BERMUDA MONETARY AUTHORITY

CORPORATE GOVERNANCE POLICY

BANKS AND DEPOSIT COMPANIES ACT 1999

DECEMBER 2012

Table of Contents

Introduction

This Policy paper (the "Policy") is applicable to deposit taking institutions licensed under the Banks and Deposit Companies Act 1999 (the "Act") and sets out 13 principles and related guidance which reinforce key elements of corporate governance.

0.1. The Organisation for Economic Cooperation and Development ("OECD") describes corporate governance as "a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring. The presence of an effective corporate governance system, within an individual company or group and across an economy as a whole, helps to provide a degree of confidence that is necessary for the proper functioning of a market economy."[1]

0.2. Effective corporate governance practices are essential to achieving and maintaining public confidence in the banking system. Poor corporate governance has been identified as one of the key factors contributing to banking failures during the recent financial crisis. One of the Basel Committee on Banking Supervision's responses to the financial crisis was to seek to raise the standard of international governance practice through revision of its "Principles for enhancing corporate governance."[2] The Bermuda Monetary Authority (the "Authority") has drawn on these Principles in developing the Policy.

0.3. It is a statutory minimum licensing requirement under the Act that a bank implements corporate governance policies and processes.[3] The Authority will take into consideration compliance with the Policy when assessing whether an institution meets this criterion. The Policy consists of principles and underlying guidance. The principles are the core of the Policy and the Authority expects that all banks will comply with the principles. It is important to point out, however, that there is a degree of discretion afforded to institutions in how they choose to comply with the principles. In assessing compliance, the Authority will bear in mind that implementation of the guidance set forth in the Policy will reflect the

[1] OECD, revised April 2004, *Principles of Corporate Governance*, available at www.oecd.org/dataoecd/32/18/31557724.pdf.
[2] Basel Committee on Banking Supervision, October 2010, *Principles for enhancing corporate governance*, available at http://www.bis.org/publ/bcbs176.pdf.
[3] Banks and Deposit Companies Act 1999, Second Schedule Paragraph 2(1).

size, complexity, structure and risk profile of an individual bank or group and that approaches between different institutions may vary.

0.4. It should also be noted that this Policy does not replace or reduce any existing statutory requirements.

A. Board Practices

Board's Overall Responsibilities

Principle 1

The board has overall responsibility for the bank, including approving and overseeing the implementation of the bank's risk appetite,[4] operational strategy, corporate governance and corporate values. The board is also responsible for providing oversight of senior management and establishing and overseeing key functions, including internal audit, compliance and risk management.

Responsibilities of the Board

1. The board has ultimate responsibility for the bank's business, risk strategy and financial soundness, as well as for how the bank organises and governs itself. The board may delegate authority to board committees but subject to board oversight and ratification of key decisions that impact materially the institution's operations.

1.1. Accordingly, the board should:

a) approve and monitor the overall business strategy of the bank, taking into account the bank's long-term financial interests, its exposure to risk, and its ability to manage risk effectively;[5]

b) understand the risks to which the financial institution is exposed and establish a documented risk appetite; and

c) approve and oversee the implementation of the bank's:

i. overall risk strategy, including its risk appetite (ensuring that the bank's capital resources are commensurate with its risk profile);

ii. policies for risk, risk management and compliance;

iii. internal controls system;

iv. corporate governance framework, principles and corporate values, including a code of conduct or comparable document; and

v. compensation system.

[4] "Risk appetite" reflects the level of aggregate risk that the bank's Board is willing to assume and manage in the pursuit of the bank's business objectives. Risk appetite may include both quantitative and qualitative elements, as appropriate, and encompass a range of measures.

[5] Strategic planning is an on-going and dynamic process that takes into account such changes as those in markets, activities, business environment and technology.

1.2. In discharging these responsibilities, the board should take into account the legitimate interests of shareholders, depositors and other relevant stakeholders. It should also ensure that the bank maintains an effective relationship with the Authority.

1.3. The members of the board should exercise their "duty of care"[6] to the bank under The Companies Act 1981. This includes engaging actively in the major matters of the bank and keeping up with material changes in the bank's business and the external environment, as well as acting to protect the interests of the bank.

1.4. The board should ensure that transactions with related parties (including internal group transactions) are reviewed to assess risk and are subject to appropriate terms and conditions, including pricing, and that corporate or business resources of the bank are not misappropriated or misapplied.

Corporate Values and Code of Conduct

1.5. A demonstrated corporate culture that supports and provides appropriate norms and incentives for professional and responsible behaviour is an essential foundation of good governance. In this regard, the board should take the lead in establishing the "tone at the top" and in setting professional standards and corporate values that promote integrity for itself, senior management and other employees.

1.6. A bank's code of conduct, or comparable policy, should articulate acceptable and unacceptable behaviours. It is especially important that such a policy clearly disallows behaviour that could result in the bank engaging in any improper or illegal activity, such as financial misreporting, money laundering, insider trading, fraud, bribery or corruption. It should also discourage the taking of excessive risks as defined by internal corporate policy. The code of conduct should be supported by an aligning risk-based compensation policy that disincents excessive risk-taking or inappropriate focus on short-term gains at the expense of long-term viability.

1.7. The bank's corporate values should recognise the critical importance of timely and frank discussion and elevation of problems to higher levels within the organisation. In this regard, employees should be encouraged and able to communicate, with protection from reprisal, legitimate concerns about illegal, unethical or questionable practices. Because such practices can have a detrimental impact on a bank's reputation, it is highly beneficial for banks to establish a policy setting forth adequate procedures for employees to confidentially communicate material and bona fide concerns or observations of any

[6] The Companies Act 1981, Section 97.

violations. The board should be able to receive information - communicated directly or indirectly (e.g. through an independent audit or compliance process or through an ombudsman) - independent of the internal "chain of command." The board should determine how and by whom legitimate concerns shall be investigated and addressed, for example by an internal control function, an objective external party, senior management and/or the board itself.

1.8. The board should ensure that appropriate steps are taken to communicate throughout the bank the corporate values, professional standards or codes of conduct it sets, together with supporting policies and procedures, such as the means to confidentially report concerns or violations to an appropriate body.

Oversight of Senior Management

1.9. Except where required otherwise by applicable law or regulations, the board should select and, when necessary, replace senior management and have in place an appropriate plan for succession.

1.10. The board should provide oversight of senior management as part of the bank's checks and balances. In doing so the board should:

a) monitor that senior management's actions are consistent with the strategy and policies approved by the board, including the risk appetite;
b) meet regularly with senior management;
c) question and review critically explanations and information provided by senior management;
d) set formal performance standards for senior management consistent with the long-term objectives, strategy and financial soundness of the bank and the bank's code of conduct, and monitor senior management's performance against these standards; and
e) ensure that senior management's knowledge and expertise remain appropriate given the nature of the business and the bank's risk profile.

1.11. The board should also ensure that the bank's organisational structure facilitates effective decision making and good governance supporting appropriate segregation of duties.

1.12. Internal control functions (including internal audit, risk management and compliance) should have direct communication with the board or appropriate board committees. The board should ensure that senior management regularly review policies and controls with internal control functions in order to determine areas needing improvement, as well as to identify and address significant[7] risks and issues. The

[7] Determination of significance will reflect the size, complexity, structure and risk profile of an individual bank or group and may vary between different institutions.

board should ensure that senior management has established internal control functions which are properly positioned, staffed and resourced and are carrying out their responsibilities effectively and independently of operational lines of business.

Board Qualifications

Principle 2

Board members should be and remain qualified, including through training, for their positions. They should have a clear understanding of their role in corporate governance and be able to exercise sound and objective judgment about the affairs of the bank.

2. This principle applies to a board member in his or her capacity as a member of the full board and as a member of any board committee.

Qualifications

2.1. The board should possess, both as individual board members and collectively, appropriate experience, competencies and personal qualities, including professionalism and personal integrity.[8]

2.2. The board collectively should have adequate knowledge and experience relevant to each of the material financial activities the bank intends to pursue in order to enable effective governance and oversight. The board collectively should also have a reasonable understanding of local and, if appropriate, global economic and market forces and of the legal and regulatory environment.

Training

2.3. In order to help board members acquire, maintain and deepen their knowledge and skills and to fulfill their responsibilities, the board should ensure that board members have access to programmes of tailored initial (e.g. induction) and ongoing education on relevant issues. The board should dedicate sufficient time, budget and other resources for this purpose.

Composition

2.4. The bank should have an adequate number and appropriate composition of board members. The board should identify and nominate candidates and ensure appropriate succession planning. A broad

[8] The Second Schedule of the Act makes the fitness and propriety of a bank's directors a minimum criterion for licensing. The Authority's interpretation of this provision of the Act is given in Section 2.2 of the Statement of Principles.

perspective and the ability to exercise objective judgment independent[9] of both the views of executives and of inappropriate political or personal interests can be enhanced by recruiting members from a sufficiently broad population of candidates, to the extent possible and practicable given the bank's size, complexity and geographic scope. To enhance independence, the board should comprise a majority of qualified non-executive members who are capable of exercising sound objective judgment.

2.5. In identifying potential board members, the board should ensure that the candidates are qualified to serve as board members and are able to commit the necessary time and effort to fulfill their responsibilities. Serving as a board member or senior manager of a company that competes or does a significant volume of business with the bank can compromise board independent judgment and potentially create conflicts of interest, as can cross-membership of boards.

Principle 3

The board should define appropriate governance practices for its own work and have in place the means to ensure that such practices are followed and periodically reviewed for on-going improvement.

3. The board should exemplify through its own practices sound governance principles. These practices help the board carry out its duties more effectively. At the same time, they send important signals internally and externally about the kind of enterprise the bank aims to be.

Organisation and Functioning of the Board

3.1. The board should maintain, and periodically update, organisational rules, bylaws, or other similar documents setting out its organisation, rights, responsibilities and key activities.

3.2. The board should structure itself in a way, including in terms of size, frequency of meetings and the use of committees, so as to promote efficiency, sufficiently deep review of matters, and robust, critical challenge and discussion of issues.

3.3. To support board performance, it is a good practice for the board to carry out regular assessments of both the board as a whole and of individual board members as well as its governance practices, and take any corrective actions or make any improvements deemed necessary or appropriate.

[9] The key characteristic of independence is the ability to exercise objective, independent judgment after fair consideration of all relevant information and views without undue influence from executives or from inappropriate external parties or interests.

Role of the Chairperson

3.4. The chairperson of the board plays a crucial role in the proper functioning of the board. He or she provides leadership to the board and is responsible for the board's effective overall functioning, including maintaining a relationship of trust with board members. The chairperson should possess the requisite experience, competencies and personal qualities in order to fulfill these responsibilities.

3.5. The chairperson should ensure that board decisions are taken on a sound and well-informed basis. He or she should encourage and promote critical discussion and ensure that dissenting views can be expressed and discussed within the decision-making process.

3.6. To achieve appropriate checks and balances, an increasing number of banks require the chairperson of the board to be a non-executive. Where a bank does not have this separation and particularly where the roles of the chairperson of the board and chief executive officer ("CEO") are vested in the same person, it is important for the bank to have measures in place to minimise the impact on the bank's checks and balances of such a situation (such as, for example, by having a lead board member, senior independent board member or a similar position).

Board Committees

3.7. To increase efficiency and allow deeper focus in specific areas, boards in many jurisdictions establish certain specialised board committees. The number and nature of committees depends on many factors, including the size of the bank and its board, the nature of the business areas of the bank, and its risk profile.

3.8. Each committee should have a charter or other instrument that sets out its mandate, scope and working procedures. In the interest of greater transparency and accountability, a board should publicly disclose the committees it has established, their mandates, and their composition (including members who are considered to be independent). To avoid undue concentration of power and to promote fresh perspectives, it may be useful to consider occasional rotation of membership and chairmanship of such committees provided that doing so does not impair the collective skills, experience, and effectiveness of these committees.

3.9. Committees should maintain appropriate records (e.g. meeting minutes or summary of matters reviewed and decisions taken) of their deliberations and decisions. Such records should document the committees' fulfilment of their responsibilities and help with the assessment of committee effectiveness by the Authority or those responsible for the internal control functions.

Audit Committee

3.10. A bank should establish an audit committee or equivalent. The audit committee typically is responsible for the financial reporting process; providing oversight of the bank's internal and external auditors; approving, or recommending to the board or shareholders for their approval, the appointment, compensation and dismissal of external auditors; reviewing and approving the audit scope and frequency; receiving key audit reports;[10] and ensuring that senior management is taking necessary corrective actions in a timely manner to address control weaknesses, non-compliance with policies, laws and regulations and other problems identified by auditors. In addition, the audit committee should oversee the establishment of accounting policies and practices by the bank.

3.11. The audit committee should consist of a sufficient number of independent non-executive board members (unless there are sound reasons to the contrary, all institutions should appoint at least two non-executive directors to undertake some audit committee functions and, in the case of a publicly- listed company, the Authority would expect a minimum of three). At a minimum, the audit committee as a whole should have recent and relevant experience and should possess a collective balance of skills and expert knowledge - commensurate with the complexity of the banking organisation and the duties to be performed - in financial reporting, accounting and auditing.

Conflicts of Interest

3.12. Conflicts of interest may arise as a result of the various activities and roles of the bank (e.g. where the bank extends loans to a firm while its proprietary trading function buys and sells securities issued by that firm), or between the interests of the bank or its customers and those of the bank's board members or senior managers (e.g. where the bank enters into a business relationship with an entity in which one of the bank's board members has a financial interest). Conflicts of interest may also arise when a bank is part of a broader group. For example, where the bank is part of a group, reporting lines and information flows between the bank, its parent company and/or other subsidiaries can lead to the emergence of similar conflicts of interest (e.g. sharing of potential proprietary, confidential or otherwise sensitive information from different entities). The board should ensure that policies to identify potential conflicts of interest are developed and implemented and, if these conflicts cannot be prevented, are appropriately managed (based on the permissibility of relationships or transactions under sound corporate policies.

[10] As well as risk management and compliance reports, unless the bank has separate board committees for these areas.

3.13. The board should have a formal written conflicts of interest policy and an objective compliance process for implementing the policy. The policy should include:

a) a member's duty to avoid to the extent possible activities that could create conflicts of interest or the appearance of conflicts of interest;
b) a review or approval process for members to follow before they engage in certain activities (such as serving on another board) so as to ensure that such activity will not create a conflict of interest;
c) a member's duty to disclose any matter that may result, or has already resulted, in a conflict of interest;
d) a member's responsibility to abstain from voting on any matter where the member may have a conflict of interest or where the member's objectivity or ability to properly fulfill duties to the bank may be otherwise compromised;
e) adequate procedures for transactions with related parties to be made on an arm's length basis; and
f) the way in which the board will deal with any non-compliance with the policy.

3.14. It is a leading practice to include in any conflicts of interest policy examples of where conflicts can arise when serving as a board member.

3.15. The board should ensure that appropriate information is provided to the Authority, relating to the bank's policies on conflicts of interest and potential conflicts of interest. This should include information on the bank's approach to managing material conflicts of interest that are not consistent with such policies; and conflicts that could arise as a result of the bank's affiliation or transactions with other entities within the group.

Controlling shareholders

3.16. Board members appointed by controlling shareholders have the same duty of care and responsibilities to the bank as do other board members. In cases where there are board members appointed by a controlling shareholder, the board may wish to set out specific procedures or conduct periodic reviews to ensure the appropriate discharge of responsibilities and avoidance of conflicts of interest by all board members.

Group Structures[11]

Principle 4

In a group structure, subject to the Authority's consolidated supervision[12], the board of the parent company has the overall responsibility for adequate corporate governance across the group and ensuring that there are governance policies and mechanisms appropriate to the structure, business and risks of the group and its entities.

Board of parent company

4. In the discharge of its corporate governance responsibilities, the board of the parent company should be aware of the material risks and issues that might affect both the bank as a whole and its subsidiaries. It should therefore exercise adequate oversight over subsidiaries, while respecting the independent legal and governance responsibilities that might apply to regulated subsidiary boards.

4.1. In order to fulfill its corporate governance responsibilities, the board of the parent company should:

a) establish a governance structure, consistent with the Principles, which contributes to the effective oversight of subsidiaries and which takes into account the nature, scale and complexity of the different risks to which the group and its subsidiaries are exposed;

b) assess the governance structure periodically to ensure that it remains appropriate in light of growth, increased complexity, geographic expansion, etc;

c) approve a corporate governance policy at the group level for its subsidiaries, which includes the commitment to meet all applicable governance requirements;

d) ensure that enough resources are available for each subsidiary to meet both group standards and local governance standards;

e) understand the roles and relationships of subsidiaries to one another and to the parent company; and

f) have appropriate means to monitor that each subsidiary complies with all applicable governance requirements.

[11] This section relates to deposit-taking institutions licensed in Bermuda, either as a parent company of a group of companies or a subsidiary of another company.

[12] The identification of group structures for regulatory purposes is explained in the Authority's May 2007 policy paper entitled, *Banks and Deposit Companies Act 1999: The Approach to Consolidated Supervision*.

Board of regulated subsidiary

4.2. In general, the board of a Bermuda-licensed banking subsidiary should adhere to the corporate values and governance principles espoused by its parent company. However, in doing so the board should take into account the nature of the business of the subsidiary and the specific legal requirements that are applicable, and make appropriate adjustments to its corporate governance practices.

4.3. The board of a Bermuda-licensed banking subsidiary should evaluate any group-level decisions or practices to ensure that they do not put the regulated subsidiary in breach of Bermuda laws and regulations or the Policy. The board of the licensed banking subsidiary should also ensure that such decisions or practices are not detrimental to:

a) the sound and prudent management of the subsidiary;
b) the financial health of the subsidiary; or
c) the legal interests of the subsidiary's stakeholders.

4.4. In order to exercise its corporate governance responsibilities independently, the board of the subsidiary should have an adequate number of qualified, independent non-executive board members, who devote sufficient time to the matters of the subsidiary.

B. Senior Management

Principle 5

Under the direction of the board, senior management should ensure that the bank's activities are consistent with the business strategy, risk appetite and policies approved by the board.

5. Senior management consists of a core group of individuals who are responsible and should be held accountable by the Board for overseeing the day-to-day management of the bank[13]. These individuals should have the necessary experience, competencies and integrity to manage the businesses under their supervision as well as have appropriate control over the key individuals in these areas.

5.1. Senior management contributes substantially to a bank's sound corporate governance through personal conduct (e.g. by helping to set the "tone at the top" along with the board) by providing adequate oversight of those they manage, and by ensuring that the bank's activities are consistent with the business strategy, risk appetite and policies approved by the bank's board.

[13] Senior management should include, at a minimum, the chief executive officer and senior executives as defined under Section 7 of the Banks and Deposit Companies Act 1999.

5.2. Senior management is responsible for delegating duties to the staff and should establish a management structure that promotes accountability and transparency. Senior management should remain cognisant of its obligation to oversee the exercise of such delegated responsibility and its ultimate responsibility to the board for the performance of the bank.

5.3. Senior management should implement, consistent with the direction given by the board with respect to strategic direction and risk management, appropriate systems for managing the risks - both financial and non-financial - to which the bank is exposed. This includes a comprehensive and independent risk management function and an effective system of internal controls, as discussed in greater detail in Principles 6 and 7 below.

5.4. The management structure adopted should be appropriate to the size, complexity, structure and risk profile of an individual bank.

C. Risk Management and Internal Controls

Principle 6

Banks should have an effective internal controls system and a risk management function with sufficient authority, stature, independence, resources and access to the board.

Risk management vs. internal controls[14]

6. Risk management generally encompasses the process of:

a) identifying key risks to the bank;
b) assessing these risks and measuring the bank's exposures to them;
c) monitoring the risk exposures and determining the corresponding capital needs (i.e. capital planning) on an ongoing basis;[15]
d) monitoring and assessing decisions to accept particular risks, risk mitigation measures and whether risk decisions are in line with the board-approved risk appetite and risk policy; and
e) reporting to senior management and the board on all the items noted in this paragraph.

[14] While risk management and internal controls are discussed separately in this document, some banks may use "internal controls" as an umbrella term to include risk management, internal audit, compliance, etc. The two terms are in fact closely related and where the boundary lies between risk management and internal controls is less important than achieving, in practice, the objectives of each.

[15] While the design and execution of a bank's capital planning process may primarily be the responsibility of the chief financial officer, the treasury function, or other entities within the bank, the risk management function should be able to explain clearly and monitor on an on-going basis the bank's capital and liquidity position and strategy.

6.1. Internal controls are designed, among other things, to ensure that each key risk has a policy, process or other measure, as well as a control to ensure that such policy, process or other measure is being applied and works as intended. As such, internal controls help ensure process integrity, compliance and effectiveness. Internal controls help provide comfort that financial and management information is reliable, timely and complete and that the bank is in compliance with its various obligations, including applicable laws and regulations. In order to avoid actions beyond the authority of the individual or even fraud, internal controls also place reasonable checks on managerial and employee discretion. Even in very small banks, for example, key management decisions should be made by more than one person ("four eyes principle").[16] Internal control reviews should also determine the extent of an institution's compliance with company policies and procedures, as well as with legal and regulatory policies.[17]

Scope of responsibilities, stature and independence of the risk management function

6.2. The risk management function is responsible for identifying, measuring, monitoring, controlling or mitigating and reporting on risk exposures. This should encompass all risks to the bank, on- and off-balance sheet and at a group-wide, portfolio and business-line level, and should take into account the interdependencies among risks (e.g. lines between market and credit risk and between credit and operational risk are increasingly blurred). This should include a reconciliation of the aggregate level of risk in the bank to the board-established risk appetite.

6.3. The risk management function - both firm-wide and within subsidiaries and business lines - should have sufficient stature within the bank such that issues raised by risk managers receive the necessary attention from the board, senior management and business lines. While the risk management function may report to the CEO or other senior management, it should also report or, at a minimum, have direct access to the board or the appropriate board committee. Business decisions by the bank typically are a product of many considerations. By properly positioning and supporting its risk management function, a bank helps ensure that the views of risk managers will be an important part of those considerations.

6.4. While it is not uncommon for risk managers to work closely with individual business units and, in some cases, to have dual reporting lines, the risk management function should be sufficiently independent of the business units whose activities and exposures it reviews.

[16] Refer to Section 2.3 of the Statement of Principles.
[17] Detailed guidance with respect to the features and objectives of the internal control system is provided in an Annex to this paper.

6.5. While such independence is an essential component of an effective risk management function, it is also important that risk managers are not so isolated from business lines - geographically or otherwise - that they cannot understand the business or access necessary information. Moreover, the risk management function should have access to all business lines that have the potential to generate material risk to the bank. Regardless of any responsibilities that the risk management function may have to business lines and senior management, its ultimate responsibility should be to the board.

Resources

6.6. A bank should ensure through its planning and budgeting processes that the risk management function has adequate resources (in both number and quality) necessary to assess risk, including personnel, access to information technology systems and systems development resources, and support and access to internal information. These processes should also explicitly address and provide sufficient resources for internal audit and compliance functions. Compensation and other incentives (e.g. opportunities for promotion) of risk management staff should be sufficient to attract and retain qualified personnel.

Qualifications

6.7. Risk management personnel should possess sufficient experience and qualifications, including market and product knowledge as well as mastery of risk disciplines.[18] Staff should have the ability and willingness to challenge business lines regarding all aspects of risk arising from the bank's activities.

Principle 7

Risks should be identified and monitored on an on-going firm-wide and individual entity basis, and the sophistication of the bank's risk management and internal control infrastructures should keep pace with any changes to the bank's risk profile (including its growth), and to the external risk landscape.

Risk Methodologies and Activities

7. Risk analysis should include both quantitative and qualitative elements. While risk measurement is a key component of risk management, excessive focus on measuring or modelling risks at the expense of other risk management activities may result both in overreliance on risk estimates that do not

[18] Some firms have found it to be a sound practice to encourage or require staff to serve in both business line and risk management roles, on a rotational basis, as a requirement for career development. Such an approach can have several benefits, including giving risk management stature within the bank commensurate with business lines and other functions, promoting firm-wide dialogue regarding risk, and ensuring that business lines understand the importance of risk management and that risk managers understand how business lines operate.

accurately reflect real exposures and in insufficient action to address and mitigate risks. The risk management function should ensure that the bank's internal risk measurements cover a range of scenarios, are not based on overly optimistic assumptions regarding dependencies and correlations, and include qualitative firm-wide views of risk relative to return and to the bank's external operating environment. Senior management and, as applicable, the board should review and approve scenarios that are used in the bank's risk analysis and should be made aware of assumptions and potential shortcomings embedded in the bank's risk models.

7.1. As banks make use of certain internal and external data to identify and assess risk, make strategic or operational decisions, and determine capital adequacy, the board should give special attention to the quality, completeness and accuracy of the data it relies on to make risk decisions.

7.2. As part of its quantitative and qualitative analysis, the bank should also utilise forward-looking stress tests and scenario analysis to better understand potential risk exposures under a variety of adverse circumstances.[19] These should be key elements of a bank's risk management process, and the results should be communicated to, and given appropriate consideration by, the relevant business lines and individuals within the bank. A forward-looking approach to risk management should include on-going monitoring of existing risks as well as identifying new or emerging risks.

7.3. In addition to these forward-looking tools, banks should also regularly review actual performance after the fact relative to risk estimates (i.e. back-testing) to assist in gauging the accuracy and effectiveness of the risk management process and making necessary adjustments.

7.4. The risk management function should promote the importance of senior management and business line managers in identifying and assessing risks critically, rather than relying excessively on external risk assessments. While external assessments such as external credit ratings or externally-purchased risk models can be useful as an input into a more comprehensive assessment of risk, the ultimate responsibility for assessing risk lies solely with the bank. For example, in the case of a purchased credit or market risk model, the bank should take the steps necessary to validate the model and calibrate it to the bank's individual circumstances to ensure accurate and comprehensive capture and analysis of risk. In any case, banks should avoid over-reliance on any specific risk methodology or model.

[19] See Bermuda Monetary Authority's February 2010 policy paper entitled, *Guidelines on Stress Testing for the Bermuda Banking Sector*.

7.5. In the case of subsidiary banks, a similar approach is necessary. The board and management of a subsidiary remain responsible for effective risk management processes at the subsidiary. While parent companies should conduct strategic, group-wide risk management and prescribe corporate risk policies, subsidiary management and boards should have appropriate input into their local or regional adoption and to assessments of local risks. If group risk management systems and processes are prescribed, subsidiary management, with subsidiary board oversight, is responsible for assessing and ensuring that those systems and processes are appropriate, given the nature of the operations of the subsidiary. Furthermore, adequate stress testing of subsidiary portfolios should occur, based not only on the subsidiaries' economic and operating environments, but also based on the ramifications of potential stress on the parent company (e.g. liquidity, credit, reputational risk, etc.). In some cases, such evaluations may be accomplished through joint head office and subsidiary teams. Local management and those responsible for the internal control functions are accountable for prudent risk management at the local level. Parent companies should ensure that adequate tools and authorities are provided to the subsidiary and that the subsidiary understands what reporting obligations it has to the head office.

7.6. In addition to identifying and measuring risk exposures, the risk management function should evaluate possible ways to manage these exposures. In some cases, the risk management function may direct that risk be reduced or hedged to limit exposure. In other cases, the risk management function may simply report risk positions and monitor these positions to ensure that they remain within the bank's framework of limits and controls. Either approach may be appropriate provided the independence of the risk management function is not compromised.

7.7. The sophistication of the bank's risk management and internal control infrastructures - including, in particular, a sufficiently robust information technology infrastructure - should keep pace with developments such as balance sheet and revenue growth, increasing complexity of the bank's business or operating structure, geographic expansion, mergers and acquisitions, or the introduction of new products or business lines. Strategic business planning, and periodic review of such plans, should take into account the extent to which such developments have occurred and the likelihood that they will continue going forward.

7.8. Banks should have approval processes for new products. These should include an assessment of the risks of new products, significant changes to existing products, the introduction of new lines of business and entry into new markets. The risk management function should provide input on risks as a part of such processes. This should include a full and frank assessment of risks under a variety of scenarios, as well as an assessment of potential shortcomings in the ability of the bank's risk management

and internal controls to effectively manage associated risks. In this regard, the bank's new product approval process should take into account the extent to which the bank's risk management, legal and regulatory compliance, information technology, business line, and internal control functions have adequate tools and the expertise necessary to manage related risks. If adequate risk management processes are not yet in place, a new product offering should be delayed until such time that systems and risk management are able to accommodate the relevant activity. There should also be a process to assess risk and performance relative to initial projections, and to adapt the risk management treatment accordingly, as the business matures.

7.9. Mergers and acquisitions can pose special risk management challenges to the bank. In particular, risks can arise from conducting insufficient due diligence that fails to identify risks that arise post-merger, or activities that conflict with the bank's strategic objectives or risk appetite. The risk management function should therefore be actively involved in assessing risks that could arise from mergers and acquisitions, and should report its findings directly to the board and/or its relevant specialised committee.

7.10. While the risk management function plays a vital role in identifying, measuring, monitoring and reporting on risk exposures, other units in the bank also play an important role in managing risk. In addition to business lines, which should be accountable for managing risks arising from their activities, the bank's treasury and finance functions should promote effective firm-wide risk management not only through supporting financial controls but also, where appropriate, through applying robust internal pricing of risk especially at large banks and internationally active banks. A business unit's internal cost of funds should reflect material risks to the bank arising from its activities. Failure to do so may result in greater investment in high-risk activities than would be the case if internal pricing were risk-adjusted.

7.11. Although the risk management function has a key leadership and coordinating role on risks, the operational responsibility for making operational decisions on risks and managing risk rests with management and ultimately extends to other employees of the bank. The bank's risk management framework should be clear and transparent regarding staff and organisational responsibilities for risk.

Principle 8

Effective risk management requires robust internal communication within the bank about risk, both across the organisation and through reporting to the board and senior management.

8. Sound corporate governance is evidenced, among other things, by a culture where senior management and staff are expected and encouraged to identify risk issues as opposed to relying on the

internal audit or risk management functions to identify them. This expectation is conveyed not only through bank policies and procedures, but also through the "tone at the top" established by the board and senior management.

8.1. The bank's risk exposures and strategy should be communicated throughout the bank with sufficient frequency. Effective communication, both horizontally across the organisation and vertically up the management chain, facilitates effective decision-making that fosters safe and sound banking and helps prevent decisions that may result in amplifying risk exposures.

8.2. Information should be communicated to the board and senior management in a timely, complete, understandable and accurate manner so that they are equipped to make informed decisions. This is particularly important when a bank is facing financial or other difficulties and may need to make prompt, critical decisions. If the board and senior management have incomplete or inaccurate information, their decisions may magnify risks rather than mitigate them. Serious consideration should be given by the board to instituting periodic reviews of the amount and quality of information the board receives or should receive.

8.3. In ensuring that the board and senior management are sufficiently informed, management and those responsible for the internal control functions should strike a balance between communicating information that is accurate and "unfiltered" (i.e. that does not hide potentially bad news) and not communicating so much extraneous information that the sheer volume of information becomes counterproductive.

8.4. Risk reporting to the board requires careful design in order to ensure that firm-wide and individual portfolio and other risks are conveyed in a concise and meaningful manner. Reporting should accurately communicate risk exposures and results of stress tests or scenario analyses, and should provoke a robust discussion of, for example, the bank's current and prospective exposures (particularly under stressed scenarios), risk/return relationships, risk appetite, etc. In addition to internal measurement and assessment of bank risks, reporting should include information about the external environment to identify market conditions and trends that may have a bearing on the bank's current or future risk profile.

8.5. Risk reporting systems should be dynamic, comprehensive and accurate, and should draw on a range of underlying assumptions. Risk monitoring and reporting should occur not only at the disaggregated level (including risk residing in subsidiaries that could be considered significant), but should also be aggregated upward to allow for a firm-wide or consolidated picture of risk exposures. Risk reporting systems should be clear about any deficiencies or limitations in risk estimates, as well as any

significant embedded assumptions (e.g. regarding risk dependencies or correlations). These systems should not only aggregate information to provide a firm-wide, integrated perspective on risk (geographically and by risk type), but should also highlight emerging risks that have the potential to become significant and may merit further analysis.

8.6. In this regard, organisational "silos"[20] can impede effective sharing of information across a bank and can result in decisions being made in isolation from the rest of the bank. Overcoming information-sharing obstacles posed by silo structures may require the board and senior management to review or rethink established practices in order to encourage greater communication. Some firms have found it useful to create risk management committees - distinct from the board's risk committee - that draw members from across the firm (e.g. from business lines and the risk management function) to discuss issues related to firm-wide risks.

Principle 9

The board and senior management should effectively utilise the work conducted by internal audit functions, external auditors and internal control functions.

9. The board should recognise and acknowledge that independent, competent and qualified internal and external auditors, as well as other internal control functions (including the compliance functions), are vital to the corporate governance process in order to achieve a number of important objectives. Senior management should also recognise the importance of the effectiveness of these functions to the long-term soundness of the bank.

9.1. The internal audit function generally should be located within the licensed institution itself, although it may be located elsewhere within a consolidated group, provided the Authority is satisfied as to the management and control of the process. The Authority generally views it as inappropriate for internal audit functions to be outsourced to an external auditor, given the risk of undermining the ultimate effectiveness of the external audit process. However, in the case of a smaller institution, the Authority may be prepared to permit the internal audit function to take the form of appropriate independent reviews by external experts rather than by a dedicated in-house unit.

[20] Organisational silos can be characterised by business lines, legal entities, and/or geographic units being run in isolation from each other, with limited information shared and, in some cases, competition across silos.

9.2. The board and senior management can enhance the ability of the internal audit function to identify problems with a bank's governance, risk management and internal control systems by:

a) encouraging internal auditors to adhere to national and international professional standards, such as those established by the Institute of Internal Auditors;
b) requiring that audit staff have skills that are commensurate with the business activities and risks of the firm;
c) ensuring that the internal audit function is appropriately structured and resourced;
d) ensuring that the internal audit function has no authority or responsibility for the activities it audits;
e) promoting the independence of the internal auditor, for example by ensuring that internal audit reports are provided to the board and the internal auditor has direct access to the board or the board's audit committee;
f) recognising the importance of the audit and internal control processes and communicating their importance throughout the bank;
g) ensuring that the internal audit function has unrestricted access to all of an institution's activities, records, property and personnel to the extent necessary for the effective completion of its work;
h) requiring the timely and effective correction of identified internal audit issues by senior management; and
i) engaging internal auditors to judge the effectiveness of the risk management function and the compliance function, including the quality of risk reporting to the board and senior management, as well as the effectiveness of other key internal control functions.

9.3. The board and senior management are responsible for the preparation and fair presentation of financial statements in accordance with applicable accounting standards, as well as the establishment of effective internal controls related to financial reporting. The board and senior management can also contribute to the effectiveness of external auditors[21] by, for example, including in engagement letters the expectation that the external auditor will be in compliance with applicable domestic and international codes and standards of professional practice.

9.4. The bank should maintain sound internal control functions, including an effective compliance function that, among other things, routinely monitor compliance with laws, corporate governance rules,

[21] See May 2007, *Banks and Deposit Companies Act 1999: The Bermuda Monetary Authority's Relationship with Auditors and Reporting Accountants of Banks and Deposit Companies.*

regulations, codes and policies to which the bank is subject[22] and ensure that deviations are reported to an appropriate level of management and, in case of material deviations, to the board.

9.5. Senior management should promote strong internal controls and should avoid activities and practices that undermine their effectiveness. Examples of problematic activities or practices include failing to ensure that there is effective segregation of duties where conflicts could arise; not exercising effective control over employees in key business positions (even apparent "star" employees); and failing to question employees who generate revenues or returns out of line with reasonable expectations (e.g. where supposedly low-risk, low-margin trading activity generated unexpectedly high returns) for fear of losing either revenue or the employees.

D. Compensation

Principle 10

Remuneration policies and practices should be consistent with the bank's corporate culture, long-term objectives, strategy and control environment.

10. The board should approve policies that are consistent with effective risk management and avoid creating incentives that encourage inappropriate risk-taking inconsistent with the risk appetite established by the board.

10.1. The compensation of internal control function staff should be structured in a way that is based principally on the achievement of their objectives and does not compromise their independence.

E. Complex or Opaque Corporate Structures

Principle 11

The board and senior management should know and understand the bank's operational structure and the risks that it poses (i.e. "know-your-structure").

11. Some banks create structures for legal, regulatory, fiscal or product-offering purposes in the form of units, branches, subsidiaries or other legal entities that can considerably increase the complexity of the organisation. The sheer number of legal entities, and in particular the interconnections and intra-group

[22] Banks should ensure that appropriate controls are in place to ensure compliance with the requirements of the *Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008*.

transactions among such entities, can lead to challenges in identifying, overseeing and managing the risks of the organisation as a whole, which is a risk in and of itself.

11.1. The board and senior management should understand the structure and the organisation of the group, i.e. the aims of its different units/entities and the formal and informal links and relationships among the entities and with the parent company. This includes understanding the legal and operational risks and constraints of the various types of intra-group exposures and transactions and how they affect the group's funding, capital and risk profile under normal and adverse circumstances. Sound and effective measures and systems should be in place to facilitate the generation and exchange of information among and about the various entities, to manage the risks of the group as a whole, and for the effective supervision of the group. In this regard, senior management should inform the board regarding the group's organisational and operational structure and the key drivers of the group's revenues and risks.

11.2. Another governance challenge arises when banks establish business or product line management structures that do not match the bank's legal entity structure. While this is a quite common practice, it nevertheless introduces additional complexity. Apart from ensuring the appropriateness of these matrix structures, the board or senior management as appropriate should ensure that all products and their risks are captured and evaluated on an individual entity and group-wide basis.

11.3. The board should approve policies and clear strategies for the establishment of new structures and should properly guide and understand the bank's structure, its evolution and its limitations. Moreover, senior management, under the oversight of the board, should:

a) avoid setting up unnecessarily complicated structures;
b) have a centralised process for approving and controlling the creation of new legal entities based on established criteria, including the ability to monitor and fulfil on an on-going basis each entity's requirements (e.g. regulatory, tax, financial reporting, governance);
c) understand and be able to produce information regarding the bank's structure, including the type, charter, ownership structure and businesses conducted for each legal entity;
d) recognise the risks that the complexity of the legal entity structure itself may pose, including lack of management transparency, operational risks introduced by interconnected and complex funding structures, intra-group exposures, trapped collateral and counterparty risk; and
e) evaluate how the aforementioned risks of the structure and legal entity requirements affect the group's ability to manage its risk profile and deploy funding and capital under normal and adverse circumstances.

11.4. In order to enhance the sound governance of a banking group, internal audits of individual entities could be complemented with regular assessments of the risks posed by the group's structure. Periodic reports that assess the bank's overall structure and individual entities' activities, confirm compliance with the strategy previously approved by the board, and disclose any possible discrepancies could be useful for the audit and risk committees, senior management and the board of the parent company.

11.5. Senior management, and the board as necessary, should discuss with the Authority policies and procedures for the creation of new structures that may add complexity to the group.[23]

Principle 12

Where a bank operates through special-purpose or related structures or in jurisdictions that impede transparency or do not meet international banking standards, its board and senior management should understand the purpose, structure and unique risks of these operations. They should also seek to mitigate the risks identified (i.e. "understand-your-structure").

12. The bank may have legitimate purposes for operating in particular jurisdictions (or with entities or counterparties operating in these jurisdictions) or for establishing certain structures (e.g. special purpose vehicles or corporate trusts). However, operating in jurisdictions that are not fully transparent or do not meet international banking standards (e.g. in the areas of prudential supervision, tax, anti-money laundering or anti-terrorism financing),[24] through complex or non-transparent structures or through structures organised in jurisdictions with insufficient legal infrastructure/case law (e.g. such that the enforceability of contracts cannot be ascertained or is questionable) may pose financial, legal, reputational and other risks to the banking organisation; may impede the ability of the board and senior management to conduct appropriate business oversight; and could hinder effective banking supervision. The bank should evaluate proposed activities and transactions such as described above and carefully consider, prior to approval, how it will implement effective board and/or managerial oversight.

12.1. In addition to the risks discussed above, the bank may also be indirectly exposed to risk when it performs certain services or establishes structures on behalf of customers. Examples include acting as a company or partnership formation agent, providing a range of trustee services and developing complex structured finance transactions for customers. While these activities are often profitable and can serve the

[23] Institutions should note both the requirement under the Statement of Principles to inform the Authority of any proposed material change in their business and the statutory requirement to seek approval for the establishment of a subsidiary or branch under the Bermuda Monetary Authority (Financial Institutions) (Control) Regulations 1994.

[24] This could include jurisdictions in which a lack of transparency and weak enforcement mechanisms foster opacity and hinder effective management and supervision.

legitimate business purposes of customers, in some cases customers may use products and activities provided by banks to engage in illegal or inappropriate activities. This can, in turn, pose significant legal and reputational risks to a bank that provides such services, could cause it to deviate from its core business and could preclude adequate control of the risks posed by the client to the group as a whole.

12.2. Senior management, and the board as appropriate, should note these challenges and take appropriate action to avoid or mitigate them by:

a) maintaining and reviewing, on an on-going basis, appropriate policies, procedures and strategies governing the approval and maintenance of those structures or activities;
b) periodically monitoring such structures and activities to ensure that they remain consistent with their established purpose so that they are not held without adequate justification; and
c) establishing adequate procedures to identify and manage all material risks arising from these activities. The bank should only approve these operations if the material financial, legal and reputational risks can be properly identified, assessed and managed.

12.3. In addition, consistent with guidance from the board, senior management should ensure the bank has appropriate policies and procedures to:

a) establish processes for the approval of such activities (e.g. applicable limits, measures to mitigate legal or reputational risks, and information requirements), taking into account the implications for the resulting operational structure of the organisation;
b) define and understand the purpose of such activities, and ensure that the actual exercise of these activities is consistent with their intended purpose;
c) document the process of consideration, authorisation and risk management to make this process transparent to auditors and the Authority;
d) regularly evaluate the continuing need to operate in certain jurisdictions or through complex structures that reduce transparency;
e) ensure that information regarding these activities and associated risks is readily available to the bank's head office, is appropriately reported to the board and the Authority; and
f) ensure that these activities are subject to regular internal and external audit reviews.

12.4. The board of the parent company can enhance the effectiveness of the above efforts by requiring an internal control function (such as internal audit, risk management or compliance) to conduct a formal review of the structures, their controls and activities, as well as their consistency with board-approved strategy and report to the board and senior management on its findings.

12.5. The board should be prepared to discuss with, and as necessary report to, the Authority the policies and strategies adopted regarding the establishment and maintenance of these structures and activities.

F. Disclosure and Transparency

Principle 13

The governance of the bank should be adequately transparent to its shareholders, depositors, other relevant stakeholders and market participants.

13. Transparency is essential for sound and effective corporate governance. It is difficult for shareholders, depositors, other relevant stakeholders and market participants to effectively monitor and properly hold accountable the board and senior management when there is insufficient transparency. The objective of transparency in the area of corporate governance is therefore to provide these parties with key information necessary to enable them to assess the effectiveness of the board and senior management in governing the bank.

13.1. Although transparency may be less detailed for non-listed banks, especially those that are wholly owned, these institutions can nevertheless pose the same types of risk to the financial system as publicly traded banks through various activities, including their participation in payments systems and acceptance of retail deposits.

13.2. The bank should disclose relevant and useful information that supports the key areas of corporate governance addressed in this paper. Such disclosure should be proportionate to the size, complexity, structure, economic significance and risk profile of the bank. There is no intention to impose on banks a single standard disclosure obligation nor require an institutuion to disclose any proprietary information that might put a bank at competititve disadvantage.

13.3. Disclosure should include, but not be limited to, material information on the bank's objectives, organisational and governance structures and policies (in particular the content of any corporate governance code or policy and the process by which it is implemented), major share ownership and voting rights, the financial and operating results of the company, foreseeable risk factors and related parties transactions. The bank should also disclose information about board members, including their qualifications, the selection process, other company directorships and whether they are regarded as independent by the board.

13.4. Disclosure should be accurate, clear and presented in an understandable manner and in such a way that shareholders, depositors, other relevant stakeholders and market participants can consult it easily. Timely public disclosure is desirable on a bank's public website, in its annual and periodic financial reports or by other appropriate forms. It is good practice that an annual corporate governance-specific and comprehensive statement is in a clearly identifiable section of the annual report depending on the applicable financial reporting framework. All material developments that arise between regular reports should be disclosed without undue delay.

Annex – Internal Controls

The Internal Control System

1. The Authority sees it as inappropriate to prepare a single comprehensive list of internal control procedures which would be applicable to any institution. However, internal control systems need to be adequate for the size and complexity of the business and should provide reasonable assurance that:

a) the business is planned and conducted in an orderly and prudent manner in adherence to established policies;

b) transactions and commitments are entered into in accordance with management's general or specific authority;

c) management is able to safeguard the assets and control the liabilities of the business;

d) there are measures to minimise the risk of loss from irregularities, fraud and error, and to identify cases promptly when they occur;

e) the accounting and other records of the business provide complete, accurate and timely information;

f) management is able to monitor on a regular and timely basis, among other things, the adequacy of the institution's capital, liquidity, profitability and the quality of its assets;

g) management is able to identify, regularly assess and, where appropriate, quantify the risk of loss in the conduct of the business so that:

   i. the risks can be monitored and controlled on a regular and timely basis; and

   ii. appropriate provisions can be made for bad and doubtful debts, and for any other exposures both on and off balance sheet;

h) management is able to prepare returns made to the Authority completely and accurately in accordance with the relevant reporting instructions, and to submit them on a timely basis; and

i) the institution fulfills its notification responsibilities under the Banks and Deposit Companies Act (e.g. Section 38 reports of large exposures).

2. In seeking to secure reasonable assurance that their internal control objectives are achieved, management must exercise judgement in determining the scope and nature of the control procedures to be adopted. They should also have proper regard to the cost of establishing and maintaining a control procedure in relation to the benefits, financial or otherwise, that it is expected to provide.

Control Objectives

3. The scope and nature of the specific control objectives which are required for the business to be conducted in a prudent manner should be commensurate with an institution's needs and particular circumstances, and should have regard to the manner in which the business is structured, organised and managed, to its size and to the nature, volume and complexity of its transactions and commitments.

4. It is inappropriate to provide an exhaustive and prescriptive list of detailed control requirements which should apply to all institutions. However, each institution should address the following control objectives, where relevant:

a) Organisational structure: Institutions should have documented the high level controls in their organisation which:
   i. define allocated responsibilities; and specify the delegation of authority and responsibility, together with the limits that are applicable; and
   ii. identify lines of reporting for all aspects of the enterprise's operations, including the key controls and giving outline job descriptions for key personnel.

b) Monitoring procedures: An institution should have procedures in place to ensure that relevant and accurate management information covering the financial state and performance of the institution and the exposures which it has entered into are provided to appropriate levels of management on a regular and timely basis. Procedures should also be in place to ensure compliance with the institution's policies and practices, including any limits on delegated authority referred to above, and with statutory, supervisory and regulatory requirements.

c) Segregation of duties: A prime means of control is the separation of those responsibilities or duties which would, if combined, enable one individual to record and process a complete transaction. Segregation of duties reduces the risk of intentional manipulation or error and increases the element of checking. Functions which should be separated include those of authorisation, execution, valuation, reconciliation, custody and recording. In the case of a computer-based accounting system, systems development and daily operations should be separated.

d) Authorisation and approval: All transactions should require authorisation or approval by an appropriate person and the levels of responsibility should be recorded as prescribed above.

e) Completeness and accuracy: Institutions should have controls to ensure that all transactions to be recorded and processed have been authorised, are correctly recorded and are accurately processed. Such controls include:

i. checking the arithmetical accuracy of the records;
ii. checking valuations;
iii. the maintenance and checking of totals;
iv. reconciliations;
v. control accounts and trial balances; and
vi. accounting for documents.

f) Safeguarding assets: An institution should have controls designed to ensure that access to assets or information is limited to authorised personnel. This includes both direct access and indirect access via documentation to the underlying assets. These controls are of particular importance in the case of valuable, portable or exchangeable assets and assets held as custodian.

g) Personnel: There should be procedures to ensure that personnel have capabilities commensurate with their responsibilities. The proper functioning of any system depends on the competence and integrity of those operating it. The qualifications, recruitment and training as well as the innate personal characteristics of the personnel involved are important features to be considered in setting up any control system.

Controls in an Information Technology Environment

5. The information held in electronic form within an institution's information systems is a valuable asset that needs to be protected against unauthorised access and disclosure. It is the responsibility of management to understand the extent to which their institution relies on electronic information, to assess the value of that information and to establish an appropriate system of controls. The control objectives are usually achieved by a combination of manual and automated controls, the balance of which will vary between institutions, reflecting the need for each to address its particular risks in a manner which is cost effective.

6. The types of risk often associated with the use of information technology in financial systems may be classified as follows:

a) Fraud and theft: access to information and systems can create opportunities for the manipulation of data in order to create or conceal significant financial loss. Additionally, information can be stolen, even without its physical removal or awareness of the fact, which may lead to loss of competitive advantage. Such unauthorised activity can be committed by persons with or without legitimate access rights.

b) Errors: although they most frequently occur during the manual inputting of data and the development or amendment of software, errors can be introduced at every stage of an information system.

c) Interruption: the components of electronic systems are vulnerable to interruption and failure. Without adequate contingency arrangements, there may be serious operational difficulty and/or financial loss.

d) Misinformation: problems may emerge in systems that have been poorly specified or inaccurately developed. These may become immediately evident, but can also pass undetected for some time. This is a particular risk in systems where audit trails are poor and the processing of individual transactions difficult to follow.

7. Management should be aware of its responsibility to promote and maintain a climate of security awareness and vigilance throughout the organisation. In particular, it should give consideration to:

a) IT security education and training, designed to make all relevant staff aware of the need for, and their role in supporting, good IT security practice and the importance of protecting company assets; and

b) IT security policy, standards, procedures and responsibilities, designed to ensure that arrangements are adequate and appropriate.