Office of the Superintendent
of Financial Institutions Canada

Bureau du surintendant
des institutions financières Canada

255 Albert Street
Ottawa, Canada
K1A 0H2

255, rue Albert
Ottawa, Canada
K1A 0H2

Guideline

Subject: **Standards of Sound Business and Financial Practices -- Internal Control**

No: **F-11** **Date:** **February 1998**

A. PURPOSE

Companies are subject to continual changes in their business environment that may have an impact on the risk profile of the company. These changes may arise from both external and internal sources, including economic, industry, regulatory, and operational changes.

Each company needs to take steps to ensure that it has in place and applies sound and prudent policies and appropriate procedures and 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. A number of such significant risks and business activities are set out in the standards of sound business and financial practices.

The Canadian Institute of Chartered Accountants issued "Guidance on Control" in November 1995. In the United States, "Internal Control - Integrated Framework" was issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in September 1992. Both of these documents provide guidance on establishing internal control frameworks.

Companies are encouraged to adopt an internal control framework suitable to its business. This guideline sets out the minimum internal controls that each company needs to have in place and apply, and the control environment within which these controls need to be applied, designed to provide reasonable assurance that the company operates in a sound and prudent manner.

The establishment and maintenance of effective internal controls within a strong and effective internal control environment are fundamental components in the safe and sound management of companies. In this context, the standards of sound business and financial practices set out a company's responsibilities in terms of managing and controlling specific business and financial practices and risks.

An important aspect of a company's responsibility is to provide policyholders, shareholders, creditors, and regulators with reasonable assurance that the company's business is appropriately controlled and that its risks are prudently and soundly managed.

Canada

In this regard, internal control, no matter how well designed and operated, can provide only reasonable assurance regarding achievement of a company's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that human judgement in decision-making can be faulty, that persons responsible for establishing internal controls need to consider their relative costs and benefits, and that breakdowns can occur because of human failures such as simple error or mistake. Moreover, controls can be circumvented by collusion of two or more people. Finally, management has the ability to override the internal control system.

B. DEFINITIONS

Internal control is the process, effected by a company's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the effectiveness and efficiency of operations, the reliability of financial reporting and compliance with applicable laws, regulations, and internal policies.

Internal controls are the policies and procedures established and implemented alone, or in concert with other policies or procedures, to manage and control a particular risk or business activity, or combination of risks or business activities, to which the company is exposed or in which it is engaged.

The internal control environment is 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 to soundly and prudently manage these risks, and that reliable and comprehensive systems are in place to appropriately monitor the effectiveness of these controls.

C. INTERNAL CONTROL ENVIRONMENT

Each company needs to 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 control environment are:

- 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;

- a management that actively manages and operates the company in a sound and prudent manner;

- organizational and procedural controls supported by an effective management information system to soundly and prudently manage the company's exposure to risk; and

- an independent audit mechanism to monitor the effectiveness of the organizational and procedural controls.

BOARD OF DIRECTORS

A board of directors is one of a number of components which must have a strong interest in the effective corporate governance of a company. The responsibilities of boards of directors are governed by a framework of federal and provincial legislation, regulations and rules, and the common law. Standards of sound business and financial practices are not intended to modify the legal requirements and framework within which boards of directors are required to carry out their responsibilities. Rather, they are intended to provide guidance to directors in meeting the expectations of the relevant regulator in directing the business and affairs of companies.

A board of directors has an important role in providing direction, guidance and oversight to companies and in ensuring that the affairs of the company are carried out in the best interests of the company. In fulfilling this role, a director's responsibilities fall into two categories: a duty of loyalty and a duty of care.

The fiduciary duty of loyalty is manifested in statutory and common law, and commits directors to act in the best interests of the company. It includes principles such as observing the utmost good faith toward the company, acting honestly in exercising powers, ensuring strict accountability for conflicts of interest, and adhering to a strict practice of preserving the confidentiality of matters involving the company.

Directors also assume a duty to act carefully in fulfilling the important task of directing and monitoring the activities of management. The duty of care requires directors to follow the "reasonably prudent person" rule, which requires them to act with the degree of diligence, care and skill that a reasonably prudent person would exercise in comparable circumstances.

Effective corporate governance requires a high level of cooperation between a company's board of directors and its management. Management supervision is one of the board's most direct responsibilities. A board of directors should ensure that the company's day-to-day operations are in the hands of qualified, honest and competent management. This necessitates that each director exercise independent judgement in evaluating management's actions and competence. Carrying out this responsibility generally requires periodic goal setting, review, and evaluation of management performance.

A board of directors usually discharges this management supervision responsibility by:

- defining the duties and responsibilities of the chief executive officer (CEO);
- selecting or approving an individual with appropriate ability, integrity and experience to fill the CEO position;
- reviewing proposed senior management appointments;
- ensuring the selection, appointment and retention of qualified and competent management;
- reviewing the company's personnel and human resource policies, including reviewing and approving changes to the compensation plan for all employees and management;
- reviewing the company's management succession plan; and
- reviewing management of the sufficiency and qualifications of the company's human resources.

It is recognized that boards of directors of subsidiaries of companies will not typically perform all of the above duties where the duties are being performed on their behalf by the parent company's board of directors.

Although a board of directors is ultimately accountable for its responsibilities, a board of directors may wish to fulfil some board functions through authority delegated to board committees. In some situations, functions of a board of directors are mandated to be fulfilled by establishing board committees. Examples include the formation of an audit committee and a conduct review committee. In other situations, a board of directors may wish to establish committees to assist and advise the board in fulfilling its responsibilities.

Where a board of directors is fulfilling some board functions through authority delegated to board committees, a board needs to ensure that:

- committees, including their terms of reference, are established by a formal resolution of the board or through the company's corporate by-laws;
- board members are appropriately represented on the committees;
- committee members are appointed by the board; and
- board members are regularly informed of each committee's activities, findings, conclusions and recommendations.

MANAGEMENT

The operations and the handling of the day-to-day business and affairs of each company are functions of management. In this regard, the competence, skills, integrity and prudence of management are probably the most important factors in the safety and soundness of a company.

A key management responsibility is the breadth, scope and effectiveness of the company's organizational and procedural controls, without which the stability and soundness of the company would be at risk.

The CEO is ultimately accountable for the company's organizational and procedural controls. A CEO usually fulfils this responsibility by:

- ensuring the integrity of internal controls by providing the appropriate leadership and direction that will set an operational tone of respect for the priority and integrity of the internal control of the company and that will influence the control consciousness of individuals within the organization who develop, administer and monitor the controls;

- ensuring that the company has in place an effective management team that:

    - bears specific responsibility for the development and implementation of particular organizational and procedural controls;

    - is aware of its responsibilities;

    - discharges these responsibilities in a diligent manner; and

    - is accountable to the CEO regarding the performance of these responsibilities; and

- having a process whereby members of the management team periodically review and confirm their responsibilities and performance with respect to risk management.

ORGANIZATIONAL AND PROCEDURAL CONTROLS

A properly-functioning system of organizational and procedural controls is essential in assisting a company to effectively manage and control its operations and to carry on business in an orderly manner.

The scope and particulars of a system of effective organizational and procedural controls that are required by companies to conduct their business in a sound and prudent manner will differ among companies depending on factors such as: the nature and diversity of business; the volume, size and complexity of transactions; the degree of risk associated with each area of operation; the degree of centralization and delegation of authority; and the extent and effectiveness of information technology.

A comprehensive set of organizational controls to address significant risks requires:

- developing and implementing a formal code of conduct for the company;

- developing, at least annually, and implementing a comprehensive business plan for the company;

- establishing, within the management structure, either a reporting requirement or another method of ensuring that the significant risks to which the company is exposed and the business activities in which the company is engaged are identified and evaluated, and that sound, prudent, and effective business and risk management policies and procedures are developed and implemented to manage and control these risks and business activities with the objective of maintaining a sound and prudent institutional risk profile; and

- developing and implementing appropriate and effective human resource policies and procedures.

A comprehensive set of procedural controls requires:

- developing and maintaining comprehensive documentation that clearly sets out the company's organizational and procedural controls;

- clearly defining prudent and appropriate levels of delegation of authorities;

- ensuring a prudent segregation of functional responsibilities within the company;

- establishing and maintaining an effective management information system, including appropriate accounting and record-keeping controls;

- developing and implementing appropriate and effective asset and liability management safeguards and controls (both on- and off-balance sheet);

- developing and implementing sound and conservative valuation policies and procedures; and

- developing and implementing prudent and appropriate information technology controls.

Code of Conduct

Although all business organizations depend on public confidence, this is especially true for life and health insurers. Each company is in a position of special trust and so must conduct itself according to the highest standards of ethical behaviour. Therefore, a strong ethical corporate climate at all levels is vital to the well-being of each company.

The conduct of any corporation is reflected in the actions of the individuals who act on its behalf -- such as its board of directors, management, employees, and sales representatives. The integrity of a company depends on the personal integrity of each and every representative of the company. In this context, ethical behaviour must be incorporated into every decision a company makes. A code of conduct outlines the company's approach to help representatives make these decisions consistently and alert them to potential problem areas. It should serve as a tool in promoting the practice of ethical decision making on a daily basis. In this way, a code of conduct creates conditions that are conducive to ethical behaviour and so is an important element of a company's internal control system, a system which is designed to detect and report actions that are not ethical.

A comprehensive code of conduct requires:

- establishing prudent and appropriate rules governing the proper business conduct and ethical behaviour of the company and its board of directors, management and employees with respect to:
    - complying with applicable legislation, regulations and rules in jurisdictions where the company operates;
    - respecting the privacy of client and institutional information;
    - transactions with related parties of the company and other situations involving potential conflicts of interest; and
    - trading in securities generally and particularly in securities of the company and its affiliates; and
- implementing an effective mechanism to ensure that directors, management and employees understand and adhere to the code of conduct.

To ensure that the company's code of conduct is appropriate and that the directors, management and employees understand and adhere to it, each company needs to ensure that:

- the code is reviewed periodically and ratified by the company's board of directors; and
- employees and management are required to sign an acknowledgement indicating their awareness of, and compliance with, the code.

Companies should consider the need for adopting specialized codes of conduct for individuals who may have special duties and responsibilities imposed on them as a result of the nature of their work, such as those involved in the investment, treasury, or distribution functions.

Business Plan

A business plan is an important management and control tool in or through which a company will:

- identify opportunities in the marketplace, anticipate and initiate changes in strategic direction, forecast results and highlight financial and other resources that may be needed to achieve its plan;
- communicate the company's business objectives throughout the company; and
- establish benchmarks against which the company's performance can be monitored.

A comprehensive business plan requires:

- outlining the company's current financial and strategic positioning in the marketplace;
- identifying the company's business objectives, including the core businesses or target markets;
- developing short- and long-term strategies for achieving these objectives, including identifying potential risks to which the company is exposed and assessing the key resources required to enable the company to achieve these objectives; and
- establishing financial and other indicators against which the company's performance may be measured and assessed.

In order to develop a business plan effectively, there must be a formal process that:

- clearly allocates planning-related tasks and appropriate successive levels of plan approval within the company; and

- ensures that the conclusions, recommendations, projections and assumptions set out in the plan are supported by adequate and appropriate information, scrutiny and analysis.

Risk Identification, Evaluation and Management

Each company needs to take steps to ensure that it has in place and applies sound and prudent policies and appropriate procedures and 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.

This necessitates having in place an effective and appropriate reporting requirement or other method for:

- identifying and evaluating, on an on-going basis, the significant risks to which the company is exposed and their potential impact on the company;

- ensuring that appropriate and effective organizational and procedural controls are developed and implemented to prudently manage and control these risks;

- regularly reviewing the company's organizational and procedural controls implemented to manage and control risks to ensure that circumstances for which these controls originally were designed continue to apply and that they continue to be appropriate and effective;

- ensuring that effective and appropriate procedures are in place for planning, authorizing and commencing new types of business activities, evaluating the risks involved, and establishing the necessary organizational and procedural controls-including the setting of sound and prudent exposure limits and risk management policies; and

- ensuring that the overall risk profile of the company is sound and prudent.

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:

- 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;

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

- regular personnel evaluation and review.

Documentation of Controls

Documenting the company's organizational and procedural controls required to manage significant risks:

- provides the necessary guidance to individuals responsible for the company's policies, procedures and controls; and

- assists in ensuring that the controls used are adequate.

Documentation should be in written or electronic media form and describe each key organizational and procedural control.

Approval Authorities

Clearly defined responsibilities and levels of authority help to ensure that decisions are made by duly authorized persons who are in a position to assess their overall implications, that individuals report to an appropriate level of authority and that delegated authority is adequate and appropriate. Authority may be absolute or incremental, or a combination thereof, and may also be individual, pooled or shared within a committee.

The delegation of authority needs to be clearly documented and must specify:

- the absolute and/or incremental general or specific authority being delegated;
- the units, individuals, positions or committees to whom authority is being delegated;
- the authority of recipients to further delegate authority; and
- any restrictions placed on the use of the delegated authority.

The extent to which authority is delegated will vary among companies according to a number of factors including:

- the types of risks being assessed; and
- the experience of the company's officers.

Segregation of Duties

Effective controls respecting the segregation of duties 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 or defalcations 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.

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 utilize 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.

An effective comprehensive management information system needs to ensure that relevant, accurate and timely information is reported to appropriate persons within the company to enable the company to:

- identify, quantify, assess and monitor its business activities, exposure to risk, financial position and performance and take effective decisions related thereto; and

- monitor the effectiveness of, and compliance with, its organizational and procedural controls and report any exceptions related thereto.

The frequency with which information is prepared, its level of detail and the amount of narrative analysis and explanation will depend upon the level of authority to which it is addressed. Some types of information will be needed on a more frequent basis than others. Management information reports need to be prepared frequently enough to provide timely and relevant information about the business area or risk reported on.

The nature and importance of the procedure will determine the appropriate level of management required to undertake it. Internal control deficiencies need to be reported to those individuals, or groups of individuals, with appropriate authority to rectify the situation. Serious deficiencies in policies, procedures or controls should be brought to the attention of senior management, the audit function and the board of directors.

It may be appropriate for some information to be presented as activity reports showing actual business activity or risk positions against established norms, plans or position limits or as exception reports that highlight exceptions from agreed limits.

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.

Accounting and Record-Keeping Controls

Each company needs to establish and maintain sufficient appropriate controls over the accounting and other record-keeping process 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.

Companies need to maintain and follow accounting policies and practices that are conservative and appropriate in the circumstances.

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 or authorized depository; and
- effective procedures exist for limiting access to the company's accounting and other records of assets and liabilities and client information to authorized personnel.

No internal control structure can completely prevent errors, illegal acts or fraudulent activities. Nevertheless, each company needs to identify areas of its operations which are susceptible to these risks and ensure that sufficient and effective preventive and detective control mechanisms are in place to safeguard the assets of the company and its clients.

The nature and extent of controls necessary depends on:

- the value of the asset or assets in question;
- their qualities of portability and negotiability;

- how easily loss or misappropriation can be concealed; and

- the repercussions of loss or misappropriation on the company's financial position, operations and reputation.

Valuation Policies and Procedures

Valuation policies and procedures assist in ensuring that appropriate provisions are made for the depreciation or decline in value of a company's assets or liabilities (both on- and off-balance sheet).

Each company needs to develop and implement prudent valuation policies and procedures to:

- regularly monitor, review and quantify the quality and value of its assets and liabilities (both on- and off-balance sheet) based on the risk of loss (including contingent losses) in the conduct of its business that will, or is expected to, be incurred; and

- value these items by making and recording prudent provisions or other appropriate adjustments against these assets and liabilities in order to conform with the company's valuation policies, regulatory requirements and accounting standards.

Information Technology Controls

The dependence of financial institutions on information technologies such as computer systems and telecommunications has rapidly expanded in recent years. These systems often support critical services of a company. The potential loss or extended disruption of these systems presents a significant risk to these companies. Accordingly, the effective management of these risks is an important element of internal control of companies.

Comprehensive information technology controls require developing and implementing appropriate and effective information technology systems and security controls, including adequate backup and recovery procedures.

i) Information Technology Systems Development

Each company needs to ensure that:

- the company's information technology strategy is consistent with its business plan and strategies;

- systems hardware and software satisfy this strategy;

- systems are appropriately tested before they are implemented; and

- operational and procedural controls are developed and implemented to ensure that:

  - changes to systems hardware, software and data are properly authorized, tested, and implemented; and

  - the system is appropriately documented, including a record of systems changes.

ii) Information Technology Security Controls

Comprehensive information technology security controls require the development and implementation of appropriate and effective:

- systems access security; and

- business interruption backup and recovery arrangements.

Systems access security controls need to ensure:

- the integrity of the hardware, software and data;

- that physical access to systems hardware, software and data is restricted to authorized persons; and

- that security devices and logical systems access sufficiently minimize the risk of unauthorized access to systems programs and data.

At appropriate stages of information technology development, consideration needs to be given to promoting the involvement of an independent audit function to ensure that the proper degree of controls has been included as part of the design process.

Business Interruption Controls

Business interruption controls need to ensure that:

- the company has adequate systems backup and recovery procedures and standby arrangements in case of an interruption, destruction or other loss of systems or office facilities, data files, hardware, software and documentation; and

- these business interruption arrangements are periodically reviewed and tested.

INDEPENDENT AUDIT

Independent audits are a key element in monitoring and assessing the integrity of internal controls and the internal control environment. Each company needs to have in place an independent audit function through which the company may be provided with reasonable assurance that its key organizational and procedural controls are effective and appropriate and are being complied with.

The need to establish and maintain a system of independent audit is distinct from the requirement to establish and maintain internal controls over day-to-day transactions and operations. The independent audit function does not have primary responsibility for establishing or maintaining internal controls. Rather, independent auditors evaluate the effectiveness of these controls and thus contribute to their ongoing effectiveness. In this way, an independent audit function forms an integral part of each company's internal control environment.

Although independent audits are usually performed within the company using an internal audit department, companies may have this function carried out by outside organizations such as their parent or affiliate, or, through special mandate, an external provider of internal audit services.

Independent audit assessments should be presented to the company's board of directors on a timely basis for review, but at least once a year.

To be effective, the independent audit function must:

- have an appropriate mandate governing its duties and objectives;
- be independent of the functions and internal controls that it inspects;
- have sufficient resources to achieve this mandate; and
- be conducted through a professional audit program.

i) Mandate

A mandate is a written statement of objectives and authority.

The mandate of the audit function should ensure that:

- the function has sufficient authority to carry out its responsibilities objectively and independently and that the function has appropriate access to the highest level of management and to the board of directors;
- audit personnel have access to the company's records, information, and personnel;

- its scope and objectives allow for the expression of opinions about the adequacy and effectiveness of the company's existing and proposed internal controls;

- audit recommendations are adequately considered and acted on, by providing the function with the authority to follow up on findings and recommendations; and

- the company's management and board of directors are informed of the results of evaluations.

To be effective, the mandate needs to be approved by management and the board of directors.

ii) Independence

The objectivity of the independent audit function is vital to its effectiveness. Therefore, auditors need to be independent of the activities, functions and internal controls they audit.

Generally, there is a greater degree of independence when:

- the mandate and authority of the independent audit function is separate from that of day-to-day control over transactions and operations;

- the function reports to a level of management that is senior enough to ensure that it may act independently of the individuals responsible for the activities being inspected;

- the function has a direct access to the CEO and to the board of directors, if necessary; and

- the selection and dismissal of the independent audit head can be made only with the express agreement of the board of directors.

iii) Resources

A competent, qualified, well-trained and independent internal audit department is a key component of an effective internal control environment. Each company needs to ensure that personnel who perform this function possess the qualifications, knowledge, skills, experience and training to fulfil the audit requirements of the company.

iv) Audit Program

Audit programs are usually designed to provide reasonable assurance that control objectives are met. The extent of testing of particular business activities or risk areas is a matter of professional judgement. Although the complete testing of all transactions and other aspects of an activity under review may provide further assurance as to the integrity of its operations, this may not be necessary or practical for sound auditing reasons. Reasonable assurance may be attained by developing a comprehensive audit program based on the assessment of risk and the materiality of that risk, either alone or in combination with other risk factors.

The key elements of a comprehensive audit program include:

- a comprehensive plan governing the audit objectives for the period under review. The plan needs to identify the risk activities, operations and internal control systems to be reviewed, specify the frequency of the audit and identify the necessary resources to carry out the plan;
- comprehensive procedures for achieving the audit plan, including:
    - identifying the risk and/or control objectives for each area to be reviewed;
    - specifying how the risk and/or control mechanism will be assessed, including, where applicable, sample sizes and method of selection; and
    - criteria for assessing the adequacy of specific policies, procedures and controls established to address these risks and/or control objectives;
- documenting the work performed, who performed it, how it was controlled and supervised, and the resulting findings, conclusions and recommendations; and
- a system for reporting and following-up on audit findings, conclusions and recommendations.

- END -