Insurance Rule 27 of 2009

Insurers' Internal Controls

Rule pursuant to article 4 of the Act

1. (1) This Insurance Rule on internal controls ("this Rule") is made by the Authority pursuant to, and for the purposes of, article 4 of the Act and the Insurance Business (Criteria of Sound and Prudent Management) Regulations, 1999.

(2) This Rule shall come into force on the 30th April 2009.

Application

2. This Rule applies to a company desirous of applying for authorisation to carry on and, a company authorised to carry on, the business of insurance ("the company").

Scope

3. (1) The scope of this Rule is to determine the internal controls required to be implemented by the Board of Directors of the company, as are appropriate to its business and which would enable the company to verify that:

(i) the business of the company is conducted in a sound and prudent manner in accordance with internal controls established by the Board of Directors;

(ii) transactions are only entered into with appropriate authority;

(iii) assets are safeguarded;

(iv) accounting and other records provide complete, accurate, verifiable and timely information; and

(v) management is able to identify, assess, manage and control the risks of the business and hold sufficient capital for these risks.

(2) This Rule does not attempt to modify the legal requirements and framework within which Board of Directors are required to carry out their responsibilities in terms of the Companies Act, 1995. Rather, it provides a guidance for the company in meeting the expectations of the Authority in directing its business and affairs.

Definition

4. In this Rule, unless the context otherwise requires:

"internal control" means the policies, systems and processes, established by the Board of Directors and effected by senior management and other personnel of the company, designed to provide reasonable assurance regarding the achievement of objectives in the effectiveness and efficiency of operations, the reliability of financial and non-financial reporting, adequate control of risks, a prudent approach to business and compliance with applicable legislation.

Internal controls

5. In this Rule, guidelines on internal controls and specific examples of the areas to be considered by a company in establishing and maintaining internal controls, are set out in the Schedule to this Rule.

Savings

6. The requirements of this Rule are without prejudice to the requirements of:

(a) the Insurance Business (Criteria of Sound and Prudent Management) Regulations, 1999;

(b) the Code of Principles of Good Corporate Governance included in the Malta Financial Services Authority Listing Rules applying to any Listed Company as defined in the Financial Markets Act (Cap. 345);

(c) the Corporate Governance Guidelines for Public Interest Companies issued by the Authority; and

(d) Insurance Rule 30 of 2012 on Complaints-Handling by Authorised Companies.

Repeals and Savings

7. (1) Saving the provisions of paragraph (2) of this article, Insurance Directive 27 of 2005 – Insurers' Internal Controls, is hereby repealed.

(2) Every action, directive, instruction, guideline or order whatsoever taken or commenced thereunder, shall continue to be valid and in force, as if such action, directive, instruction, guideline or order whatsoever were taken or commenced under this Rule.

S C H E D U L E

Guidelines on Internal Controls and Specific Examples of the Areas to be Considered by an Insurer in Establishing and Maintaining Internal Controls

1. In this Schedule –

"chief executive", in relation to a company or body corporate of which it is a subsidiary, means an employee of the company or that body corporate, who, either alone or jointly with others, is responsible under the immediate authority of the directors for the conduct of the whole of the business of insurance of the company or that body corporate;

"internal control environment" means the framework under which internal controls are developed, implemented and monitored. It consists of the mechanisms and arrangements that ensure internal and external risks to which the company is exposed are identified, that appropriate and effective internal controls are developed and implemented according to the Insurance Business (Criteria of Sound and Prudent Management) Regulations, 1999 to manage these risks, and that reliable and comprehensive systems are in place to appropriately monitor the effectiveness of these controls;

"senior manager" –

(a) in relation to a company whose head office is in Malta, means an employee of the company (other than a chief executive) who, under the immediate authority of a director or the chief executive of the company exercises managerial functions or is responsible for maintaining accounts or other records of the company;

(b) in relation to a branch in Malta of a company whose head office is in a country outside Malta, means an individual who is an employee of the company who satisfies the provisions of subarticle (2) of article 11 of the Act in so far as they apply to an individual, and who exercises managerial functions which relate exclusively to business of insurance conducted from the branch of the company in Malta;

"senior management" shall include the chief executive, the compliance officer, the money laundering reporting officer and the senior managers of the company.

2 (1) A company should take reasonable care to establish and maintain internal controls as are appropriate to its business.

(2) The nature and extent of the internal controls which a company needs to maintain according to this Rule will depend upon a variety of factors including:

(a) the nature, scale and complexity of its business;

(b) the diversity of its operations, including geographical diversity;

(c) the volume and size of its transactions; and

(d) the degree of risk associated with each area of its operation.

(3) To enable it to comply with its obligation to maintain appropriate internal controls, a company should carry on a regular review of these controls, including the identification of any faults and/or fragilities detected, either when evaluated on an isolated basis or in an aggregated manner.

3. Each company should have in place an appropriate and effective internal control environment to ensure that the company is managed and controlled in a sound and prudent manner. The factors which together comprise the internal control environment are:

(a) a board of directors that is actively concerned with sound corporate governance and that understands and diligently discharges its responsibilities by ensuring that the company is appropriately and effectively managed and controlled;

(b) a management that actively manages and operates the company in a sound and prudent manner;

(c) organisational and procedural controls supported by an effective management information system to soundly and prudently manage the company's exposure to risk; and

(d) an independent audit mechanism to monitor the effectiveness of the internal controls.

4. The board of directors is ultimately responsible to approve and review the overall business strategies and important policies of the company. The board has also to establish and maintain effective internal controls, be aware of the major risks facing the company and provide guidance and oversight to senior management. The board members shall be objective, capable and inquisitive with a good knowledge of the company's activities and related risks. The Authority expects that the board of directors comprises one or more non-executive directors (including independent non-executives) with appropriate experience to help in providing the necessary skill and balance on the board.

5. The activities of the board of directors in relation to internal controls should include:

(i) the establishment of internal controls;

(ii) periodic discussions with senior management regarding the effectiveness of the internal controls;

(iii) regular and timely review of the effectiveness of internal controls made by senior management, internal auditors, external auditors and other control personnel;

(iv) assurance that all concerns raised, including those by external auditors and supervisory authorities on internal control weaknesses, are followed up by senior management;

(v) the establishment and oversight of a risk management system that includes setting and monitoring internal controls so that all major risks are identified, measured, monitored and controlled on an ongoing basis;

(vi) periodic review of risk management systems, strategies and policies; and

(vii) oversight of implementation of the strengthening of any weaknesses found above.

6. Senior management is responsible to:

(i) effectively implement internal controls. This responsibility is normally delegated, by establishing more specific internal controls, to particular business units. Notwithstanding such delegation, senior management remains responsible to oversee that the managers with the delegated responsibility also develop and enforce appropriate internal controls;

(ii) ensure compliance with the established internal controls. This depends on a well defined organisational structure, which clearly shows the lines of reporting responsibility and authority and provides for effective communication throughout the company; and

(iii) ascertain that qualified and competent staff carry out the company's activities, and that staff training and skills are regularly updated. Effective policies in identifying and recognising employees with the appropriate attitude towards efficient controls may enhance internal controls. Such policies may also deter those employees who ignore or override existing internal controls.

7. The following are some of the areas which a company is expected to consider when establishing and maintaining internal controls.

A. <u>Compliance</u>

A company should take reasonable care to establish and maintain effective internal controls for compliance with applicable requirements, conditions of authorisation and obligations in terms of the Act, the Insurance Intermediaries Act, 2006 and any regulations and insurance rules issued thereunder, and other laws of Malta, in so far as they apply.

Depending on the nature, scale and complexity of its business, it may be appropriate for a company to have a separate compliance function. The organisation and responsibilities of a compliance function should be documented. A compliance function shall be

staffed by an appropriate number of competent staff who are sufficiently independent to perform their duties objectively. It shall be adequately resourced and shall have unrestricted access to the company's relevant records.

B. Risk identification, evaluation and management

Each company should take steps to ensure that it has in place and applies internal controls in order to prudently manage and control the significant risks to which the company is exposed and the significant business activities in which the company is engaged, commensurate with the nature, scale and complexity of its business. Risks which the company may face, may not be limited only to underwriting or reinsurance risks but may also extend to other forms of risk such as credit, concentration, market, liquidity and operational.

This requires a company to have in place effective and appropriate internal controls for:

(a) identifying, assessing and evaluating, on an on-going basis, the significant risks to which the company is exposed across all hierarchy levels, operational processes and functional areas and their probability and potential impact on the company. Risk assessment should include a quantitative assessment (e.g. stress tests etc) for a range of adverse scenarios and qualitative analysis;

(b) prudently managing and controlling these risks including the development and implementation of appropriate internal controls relating to risk mitigation and risk transfer arrangements and the establishment of contingency plans;

(c) deciding on risk tolerances limits and resilience strategies (that is, strategies to help manage the impact of risk on the company) and regularly reviewing these limits and strategies;

(d) ensuring that circumstances for which these controls and limits were originally designed, continue to apply and that they continue to be appropriate and effective;

(e) planning, authorising and commencing new types of business activities, evaluating the risks involved, and setting of sound and prudent exposure limits and risk management policies; and

(f) ensuring that the overall risk profile of the company is sound and prudent.

C. Management Information Systems

Companies require quality information at all levels within the company to assist in making informed business decisions, to facilitate the effective management and control of the company's operations and to facilitate external reporting.

Management information systems are those arrangements by which information about a company's business, the state of its affairs and the risks to which it is exposed is produced and supplied to individuals or groups of individuals within the company in a form that enables them to monitor, review and act on the information in carrying out their responsibilities, as well as to external users of information such as policyholders, shareholders and regulators.

In this context, reports and information generated from an effective management information system may also assist a company to monitor compliance with certain internal controls, thereby providing some reasonable assurance that its controls are being complied with and are functioning appropriately.

Each company needs to develop, maintain and utilise an effective comprehensive management information system in order that sufficient, timely and relevant information may be produced to enable the business of the company to be prudently managed and controlled.

Management information systems need to be reviewed regularly to assess the current relevance of information generated and the adequacy and quality of the system's performance over time.

D. Human Resource Management/Training

Human resource policies and procedures assist companies to ensure that their human resource requirements are identified and that they

have the personnel required to prudently and effectively achieve their objectives.

The elements of a human resource program need to include:

(a) the development and implementation of long-range human resource plans to ensure that the company has enough experienced and skilled personnel to carry out its business activities in a prudent manner;

(b) the development and regular review of remuneration programs to ensure, among other things, that the company is managing prudently the risk associated with its variable remuneration policies; and

(c) regular personnel evaluation and review.

E. Internal audit

The company should have an on-going internal audit function, which shall be objective and independent from the operational functions, of a nature and scope appropriate to the business. This includes an examination of the compliance of the activities of the company with all its internal strategies, processes and reporting procedures and shall also include an evaluation of whether the internal control systems of the company remain sufficient and appropriate for its business. An internal audit should:

(a) have unfettered access to all the company's business lines and support departments;

(b) assess outsourced functions;

(c) have appropriate independence, including reporting lines to the board of directors;

(d) have status within the company to ensure that senior management reacts to and acts upon its recommendations;

(e) have sufficient resources and staff that are suitably trained and have relevant experience to understand and evaluate the business they are auditing;

(f) employ a methodology that identifies the key risks run by the company and allocates its resources accordingly.

The Authority should have access to reports of the internal audit function.

F. Audit committee

Depending on the nature, scale and complexity of its business, it may be appropriate for a company to form an audit committee.

An audit committee is normally constituted as a sub-committee of the board of directors, to whom it is answerable and report regularly. The company is expected to have clear written terms of reference specifying membership, authority and duties of the audit committee.

The audit committee is normally made up of a minimum of three members. The membership should be mainly confined to non-executive directors of the company. At least, one member of the audit committee shall be independent and shall have competence in accounting and/or auditing. The independence requirements and the financial expertise requirement may be fulfilled by one and the same person.

Where the functions assigned to the audit committee are performed by the board of directors of the company and the chairman of the company is an executive member, such person shall not be the chairman of the audit committee.

An audit committee could typically examine senior management's process for ensuring the appropriateness and effectiveness of internal controls, examine the arrangements made by senior management to ensure compliance with requirements and standards under the relevant legislation, oversee the functioning of the internal audit function (if applicable) and provide an interface between senior management and the external auditors. The audit committee shall, *inter alia:*

(a) monitor the financial reporting process;

(b) monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems;

(c) monitor the statutory audit of the annual and consolidated accounts;

(d) review and monitor the independence of the approved auditor, and in particular the provisions of additional services to the company by the said auditor;

(e) make a recommendation to the Board of directors for the appointment of the approved auditor.

The audit committee should have explicit authority and the necessary resources and full access to information to enable it to investigate any matters within its terms of reference.

G. Business strategy

A company should plan its business appropriately so that it is able to identify, measure, manage and control risks of regulatory concern. Business plans or strategy plans should be regularly documented and updated to take account of changes in the business environment.

H. Business continuity and contingency planning

A company should have in place appropriate arrangements, having regard to the nature, scale and complexity of its business to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. These arrangements should be included in a contingency plan which would normally consider minor or temporary disruptions as well as major disasters or long term loss of key installations or existing facilities. It is important that contingency plans are regularly updated, tested, tests documented and reinforcements made as necessary.

I. Accounting and record-keeping controls

A company should have appropriate internal controls in place to fulfil its regulatory and statutory obligations with respect to adequacy, excess, periods of retention and security of records. The general principle is that records should be retained for as long as is relevant for the purposes for which they are made, which period shall not be less than that provided for in applicable legislation.

Each company needs to establish and maintain appropriate internal controls over the accounting and other record-keeping process, including sufficient accounting procedures, reconciliation of accounts and control lists, with respect to both on and off balance sheet assets and liabilities to reasonably ensure the completeness of accounting information, the accuracy of all amounts reported, timeliness in the reporting of transactions/business activity, the validity of transactions and the proper maintenance of records. Internal controls should also address checks and balances; e.g. cross-checking, dual control of assets, double signatures.

The accounting records should:

(a) disclose with reasonable accuracy, at all times, the financial position of the company; and

(b) enable the financial statements required by the Authority to be prepared within the time limits specified in the conditions of authorisation.

In particular, the financial records should contain:

(a) entries from day to day of all sums of money received and expended and the matters to which they relate;

(b) a record of all income and expenses, explaining their nature; and

(c) a record of all assets and liabilities, including any guarantees, contingent liabilities or other financial commitments.

J. Segregation of duties

Depending on the nature, scale and complexity of its business, a company must have in place effective internal controls respecting the segregation of duties in order to ensure that there exists a clear and distinct separation of incompatible duties.

The segregation of duties, both between individuals and between departments, reduces the risk of intentional or unintentional manipulation or error by increasing the element of independent verification. The underlying principle is that no one person should be

in a position to control sufficient stages of processing a transaction that errors, misappropriations or misuse could occur without a reasonable chance of detection. Ideally, the flow of activity should be designed so that the work of one person is either independent of, or serves as a check on, the work of other persons.

K. Safeguarding controls

Appropriate and effective safeguards ensure that procedures exist for the safekeeping and protection of the company's assets and those of its customers or other parties held in physical custody or on a book-based system of the company. Safeguards should also ensure that effective procedures exist for limiting access to the company's accounting and other records of assets and liabilities and client information to authorised personnel.

Each company needs to identify areas of its operations which are susceptible to errors, illegal acts or fraudulent activities and ensure that sufficient and effective preventive and detective control mechanisms are in place to safeguard the assets of the company and its clients.

L. Consumer protection and Complaints

A company should act with due skill, care and diligence in its dealing with consumers. Internal controls should be in place as to how to treat consumers fairly and to have systems for recording and handling a complaint, whether oral or written, and provide training to ensure compliance with those controls by its employees.

M. Outsourced functions

The company should set controls and monitor on an ongoing basis all outsourced functions as if these functions were performed internally and subject to the normal standards of internal controls.

N. Actuarial reports

Where the appointment of an actuary is called for by applicable legislation or by the nature of the company’s operations, the Authority requires that actuarial reports be made to the board. The board and senior management review the recommendations of the actuary and the senior management will implement the adequate

measures in the circumstances. To this effect, internal controls should be set up to ensure compliance with measures implemented.