

Risk Management Policy and Framework Statement

McMillan Shakespeare Group of Companies



McMillanShakespeareGroup

Document Owner	Group General Counsel
Version Control	Version 6.0 – May 2021
Approved by the Board	24 May 2021

Background

McMillan Shakespeare Limited (**MMS**) has a responsibility to appropriately manage the risks MMS faces in its business. Effective risk management is required in order to achieve its business objectives. This is not only for the sake of its customers, shareholders, and employees, but also to meet its responsibilities as the holder of a Financial Services and Credit Licence and as a company listed on the Australian Securities Exchange.

Responsibilities of the Board

This risk management policy and framework has been approved by the Board of MMS, and applies to all entities within the MMS Group. The Board of MMS is responsible for establishing the risk appetite for MMS, and approving its risk management policy and framework. Given the nature and size of MMSG's operations the Board has established the Audit, Risk and Compliance Committee to oversee risk management. Risk management remains a direct responsibility of the full Board.

Audit, Risk and Compliance Committee (ARCC)

The ARCC reviews and assesses the ongoing activities of MMSG and the effectiveness of its risk management framework, policy and procedures on an ongoing basis, and provides a formal report to the Board. It is assisted in these activities by reports from the Risk and Compliance Committees.

Membership

The ARCC solely consists of non-executive Directors with a majority being independent directors and is chaired by an independent non-executive Director. The ARCC usually meets eight times a year. The remaining non-executive and executive Directors normally attend the meeting of the Committee as observers.

MMS Risk and Compliance Committee (RCC)

The MMS RCC is a management committee that has responsibility for actively managing the risks facing MMSG, including reviewing on a monthly basis (except January of each year) the key risks and any relevant mitigation measures.

In relation to financial reports, the Board receives a written statement, signed by the Chief Executive Officer (**CEO**) and the Chief Financial Officer (**CFO**), confirming that MMSG's financial reports give a true and fair view, in all material respects, of MMSG's financial position and comply in all material respects with relevant accounting standards. This statement also confirms that MMSG's financial reports are founded on a sound system of risk management and internal controls and that the system is operating effectively in relation to financial reporting risks.

Membership

The RCC includes membership from the CEO, the CFO, Chief Operating Officer (**COO**) and relevant Executives and is chaired by the Group General Counsel and attended by the Group Risk Manager (**GRM**). The CEO and CFO report to the ARCC on the activities of the RCC as required, and otherwise eight times a year (except January).

Retail Risk and Compliance Committee (RRCC)

The RRCC is a management committee that has responsibility for actively managing the risks in the Retail Finance Services (**RFS**) including reviewing on a monthly basis (except January of each year) the key risks and any relevant mitigation measures.

Membership

The RRCC is chaired by the GRM and has membership from the RFS Senior Executives, RFS management and legal, risk and compliance staff. The RRCC reports monthly to the Board of each subsidiary in the RFS segment (except January).

Operational Risk and Compliance Committee (ORCC)

The ORCC is responsible for considering and managing material operational risks and material compliance matters faced by MMSG across the GRS, AM and RFS segments in Australia and New Zealand. The ORCC meets on a monthly basis (except January of each year).

Membership

The ORCC consists of the COO, their direct reports (who are Group Executives) and the GRM. The COO chairs the ORCC meetings.

The UK Risk and Compliance Committee (UKRCC)

The UKRCC is a management committee that has responsibility for monitoring and managing material risk and compliance matters for the UK entities.

Membership

The UK Risk and Compliance Committee membership consists of relevant members of the UK Senior Executive team (Managing Director Asset Finance, Group Finance Director and Managing Director CLM, UK Risk and Compliance Manager), the MMSG COO, the GRM and Group Manager Finance UK and Financial Reporting.

Management of Specific Risk Areas

MMSG considers that particular risks may require more detailed and close management, in particular, Credit Risk, Treasury Risk and Residual Value Risk. As a result, separate policies have been approved for the management of Credit Risk, Treasury Risk, and Residual Value Risk. Under each of these policies, the relevant risk has been defined, responsibility for managing the risk has been allocated appropriate committees and reporting structures have been adopted to appropriately manage these specific risks.

The successful management of IT projects and the associated resource allocation is essential to the operational performance and competitive position of MMSG. The Project Governance Committee has been

established to provide oversight of and guidance to MMSG's Project Management Office which is charged with the day to day management of these issues.

Responsibilities of Senior Executive and Management of MMS

Each Senior Executive is responsible for managing risks within their area of responsibility, including identification of risks, implementation of appropriate management measures including mitigation plans and processes where appropriate, and reporting and escalating any matters to the ARCC or Board via the UKRCC, RRCC, ORCC, RCC, Credit Committee, Interest Committee, Residual Value Committee or the Project Governance Committee, as the case may be. Senior Executives refers to members of the key management personnel of MMS and the direct reports of the CEO and the COO.

Risk Management Procedures

MMSG bases its risk management procedures on the Risk Management Standard AS ISO 31000:2018. As part of their normal business activities, the Senior Executives are required to formally identify and/or review key risks they face, at least quarterly. The results of these reviews are recorded in the MMSG risks register, which is used by the RRCC and the RCC to actively monitor risks. The risks register includes the category of risk, risk identification, risk assessment, mitigation plan, and a Senior Executive owner(s) of the risk.

MMSG relies on the Three Lines of Defense model in identifying, managing and controlling risks–

1. management control – functions (operational managers) that own and manage risks are responsible for identifying risks and implementing suitable controls to address the risks;
2. risk management and compliance oversight –
 - (a) the UKRCC oversees the risk management process for the UK entities;
 - (b) the RRCC oversees the risk management process for RFS entities;
 - (c) the ORCC oversees operational risks; and
 - (d) the RCC oversees the risk management process at a Group level.
3. independent assurance (internal audit performed by an independent third party audit firm).

Risks Managed by MMS

MMS' activities give rise to a range of risks, like many other businesses. The key risks being managed by MMS include Reputation, Growth – Acquisitions, Growth - Diversification and Innovation, Customer, Financial, Credit Management, Regulatory Compliance, Conduct, Data/Technology, People, Leased Vehicles and Climate Change.