all key risks and controls across the Group, including material outsourced activities. The work undertaken by IA is determined by the business strategy as well as an independent view of the key risks facing the organisation and how those risks are being managed.
- 4.2 IA will make a risk-based decision as to which areas within its scope will be included in the audit plan and will not necessarily cover all the potential scope areas every year.
- 4.3 IA's scope includes assessing and providing opinion on, but is not limited to:
- Design and/or operating effectiveness of internal governance structures and processes, and risk management systems to assess the extent to which these are effective and efficient in assisting the organisation to achieve its objectives;
 - Information presented to the Board and Executive Management for strategic and operational decision making;
 - The setting of, and adherence to risk appetite;
 - The risk and control culture of the organisation including whether the processes, actions and 'tone at the top' are in line with the values, ethics, risk appetite and policies of the organisation;
 - An evaluation as to whether the organisation is acting with integrity in its dealings with customers and whether the design and control of products, services and supporting processes deliver appropriate customer outcomes and experience;
 - Funding, capital and liquidity risks;
 - Key corporate events including the information used to support key decisions (such as significant business process changes, divestments, acquisitions, major outsourcing and the introduction of new products); and
 - An evaluation of the design and operating effectiveness of the organisation's policies and processes and whether the outcomes are in line with the objectives, risk appetite, purpose and values of the organisation.

In delivering this scope IA will:

- Recommend improvements in procedures and systems to prevent loss and increase efficiency and effectiveness;
- Advise on appropriate systems of internal control and other operational matters;
- Draw attention to any failure by management to take remedial action to address key issues identified; and

- Carry out ad hoc appraisals, inspections, investigations, examinations, consulting services³ or reviews in related areas of fraud control, risk management, policy compliance, regulatory requirements, safety and security and any other areas of focus as approved by the BACs.

4.4 IA will liaise regularly, co-ordinate with and take account of the work of the first and second lines of defence. An agreed framework will maintain awareness of the activities of the various assurance providers and to provide visibility of assurance gaps or overlaps. In determining whether reliance can be placed on the work of the other assurance providers, guidance provided by the PRA would be applied and a thorough evaluation of the effectiveness of the approach, competency of the team and re-performance of their work would be undertaken.

5. INDEPENDENCE, OBJECTIVITY AND AUTHORITY

- 5.1 It is the responsibility of the Board to maintain, promote and support IA as an audit and assurance function operating independently of Executive and Business Unit management and with separate functional reporting lines.
- 5.2 The IA function is under the control of the GDIA who has an independent functional reporting line to the CYBG/CB and VM BAC Chairs and a secondary Executive reporting line to the Chief Executive Officer.
- 5.3 The GDIA and direct reports have equivalent authority to his/her Executive peers to provide the appropriate standing, access and authority to challenge Executive Management. The CYBG/CB and VM BAC Chairs are responsible for recommending to the Board the appointment of the GDIA and removing him/her from post. The Chairs in conjunction with Chief Executive Officer, set the GDIA objectives and appraises performance and associated remuneration.
- 5.4 This appraisal should consider the independence, objectivity and tenure of the GDIA. Where the tenure of the GDIA exceeds seven years, the CYBG/CB and VM BACs should explicitly discuss annually the Chair's assessment of the GDIA's independence and objectivity
- 5.5 The GDIA or delegate will attend each meeting of the CYBG/CB and VM BACs and the CYBG/CB and VM Board Risk Committees.
- 5.6 The GDIA has the right to attend and observe all or part of Leadership Team meetings and any other key management decision making fora.
- 5.7 The GDIA will meet with the Chief Executive Officer and CYBG/CB and VM BAC Chairs on a regular basis to discuss significant emerging issues from the work of IA.
- 5.8 IA is functionally independent of management and the external auditors and has the right to full, free and unrestricted access to all functions, premises, property, personnel, records and other documentation and information that is necessary for IA to meet its responsibilities. This includes access to the CYBG Chair, Board members and Board and Executive Management papers. Management must respect IA's rights in this regard.
- 5.9 The BACs have the right to access anyone in the IA function who must comply with any such request from any member of the BACs.
- 5.10 The GDIA has the right to outsource assignments to external experts where the required expertise is not available within IA function, in accordance with policy.
- 5.11 IA staff must remain objective at all times and not be influenced by personal, business or other matters that may impair impartiality. IA staff must have no line responsibility or authority over any of the activities or operations they review and (except in circumstances approved by the BACs) are not authorised to:
- Perform any operational duties of the organisation except within IA;
 - Provide audit services in relation to a business area or activity for which they have held responsibility within the previous twelve months.
 - Develop or implement procedures or systems external to IA;
 - Initiate or approve any transactions external to IA;
 - Direct the activities of any employee not employed by IA; and
 - Engage on any other activity which could compromise their objectivity.
- 5.12 It is the responsibility of the GDIA to communicate to the BACs and the Chief Executive Officer any perceived or potential conflicts of interest that may compromise the objectivity or independence of IA.

³ Consulting activities for CYBG IA are described as reviews requested by management to support their activities and decision making, including, supporting change initiatives, control design and process efficiency and effectiveness. These services do not follow the standard audit methodology and may not result in the issuance of an Audit report assessing the control environment. IA may be involved in the design of the processes and controls, although will not be involved in the build or operation of such processes.

5.13 The GDIA will confirm the independence of the IA function annually to the BACs.

5.14 IA has the authority to:

- Conduct internal audits in accordance with the approved annual IA Plan and any approved changes thereto;
- Conduct or direct any investigation required to fulfil its responsibilities and retain at the Bank's expense such legal, accounting, financial, corporate governance or other advisors, consultants or experts as it considers necessary from time to time in the performance of its responsibilities.

5.15 IA must have an avenue for dispute resolution (e.g. for disputes on the context of internal audit or matters that inhibit them from executing their duties). The GDIA will raise such matters with the CYBG/CB BAC Chair and/or the VM BAC Chair to provide the avenue for dispute resolution.

6 REPORTING

6.1 IA has reporting obligations to the BACs, and Executive Management. Reporting covers:

- Periodic assessments, at least annually, of the adequacy and effectiveness of the GRCF of the organisation, including the reporting on risk management to the Board and senior management and remediation plans to address weaknesses, based on the work of IA;
- Significant control weaknesses and breakdowns together with root cause analysis;
- Thematic issues and trends identified across the Bank, and their impact on the organisation's risk and control profile;
- Management Risk Awareness and organizational culture assessments (as applicable);
- The IA Plan (the BACs will review and approve the Plan and key changes) and delivery of IA strategy; and
- Regular information on the delivery of the plan and results.

7. EXTERNAL AUDIT AND REGULATORS

7.1 IA will maintain a close relationship and co-operate with the Bank's external auditors in order to optimise the effectiveness and productivity of audit work completed throughout the Bank. IA's role, responsibilities and scope however will remain independent of the Bank's external auditors.

7.2 IA will have an open, constructive and co-operative relationship with regulators which supports sharing of information relevant to carrying out their respective responsibilities.

8. PROFESSIONAL STANDARDS

IA will comply with the Codes of Conduct, Standards and Professional Ethics laid down by the Institute of Internal Auditors in the locations where IA operates. The IA function will operate within the context of the Chartered Institute of Internal Auditors guidance on Effective Internal Auditing in Financial Services Second Edition September 2017.

9. EFFECTIVE DATE

9.1 This charter will be reviewed and approved annually by the CYBG/CB and VM BACs.

9.2 This Charter dated 8th May 2019 supersedes any terms of reference previously in force.