

Paragon Banking Group PLC (“PBG”)

&

Paragon Bank PLC (the “Bank”)

Terms of Reference: Risk and Compliance Committee (the “Committee”)

Approved: 30 November 2023

## Contents

Section 1: Overview .....	1
1.1 Board approval and review .....	1
1.2 Interpretation.....	1
Section 2: Terms of Reference .....	4

Paragon Banking Group PLC (“PBG”) &  
Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)  
Section 1: Overview

1.1 Board approval and review

This revised version was approved by the Boards of each of PBG and the Bank on 30 November 2023.

The Terms of Reference will be reviewed annually, or when required by changes to regulation/legislation.

1.2 Interpretation

- 1.2.1 The boards and committees of PBG and the Bank have identical membership and sit jointly on most occasions. Where a joint meeting of the Committee takes place, these Terms of Reference shall apply. Where the Committee of PBG or the Bank sit separately, these Terms of Reference shall apply to each Committee except where, due to applicable law, regulation or other reasons considered appropriate by the non-executive directors, they cannot or should not apply. On the date of adoption of these Terms of Reference all such items have been noted in Appendix 1, but they are not exclusive and can be amended from time to time on an ad hoc or continuous basis, separate to any agreement to amend the Terms of Reference, provided that a quorum of the relevant Board/Committee agrees, and this amendment is minuted as such.
- 1.2.2 For the purpose of these Terms of Reference the term ‘Group’ shall mean, when the Committee is sitting as a joint Committee, PBG and its subsidiaries as defined by the Companies Act 2006. Should the Committee sit solely as a Committee of PBG then the same definition shall apply, but when meeting as a Committee only of the Bank then this definition shall mean only the Bank and those subsidiaries of the Bank as defined by the Companies Act 2006.
- 1.2.3 For the purpose of these Terms of Reference the term ‘Company’ shall mean, when the Committee is sitting as a joint Committee, each of PBG and the Bank. Where the Committee is sitting as either a Committee of PBG or the Bank then it shall mean the relevant company only.
- 1.2.4 For the purpose of these Terms of Reference the term ‘Board’ shall mean, when the Committee is sitting as a joint Committee, the Boards of each of PBG and the Bank. Where the Committee is sitting as either a Committee of PBG or the Bank then it shall mean the relevant Board only.

# Paragon Banking Group PLC (“PBG”) & Paragon Bank PLC (the “Bank”) Risk and Compliance Committee (the “Committee”)

## Section 2: Terms of Reference

### 1 Role

The role of the Committee is to review, on behalf of the Board, management’s recommendations on enterprise risk, in particular:

- 1.1 the Group’s current and future risk appetite including the extent and categories of risk which the Board regards as acceptable;
- 1.2 the Group’s enterprise risk management framework including principles, supporting frameworks, risk policies, personnel and procedures;
- 1.3 the Group’s risk culture, to ensure that it supports the Group’s risk appetite;
- 1.4 the Group’s strategy to ensure that it promotes integrity in the market, the fair treatment of customers and good outcomes for retail customers as central to the Group’s operations and culture; and
- 1.5 the Group’s processes for compliance with laws, regulations and ethical codes of practice and prevention of fraud.

### 2 Authority

- 2.1 The Committee is a committee of the Board from which it derives its authority and to which it regularly reports.
- 2.2 The Committee has delegated authority from the Board in respect of the functions and powers set out in these Terms of Reference. The Committee may sub-delegate any or all of its powers and authority as it deems appropriate, including without limitation the establishment of sub-committees to analyse particular issues or themes and to report back to the Committee.
- 2.3 The Committee is concerned with the business of the Group and accordingly its authority extends to all relevant matters relating to the Group.
- 2.4 The Committee has authority to investigate any matters within its responsibilities and to request the attendance of any directors, officer or employee of the Group and/or seek information it requires from any director, officer or employee of the Group in order to perform its duties.
- 2.5 The Committee Chair is authorised to request that remedial action be taken in relation to any matter within the Committee’s Terms of Reference which the Committee Chair considers has not been addressed promptly or sufficiently.
- 2.6 The Committee is authorised by the Board to obtain, at the Company’s expense, independent legal or other professional advice on any matters within its Terms of Reference if it believes it is necessary to do so. If the proposed professional advisor provides statutory audit services to any part of the Group, discussion shall be had with the Chair of the Audit Committee (“AC”) before the proposed appointment is agreed.
- 2.7 The Committee shall have direct access to the Group’s Chief Risk Officer and Director of Internal Audit.
- 2.8 The Committee shall have the right to publish in the Company’s annual report details of any issues that cannot be resolved between the Committee and the Board.

### 3 Relationship with other Committees

Paragon Banking Group PLC (“PBG”)  
& Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)

Section 2: Terms of Reference

- 3.1 It is recognised that the Committee and AC have duties in potentially overlapping areas of the Group’s operations. Consequently, the Chair of the Committee, in conjunction with the Chair of the AC, has the authority to determine, from time to time, in relation to any matter whether it falls within the remit of the Committee or the AC or is the responsibility of both the Committee and AC.
- 3.2 In respect of its sub-committee, which at the date of adoption of these Terms of Reference was the Model Risk Committee, the Committee shall act as a mechanism for oversight and challenge as well as being the final arbiter on decisions if required.
- 3.3 The Committee shall work and liaise as necessary with all other Board Committees in addition to the points noted at items 3.1 and 3.2 above (as relevant).

4 Membership

- 4.1 The Committee shall comprise at least three members. Membership shall include at least one member of the AC. Members of the Committee shall be appointed by the Board, on the recommendation of the Nomination Committee, in consultation with the Chair of the Committee.
- 4.2 Only members of the Committee have the right to attend Committee meetings. However, the Chief Executive, Chief Financial Officer, Chief Operating Officer, Chief Risk Officer, General Counsel and Director of Internal Audit will be invited to attend meetings of the Committee on a regular basis and other non-members (including external advisers) may be invited to attend all or part of any meeting as and when appropriate.
- 4.3 Appointments to the Committee shall be for a period of up to three years, extendable by no more than two additional three-year periods, so long as members (other than the Chair of the Board, if he or she is a member of the Committee) continue to meet the criteria for membership of the Committee.
- 4.4 The Board shall appoint the Committee Chair. In the absence of the Committee Chair and/or an appointed deputy at a Committee meeting, the remaining members present shall elect one of themselves to chair the meeting.
- 4.5 The Committee Chair shall review membership of the Committee annually, as part of the annual performance evaluation of the Committee.
- 4.6 All members of the Committee shall be independent non-executive directors (within the meaning of the UK Corporate Governance Code (the “Code”). The members of the Committee shall have the appropriate knowledge, skills and expertise to fully understand and monitor the risk strategy and the risk appetite of the Group. The Committee as a whole shall have competence relevant to the financial services sector. Additionally, the Chair of the Board may serve on the Committee as a Committee member if he or she was considered independent on appointment as Chair of the Board.

5 Secretary

- 5.1 The Company Secretary, or his or her nominee, shall act as the secretary of the Committee and provide all necessary support to the Committee.

6 Quorum

Paragon Banking Group PLC (“PBG”)  
& Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)

Section 2: Terms of Reference

- 6.1 The quorum necessary for the transaction of business shall be two members.
- 6.2 Significant decisions, such as determining the Group’s risk appetite, should, in all practical circumstances, be taken by the Committee as a whole.

7 Meetings

- 7.1 The Committee shall meet at least four times a year at such times as shall be necessary or appropriate and otherwise as required.
- 7.2 Meetings of the Committee may be conducted when the members are physically present together, in the form of either video or audio conference or as a hybrid.

8 Notice of meetings

- 8.1 Meetings of the Committee shall be called by the Secretary of the Committee at the request of the Committee Chair or any of its members or the Chief Risk Officer or Director of Internal Audit if they consider it necessary.
- 8.2 Unless otherwise agreed, notice of each meeting confirming the venue, time and date of the meeting, together with an agenda of items to be discussed, shall be forwarded to each member of the Committee, any other person requested to attend and all other non-executive directors, no later than five working days before the date of the meeting, unless otherwise agreed by the Committee members. Supporting papers shall be sent to Committee members and to other attendees, as appropriate, at the same time. Late papers will be accepted by agreement with the Committee Chair.
- 8.3 The Committee may send notices, agendas and supporting papers in electronic form where the recipient has agreed to receive documents in such a way.

9 Minutes of meetings

- 9.1 The Secretary of the Committee, or their nominated alternate, shall minute the proceedings and resolutions of all Committee meetings, including the names of those present and in attendance and the existence of any conflicts of interest.
- 9.2 Draft minutes of Committee meetings shall be circulated to the members/those in attendance normally no later than 10 working days after the meeting or as soon as practicable. Once finalised, draft minutes will be made available to all members of the Committee before formal approval at the next Committee meeting. Once approved, minutes should be made available to all members of the Board unless, exceptionally, it would be inappropriate to do so.

10 Shareholder engagement

- 10.1 The Committee Chair should attend the Annual General Meeting to answer any shareholder questions on the Committee’s activities.
- 10.2 The Committee Chair should also seek engagement with shareholders on significant matters related to the Committee’s areas of responsibility.

11 Duties

Paragon Banking Group PLC (“PBG”)  
& Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)  
Section 2: Terms of Reference

The Committee should have oversight of the Group as a whole and, unless required otherwise by applicable law or regulation, carry out the following duties for the Group and its major subsidiary undertakings as appropriate:

**11.1 General**

- 11.1.1 provide advice to the Board on risk appetite, tolerance and strategy, including oversight of the Group’s current and emergent risk exposures. Particular focus will be given to the identification of significant horizon risks which have the potential to materially affect the achievement of the Group’s short and long-term strategic objectives;
- 11.1.2 notify the Board promptly of actual or likely material breaches of risk appetite, and provide advice on the likelihood and the impact of principal risks materialising, and comment on management’s response to a potential or actual material breach of risk appetite, including recommending further actions where appropriate;
- 11.1.2 review whether prices of liabilities and assets offered to customers take fully into account the Group’s business model and risk strategy;
- 11.1.3 consider whether there is appropriate alignment between the Group’s overall product and service offering (including pricing and profitability), and the Group’s risk strategy and risk appetite; and
- 11.1.4 approve and keep under review the enterprise risk management framework including the principal risks and approval of their respective risk policies; approval of proposals for consideration by the Board in respect of overall risk appetite, risk tolerance and risk strategy, as well as the metrics to be used to monitor the Group’s risk management performance.

For the avoidance of doubt, risks to be considered in respect of risk appetite include but are not limited to strategic risk, capital risk, credit risk, conduct risk, liquidity and funding risk, market risk, operational risk (including financial crime risks), model risk, reputational risk and climate change.

In considering risk appetite and the continuing appropriateness thereof, account will be taken of the current and prospective macro-economic, macro prudential and financial environment, drawing on financial stability assessments published by the Bank of England (the “BoE”), the Prudential Regulation Authority (the “PRA”), the Financial Conduct Authority (the “FCA”), any successor regulatory bodies and any other authoritative sources.

The Committee, in respect of the following risks, shall:

**Strategic Risk**

- 11.1.5 provide oversight and challenge of due diligence on risk aspects relating to material transactions and strategic proposals that are subject to approval by the Board (focussing the due diligence appraisal of the proposition on implications for the risk appetite, tolerance and strategy of the Company, and taking independent external advice where appropriate and available) and advise the Board on the risk aspects of

Paragon Banking Group PLC (“PBG”)  
& Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)  
Section 2: Terms of Reference

proposed changes to strategy and strategic proposals including acquisitions or disposals;

11.1.6 consider the Group’s risk appetite relative to its current and future strategy for approval by the Board;

11.1.7 review the Group’s capability to identify and manage new risk types;

**Capital Risk**

11.1.8 consider target capital ratios and monitoring of performance against target, including the potential impact of developments in market conditions, business development and the regulatory framework, reporting conclusions to the Board;

11.1.9 consider and approve the Group’s capital stress test scenarios and the results of different stress and reverse stress test assumptions;

11.1.10 review the Internal Capital Adequacy Assessment Process (“ICAAP”) framework and report on this to the Board for inclusion within the ICAAP;

**Conduct Risk**

11.1.11 provide oversight and challenge in the design and on-going support of a conduct risk framework, appetite and strategy for use in the business, for Board approval;

11.1.12 provide oversight and challenge of the Group’s strategy to ensure this is consistent with the Group’s objectives, including that of being an organisation where the fair treatment of customers is central to operations and culture, and that the Group acts with integrity in the market;

**Credit Risk**

11.1.13 review the Group’s current credit profile and future indicators and make recommendations to the Board on the credit risk framework and overall risk appetite taking into account emerging trends that may result in future adverse developments, undertaking product and business area specific ‘deep dives’ as appropriate;

**Liquidity and Funding Risk**

11.1.14 review the Group’s liquidity profile, including to ensure that the Group has sufficient financial resources to enable it to meet its obligations as they fall due, and make recommendations to the Board for approval of the liquidity risk framework, including the review of scenarios for, and considering the results of, different stress and reverse stress test assumptions including those proposed by the PRA and other regulatory bodies;

11.1.15 oversee the Bank’s Internal Liquidity Adequacy Assessment Process (“ILAAP”) and contingency funding plan;

**Market Risk**

11.1.16 review the Group’s current market risk profile and future indicators and make recommendations to the Board on the market risk framework and overall risk appetite taking into account emerging trends that may result in future adverse developments;



Paragon Banking Group PLC (“PBG”)  
& Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)  
Section 2: Terms of Reference

**Operational Risk**

- 11.1.17 provide oversight and challenge of the operational risk and control self-assessment framework;
- 11.1.18 review the risk profile of the Group’s internal procedures, including in relation to management of people, health & safety, IT & security and data protection;
- 11.1.19 oversee the effectiveness of risk management undertaken by all key outsourced functions on behalf of the Group including, but not limited to, those managed by third parties;
- 11.1.20 consider and review the adequacy and effectiveness of the technology infrastructure supporting the risk management framework;
- 11.1.21 oversee the financial crime risk management framework, including outputs from financial crime business wide risk assessments and the review of the annual Money Laundering Reporting Officer’s report;

**Model Risk**

- 11.1.22 consider the Group’s internal models and the inputs and assumptions made on the basis of such models, including their development and the risk profile of misreporting the output;

**Reputational Risk**

- 11.1.23 keep under review the risk profile of the Group’s reputation in the market and the importance of meeting market expectations on the standards of the Group’s operations, relationship with regulators and being consistent with the Group’s objectives;
- 11.1.24 consider the risk profile of the Group’s brand, including in relation to its approach to corporate responsibility and ESG promotion;

**Climate Change Risk**

- 11.1.25 provide oversight of the Group’s impact on climate change;
- 11.1.26 consider and review the direct and indirect challenges on the Group’s approach to climate change and its relationships with its supply chain, physical operations and the cost of doing business;

**Consumer Outcomes**

- 11.1.27 provide oversight and challenge of the Group’s overall strategy for the implementation and monitoring of its arrangements for the promotion of good outcomes for retail customers;

**11.2 Risk assessment**

In respect of risk assessment, the Committee shall:

- 11.2.1 keep under review the Group’s overall risk assessment processes that inform the Board’s decision making, ensuring where possible, quantitative metrics are used;
- 11.2.2 review and challenge the status of Board level (Level 1) risk appetite measures against agreed thresholds, including the actions to bring amber and red related measures back to green status or to address significant negative trends in green status, and escalate any issues of concern to the Board;

Paragon Banking Group PLC (“PBG”)  
& Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)  
Section 2: Terms of Reference

- 11.2.3 review annually and approve the parameters used in these measures and the methodology adopted; and
- 11.2.4 set a standard for the accurate and timely monitoring of large exposures and certain risk types of critical importance.

**11.3 Risk management systems**

The Committee shall:

- 11.3.1 on behalf of the Board (which retains overall responsibility for risk management), review and monitor the Group's risk management system, and annually, carry out a review of its effectiveness, and review and approve the statement to be included in the annual report concerning risk management; and
- 11.3.2 advise the Board on the likelihood and impact of emerging and principal risks facing the Group (including those risks that would threaten its business model, future performance, solvency, liquidity or reputation) and provide advice on the management and mitigation of principal risks to reduce the likelihood of their incidence or their impact.

**11.4 Internal controls**

The Committee shall:

- 11.4.1 review the adequacy and effectiveness of the Group's internal control systems and risk management systems and additionally carry out a review of their design, implementation and effectiveness if requested to do so by the Board;
- 11.4.2 review the appropriateness of the Group's values and culture and reward systems for managing risk and internal controls, and the extent to which the culture and values are embedded at all levels of the Group;
- 11.4.3 consider whether executive management's approach towards and treatment of the Chief Risk Officer, and their approach to internal control function and external audit recommendations, is supportive of a healthy risk culture;
- 11.4.4 review the effectiveness and relative costs and benefits of particular controls; and
- 11.4.5 ensure the Chief Risk Officer's right of direct access to the Chair of the Board, the Board itself, the external auditor and to the Committee.

**11.5 Ongoing viability**

The Committee shall, where requested by the Board, and subject to overlap with the AC, provide advice on how, taking into account the Group's position and principal risks, the Group's prospects have been assessed, over what period and why the period is regarded as appropriate. The Committee shall also advise on whether there is a reasonable expectation that the Group will be able to continue in operation and meet its liabilities as they fall due over the said period, drawing attention to any qualifications or assumptions as necessary.

**11.6 Risk reporting**

The Committee shall:

Paragon Banking Group PLC (“PBG”)  
& Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)  
Section 2: Terms of Reference

- 11.6.1 review the principal risk register, challenging the assessment and measurement of key material and emerging risks and monitoring the impact of mitigating actions, set out in the register, being taken to manage these risks;
- 11.6.2 review and challenge the key risk reporting indicators used to monitor risk events and trends;
- 11.6.3 monitor and report to the Board on risk capacity and profile and risk monitoring, in particular performance versus risk appetite, risk trends, risk concentrations, impairment experience against budget and key performance indicators for risk;
- 11.6.4 provide oversight and challenge of the model governance framework;
- 11.6.5 provide oversight and challenge of the stress testing framework and the execution of stress and scenario testing;
- 11.6.6 provide oversight of the effectiveness of and challenge of the day to day risk management and oversight arrangements of the executive; and
- 11.6.7 review and, if thought fit, recommend to the Board the ICAAP, ILAAP, Recovery Plan and any other equivalent documents required by a regulator from time to time and considered appropriate by the Committee Chair to be reviewed by the Committee.

**11.7 Risk and Compliance department**

The Committee shall:

- 11.7.1 approve the appointment and removal of the Chief Risk Officer;
- 11.7.2 review the quality, adequacy, resources, scope and nature of the work of the risk and compliance function; receive and review reports from the Chief Risk Officer and, where appropriate, seek assurances in relation to any items of concern;
- 11.7.3 ensure the Board establishes and maintains effective systems and controls for compliance with applicable requirements and standards under the regulatory system; and
- 11.7.4 consider and approve the remit of the risk management function and ensure it has adequate resources and appropriate access to information to enable it to perform its function effectively and in accordance with the relevant professional standards. The Committee shall also ensure the function has adequate independence and is free from management interference and other restrictions.

In addition the Chief Risk Officer shall have a right of direct access to the Committee Chair at all times, the Board itself and the external auditor, and shall meet with the Committee at least once a year without executive directors present.

**11.8 Remuneration**

- 11.8.1 The Committee Chair shall be consulted on the annual remuneration package of the Chief Risk Officer subject to the final approval of the Board and the Remuneration Committee (“RemCo”).

Paragon Banking Group PLC (“PBG”)  
& Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)  
Section 2: Terms of Reference

11.8.2 The Chief Risk Officer and the Committee Chair shall work with and provide advice to RemCo on the management of remuneration risk, with support from the Committee where necessary and appropriate, including on, where relevant:

11.8.2.1 the measurement of performance in the context of incentives;

11.8.2.2 the vesting of long-term incentives;

11.8.2.3 the application of risk adjustments, malus or clawback; and

11.8.2.4 the risk profile of the Company, including performance against risk appetite and an assessment of all current and future risks, to support RemCo in its decisions. This information will inform the risk weightings to be applied to performance objectives incorporated into executive remuneration as well as overall bonus outcomes for employees.

In the event of any material difference of view, appropriate performance objectives will be decided by the non-executive members of the Board.

## 11.9 Other

The Committee shall review:

11.9.1 the Group’s systems and controls for ethical behaviour and the mitigation of financial crime risks, including money laundering, terrorist financing, bribery and corruption, tax evasion, modern slavery, internal and external fraud and sanctions breaches;

11.9.2 and oversee the Group’s operational resilience framework;

11.9.3 reports from the Internal Audit department and the external auditors on risk control issues, and shall have regard to any relevant advice from the AC and internal audit function concerning the effectiveness and adequacy of the Group’s framework of internal controls to manage those risks including the review and evaluation on an annual basis of the appropriateness of the Group’s risk measurement systems;

11.9.4 relationships with regulatory authorities in the UK and prospective changes in the regulatory environment;

11.9.5 whether pricing of the Group’s product offerings takes fully into account the Group’s business model and risk strategy and whether the Group has satisfactory controls in place to ensure customers are treated in accordance with both internal policies and regulatory requirements;

11.9.6 whether the Board’s stated risk culture expectations have been appropriately translated into a framework of ethics, values and desired behaviours, supported with appropriate metrics and indicators, and embedded effectively throughout the organisation;

11.9.7 risk mitigation points arising from regulatory reviews. Monitoring and challenging the process for resolving issues raised;

11.9.8 all material breaches, or potential breaches of applicable law and regulation; and

11.9.9 any material existing or prospective legal actions or regulatory investigations.

## 12 Reporting responsibilities

Paragon Banking Group PLC (“PBG”)  
& Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)

Section 2: Terms of Reference

- 12.1 The Committee Chair shall report formally to the Board on the Committee’s proceedings after each meeting on all matters within the Committee’s duties and responsibilities.
- 12.2 The Committee shall make whatever recommendations to the Board it deems appropriate on any area within its remit where action or improvement is needed.
- 12.3 The Committee will compile a report of its activities for inclusion in the annual report. This report will describe the work of the Committee and explain how the responsibilities of the Committee have been discharged and the issues considered during the year.
- 12.4 The Committee has the right to publish in the annual report details of any issues that cannot be resolved between the Committee and the Board.
- 12.5 The Committee shall make publicly available the Committee’s Terms of Reference by placing them on the Group’s website.

13 Other matters

The Committee shall:

- 13.1 have access to sufficient resources (e.g. financial) to carry out its duties, including unfettered access to the Company Secretariat, Internal Audit, Risk and Compliance and Group Finance departments for advice and assistance as required;
- 13.2 determine the nature, amount, format and frequency of the information it receives;
- 13.3 be provided with appropriate and timely training, both in the form of an induction programme for new members and on an ongoing basis for all members;
- 13.4 give due consideration to all applicable laws and regulations, in particular, the directors' duties contained in the Companies Act 2006, the provisions of the Code and published guidance (as updated from time to time), the requirements of the FCA’s Listing Rules, Prospectus Regulations and Disclosure Guidance and Transparency Rules sourcebook, the requirements of the BoE, PRA and FCA and any other applicable rules as appropriate;
- 13.5 oversee any investigation of activities which are within the Terms of Reference; and
- 13.6 ensure periodic reviews of its own performance are carried out and, at least annually, review its constitution and Terms of Reference to ensure it is operating at maximum effectiveness and recommend any changes it considers necessary to the Board for approval.

Paragon Banking Group PLC (“PBG”)  
& Paragon Bank PLC (the “Bank”)  
Risk and Compliance Committee (the “Committee”)  
Section 2: Terms of Reference

**Appendix 1**

	<b>Item Number</b>	<b>Additional comment/explanation</b>
Items which do not apply to or are amended for the Bank	<b>3.1, 3.3, 10 and 11.5</b>	These are not applicable to Paragon Bank PLC as it is not a listed entity and (3.3) does not have a Model Risk Committee