Risk & Assurance Committee

TERMS OF REFERENCE

1. Scope

1.1. Purpose

Provides scrutiny, review and assurance to the board of trustees, on the effectiveness of the risk management framework and strategy, that the significant risks and events faced by the organisation in the UK and internationally are identified, assessed, and monitored, and that appropriate mitigation actions are in place where necessary.

Assures the board that the organisation is operating as far as possible within the risk appetite defined by the board, is working to mitigate risks where this is not the case, achieves required standards, meets statutory and regulatory requirements, and remains focused on continuous improvement and learning.

1.2. Authority

The committee has delegated authority from the board of trustees in accordance with the terms of reference.

1.3. Reporting

The committee reports to the board of trustees.

2. Membership

2.1. Chair

The committee will be chaired by a trustee appointed by the chair of the board.

2.2. Members

Core membership of the committee will comprise:

- Up to four trustees (one of whom will be chair of the committee; and one of whom will be a member of the finance and audit committee)
- Up to two external advisors

2.3. Other attendees

Attendance on a regular basis:

- Executive director UK operations
- Chief operating officer
- Executive director of international
- Senior director of professional services
- Corporate risk manager

In addition:

- The chief executive officer may attend
- The chair of the board of trustees may attend.

The committee may invite other attendees (non-voting) to act in an advisory capacity, as deemed necessary.

2.4. Term of office

Two terms of four years each; coterminous with each trustee’s terms of office.

2.5. Quorum

Quorum is set at three members, at least two to be trustees.

3. Responsibilities

The responsibilities of the committee shall be:

3.1. To review and scrutinise the effectiveness of the risk management framework and strategy on behalf of the board.

3.2. To review, scrutinise and challenge the integrated risk and assurance report, which will include information on:

- The top risks to which BRC is exposed. These include risks that relate to legal, regulatory and policy compliance (for example health, safety, security, and safeguarding), operational risks that impact the delivery of operations, services and programmes (for example safe delivery of our services, business continuity, and cyber risks), and any other risk that could significantly impact our reputation. The committee is responsible for overseeing risk and assurance at the British Red Cross covering both UK and international work.
- The causes, potential impact and probability associated with each risk.
- The existing key internal controls for each risk, including compliance activities for regulated services.
- Assurance relevant to the corporate risks including that provided by internal audit.
- Mitigating actions for each risk as appropriate so that risks are managed within the agreed risk appetite by an agreed date.
- Related significant risk events and incidents, their investigation, and the associated corporate learning.
- Related regulatory and third-party reports and associated remedial actions.

3.3. To review and approve policy or strategy documents, for example approving the annual health and safety policy statement as delegated by the board.

3.4. To help drive continuous improvement in the organisation's risk and compliance culture and practice.

3.5. To receive the annual quality account, recommend the annual self certificate for NHS work for approval to the board of trustees and any other externally required report of notification on behalf of the board.

3.6. To oversee fundraising quality assurance activity; provide oversight of existing fundraising quality assurance policies; review performance against agreed frameworks through regular reports and advise on fundraising quality assurance as requested by the board.

3.7. To monitor and evaluate IT resilience; cyber, data protection and information security, particularly to ensure that these risks are mitigated and threats reduced.

3.8. To escalate risk and assurance matters as appropriate to the board of trustees.

3.9. To consider other matters as referred by the board from time to time, apart from financial risks which are overseen by the finance and audit committee.

3.10. Internal audits which receive limited assurance will be shared with the committee where appropriate apart from those which are within the finance and audit committee's remit.

3.11. The committee is authorised, where necessary, to obtain external advice required to discharge its responsibilities.

4. Management

4.1. Secretary

A secretary shall be appointed who will arrange, convene, attend and record all meetings of the committee.

4.2. Papers / Agenda

The secretary to the committee is responsible for circulating papers for the meetings. Agenda and papers will be circulated to all members at least 5 working days before the meeting.

4.3. Meetings

The committee will normally meet three times a year. Additional meetings may take place at the committee chair's request.

4.4. Attendance

Members are expected to attend all meetings of the committee unless agreed by the chair. Ex-officio members must nominate a suitable deputy if unable to attend. Attendance by tele/video conference can be agreed with the chair.

4.5. Minutes / reporting

The secretary to the committee shall aim to distribute minutes of each meeting to committee members within ten working days. Minutes will be shared with the board at the following board meeting.

The committee chair will report formally to the board on the committee's proceedings.

4.6. Sub-groups

The committee may establish sub-groups to oversee specific issues, setting their terms of reference and membership as required.

5. Version Control

5.1. Approval

These terms of reference were approved by the board of trustees at their meeting on 20 February 2024.