

The Board Risk & Compliance Committee (the "Committee") has been established by the board of directors (the "Board") of Mattioli Woods plc (the "Company" or the "Group") as a committee of the Board.

## **1 PURPOSE**

- 1.1 The purpose of the Committee is to provide oversight and advice to the Board in relation to current and future risk exposure of the Company and its subsidiaries and the future risk strategy, including the determination of risk appetite and tolerance and the effectiveness of the risk management framework and (in conjunction with the Audit Committee) internal controls required to manage risk. The Committee shall also promote a risk awareness culture within the Company.
- 1.2 The Committee may sub-delegate any of its powers and authority as it sees fit, including, without limitation, through the establishment of sub-committees to consider particular issues and report back to the Committee.
- 1.3 The Committee has delegated day-to-day operational management of the Group to the Operational Risk and Compliance Committee ("ORCC") and authorises the ORCC to seek any information it requires from any employee or director of the Group and all Group companies, and all employees or directors shall co-operate with any request made by the Committee.

## **2 COMMITTEE COMPOSITION**

- 2.1 Membership will be made on the recommendation of the Nomination Committee and in consultation with the Chair of the Committee.
- 2.2 The Committee shall have at least three members and the majority of members shall be independent non-executive directors. The Committee shall include at least one member of the Audit Committee.
- 2.3 The current membership of the Committee is found at appendix 1.
- 2.4 Only members of the Committee, and, at the invitation of the Chair, other members of The Board, shall have the right to attend meetings. Membership is personal to the position holder and cannot be delegated.
- 2.5 Membership shall be for a period of three years, which may be extended for up to two additional three-year periods, provided the member still meets the criteria for both independence and membership of the Committee.
- 2.6 The Committee's Chair shall be appointed by the Board and shall be accountable for the effective operation of the Committee. In the absence of the Committee Chair, their deputy, or in their absence the remaining members shall elect one of themselves to chair the meeting.
- 2.7 All members shall have appropriate knowledge, skills and expertise to fully understand and

monitor the risk strategy and appetite of the Company.

- 2.8 Other individuals may also be invited to attend all or part of any meeting as and when the Chair deems appropriate and necessary.
- 2.9 Regular invited attendees are likely to be, but are not limited to, Chief Executive Officer, Group Compliance Officer, Chief Operating Officer, Corporate Reporting Officer, Compliance Manager and internal auditors.

### **3 MEETINGS**

- 3.1 The secretary of the Committee shall be the Company Secretary or such other person as the Committee may appoint.
- 3.2 The Committee shall meet at least four times per annum. The Chair has the discretion to cancel, reschedule or call additional meetings as required. Meetings shall be called by the Secretary at the request of its Chair or any of its members or at the request of the Group Compliance Officer, if they consider it necessary or appropriate.
- 3.3 Meetings may be conducted by telephone or video conference and decisions made by such means shall be appropriately recorded and shall have the same effect as those conducted in person.
- 3.4 The quorum necessary for the transaction of business shall be two members, both of whom shall be independent non-executive directors.
- 3.5 At least once per year the Committee shall meet with the Group Compliance Officer without any executive director present.
- 3.6 In addition, the Committee Chair shall maintain a dialogue with key individuals involved in the Company's risk management and compliance including, the Chair of the Board, the Chief Executive Officer, Chief Financial Officer, the external lead audit partner and the Group Compliance Officer.
- 3.7 The agenda for each meeting shall be approved by the Chair. Notice of each meeting, together with an agenda of items to be discussed shall be forwarded to each Committee member, and any attendees, no later than 5 working days before the meeting. Supporting papers shall be sent to Committee members, and other attendees as appropriate, at the same time.
- 3.8 The Secretary shall prepare formal minutes for every meeting capturing key issues raised and any decisions/approvals made/granted by the Committee.

### **4 RESPONSIBILITIES**

The duties of the Committee shall be to:

#### **Risk Appetite Framework**

- 4.1 Advise the Board on the Company's overall risk appetite tolerance and strategy, which shall

also take into consideration environmental and economic factors.

- 4.2 If requested by the Board, to review proposed strategic actions impacting the Company including strategic acquisitions or disposals, ensuring that due diligence of the proposition has been carried out, in particular focusing on the implications for the risk appetite and tolerance of the Company.
- 4.3 Oversee management implementation of the risk appetite framework, including management's response to breaches of risk appetite.

### **Risk Management**

- 4.4 Review the design and implementation of the risk management framework at least annually.
- 4.5 Review the effectiveness of the risk management framework and, in conjunction with the Audit Committee, the internal controls required to manage risks. In undertaking these responsibilities, the Committee will:
  - 4.5.1 Review the performance of the Company relative to risk appetite and monitor any risk trends and concentrations. Review all material risk exposures and management's recommendations to monitor and control such exposures.
  - 4.5.2 Ensure that an annual robust assessment of the emerging and principal risks facing the Company is undertaken, including those risks that would threaten its business model, future performance, solvency and liquidity, and provide advice on the management and mitigation of those risks.
  - 4.5.3 Review the methodology for reporting risk to the Board, including both quantitative and qualitative measures. Consider the Company's risk profile relative to current and future strategy and confirm that the Company is operating within the Board approved risk appetite framework.
  - 4.5.4 Keep under review the risk assessment processes that inform the Board's decision making.
  - 4.5.5 Consider material findings from regulatory reviews and interaction with regulators which impact risk governance or risk management processes.
  - 4.5.6 Report to the Board on its consideration of the above, identifying areas where improvement is needed and make recommendations as appropriate.
- 4.6 Receive regular reports from the Group Compliance Officer, including reports of any material breaches of risk limits and the adequacy of proposed action, and review and challenge the risk register.
- 4.7 Oversee the stress testing framework and challenge the design and execution of stress and scenario testing.
- 4.8 Recommend the appointment or removal of the Group Compliance Officer for approval by

the Board.

- 4.9 Approve the remit and oversee the performance of the Risk and Compliance Function (including performance of the Group Compliance Officer) as well as ensuring it has adequate resources and appropriate access to information to enable it to perform its function effectively with sufficient independence such as it is free from management interference.
- 4.10 The Group Compliance Officer will report directly to the Chief Executive, with a secondary reporting line to the Chair of the Committee and a right of access to the Chair of the Board.
- 4.11 The Committee Chair will discuss the remuneration of the Group Compliance Officer with the Chair of the Remuneration Committee.

### **Conduct Risk**

- 4.12 Ensure that conduct risks inherent in the Company's business model and/or strategy are identified, mitigated and monitored.
- 4.13 Provide oversight of conduct risk across the business and its adherence with the conduct risk appetite and policy once they have been developed.
- 4.14 Monitor business and relevant working group outputs to identify potential conduct risks, oversee mitigating actions and track to conclusion where appropriate.
- 4.15 Review and oversight of significant compliance trends.
- 4.16 Approve and monitoring of training for the FCA's Conduct Rules.
- 4.17 Monitor and review of conduct breaches.
- 4.18 Review the conduct risk management information and provide appropriate challenge and direction.
- 4.19 Report to the Board and other Committees through the conduct risk management information.

### **Compliance Function**

- 4.20 Review the effectiveness of the Risk and Compliance Function by assessing the adequacy and effectiveness of the measures and procedures put in place and the actions taken to address any deficiencies in the Company's compliance with its obligations, including FCA regulatory requirements, Codes of Practice and implementation of new legislation or rules.
- 4.21 In its review of the work of the Risk and Compliance Function, the Committee will:
  - 4.21.1 Review and assess the Compliance Monitoring plan.
  - 4.21.2 Receive a report on the results of the Compliance function's work on a periodic basis, including reference to data emerging from the firm's approach to vulnerable customers.
  - 4.21.3 Review and monitor management's responsiveness to the Compliance function's

findings and recommendations.

- 4.21.4 Review regular reports from the Money Laundering Reporting Officer and the adequacy and effectiveness of the Company's anti-money laundering systems and controls.
- 4.22 Review annually the Company's procedures for detecting fraud Review the Company's systems and controls for the prevention of bribery and modern slavery and receive reports on non-compliance.
- 4.23 On an annual basis, as part of the Internal Capital and Risk Assessment ("ICARA"), oversee and challenge the design and execution of stress and scenario testing, ensure that a robust assessment of the emerging and principal risks facing the Company has been undertaken, that procedures are in place to identify emerging risks, provide advice on the management and mitigation of those risks and the required capital is held by the Company to recognise the risk.
- 4.24 Review the consolidated ICARA for recommendation to the Board.

### **Regulatory Matters**

- 4.25 Oversee and review the Pillar 3 submission, for recommendation to the Board.
- 4.26 Approve the annual regulatory monitoring plan.
- 4.27 Consider any material findings from regulatory reviews and interactions with the Regulators in relation to risk governance, risk assessment or risk management processes and oversee management's response to such findings or interactions.

### **Consumer Duty**

- 4.28 Oversee and challenge the Consumer Duty implementation plan by assessing the adequacy and effectiveness of the measures and procedures put in place and the actions taken to address any deficiencies in the Company's compliance with its obligations.
- 4.29 In its overseeing of the plan, the Committee will:
  - 4.29.1 Review and assess the implementation plan.
  - 4.29.2 Receive a report on the results of the implementation work on a periodic basis.
  - 4.29.3 Review and monitor management's responsiveness to the plan.

### **Remuneration**

In conjunction with the Group Compliance Officer:

- 4.30 Provide advice to the Remuneration Committee to enable it to consider adjustments to remuneration to reflect risk management.
- 4.31 Provide input to the Remuneration Committee regarding the annual risk and control

objectives of Senior Management Function holders (“SMFs”) within the business.

- 4.32 Review the year-end performance of the SMFs against risk and control objectives and advise the Remuneration Committee of any specific recommendations.
- 4.33 Consider regulatory reportable events/other significant investigations and resulting accountability reviews and to advise the Remuneration Committee on robustness of approach, which may include expressing a view on the appropriateness of the recommendations.
- 4.34 To review and provide recommendations to the Remuneration Committee regarding (i) performance related pay or share incentive plan performance measures for SMFs, to monitor that risk perspectives are appropriately reflected; and (ii) the effectiveness of risk management during the relevant performance related pay or share incentive plan performance period(s) prior to the grant and vesting of any awards to SMFs.

## **5 SHAREHOLDER ENGAGEMENT**

- 5.1 The Chair of the Committee should attend the Company’s Annual General Meeting for the purpose of handling any questions or enquiries at the meeting about risk management or compliance.

## **6 REPORTING RESPONSIBILITIES**

- 6.1 The Chair shall report to the Board on the Committee’s proceedings on all matters within its accountabilities and responsibilities and the minutes for all Committee meetings shall be included in the papers for the subsequent Board meeting.
- 6.2 The Committee shall also formally report to the Board on how it has discharged its responsibilities, including the significant issues it considered in relation to the risk strategy and appetite of the Company.
- 6.3 The Committee shall make whatever recommendations to the Board it deems appropriate on any area within its remit where action or improvement is needed, and adequate time should be made available for Board discussion when necessary.
- 6.4 The Committee Chair shall make a statement in the Company’s Annual Report about the activities of the Committee.
- 6.5 If an external search consultancy has been engaged, it should be identified in the annual report alongside a statement about any other connection it has with the company or individual directors.

## **7 OTHER MATTERS**

- 7.1 The Committee shall:
  - 7.1.1 Have access to sufficient resources in order to carry out its duties, including access to

the Company secretary for advice and assistance as required.

- 7.1.2 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.
  - 7.1.3 Give due consideration to all relevant laws and regulations, the provisions of the QCA Corporate Governance Code and associated guidance, the requirements of the London Stock Exchange plc, AIM Rules for Companies, the Market Abuse Regulations (to the extent applicable) the Disclosure Guidance and Transparency Rules, the Senior Managers and Certification Regime, and any other applicable rules, as appropriate.
  - 7.1.4 Ensure that a periodic evaluation of the Committee's own performance is carried out.
  - 7.1.5 At least annually, review the Committee's 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.
  - 7.1.6 Review minutes from the ORCC.
- 7.2 The Committee is authorised by the Board to:
- 7.2.1 Investigate any activity within its terms of reference.
  - 7.2.2 Obtain any information it requires from any employee, director, and all such employees or directors will be directed to co-operate with any request made by the Committee.
  - 7.2.3 Obtain outside legal or other independent professional advice at the Company's expense.
  - 7.2.4 Instruct external professional advisers to attend any meeting if it considers this necessary or appropriate at the Company's expense.
- 7.3 The Committee will consider reports or topics, as may be requested by the Board.
- 7.4 The Committee will perform oversight functions as requested by the Board.
- 7.5 The Committee shall make available these terms of reference and include the information on the Company's website.

These terms of reference were adopted on 11 December 2023.

## **Appendix 1**

- 1 Alison McKinna (Chair)
- 2 Anne Gunther
- 3 Martin Reason