

## Quality and Risk Management Committee - Terms of Reference

### Purpose and objectives of the body

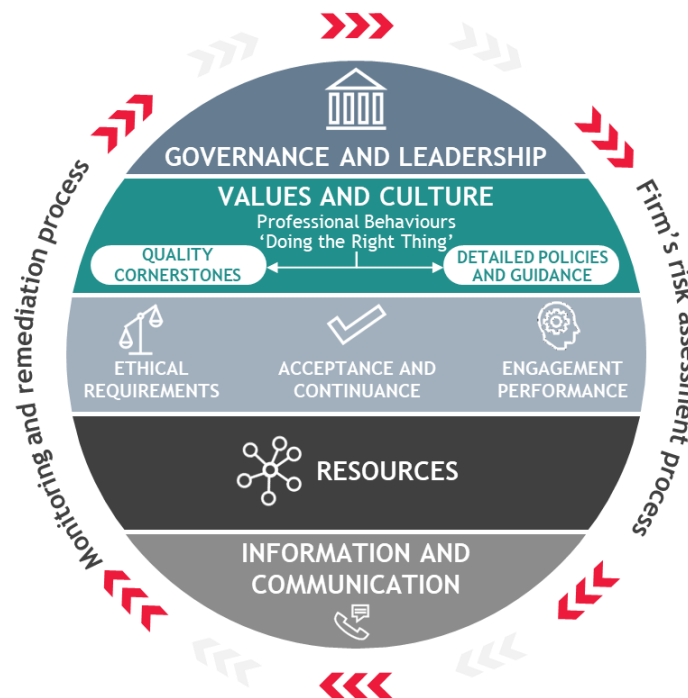
#### Overview

The objectives of the Firm's system of quality and risk management is as follows:

To provide the firm with reasonable assurance that:

- The firm and our personnel fulfil our responsibilities in accordance with professional standards and applicable legal and regulatory requirements, and conduct engagements in accordance with such standards and requirements; and
- Engagement reports and/or advice issued by the firm or engagement partners are appropriate in the circumstances.

The components of the Firm's system of quality and risk management are set out in the diagram below. This is based on the framework set out in ISQM1 and ensures that the firm's overall approach to risk management and quality management are aligned.



In line with the above objectives, the QRMC's role is to ensure appropriate strategies and plans are drawn up, implemented and monitored to ensure the quality objectives of the Firm are achieved and the effective management of risk consistent with the Firm's strategy. This includes understanding and monitoring all the risks facing BDO as a business (be they strategic, reputational, financial, operational) and for scrutinising the processes in place within the business for managing and mitigating these risks.

The QRMC will report to the Leadership Team.

The role of the Quality and Risk Committee includes:

- Promoting a quality and risk management culture throughout the Firm that is based on:
  - Ethical standards, laws and professional regulations and standards, best practice and professional scepticism
  - The Firm's quality cornerstones
  - The Firm's Values and Code of Conduct
  - Effective project management
  - Effective communication
  - Technical and professional quality.
- Monitoring and evaluating the exposure and risk profile of the activities of the Firm and assessing the Firm's appetite for risk.
- Ensuring that the Firm has a comprehensive map of risk to the business.
- Monitoring changes in risk profile and ensuring appropriate responses are initiated.
- Operational responsibility for the system of quality and risk management<sup>1</sup>, including oversight of the overall structure of the Firm's three lines of defence and risk assurance map.
- Periodically reviewing the organisational structure and assignment of roles, responsibilities and authority is appropriate to enable the design, implementation, and operation of the firm's system of quality and risk management<sup>2</sup>.
- Reviewing and evaluating the resources devoted by Streams, Practice Management Departments (PMDs) and the Firm, centrally, to quality and risk management.
- Reviewing and evaluating the risks arising from the development of new or amended services.
- Monitoring whether all areas of service delivery meet the required levels of quality and following up where necessary.
- Monitoring compliance with the firm's non-negotiables and following up where necessary.
- Monitoring the success of implemented plans against requirements and making changes where necessary.
- Monitoring compliance with professional standards and regulations and the Firm's policies and guidelines through cold review programmes and other monitoring procedures and reviewing cold review programme results to identify opportunities for improvement and focus.
- Evaluating, at least annually, the firm's system of quality and risk management and providing evidence of that review and the Committee's conclusion to the Leadership Team<sup>3</sup>.

---

<sup>1</sup> ISQM1 (UK) paragraph 20

<sup>2</sup> ISQM1 (UK) paragraph 28(d)

<sup>3</sup> ISQM1 (UK) paragraphs 53 and 54



- Reviewing the annual summary engagement monitoring and inspection reports (ie cold review reports) for each Stream (Audit, Tax, Advisory). In the context of Audit, this includes the report required by ISQM1 (UK) paragraph 56-1.
- Approving significant Q&R policies and material changes of such policies.
- Promoting effective management of practice protection issues (claims and regulatory investigations).
- Sharing knowledge and best practice on quality and risk matters across the Firm.

## **Membership**

There will be no minimum or maximum number of members. The membership will be determined by the Chair of QRMC along with the LT (and approval from BIOB).

Members will include:

- Stream Heads of Q&R
- Other partners with relevant Q&R expertise
- Other experienced partners to provide challenge.

Members will be appointed by the Chair - normally in discussion with the Committee and/or the LT and with approval from Business Interest Oversight Board.

At least one INE will attend as an observer.

There will be no fixed tenure defined. Membership is based on role, and therefore ability to influence, make decisions or implement actions. Tenure is therefore as long as the members remain effective in those roles.

### *Removal process before tenure is complete*

Members can be removed at the behest of the Chair, with the approval of the LT and the BIOB.

## **Chairing the body**

The QRMC is chaired by the Head of Quality and Risk Management.

The Chair will remain in place until replaced by a new Head of Quality and Risk Management or at the behest of the Leadership Team, with the approval of BIOB.

The Chair can be removed by the Leadership Team, with the approval of BIOB.

### *Skills and attributes required*

- Significant regulatory and risk management knowledge and experience.
- Ability to analyse and explain clearly complex issues
- One firm mindset
- Values-led, being Bold, Collaborative, Genuine and Responsible, and acting with integrity
- Aligned to the firm's strategic ambitions



- Connected into, and respected by, key stakeholders across the organisation
- Skilled in listening to understand, not just to respond
- Good communication skills
- Able to focus the Committee on key decisions required.

#### *Responsibilities as Chair*

Determining agendas for monthly meetings and periodic special purpose meetings, controlling meetings, ensuring actions are properly followed up.

#### **Meetings**

The QRMC will meet at least six times per annum but normally meets on a monthly basis with approximately two additional special purpose meetings (eg to refresh the Firm's Top Risks)

The Chair or any member by agreement with the Chair, the Managing Partner or the Leadership Team can call a special purpose meeting outside of the normal cycle.

The meeting will be deemed quorate if two thirds of the members are present.

Any individual whether inside or outside the firm can be invited to attend a QRMC meeting (as a non-voting attendee).

The requirement for a QRMC member to declare a conflict of interest will be stated at the outset of each meeting or in the papers convening the meeting.

#### **Decision making**

Briefing papers are prepared in advance and distributed via a secure platform, eg Diligent. These are supplemented by presentations to committee meetings.

There is no formal voting process. All decisions are agreed by consensus.

Decisions are recorded in detailed minutes.

Decisions are reported to the Leadership Team by reporting from the Head of Quality and Risk Management to LT or via the minutes which are circulated to LT. Decisions which need to be cascaded to the business are agreed as actions to be followed by management/PMDs leaders at the time of giving presentations to the QRMC, or members of the committee.

Decisions and implementation of decisions can be delegated to members of the committee who report back on actions taken.

The QRMC has oversight responsibility for the Information Security Committee.

Other sub-groups can be created as considered necessary by the committee or at the request of the Leadership Team.

Any unresolved disagreements would be escalated to the Managing Partner and/or the Leadership Team.



#### ***Connectivity with other bodies***

The committee reports to the Leadership Team. Decisions and important matters are reported to by the Head of Quality and Risk Management to LT in his monthly report or via the minutes which are circulated to LT.

The Information Security Committee (ISC) reports to the QRMC. Decisions of the ISC are reported on a bi-monthly basis to the QRMC and the minutes of the ISC are circulated to the QRMC. The QRMC also receives periodic updates on information security risks from the CIO and the CISO.

The QRMC receives regular reports from the Head of Internal Audit on the implementation of the internal audit plan, the reviews carried out and the implementation of the management actions arising from those reviews. This is to assist the QRMC with its evaluation of the Firm's system of quality and risk management. The QRMC also reviews the annual internal audit plan.

#### ***Assessing effectiveness of the Chair and the body***

Board effectiveness reviews will be undertaken annually utilising our in-house expertise and experience.

#### ***Schedule for reviewing Terms of Reference***

The terms of reference will be reviewed annually as part of the effectiveness review.