1. RISK MANAGEMENT STATEMENT

Medibank is committed to establishing a sound system of risk oversight and management and internal control to identify, assess, monitor and manage material risks related to the conduct of Medibank's activities.

Our aim is to:

- Continually improve the management of risk;
- Better understand the reward-to-risk balance; and
- Reduce the risks to acceptable levels.

Wherever we operate we will develop, implement and maintain management systems for all material risks that enable us to:

- Identify, assess and manage risks in an effective and efficient manner;
- Make decisions based on a comprehensive view of the reward-to-risk balance;
- Provide greater certainty of the delivery of objectives; and
- Satisfy our corporate governance requirements.

We will do this by:

- Implementing a comprehensive and systematic risk assessment and reporting process across the organisation;
- Integrating the outputs of risk specialist functions to provide a holistic view of the risks associated with our business activities; and
- Embedding risk management into the business, with an awareness instilled in all employees.

The level of risk control will be balanced by our continued encouragement of enterprise and innovation, with corporate governance being exercised through the regular measurement and reporting of our risk management processes.

2. RISK, CONTROL AND ASSURANCE FRAMEWORK AND RESPONSIBILITIES

Medibank maintains a system of risk oversight, risk management and internal control over material business risks, including the accuracy of financial reporting. This is designed to provide reasonable assurance in all material respects of the implementation of the Board's financial reporting policies, the integrity of the Group's financial reporting and management of its material business risks within the Board-approved risk appetite. Similarly, the compliance management systems provide the same underpinning for the oversight and management of material compliance risks.

Please see Appendix 'A' – Risk Framework and Responsibilities (below).

Appendix 'A' – Risk Framework and Responsibilities

Medibank maintains a system of risk oversight, risk management and internal control over material business risks, including the accuracy of financial reporting. This is designed to provide reasonable assurance in all material respects of the implementation of the Board's financial reporting policies, the integrity of the Group's financial reporting and management of its material business risks within the Board-approved risk appetite. Similarly, the compliance management systems provide the same underpinning for the oversight and management of material compliance risks.

Medibank's risk, control and assurance framework can be viewed as a 'Three Lines of Defence' model, as set out in the diagram below. Independence of the risk and compliance monitoring function within the second line of defence is maintained by ensuring that the Chief Risk Officer reports (with a dotted line) to the Chair of the Audit & Risk Management Committee (ARMC). Similarly, to ensure the independence of the audit function within the third line of defence, the General Manager Internal Audit reports directly (with a solid line) to the Chair of the ARMC.

Adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41

1. BOARD OF DIRECTORS

The Board has overall responsibility for Medibank's Risk Management systems. Specifically, the Board is responsible for reviewing, at least annually, the policies and procedures on risk oversight and management and satisfying itself that Management has developed and implemented a sound system of risk management and internal control to meet prudential and statutory requirements.

The Board is also responsible for approving the Risk Management Policy and determining the overarching Risk Appetite of Medibank.

2. AUDIT & RISK MANAGEMENT COMMITTEE

The ARMC assists the Board by:

- Providing oversight of the governance, risk management, compliance and financial reporting responsibilities of Medibank;
- Making recommendations to the Board in relation to its responsibilities to determine the Risk Appetite and review, at least annually, the policies and procedures on risk oversight and management and internal control;
- Making recommendations to the Board in relation to its responsibilities to approve the Risk Management Policy and to determine the overarching Risk Appetite;
- Monitoring the risk profile in the context of the overall Risk Tolerance and Risk Appetite;
- Monitoring progress in identifying and addressing material risk issues;
- Monitoring the adequacy and effectiveness of the risk management and internal compliance and control systems;
- Monitoring compliance with any regulatory obligations in respect of risk management;
- Monitoring compliance with other laws, regulations, codes and company policies; and
- Reporting to the Board on material matters, findings and recommendations pertaining to risk management and the internal compliance and control framework.

3. MANAGING DIRECTOR AND CHIEF FINANCIAL OFFICER

The Managing Director has overall accountability for ensuring that Medibank has established a sound system of risk oversight and management and internal control to assess, monitor and manage material risks related to the conduct of Medibank's activities. Further, the Managing Director is ultimately accountable for managing material risks in accordance with the Board-approved Risk Management Policy and Risk Appetite.

The Chief Financial Officer has the delegated authority (and responsibility) for the system of risk oversight and management and internal control.

4. CHIEF RISK OFFICER

The Chief Risk Officer is accountable for managing the strategic direction of the risk function and the development and management of group-wide risk governance and improvement programmes for identifying, evaluating, controlling, monitoring and reporting to the Board on all material risks across Medibank.

5. LINE MANAGEMENT

The Executive Committee is responsible for raising awareness of the relevant risks to staff and for ensuring compliance with Medibank policy, procedures and controls.

The identification and management of risk is delegated to Management. Management is responsible for the effective design and implementation of detailed Risk Management strategies, policies and processes to facilitate the achievement of business plans and goals.

6. INTERNAL AUDIT

Internal Audit is independent of Management and its role is to provide independent assurance to the ARMC and the Board on the adequacy and effectiveness of the Risk Management framework, financial reporting processes and internal control and compliance systems. The primary objective is to assist the ARMC and Board in the effective discharge of their responsibilities. The organisation employs a 'Three Lines of Defence' model with Internal Audit providing assurance over first and second line.

The General Manager Internal Audit reports directly to the ARMC Chair with a direct communication line to the Managing Director and the external auditor, reporting administratively to the Chief Financial Officer. The ARMC annually reviews the effectiveness of the Internal Audit Function. Internal Audit regularly seeks feedback from stakeholders to assess the value provided by the function to ensure continuous improvement.

The Internal Audit Strategy and Plan is approved annually by the Board (through the ARMC). Regular progress against the approved plan is reported to the ARMC. The Plan is dynamic to accommodate the organisation's changing circumstances, risk profiles and business unit requests, with all changes approved by the ARMC.

The General Manager Internal Audit provides activity reports to the ARMC which includes progress against the Plan, significant audit findings and recommendations, business insights and the status of implemented management actions.

The Internal Audit Strategy and Plan is designed to meet the assurance needs of the ARMC and Board ensuring adequate resourcing, capability and budget. The Plan is developed using a risk-based approach and is driven by the organisation's strategy, risk profile and governance principles.