

**BERMUDA MONETARY AUTHORITY**  
**INSURANCE DEPARTMENT**

**GUIDANCE NOTE #13**

**RISK MANAGEMENT AND INTERNAL CONTROLS**

**MARCH 2005**

## **GUIDANCE NOTE: RISK MANAGEMENT AND INTERNAL CONTROLS**

### **Introduction**

- 1 Insurers must be prudently managed. The prime responsibility for the sound and prudent management of an insurer rests with the board of the insurer. Corporate governance refers to the rules and procedures put in place within a corporation for the management and control of its business and affairs. Risk management and internal controls systems are an integral part of a corporate governance framework. Risk management and internal control systems and practices may differ depending on the size and complexity of the insurer, and the nature of the insurer's risk exposures. This guidance note sets out factors that the board of directors and the management of an insurer should consider when establishing and implementing risk management and internal control systems and procedures.
- 2 The Bermuda Monetary Authority (the "Authority") recognizes the need for clarity as to the scope and implementation of the provisions of the Insurance Act and related regulations ("the Act")<sup>1</sup> if the regulatory system is to command the confidence of both insurers and policyholders. It seeks, therefore, to ensure that those operating in Bermuda have a good understanding of the nature of the requirements and of the Authority's approach in implementing the Act.
- 3 While the Authority aims to provide clarity as to its approach, this guidance note cannot be exhaustive. The Authority will do its best through this and other guidance notes to set out information about its regulatory approach and expectations regarding a registered insurer's risk management and internal control systems.
- 4 Other guidance issued by the Authority may contain additional information on risk management and internal control systems or related matters.<sup>2</sup>
- 5 The Authority's guidance is of a general application and seeks to take account of the wide diversity of institutions that may be licensed under the Act. There is likely to be a need for the Guidance to be revised and developed over time.

---

<sup>1</sup> The insurance legislation is comprised of the Insurance Act 1978 (as amended by the Insurance Amendment Acts, 1981, 1983, 1985, 1995, 1998 and 2001) and the regulations promulgated under that Act (the "Regulations"). The Regulations are the Insurance Accounts Regulations 1980 (as amended by The Insurance Accounts Amendment Regulations 1981, 1985 and 1989) and the Insurance Returns and Solvency Regulations 1980 (as amended by The Insurance Returns and Solvency Amendment Regulations 1981, 1985 and 1989). References herein to the "Act" are to the Insurance Act 1978 (as amended) and the Regulations.

<sup>2</sup> Risk management and internal controls directly impact on an insurer's corporate governance. The Authority has issued separate guidance notes on a number of subject matters relating to corporate governance and the decision making process, including corporate governance, investments, and insurance activities.

Material changes in the Guidance will be published, generally through the issue of revised versions.

- 6 For references in these Guidance Notes with respect to the changes in legislation contained in the Insurance Amendment Act 2004 insurers must take immediate steps to ensure they are in compliance with the Act. In relation to other matters contained in the Guidance Notes, the Authority encourages insurers to come into compliance as soon as possible and, in any event, not later than 31<sup>st</sup> December 2005 or a later date as may be agreed with the Authority in a particular case.

### **Application**

- 7 This guidance applies to all insurers registered under the Act.
- 8 In managing its affairs, an insurer should have regard to the principles of good risk management and internal controls. Taking into account the size, nature, complexity and risk profile of the business of the licensed insurer, the board must exercise its judgement in determining the nature and scope of the risk management and internal control systems and practices that are necessary. It is the responsibility of the board to determine which specific provisions of this guidance should be applied
- 9 As part of its supervisory process, the Authority will look for indications that, overall, processes or procedures for effective risk management and internal control systems are in place, that they are appropriate to the individual insurer, and that they are operating effectively. The Authority will formulate its judgment on the effectiveness of an insurer's risk management and internal control systems based on a variety of indicators. The degree of applicability and weighting of individual elements in this guidance will depend on the size, nature, complexity and risk profile of each insurer. For example, the Authority recognizes that insurers which only insure or reinsure the risks of their owners and are part of the same organization may pose less risk to the public than other insurers or reinsurers, and that it may be appropriate for the risk management and internal control policies and procedures for these entities to be less complex than for other insurers.<sup>3</sup>
- 10 The Authority recognizes that security commissions, stock exchanges, governments and international bodies, and others have issued laws, guidance or best practices on risk management and control processes ("other standards"). The

---

<sup>3</sup> As stated in the IAIS Principles on Minimum Requirements for Supervision of Reinsurers approved in October 2002 "*where captives only insure the risks of their owners and are part of the same organization they may not pose the same risk to the financial system and separate regulations may be established recognizing this reduced risk.*" This approach is also consistent with international best practices as described by the International Association of Insurance Supervisors, which recognize that the principles adopted in a jurisdiction should take into account the domestic context and industry.

Authority expects registered insurers to be aware of other emerging and in-force standards that are applicable to their organizations (which may depend, for example, on whether the institution is a publicly-traded entity<sup>4</sup>) and to consider and, where appropriate, incorporate these into the institution's risk management practices. The Authority also recognizes that these other standards may overlap or exceed some of the expectations for risk management and internal controls described in this and other guidance issued by the Authority, and that developments in these other standards may have an implication for insurers with respect to time and effort involved in meeting these other standards.

- 11 The Authority's supervisory approach is forward-looking (the Authority seeks to be preventative) and risk-based. The Authority's guidance for risk management and internal controls is principle based and is of general application. Where other standards for risk management and internal controls are consistent with the Authority's expectations as described in this and other guidance, and where the Authority can rely on an insurer's compliance with these other standards, it is not the intention of the Authority to require a company to undergo additional costs in order to comply with both the Authority's guidance as well as the other standards.

### **Role of the board**

- 12 The board of directors, along with management, is responsible for suitable prudential oversight of the risk management and internal control systems, strategies and policies. Insurers should review their policies and practices regularly to ensure that they remain appropriate in light of changing circumstances and in light of how policies and practices have performed.
- 13 Development and implementation of an adequate and sound system of internal controls is normally the responsibility of management. The board of directors, however, is ultimately responsible for ensuring that such a system is established and maintained.

## **RISK ASSESSMENT AND MANAGEMENT**

### **Risk management processes**

- 14 The types of risks assumed and the relative importance of particular types of risks in an insurer's risk management process will differ depending on the insurer's business and risk tolerance. Risk management means, in part, understanding the quality of assets and the nature of associated liabilities. An insurer should identify, understand, and manage the significant risks that it faces.

---

<sup>4</sup> For example, management of Securities and Exchange Commission ("SEC") registrants are required to evaluate and report on internal control over financial reporting under Section 404 of the Sarbanes-Oxley Act of 2002.

- 15 Risk management systems and practices will differ depending on the size and complexity of the insurer, and the nature of its risk exposures. The risk management process should be tailored to the particular nature of the insurer and can, for example, have different degrees of centralization or decentralization and be organized in different ways. It should enable the board and senior management to meet their organization-wide responsibilities. Comprehensiveness is a key attribute of effective risk management.
- 16 Insurers should implement and maintain sound and prudent risk management policies and systems capable of promptly identifying, measuring, assessing, reporting and controlling their risks. The circumstances of each insurer are unique, and the risk management systems and practices will differ, depending on the scope and size of the insurer and the nature of its risk exposures. Whatever the particular approach to risk assessment and management, every insurer should have integrated policies that, taken together, apply to the insurer's significant activities regarding the corporate philosophy on risk management, the insurer's permissible exposure to risk, objectives of risk management, delegation of authorities and responsibilities, and processes for identifying, monitoring and controlling/managing risk.
- 17 Insurers should be in a position to identify all material risks, financial and non-financial, that they face, assess their potential impact and have policies in place to manage them effectively. The insurer should establish an appropriate tolerance level or risk limit for material sources of risk.
- 18 Insurers should regularly review the market environment in which they operate, draw appropriate conclusions as to the risks posed and take appropriate actions to manage adverse impacts of the environment on the insurer's business.
- 19 The primary components of a sound risk management process include policies, procedures and practices that:
  - clearly delineate lines of responsibility for managing risk;
  - set in place adequate systems for measuring risk;
  - create appropriately structured limits on risk taking;
  - establish effective internal controls; and
  - describe comprehensive and timely risk monitoring and reporting.

20 While the risk management systems of an insurer should address all material risks, the following categories should be addressed in an insurer's risk management systems:

- credit risk;
- investment risk, including liquidity risk;
- insurance underwriting risk;
- market risk;
- business risk;
- group risk;
- legal/litigation risk;
- systems and operations;
- external risk; and
- reputational risk.

## **INTERNAL CONTROLS**

### **Internal control Mechanisms**

21 A system of internal control is critical to effective risk management.

22 Internal controls refers to a control system within an organisation which oversees the proper conduct of its business and affairs. Internal controls encompass the policies, processes, culture, tasks and other aspects of an insurer that support the achievement of the insurer's objective. A sound internal control system facilitates the efficiency of operations, contributes to effective risk management, assists compliance with applicable laws and regulations, and strengthens capacity to respond appropriately to business opportunities.

23 Among other matters, the purpose of internal controls is to verify that:

- the business of an insurer is conducted in a prudent manner in accordance with policies and strategies established by the Board of Directors;
- transactions are only entered into with appropriate authority;

- assets are safeguarded;
- accounting and other records provide complete, accurate, verifiable and timely information; and
- management is able to identify, assess manage and control the risks of the business and hold sufficient capital for these risks.

### **Internal Control Weaknesses**

24 The board of directors, or a committee of the board, should receive, at least annually, reporting on the effectiveness of the internal controls. Material internal control deficiencies should be reported to the board or suitable committee in a timely manner and addressed promptly.

### **Operations**

25 Insurers should have in place adequate operational procedures. Internal controls should ensure effective and efficient operations, and should address the organizational structure, in particular:

- duties and responsibilities including clear delegation of authority;
- decision-making procedures;
- separation of critical functions as far as can be reasonably undertaken; and
- internal checks and balances.

26 This may be satisfied, at the Board's direction, by reliance upon the systems adopted by a licensed insurance manager.

### **Financial Management**

27 There should be clearly established accounting procedures and reconciliation of accounts.

28 The accounting and other records should be complete and accurate, and can be used to compile financial statements, management information and returns in line with the requirements of the Act.

## **Compliance**

- 29 The internal and external audit, actuarial and compliance functions, as applicable, are part of the framework for internal control, and should test adherence to the internal controls as well as to applicable laws and regulations.
- 30 Depending on the nature and scope of the insurer's business, the Authority may expect the insurer to have an on-going internal audit function of a nature and scope appropriate to the business. This includes ensuring compliance with all applicable policies and procedures and reviewing whether the insurer's policies, practices and controls remain sufficient and appropriate for its business.
- 31 Where there is an internal audit function, the internal audit function should:
- i) have unfettered access to all the insurer's business lines and support departments;
  - ii) assess outsourced functions;
  - iii) have appropriate independence, including reporting lines to the board of directors;
  - iv) have status within the insurer to ensure that management reacts to and acts upon its recommendations;
  - v) have sufficient resources and staff that are suitably trained and have relevant experience to understand and evaluate the business they are auditing; and
  - vi) employ a methodology that identifies the key risks run by the institution and allocates its resources accordingly.
- 32 If requested, the insurer should provide the Authority with access to reports of the internal audit function.

## **Outsourcing**

- 33 Insurers may outsource functions either externally to third parties or internally to other affiliated entities. The insurer should have oversight and clear accountability for all externally outsourced functions as if these functions were performed internally and subject to the normal standards of internal controls.

End of guidance note.

***If you have questions on this or other guidance from the Insurance Department please email [info@bma.bm](mailto:info@bma.bm) . Please put "Insurance Guidance" in the title of your email.***