

**Risk Management Practices
in the Private Health Insurance Industry**

Guidelines

Reviewed March 2004

1. The Nature of Risk

1.1 Introduction

Risk is any uncertainty in relation to the business operations of an entity. It can be measured in the broadest sense as that which threatens performance or causes financial loss.

In the financial services industry generally – the health insurance industry specifically – risk is inherent, given the nature of the business. Risk can be mitigated but cannot be eliminated; it may be managed but not managed away.

Different organisations will have a different tolerance for risk. PHIAC acknowledges this, and expects registered organisations to demonstrate appropriate management of risk within the tolerance levels approved by the Board of the organisation subject to the protection of the interests of contributors.

1.2 Risk Categorisation

Risks can be broadly grouped into two main categories; financial risks and operational risks. The following paragraphs provide an overview of these principal risks. Attachment 1 defines in more detail the sub-risk groups within these two categories.

a) Financial Risks

These are the risks associated with the assets and liabilities of the organisation, and highlight the significance of the financial aspects of the business and the risks inherent in such transactions. Financial Risks include:

Asset Risks

- Credit risk
- Market Risk
- Liquidity Risk
- Valuation Risk
- Concentration Risk
- Off Balance Sheet Risks (Derivatives, Foreign Currency Exposure)
- Related Body Holdings

Liability Risks

- Pricing Risk
- Valuation Risk
- Expense Risk
- Reinsurance Risk
- Off Balance Sheet Exposures (Guarantees)

These risks are, generally, more readily quantifiable and are largely secured by the holding of minimum capital requirements. PHIAC is satisfied that these risks are appropriately addressed through the actuarial standards for solvency and capital adequacy.

b) Operational Risks

This broad category is intended to identify the non-financial risks of the business. These are the risks associated with the administrative and operational aspects of the business, and include:

- Corporate Governance Risk
- Political (Sovereign) Risk
- Transactions Risk
- IT (Technology) Risk
- Legal Risk
- Documentation (Disclosure) Risk
- Risk of Fraud

These risks are not always readily quantifiable in terms of likely occurrence or expectation of loss. They are best managed by establishing risk management processes and systems of internal control.

1.3 Examples of Particular Risks Relevant to the Health Insurance Industry

Some of the particular risks associated with health insurance activities, and the types of risk management practices which could be implemented to manage those risks, are explored below:

- Corporate Governance Risk

Board and senior management appointment practices should target appropriately qualified persons, preferably with knowledge of the health industry and its legislative framework.

The processes of the Board, and for informing the Board, should facilitate good business practice. The Board should act in the best interests of contributors, bringing to decisions a perspective independent of the management of the business.

- Political Risk

Organisations should have in place contingency plans in the event of changes in the environment as a result of government policy (eg: rapid expansion of the market due to Lifetime Health Cover)

- Legal Risk

An example of legal risk is the circumstances which could arise in entering into service contracts, that is, arrangements entered into by an organisation to

obtain services or products from an external party. Such arrangements should be arm's length dealings, and not create additional risk or conflicts of interest. Service contracts should never abrogate management control or responsibility.

- Transaction/Technology Risk

The following issues should be considered in establishing practices in these risk areas:

- physical security of financial transactions and information;
- systems to safeguard the integrity and security of data;
- systems to adequately provide for the accurate and timely capture of data;
- limiting reliance on manual processing of transactions; and
- appropriately tested disaster recovery plans.

A particular area of transaction risk for the health industry is related to the administration of reinsurance. Given the financial effect of reinsurance, consideration should be given to the establishment of specific risk management practices in this regard.

- Documentation Risk

This is an area of potential risk due to growing consumer expectations, consumer protection legislation and increased product complexity. Consideration should be given to ensuring procedures and controls are in place for the preparation of materials to be provided to customers to ensure their accuracy - including review by appropriately qualified professionals, and internal sign off protocols.

- Fraud

Consideration should be given to policies and systems to protect against fraud or other criminal activity.

2. Appropriate Risk Management Practices

2.1 Introduction

It is not appropriate, nor in practice possible, to be prescriptive in terms of the types of risks covered or the types of risk management processes, which should be established. It is the mandate and responsibility of the Board and management of organisations to assess the particular risks associated with their activities and to appropriately monitor and manage these risks.

PHIAC requires that organisations refer to the Australian Standard for Risk Management (AS/NZS 4360:1999) for appropriate risk management processes.

2.2 Role of the Board and Management

Prudent management of an organisation's business requires a management discipline which accepts responsibility for risk management and is focussed on the identification and assessment of the risks associated with all aspects of the business, as well as the ongoing monitoring of risk management practices and processes.

It is the responsibility of the Board and management to assess the risks to which an organisation is exposed as a result of the activities it undertakes and to continually monitor and control those risks.

The role of the Board in this regard could include:

- Understanding, fully, the risks associated with the organisation's activities;
- Agreeing risk management strategies which are consistent with the organisation's commitments to contributors (and with regulatory requirements);
- Approving written risk management policies;
- Ensuring risk management control systems are established and operating effectively;
- Questioning management on risk management processes and giving appropriate priority to discussion and action re risk management issues; and
- Regularly re-evaluating the organisation's tolerance for, and exposure to, risk.

2.3 Role of Senior Management

The role of senior management in regard to risk management includes:

- Clearly understanding the measurement of risk and the risk management systems of the organisation;
- Ensuring activities of the organisation are conducted within the framework of approved policies and systems; and
- Keeping the Board advised of any breach of the risk management practices.

2.4 General Requirements

For all risks to which an organisation is exposed, the risk management practices and processes should address the following matters:

- **demonstrated understanding of the risks** to which an organisation is exposed. Consideration should not be limited to the risks associated with its health activities but extend to risks to the organisation from other (non-health) activities.
- **comprehensive written policies** for risk control. The policies should :

- be Board approved;
 - identify the risk tolerances and aggregate exposure limits;
 - establish clear lines of responsibility; and
 - provide for regular reassessment.
- **clearly defined responsibilities for senior management**, establishing levels of authority and powers of delegation. A well-defined reporting structure will ensure management is provided with all information necessary to manage risk. Management should be further supported by appropriately experienced personnel, appropriate control systems and suitable technology.
 - **adequate policies and control systems** to measure monitor and manage the risks. While policies and systems will differ depending on the activities of the organisation and its risk profile, they should generally include:
 - clear identification of the positions with delegated responsibility for managing specific risks;
 - adequate systems for measuring risk;
 - structured limits on risk taking appropriate to personnel experience and the Board's agreed tolerance for risk;
 - effective internal controls, including separation of operations and internal audit; and
 - comprehensive management information systems that ensure timely monitoring and reporting of risk exposures.
 - processes for the **documentation and review** of systems and for maintenance of control procedures. The effectiveness of implementation of risk management systems should be evidenced by appropriate documentation and records, and should be subject to regular review.
 - **contingency plans** (approved by the Board). Plans should clearly establish responsibility, provide for notification, identify early warning signals, outline courses of action, and assess the likely impact of particular courses of action.

2.5 Reporting Requirements

PHIAC will require an annual statement from 30 June 2002 that the organisation has a risk management plan and appropriate implementation of the plan. The suggested reporting format is at Attachment 2.

RISK TERMINOLOGY

Provided below is a description of the different types of risk which may be considered by the organisation as relevant to health insurance activities. The list is not intended to be comprehensive.

RISK: is any uncertainty in relation to the business operations of the entity, whether statistically quantifiable or not, and which has the potential to result in financial loss to the entity.

ASSET RISK: those risks associated substantially with the nature, form and valuation of the assets (both on and off balance sheet) of the entity, regardless of the liabilities which those assets are supporting.

LIABILITY RISK: those risks associated substantially with the nature, form and valuation of the liabilities (both on and off balance sheet) of the entity, regardless of the assets backing those liabilities.

OPERATIONAL RISK: all risks not associated with the nature of the business (financial aspects of the business) itself but rather with the administration and operational aspects, both human and technical, of undertaking that business.

CREDIT RISK: the risk of loss from partial or total default by the obligors or counterparties.

CONCENTRATION RISK: (an asset or liability risk depending on the context) relates to risk associated with inappropriate levels of aggregation of asset/liability exposures. Aggregation may be considered in terms of:

- the type (class) of asset/liability to which exposed; or
- the party with whom the exposure exists.

VALUATION RISK: (an asset or liability risk depending on the context) relates to the uncertainty associated with the assets or liabilities (quality of the assets/liabilities) and the extent to which the value placed on those assets/liabilities is appropriate.

LIQUIDITY RISK: the risk that the entity will be unable to promptly meet its obligations to creditors or customers as they fall due.

MARKET RISK: the risks that the value of assets declines as a result of changes in market conditions – for example, changing interest rates, declining property values or share prices.

PRICING RISK: relates to the inherent uncertainty associated with the liabilities of an insurer in respect of the contingent events against which the insurance service is provided.

TRANSACTIONS RISK: the risks of error or failure associated with the administrative aspects (both procedural and human aspects) of the operation of the business, for example, where a transaction is not executed accurately or completely.

DOCUMENTATION RISK: the risks associated with the preparation of documents for external parties, in particular product information materials prepared for consumers.

TECHNOLOGY RISK: the risks of error or failure associated with the technological aspects (IT systems etc) of the operation of the business.

POLITICAL RISK: the risks associated with uncertainties in the external political environment (changes in government policy, regulatory policy etc.) to the extent they adversely impact on the business of the entity.

FRAUD RISK: the risks associated with intentional acts, undertaken with the objective of personal benefit, to tamper with or manipulate the financial or operational aspects of the business.

LEGAL RISK: the risks associated with the legal relationships and obligations of the entity. The risk of legal action against the entity associated with claims of negligence, breach of contract, discrimination etc.

DRAFT FORM OF REPORT TO PHIAC
RISK MANAGEMENT

I, _____ (*director*), certify that _____ (*registered organisation*) has the following risk management systems in place:

- Comprehensive written policies and procedures, and adequate control systems in place to measure monitor and manage operational risk.
- The Board reviews these policies, at least annually, as to their implementation effectiveness, and to endorse them.
- The registered organisation has adopted the Australian Standard for Risk Management (AS/NZS 4360:1999) as an accepted measure of appropriate risk management processes.
- The Board has approved the risk management system in place, and understands its contents. The Board receives regular reports on the operation of the risk management system and is satisfied with the level of compliance.

Signed (Director)

Signed (Director)

Note:

This statement is made in accordance with a resolution of Directors. It is to be signed by at least two Directors.