GROUP RISK MANAGEMENT POLICY

POLICY STATEMENT

Risk management is the set of activities that enable the identification, assessment, management and monitoring of risks that could have a material impact on the achievement of M&S's business strategy and objectives. It is a component of our wider governance, risk and internal control framework that helps protect our assets and reduce the likelihood and/or scale of business loss.

BACKGROUND

This policy sets out the Board's requirements in relation to the establishment of and compliance with a framework for facilitating the management of business risks effectively, consistently and in line with the company's risk appetite.

In addition to supporting the achievement of our strategic objectives, the risk management processes are designed and implemented to allow M&S to demonstrate compliance with the UK Corporate Governance Code.

It is the responsibility of businesses and functions to ensure that they understand and comply with this policy. A separate guidance document sets out the underpinning methodology for the risk management processes that have been established.

Risk Management Principles

Across our business, M&S will:

- Comply with all relevant UK Corporate Governance responsibilities in relation to risk management as set out in the UK Corporate Governance Code and good practice specified in the FRC's Guidance on Risk Management, Internal Control and Related Financial and Business Reporting.
- Establish and maintain a company-wide process to proactively identify and manage risks that may impact the achievement of its business strategy and objectives.
- Ensure clarity and consistency in the risk management process, including clear accountability and ownership for managing risks, at the right level, across the business.
- Establish appropriate governance and oversight at Executive Committee level.
- Appoint individuals with appropriate skills and capabilities to manage and coordinate risk management processes, alongside ensuring there is appropriate resources to address key areas of risk on a prioritised basis.
- Maintain a set of risk appetite statements approved by the Board, communicate these to the Group and make decisions about operations and projects in line with these.
- Consider and track emerging risks as part of the risk management process.
- Consider risk in the context of both threats and opportunities and incorporate risks into strategic and business planning.
- Regularly review and update the register of risks facing the business and track the timely implementation of mitigating actions.
- Ensure that risk owners design, implement, maintain and monitor control activities that effectively mitigate our risks to a target level.
- Assess how the business is operating in relation to Board risk appetite and put in place appropriate remediations to align and/or formally agree step-outs with the Audit & Risk Committee.
- Escalate significant changes to risks and non-compliance to the appropriate levels.
- Ensure that risk management is embedded as part of major programmes and projects.
- Provide the Audit & Risk Committee with a half-yearly update of the risk management processes and the principal risks and uncertainties, as well as ad hoc updates as required.
- Ensure that appropriate arrangements are in place to monitor the effectives of the risk management framework on a routine basis.
- Benchmark our risk management framework and output to recognised good practice, guidelines and standards and incorporate lessons learnt.
- Enable visibility of cross-business risks at appropriate governance forums and committees to periodically track and monitor risks throughout the year.

Specific responsibilities are summarised on pages 2-4.

Risk Management Methodology

To support delivery of our risk management principles the business has established a risk management framework that allows consistent adherence and application of the following requirements across the business:

Risk identification

- Each business and function is accountable for identifying its risks, both those impacting the business today and those that are emerging.
- Risk descriptions must include cause, event and consequence detail.

GROUP RISK MANAGEMENT POLICY

- Each risk must have an identified owner.

Risk assessment

- The impact and likelihood (over a three-year horizon) must be considered using the M&S Group Risk Assessment Criteria.
- All risks must be assessed on a Gross, Net and Target basis.
- The assessment should also include an evaluation of how the business is operating in relation to Board risk appetite across all key areas of activity, including subcomponent parts such as JVs, investments, franchise and/or where core activities differ (e.g. payroll systems).

Risk response

- For each risk, the owner is required to establish and maintain appropriate and effective controls to mitigate the potential impact of risks to the identified Target level, aligned with risk appetite.
- For all risks where the Net risk severity is higher than the Target, the owner must develop and deliver appropriate actions to reduce the risk or provide adequate justification where risks are accepted at the current level.
- Each action should be captured in a way that is measurable and evidenced, assigned an action owner and a specific completion date.
- Where risks remain outside of Board appetite, with no further remediation plans, these need to be agreed with the Audit & Risk Committee.

Risk monitoring, reporting and escalation

- Business and function risk profiles must be reviewed and agreed at the appropriate governance body (Business Board and/or Leadership team).
- Updated risk profiles, including any identified emerging risks, must be reported to Group Risk half-yearly and as part of any interim updates as required.
- On a half-yearly basis, the Audit & Risk Committee reviews the effectiveness of the risk management process, and that principal risks and uncertainties of the business are appropriately disclosed.
- The Executive Risk Committee periodically reviews and challenges significant risks and issues that impact the business.
- Where there are new or emerging risks, or significant deterioration/escalation of risks these must be reported to the Executive Risk Committee, the Executive Committee and the Audit & Risk Committee, for example –
  - where the severity of a risk increases to critical and/or any areas where leadership believe they are operating outside of appetite,
  - where there is a large delta between the Net and Target risk score; or
  - where there have been significant incidents, loss events or near misses that impact risks, including plans for remediation should be reported as part of:
    i. updates provided to the Executive Risk Committee;
    ii. bi-annual risk updates provided to the Group Risk team; and
    iii. within periodic risk and control updates to the Audit & Risk Committee.
- The Board approves the disclosure of risks in the Annual Report & Financial Statements, the Interim disclosure and any other external reports, supported by recommendation from the Audit & Risk Committee.
- Business adherence to policy should be confirmed as part of the Group Risk compliance checklist on a half–yearly basis.

KEY RESPONSIBILITIES

Risk responsibilities of individual roles (e.g. Risk Owner, Risk Lead) are specified within the Risk Guidance Manual.

Body	Ownership remit	Responsibilities
PLC Board	Groupwide	• A Set and communicate the Board's risk appetite, including periodic review to ensure it remains appropriate to the business. • Set the approach for the monitoring of the effectiveness of the risk and control framework and receive updates from the Audit & Risk Committee on this. • Receive reports from the Audit & Risk Committee on the effectiveness of the risk management and reporting process. • Approve all risk related disclosures in the annual report and accounts and other public documents.

GROUP RISK MANAGEMENT POLICY

Body	Ownership remit	Responsibilities
Audit & Risk Committee	Groupwide	• Support the Board in fulfilling its responsibilities. • Approve the Group Risk Management policy. • Review and recommend Risk Appetite Statements and Principal Risks and Uncertainties to the Board for external reporting. • Review and recommend to the Board the assessment of internal controls, including any gaps in effectiveness, and associated mitigation activities for external reporting. • Receive updates and recommendations from the Executive Risk Committee in relation to the effective management of risks. • Receive updates from the business on their risks. • Review and challenge actions taken by management to manage risks. • Receive notification of any material risk issues and agree proposed actions, including for emerging risks. • Receive updates on where the business is operating outside of risk appetite, including remediation plans and approve step-outs. • Monitor the risk management process and periodically carry out a review of effectiveness.
Executive Directors	Groupwide	• Periodic review and challenge of risks, including emerging risks, at Business Boards and leadership meetings (including the Executive Committee). • Assess the effectiveness of internal controls and agree remediation plans with businesses. • Six-monthly review and challenge of the principal risks. • Individual ownership of principal risks. • Agree business step-outs outside of appetite and remediation plans.
Executive Risk Committee	Groupwide	• Support the Executive and Audit & Risk Committees in the management of risks and overseeing business compliance with the Group Risk policy and associated corporate governance requirements. • Review the Group Risk Management policy and Risk Appetite Statements and recommend these to the Audit & Risk Committee. • Review the business updates and papers produced by Group Risk prior to submission to the Audit & Risk Committee. • Confirm to the Audit & Risk Committee the effective operation of the risk management framework, including any weaknesses and corrective actions planned. • Review and challenge significant risks at a business unit or functional level. • Receive representations from ExCo members on the effective management of risks in accordance with policy and risk appetite, including any remediation activities planned. • Lead the business wide approach to complying with corporate governance changes. • Consider significant emerging risks or issues, to understand the business' response to mitigate these risks, and provide intervention where needed.
Business Functional Leadership	Own business and functional area	• Appointment of a Risk Lead to co-ordinate the risk process and act as a point of contact with Group Risk. • Individual ownership of business level risks. • Effectively manage risks, including:

GROUP RISK MANAGEMENT POLICY

Body	Ownership remit	Responsibilities
		○ Assigning risk ownership to appropriate individuals. ○ Maintenance of effective risk mitigation plans for the area, including ensuring timely completion of risk mitigating actions. ○ Regular review of new or emerging risks impacting the business. ○ Quarterly review and challenge of own risk profile, including detailed analysis of risks through monitoring movements and ensuring appropriate and timely action is taken on further mitigations. ○ Maintain an effective system of risk management and associated internal controls. ○ Review and confirm that the business activities and operations are in line with Group Risk Appetite, highlighting areas where we are potentially outside of appetite and the actions being taken. ○ Agreement of risk profile, including action plans with the accountable ExCo member. ○ Six-monthly reporting of risk profile to the Group Risk Team. ○ Updates to the Audit & Risk Committee of the business or functional risk profile, including detailed analysis of significant risks, mitigation plans, areas where the business is operating outside of risk appetite and remediation plans and emerging risks. • Review and confirm appropriate quality, completeness and validity of the risk information being reported.
Group Risk team	Groupwide risk co-ordination and reporting	• Coordinate risk reporting activities across the business, monitor the quality of reported risk information and challenge the completeness, validity and severity of reported risks through quality reviews and interaction with Risk Leads, leadership teams and Executive Directors. • Conduct risk analysis at Group level, including undertaking risk consolidation, calibration, aggregation and trend analysis. • Facilitate and monitor the implementation of effective risk management practices across the business. • Coordinate meetings and agendas for the Executive Risk Committee, including managing updates on specific actions arising from discussions. • Produce Group-wide risk reporting for the Executive Directors, the Executive Committee, Executive Risk Committee, Audit & Risk Committee and Board. • Provide updates to the Executive Committee on the status of risk actions within business and functional risk registers. • Maintain a set of risk appetite statements for the Group, including coordinating and reporting of Key Risk Indicators linked to these to the Audit & Risk Committee and the Board, as appropriate. • Maintain the Group Risk Management policy, guidance manual and risk management tool.

GROUP RISK MANAGEMENT POLICY

COMPLIANCE

This policy is applicable to all parts of M&S's wholly owned business activities, in both the UK and overseas. MDs and Heads of each of our businesses and key functions are accountable for its application in their respective parts of the business.

For business operations which are not wholly owned, such as joint ventures and other significant undertakings, the respective business and functional leaderships are required to satisfy themselves that the underlying entity has appropriate risk management practices in place. Where there are any significant risks impacting M&S these should be reflected in our own risk registers.

Compliance will be measured and reported by:

- Confirming business and functional risk submissions for the half-year and year-end reviews are reported to Group Risk on time, complete and in line with policy requirements.
- Completion of the bi-annual reporting on risk management processes and principal risks & uncertainties to the Audit & Risk Committee; and
- Confirming business and functional updates on risks are reported to the Executive Risk Committee and Audit & Risk Committee in accordance with the agreed rolling calendars.

Additional support and information can be found through:

- The Group Risk team
- Risk Guidance Manual, which provides details of each stage of the risk management process and supporting tools, including;
  - Risk ownership and responsibilities
  - Key risk management activities
  - Risk assessment and scoring
  - Risk mitigation and action planning
  - Escalation and reporting
  - Surecloud system
  - Reporting of emerging risks.
- Designated BU/functional risk facilitator.

FURTHER INFORMATION

Policy Owner	CFO
Compliance Lead	Head of Internal Audit & Risk
Published / Effective from	September 2024
Review frequency	Annually
Next review date	September 2025