

Board Risk & Compliance Committee Terms of Reference

Document Control

Document Reference:	Board Risk & Compliance Committee TOR
Approval Authority:	Board of Directors
Document Owner:	Society Secretary
Document Author:	Society Secretary
Version Number:	V4
Approval Date:	Board in June 2026
Effective Date:	15 June 2026

Contents

1. Purpose.....	3
2. Membership.....	3
3. Quorum	4
4. Authority.....	4
4.1 Exceptions	4
4.2 Voting.....	5
5. Responsibilities.....	5
6. Meeting Frequency	8
7. Secretariat	8
8. Minutes & Reports	9
9. Other Matters.....	9
10. Document Version History.....	10

1. Purpose

The Board Risk & Compliance Committee (the “Committee”) is a committee of the Board of Directors, responsible for reviewing and monitoring Harpenden Building Society’s (the “Society”) Risk Management Framework, Risk Appetite and internal control systems and, at least annually, carrying out a review of their effectiveness, and reporting on that review in the Annual Report and Accounts.

The Committee performs its role by:

- Ensuring that the accountability and responsibility for managing risk is clearly defined;
- Determining the nature and extent of the top risks of the Society;
- Ensuring processes are in place to identify, measure, assess, monitor and control risks;
- Ensuring that the Society is compliant with regulatory requirements;
- Ensuring that adequate capital is allocated to support the Society’s key risk exposures, both to ensure regulatory compliance and the achievement of strategic objectives;
- Reviewing and monitoring the adequacy and effectiveness of the Society’s Risk & Compliance function; and
- Ensuring the Society has an effective conduct risk strategy which is developed and implemented, and that ensures the Society remains within the Conduct Risk Appetite set.

2. Membership

Members of the Committee are appointed by the Board and shall comprise three members all of whom shall be non-executive directors. The Chair of the Committee shall be appointed by the Board from amongst the Non-Executive Directors but shall not be the Chair of the Board.

Only members of the Committee have the right to attend meetings. However, other individuals, such as the Chief Executive, the Finance Director, the Chief Risk Officer, other members of the Executive Team and external advisors may be invited to attend for all or any part of any meeting, as and when appropriate and necessary.

In the absence of the Committee Chair, the remaining members shall determine between themselves who shall chair the meeting.

All new members of the Committee will be informed of the role of the Committee, their responsibilities and will be provided with the ongoing support and training required by role.

At least one member of the Committee shall also be a member of the Audit Committee and another a member of the Remuneration Committee.

Role	Status
Non-Executive Director, Chair	Member
Non-Executive Director	Member
Non-Executive Director	Member
Chief Executive	Attendee
Finance Director	Attendee
Chief Risk Officer	Attendee
Head of Compliance & MLRO	Attendee
Director of Operations	Attendee
Head of Prudential Risk	Attendee
Senior Operational Risk Manager	Attendee
Society Secretary	Secretary

3. Quorum

The quorum will be reviewed on an annual basis and is currently two members.

Quorum requirements should be reviewed annually to reflect any changes in Board membership or roles and responsibilities. A meeting can only be deemed quorate if all members have been invited to attend.

4. Authority

The Board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives. While the Board is ultimately responsible for risk and governance throughout the business, the Committee provides focused support and advice on risk and governance.

The Board has delegated responsibility for the design and oversight of appropriate risk management systems to the Committee. The Committee reviews the Society's Risk Management Framework along with its associated risk management and internal control policies.

The Committee will approve the Terms of Reference of its management committees at least annually.

The Terms of Reference of the Committee and any material amendments must be approved by the Board.

4.1 Exceptions

The Committee will review and approve exceptions to policy under its authority as prescribed by the specific policy in question (see section 5

below). Policy dispensations are submitted in writing to the Committee for approval, stating:

- The relevant policy or specific requirement(s) for which the dispensation is being requested
- What is being done instead of following the policy (i.e. the variation)
- An impact assessment of the dispensation
- The requested time period for the dispensation. Policy breaches or agreed exceptions are to be reported to the Committee through the relevant management information report as prescribed by the policy in question.

4.2 Voting

Each member of the Committee is entitled to a single vote, which can be cast either in person at the meeting, or by email prior to the meeting addressed to the Chair. Approval requires a simple majority. In the event of an even split vote, the Chair or acting chair has the option to exercise a casting vote. Committee members may not delegate their vote to a deputy, and invited guests attending the Committee are not entitled to vote.

5. Responsibilities¹

Responsibility	Details
Main Purpose	<p>The Committee provides focused support and advice on risk to the Board, including:</p> <ul style="list-style-type: none"> • providing advice on future risk strategy, including determination of Board risk appetite, and ensuring the business strategy is aligned with the agreed appetite for risk; • providing oversight and advice in relation to current and potential future risk exposures; • ensuring that the processes for identifying and managing risks (including liquidity, funding, interest rate and basis risks) are fit for purpose and implemented appropriately by management; • ensuring adequate capital is maintained for the Society’s key risk exposures, both to ensure regulatory compliance and the achievement of its strategic objective; • challenging and providing oversight of the design and execution of stress and scenario testing; • challenging and providing oversight of due diligence on risk issues relating to material transactions and strategic proposals;

¹ Responsibility for technology risk falls within the Transformation Committee’s remit although IT operational risks are reportable to the Committee.

	<ul style="list-style-type: none"> providing advice, oversight and challenge necessary to embed and maintain a supportive conduct risk culture throughout the Society.
Board Risk Appetite and Policy	<p>Oversee the development and implementation of the Board’s Risk Appetite Statement to ensure it remains fit for purpose, relevant to the business model and in line with regulatory, corporate governance and industry best practice. The Risk Appetite Statement will include quantitative and qualitative metrics.</p> <p>Recommend the Risk Appetite Statement for approval to the Board.</p>
Risk Policies and Processes	<p>Oversee the development, implementation and maintenance of the Risk Management Framework, including processes for identifying, assessing, monitoring and reporting on risks.</p> <p>Ensure the accountability and responsibility for managing risk effectively is clearly defined in the Risk Management Framework.</p> <p>Review the Internal Capital Adequacy Assessment Process, Internal Liquidity Adequacy Assessment Process document and associated appendices and recommend for approval to the Board.</p> <p>Review the Recovery Plan and Resolution Pack and recommend for approval to the Board.</p> <p>Review Climate Change and ESG Risk and approve the annual ESG Risk Assessment.</p>
Risk Monitoring and Reporting	<p>Approve the annual risk monitoring plan.</p> <p>Monitor compliance with risk appetite thresholds/targets and policies.</p> <p>Review Risk Management Information dashboards from the Executive Committees. Review and approve the Chief Risk Officer report on the Society’s risk exposures, including the assessment of the organisation’s top risk exposures.</p> <p>Challenge how the risks should be managed or mitigated to reduce the likelihood of their incidence or their impact.</p>
Other Policies & Reports	<p>Review and action regular reports for Data Protection from the Data Protection Officer.</p> <p>Review and approve the SCV Effectiveness Report.</p>

	<p>Review regular reports from the Money Laundering Reporting Officer and the adequacy and effectiveness of the Society's anti-money laundering systems and controls.</p> <p>Provide approval or recommendation to the Board (as appropriate) of policies/documents attributed to the Committee within the ERMF.</p>
Regulatory Compliance Oversight	Monitor the arrangements made by management to ensure compliance with requirements and standards under the regulatory system.
Emerging Risks	<p>Monitor significant emerging risks and significant changes in exposures to existing risks, e.g. horizon scanning.</p> <p>Re-evaluate on annual basis the validity of the main Risk Categories.</p>
Stress and Scenario Tests	Review the results and take required actions for reverse stress testing on the Society's Business Model and help to design measures to prevent or mitigate the risk of business vulnerabilities.
Risk Culture	Ensure that appropriate culture and reward systems have been embedded throughout the organisation.
Risk Management Resource	Ensure that adequate resources are allocated to the management of all material risks.
Compliance	<p>The Committee shall:</p> <ul style="list-style-type: none"> • approve the Annual Compliance Monitoring Plan. • make recommendations to the Board for the outsourcing or insourcing of compliance services. • monitor and keep under review the adequacy and effectiveness of the Society's services; • consider and approve the remit of the compliance function and ensure it is adequately resourced. The Committee shall also ensure the function has adequate standing, free from management or other restrictions and appropriate access to information to enable it to perform effectively; • review and monitor management's responsiveness to addressing any deficiencies identified by the Society's compliance monitoring activities; and • review regular reports from the Compliance Officer and keep under review the adequacy and effectiveness of the Society's compliance function.

<p>Fraud, Anti-Bribery and Data Protection</p>	<p>The Committee shall:</p> <ul style="list-style-type: none"> • review the Society’s procedures for detecting fraud; • review the Society’s systems and controls for the prevention of bribery and anti-money laundering and receive reports on non-compliance; and • review the Society’s systems and controls for data protection.
<p>Other</p>	<p>Consider its own performance, noting its conclusions in the Assurance Report that is submitted to the Board.</p> <p>Review the Committee Terms of Reference prior to submission to the Board for approval.</p>

In carrying out their risk governance responsibilities, the Committee should have regard to any relevant advice from the Audit Committee or internal audit function concerning the effectiveness of its current control framework. In addition, they should remain alert to the possible need for expert advice and support on any risk issue, taking action to ensure that they receive such advice and support as may be necessary to meet their responsibilities effectively.

6. Meeting Frequency

Meetings shall be held at least four times a year. Additional meetings may be convened following consultation with the Chair and provided that the quorate requirements are applied.

Meetings of the Committee are scheduled annually in advance by the Secretariat, in conjunction with the Chair.

7. Secretariat

The Society Secretary will act as secretary for the Committee and be responsible for maintaining the meeting minutes. The Secretary will ensure that all follow-up actions are appropriately assigned and monitored.

The Secretary will ensure that all items included within the Terms of Reference are covered as standard agenda items in Committee meetings. The Secretary in conjunction with the Chief Risk Officer and the Chair will draw up an agenda which shall be circulated prior to each meeting to each member of the Committee and to any other attendees.

The Secretary will make a best endeavour to collate and circulate relevant reports to the Committee members and other attendees 5 days before the meeting to enable papers to be reviewed.

An effectiveness review of the Committee will be performed annually, including a review of meeting content, Terms of Reference and composition. Changes or

improvements to the effectiveness of the Committee will be recommended to the Board for implementation.

8. Minutes & Reports

Committee decisions and discussions will be evidenced by minutes maintained by the Secretary and after approval by the Chair will be circulated to the Committee members and nominated attendees within 10 working days of the meeting to allow completion of actions. In addition, a summary report, including areas for action or improvement, will be presented by the Chair or acting chair to the Board at its next meeting.

9. Other Matters

The Committee has access to sufficient resources, including the Society Secretary, to carry out its duties including authority from the Board to obtain, at the Society's expenses, legal or professional advice on any matters within its terms of reference.

The Committee gives due consideration to laws and regulations, Codes of Practice and any other Rules, as appropriate.

The Chair should attend the Annual General Meeting to answer members' questions on the Committee's activities.

10. Document Version History

Date	Version	Author	Comments
21.05.24	V2.6	Shazrin Begum, Assistant Society Secretary	Annual review. Minor changes including updating Assistant Society Secretary to Society Secretary as meeting Secretary. Senior Operational Risk Manager role as an attendee.
20.05.25	V3.0	Gavin Mullen Society Secretary	Annual review. General tidy up of the ToR, including updating the list of attendees, and the addition of documents reviewed by the Committee.
21.05.26	V4.0	Gavin Mullen Society Secretary	Annual review. Minor changes to reflect the comments made by Clare Chalmers Ltd in their board performance review report and to clarify responsibility for technology risk.