Risk Governance Guidance for Listed Boards

Corporate Governance Council (10 May 2012)

DISCLAIMER

This guidance is issued by the Corporate Governance Council ("Council") to provide practical guidance for Boards on risk governance of companies listed on the Singapore Exchange. This guidance is neither exhaustive nor prescriptive. Boards should exercise their own judgment on the manner and extent to which the guidance would be applicable to them and their listed companies, having regard to each company's circumstances. While efforts have been made to arrive at practical guidance that may be relevant to Boards pursuant to the recommendations under the Code of Corporate Governance, the Council takes no responsibility for the accuracy or completeness of information in this guidance and accepts no responsibility for any errors or omissions. Readers are cautioned not to place undue reliance on this guidance and should obtain professional advice regarding any specific set of facts or issues. The Council expressly disclaims any and all loss or liability (whether in negligence or otherwise) in respect of this guidance and its use by any person. Reproduction of this guidance, or any part thereof, should be done with attribution to the Council.

Foreword

Corporate governance refers to the system by which companies are directed and managed. This involves a set of relationships between a company's board, management, employees, shareholders and other stakeholders. This also provides the structure through which the company achieves its objectives and provides accountability to stakeholders. Good corporate governance therefore is an effectual balance of promoting the long-term success of the company, and providing accountability and control systems which are symmetric with the risks involved.

In this regard, global events since the 2008 financial crisis have underscored the importance of companies taking an integrated, enterprise-wide perspective of their risk exposure. There is heightened concern and focus on risk governance, and it has become clear that companies should have a sound system of risk management and internal controls to identify, assess, manage and mitigate risk.

This Guidance has been prepared with a focus on how the Board can carry out its responsibility of risk governance of the company. The Guidance is intended to provide key information on risk governance to all Board members. This includes factors which the Board should collectively consider when overseeing the company's risk management framework and policies. The Guidance also spells out the Board's and Management's respective responsibilities in managing the company's risks. In particular, the Council hopes that the Guidance will assist the Board, as well as Management, of small to mid-capitalised listed companies in the risk governance of their companies.

The Guidance has been developed by the Council with valuable inputs from risk management practitioners and business community representatives, and contains guidance and best practices gleaned from the industry and the Council's own experiences. Reference has also been made to international risk management frameworks.

In terms of structure, the text of the Guidance provides key information on risk governance to the Board, while the appendices contain details of risk management concepts, as well as samples and templates, which the Board and Management may find useful in the company's risk governance.

The Council believes that the Guidance and its focus on risk management will contribute to better and sustained value for investors in Singapore-listed companies, raise investor confidence, and enhance Singapore's reputation as a leading and trusted international financial centre. The Council is pleased to launch the publication "Risk Governance Guidance for Listed Boards".

CHAN HENG LOON ALAN
CHAIRMAN
CORPORATE GOVERNANCE COUNCIL
10 May 2012

Acknowledgements

The Corporate Governance Council

Mr Alan Chan (Chairman)	Chief Executive Officer, Singapore Press Holdings Limited
Mr Gautam Banerjee	Executive Chairman, PricewaterhouseCoopers LLP
Ms Chua Sock Koong	Group Chief Executive Officer, Singapore Telecommunications Limited
Mr David Conner	Director, Oversea-Chinese Banking Corporation Limited
Mr Patrick Daniel	Editor-in-chief, Singapore Press Holdings Limited
Mr Daniel Ee	Chairman, CitySpring Infrastructure Management Pte Ltd
Mr David Gerald	President and Chief Executive Officer, Securities Investors Association (Singapore)
Mr John Lim	Executive Deputy Chairman, LMA International N.V. / Chairman, Singapore Institute of Directors
Ms Olivia Lum	Group President and Chief Executive Officer, Hyflux Ltd
Mr Dilhan Pillay Sandrasegara	Head, Portfolio Management and Co-Head, Singapore, Temasek Holdings Private Limited
Mr Tan Chong Huat	Managing Partner, RHT Law LLP
Mr Peter Taylor	Head of Corporate Governance, Aberdeen Asset Management Asia Limited
Mr Kenny Yap	Executive Chairman & Managing Director, Qian Hu Corporation Limited

Acknowledgements

Ex-Officio Members of the Corporate Governance Council

Mr Lee Chuan Teck	Assistant Managing Director, Capital Markets, Monetary Authority of Singapore
Mr Leo Mun Wai	Assistant Managing Director, Capital Markets, Monetary Authority of Singapore (until February 2012)
Ms Juthika Ramanathan	Chief Executive, Accounting and Corporate Regulatory Authority Singapore
Ms Yeo Lian Sim	Chief Regulatory Officer, Singapore Exchange Limited

Members of the Risk Management Working Group

Ms Alice Chua	Senior Vice President, Risk Management, Singapore Technologies Engineering Ltd
Mr Chor Khee Yang	Vice-President (Internal Audit), Singapore Telecommunications Limited
Mr Irving Low	Partner, KPMG LLP
Mr Ng Siew Quan	Partner, PricewaterhouseCoopers LLP

With special thanks to:

PricewaterhouseCoopers LLP

WongPartnership LLP

Table of Contents

Introduction

1. Background

1.1. The Singapore Code of Corporate Governance (the "Code") was first introduced in 2001 and came into effect in 2003. The Code has since undergone two revisions, the first in 2005 and the second in 2012.

1.2. In its review of the Code, the Corporate Governance Council recognised the increasing focus and importance of companies and their board of directors taking an integrated enterprise-wide perspective of their risk management practices, as well as the need to enhance the management's accountability for the company's risk management. This is reflected in Principle 11 of the revised Code issued by the Monetary Authority of Singapore on 2 May 2012 and its accompanying guidelines (set out below).

2. Principle 11 and Accompanying Guidelines of the Singapore Corporate Governance Code

2.1. Principle 11 and its accompanying guidelines are set out in the box below:

Principle 11:

The Board is responsible for the **governance of risk**. The Board should ensure that Management maintains a **sound system of risk management and internal controls** to safeguard shareholders' interests and the company's assets, and should **determine the nature and extent of the significant risks** which the Board is willing to take in achieving its strategic objectives.

Guideline 11.1:

The Board should determine the company's levels of **risk tolerance** and **risk policies**, and oversee Management in the design, implementation and monitoring of the risk management and internal control systems.

Guideline 11.2:

The Board should, at least annually, review the **adequacy and effectiveness** of the company's risk management and internal control systems, including financial, operational, compliance and information technology controls. Such a review can be carried out internally or with the assistance of any competent third parties.

Guideline 11.3:

The Board should comment on the adequacy and effectiveness of the internal controls, including financial, operational, compliance and information technology controls, and risk management systems, in the company's annual report. The Board's commentary should include information needed by stakeholders to make an informed assessment of the company's internal control and risk management systems.

The Board should also comment in the company's annual report on whether it has received assurance from the [Chief Executive Officer ("CEO")] and the [Chief Financial Officer ("CFO")]:

a. that the financial records have been properly maintained and the financial statements give a true and fair view of the company's operations and finances; and

b. regarding the effectiveness of the company's risk management and internal control systems.

Guideline 11.4:

The Board may establish a separate board risk committee or otherwise assess appropriate means to assist it in carrying out its responsibility of overseeing the company's risk management framework and policies.

[our emphasis]

3. Objectives

3.1. This document ("Guidance") seeks to provide further guidance on the Board's role on risk governance vis-à-vis the Code. Additional statutory requirements (such as those applicable to companies in regulated sectors, for instance, financial institutions regulated by the Monetary Authority of Singapore) should, where applicable, take precedence over this Guidance.

3.2. Recognising that the approach to risk governance is not "one-size-fits-all", this Guidance is intended to enable each company to apply the Code in a manner which takes into account its particular circumstances.

3.3. This Guidance aims to provide the Board and Management with an understanding of the following:

(i) What is risk governance? **(Section 4)**

(ii) Who is responsible for risk governance and implementation of risk governance policies / measures? (**Section 5** , **Appendix A** and **Appendix B**)

(iii) What constitutes a sound system of risk management and internal controls? (**Section 6**)

- What goes into a risk management policy? **(Appendix C)**
- How can risk tolerance be determined? **(Appendix D)**
- What does a risk management process look like? **(Appendix E)**
- What are some of the key Information Technology ("IT") risks? **(Appendix F)**

(iv) How to ensure that the risk management and internal controls system is adequate and effective? (**Appendix G**)

(v) What should be disclosed in the annual report with respect to risk management and internal controls? (**Appendix M**)

3.4. Directors have to exercise judgement in reviewing how their company has implemented the Code in relation to their company's risk management and internal controls.

4. Risk Governance

4.1. Risk governance is the architecture within which risk management operates in a company. It defines the way in which a company undertakes risk management. It is essential for the company to have clarity about what risks are being managed and how. It provides guidance for sound and informed decision-making and effective allocation of resources.

4.2. Sound risk governance allows for the articulation of how, in the context of its risks, a company is able to:

- achieve its business objectives;
- formulate its value proposition;
- assess its risk tolerance; and
- design its processes with respect to the reasonable expectations of stakeholders.

4.3 For this to happen, the Board should first begin with a fundamental understanding of the mission of the company and of the reasons it exists in relation to all its stakeholders.

4.4 From there, the Board should work with Management to:

- identify the risks relevant to the company (also known as the risk universe); and
- effectively allocate the company's resources to create and preserve value in ways that resonate with the company's mission.

4.5 Effective risk governance provides the appropriate level of direction and control in:

- determining the goals and strategy of the company;
- pursuing those goals;
- identifying the risks which are present or which may arise when the company pursues its goals; and
- determining measures to mitigate the risks.

5. Roles and Responsibilities

5.1. The Board is responsible for the governance of risk and sets the tone and direction for the company in the way risks are being managed.

5.2. The Board has ultimate responsibility for approving the strategy of the company in a manner which addresses stakeholders' expectations and does not expose the company to an unacceptable level of risk. It also has ultimate responsibility for approving the key risk management policies, ensuring a sound system of risk management and internal

controls, and monitoring performance against them.

5.3. It is important to establish clearly the role of the Board vis-à-vis Management in risk management.

5.4. The Role of the **Board** in the governance of risk should comprise the following:

a. determining the approach to risk governance for the company;

b. setting and instilling the right culture throughout the company for effective risk governance;

c. ensuring that the risks relevant to the company are properly identified, including those risks inherent in the company's business model and strategy, and risks from external factors as the company pursues its strategic objectives;

d. monitoring the company's exposure to risk and the key risks that could undermine its strategy, reputation or long-term viability, including provide for periodic environmental scans to gauge any possible impact on the risk profile of the company;

e. ensuring that Management put in place action plans to mitigate the risks identified where possible; and

f. providing oversight of the risk management system, and system of internal controls, and reviewing their adequacy and effectiveness at least on an annual basis.

5.5. The Board may choose to establish a separate Board Committee or other appropriate means to assist it with the above responsibilities. Further guidance is suggested in **Appendix A**.

5.6. The Role of **Management** in the management of risks is to:

a. design, implement and monitor the risk management and internal control systems of the company in accordance with Board policies on risks and controls, using effective processes and procedures;

b. identify the risks relevant to the business of the company and manage the business in accordance with risk policies / directions from the Board;

c. identify changes to risks or emerging risks and promptly bring these to the attention of the Board where appropriate; and

d. ensure the quality, adequacy and timeliness of the information that goes to the Board.

5.7. Companies may use different structures to achieve the above, such as establishing committees to scrutinise detailed risk reports and mechanisms to ensure consistency and a common understanding of the information to be provided to the Board.

6. The Enterprise Risk Management (ERM) Framework

6.1. In order for the Board and Management to carry out their roles with respect to risk management, there needs to be a framework within which they may operate. Such a framework is typically called an Enterprise Risk Management ("ERM") framework.

6.2. ERM is "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk tolerance, to provide reasonable assurance regarding the achievement of the entity's

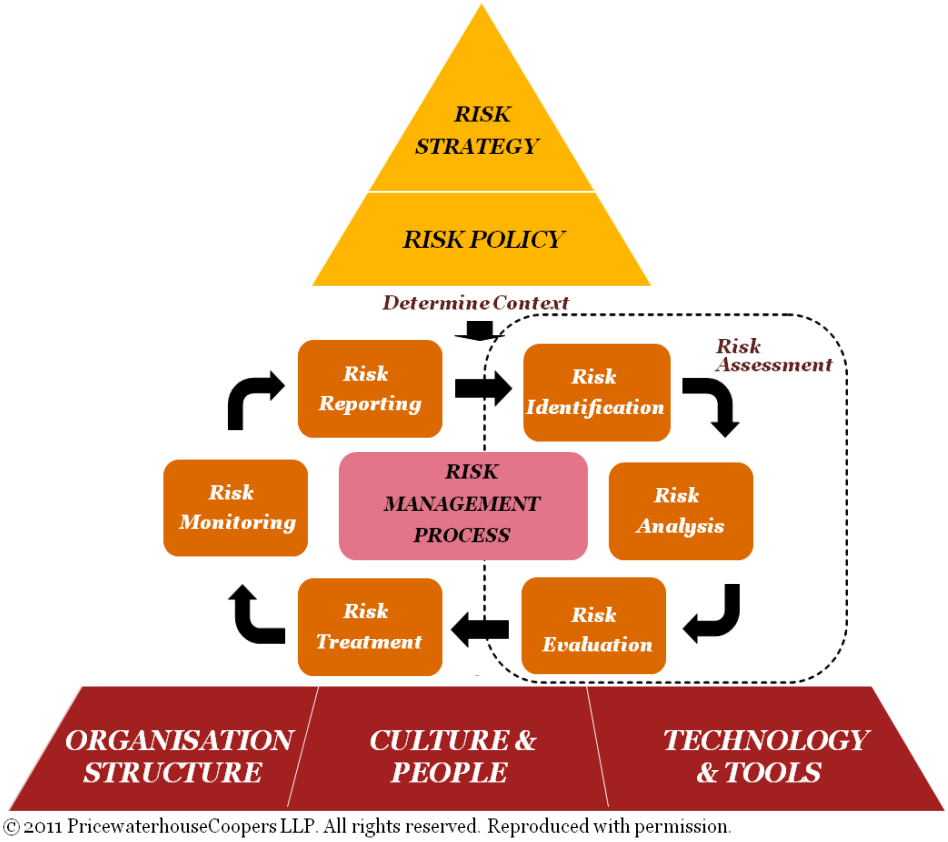
objectives."[1]

6.3. It is impossible to fully eliminate risk, and in fact it may be counter-productive to even try. The correct approach is to determine and achieve the right balance between mitigating the downside of risks to an acceptable level whilst still taking advantage of opportunities.

6.4. Effective risk assessment provides forward-looking insights, not only helping to manage risks, but providing greater and more meaningful clarity in respect of the following:

- The vast range of existing and emerging risks that a company faces;
- How these risks are managed; and
- The level of risk that is being run and the extent to which the company intends to take risks.

6.5. Although there is no definitive model of an ERM framework that fits all companies, there are certain common characteristics embodied in internationally recognised risk management standards and in the leading risk management frameworks operating in practice. An illustrative ERM framework is presented below.



[1] Definition from *Enterprise Risk Management – Integrated Framework (2004)*, published by the Committee of Sponsoring Organisations of the Treadway Commission (COSO).

6.6. With reference to the Code, in general, the ERM framework may be characterised as follows:

- Risk Strategy and Risk Policy – This relates to **Principle 11** and **Guideline 11.1** of the Code, which should be dealt with by the Board.
- Risk Management Process – This relates to matters undertaken by the Board and Management in respect of which **Guidelines 11.1, 11.2** and **11.3** of the Code are relevant.
- Organisation Structure, Culture & People and Technology & Tools – This relates to the structure and inherent features of the company. This may also be considered in relation to how the Board deals with its responsibility of overseeing the company's risk management framework and policies, as pointed out in **Guideline 11.4** of the Code.

6.7. The Board, when considering a possible ERM framework for the company, may wish to have regard to the following six common characteristics of leading, sustainable international risk management frameworks:

(i) Risk Strategy and Policy[1]

- The consideration of risk as a company sets its strategic direction
- How risk is considered as a company allocates its capital across competing priorities
- How risk is reflected in the policies that are adopted

(ii) Risk Process[2] – How risk is identified, assessed and responded to in day to day activities

(iii) Risk Structure[2] – The specific risk management functions and responsibilities established to sustain the focus on risk management

(iv) Culture[3] - The culture and behaviours that need to be developed and sustained to support effective risk management and reinforce "doing the right thing" naturally

(v) Risk Systems and Tools[2] - The systems and tools used to facilitate the risk management process

(vi) Assurance[4] - How assurance is gained over the effective operation of the risk management framework and continuously improved over time

[1] see **Appendix C** - Understanding What Constitutes a Sound System of Risk Management and Internal Controls

[2] see **Appendix E** - Understanding the Risk Management Process

Appendix F - Information Technology Risks that Boards should be aware of

[3] see **Appendix K** - Setting and Instilling the Right Culture

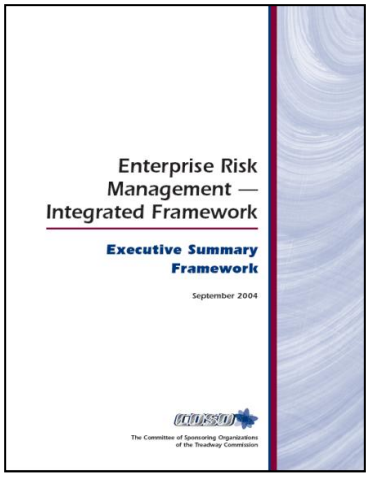
[4] see **Appendix H** - Risk Assurance and the Annual Assessment

6.8. ERM frameworks help codify and integrate a structured and disciplined approach towards managing risk into the company's core business processes and decision-making activities.

6.9. There are various ERM standards and each describes an approach for identifying, analysing, responding to and monitoring risks and opportunities within the company's internal and external environment. Some of the principal international frameworks include the following:

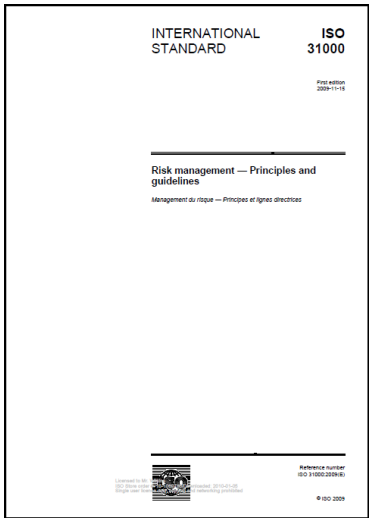
AS/NZS ISO 31000:2009

Risk Management – Principles and Guidelines



Committee of Sponsoring Organisations (COSO)

Enterprise Risk Management – Integrated Framework



ISO 31000:2009

Risk Management – Guidelines on Principles and Implementation of Risk Management

6.10. In practice, the design and pace of implementation of ERM frameworks vary enormously amongst companies, and even among those considered to be the leading risk management companies. Some companies wish to be best in class, some simply to be in the pack, whilst for others, the barest minimum of formality will suffice.

6.11. The varying desired or actual level of maturity of risk management systems can manifest itself in many different ways, including the extent to which the consideration of risk is embedded into processes and the level of sophistication (and investment) of the resources, techniques and systems used.

6.12. Further guidance on what constitutes a sound system of risk management and internal controls is set out in **Appendix C** to **Appendix M**.

Appendices

Appendix A - Ways in which the Board can Govern Risk

1. The Board as a Whole

1.1 The Board's decision to establish another committee to assist it with risk governance would depend on various factors, including:

- the size and composition of the Board;
- the scale, diversity and complexity of the company's operations; and
- the nature of the significant risks that the company faces.

1.2 In this regard, the Board may decide to set up a separate Board Risk Committee or incorporate the risk oversight function in an existing Board Committee. If it is not the Audit Committee, it may be any of the existing Board Committees, e.g. Executive Committee.

1.3 If the Board decides to set up a committee to assist it in its oversight of risk management, it is important that the Board should have clearly documented terms of reference that set out the role and responsibilities of the respective committees.

1.4 To help reduce some of the ambiguity that may arise, the Board may wish to consider common membership among the separate committees that are responsible for the oversight of different risks, or have the separate committees hold joint meetings at least once a year.

1.5 Further, the Board should consider the role of the Remuneration Committee in linking risk management with remuneration. Attention should be paid to ensure that the level and structure of remuneration is aligned with the long-term interest and risk policies of the company (as set out in Principle 8 of the Code.)

1.6 To the extent that designated Board committees carry out, on behalf of the Board, tasks that are attributed in this Guidance to the Board, the results of the relevant committees' work should be reported to, and considered by, the Board.

1.7 Regardless of the committee structure or other means which the Board employs, all directors must ensure the adequacy of their own director expertise with regard to risk awareness and management.

2 The Audit Committee

2.1 Risk traditionally is part of the Audit Committee ("AC") agenda, and because the AC already oversees risks related to the integrity of the financial statements, it is in a good position to have oversight of most of the company's risks.

2.2 While many companies may choose to rely on the AC to assist the Board in its oversight of the company's risk management function, due consideration must be given to the following which may affect the AC's ability to review risk management:

- the size and composition of AC;
- the scale, diversity and complexity of company's operations;
- the nature of significant risks faced.

2.3 If the AC is delegated the responsibility of assisting the Board with risk governance, the AC's terms of reference should reflect such responsibility.

3 The Board Risk Committee

3.1 Where the Board decides to set up a separate Board Risk Committee to assist in its oversight of risk management, the following should be considered:

- independence of the Committee from Management; and
- diversity of background and skill sets of Committee members.

3.2 The Nominating Committee should balance expertise versus objectivity in determining the composition of the Board Risk Committee. Specialists who are non-Board members could also be invited to support the Board Risk Committee.

3.3 The role and responsibilities of the Board Risk Committee should be made clear from the onset to avoid confusion, especially in relation to the Audit Committee. An illustration of the **Terms of Reference** for a Board Risk Committee can be found in **Appendix B.**

3.4 It is important that communication be maintained between the Board Risk Committee and the Audit Committee. Both committees should interact as often as possible to ensure timely information is exchanged and appropriate action taken where necessary. For example, results gleaned from workshops which assess the company's risks should feed into the Audit Plan.

4 Management – Chief Risk Officer

4.1 With regard to the role of Management, a company may decide to appoint a Chief Risk Officer ("CRO") to provide executive oversight and co-ordination of the company's risk management efforts. Such decision would depend on various factors, including the scale, diversity and complexity of the company's operations. In appointing a CRO, companies must be mindful that ownership of risks still reside with the relevant departments and not the CRO.

Appendix B – Sample Terms of Reference for a Board Risk Committee[2]

1. Duties

1.1 The Board Risk Committee (also referred to as "committee" in this Appendix B) should carry out the duties below for the company, major subsidiary undertakings and the group as a whole, as appropriate. The committee should also undertake periodic environmental scans to gauge any possible impact on the risk profile of the company. The committee shall:

1.1.1 advise the Board on the company's overall risk tolerance and strategy;

1.1.2 oversee and advise the Board on the current risk exposures and future risk strategy of the company;

1.1.3 in relation to risk assessment:

(a) keep under review the company's overall risk assessment processes that inform the Board's decision making;

(b) review regularly and approve the parameters used in these measures and the methodology adopted; and

(c) set a process for the accurate and timely monitoring of large exposures and certain risk types of critical importance;

1.1.4 review the company's capability to identify and manage new risk types;

1.1.5 before a decision to proceed is taken by the Board, advise the Board on proposed strategic transactions, focussing in particular on risk aspects and implications for the risk tolerance of the company, and taking independent external advice where appropriate and available;

1.1.6 review reports on any material breaches of risk limits and the adequacy of proposed action;

1.1.7 keep under review the effectiveness of the company's internal controls and risk management systems and review and approve the statements to be included in the annual report concerning the effectiveness of the company's internal control and risk management systems;

1.1.8 provide advice to the Remuneration Committee on risk weightings to be applied to performance objectives incorporated in executive remuneration;

1.1.9 review the company's procedures for detecting fraud, including the whistle-blowing policy (if any). The committee shall ensure that these arrangements allow proportionate and independent investigation of such matters and appropriate follow up action;

1.1.10 monitor the independence of risk management functions throughout the organisation;

[2] ICSA Guidance on Terms of Reference Risk Committee, Oct 2010.

1.1.11 review promptly all relevant risk reports on the company; and

1.1.12 review and monitor Management's responsiveness to the findings.

1.2 Note: Within the duties set out above, there are certain duties that could be undertaken by either the Audit Committee or the Board Risk Committee and there is some overlap in duties. The precise allocation of responsibilities should be detailed in the terms of reference for the Audit Committee and the terms of reference for the Board Risk Committee, both of which should be determined by the Board.

2. Membership

2.1 The committee shall comprise at least [three members[3]]. A majority of members of the committee shall be independent non-executive directors, who have the relevant experience. In addition, the committee may co-opt from time to time persons who have the relevant expertise to assist it but who may not be directors. Such persons may be associate members or invitees of the committee but shall have no decision-making powers or voting rights. Members of the committee shall be appointed by the Board, on the recommendation of the Nomination Committee in consultation with the chairman of the committee.

2.2 Only members of the committee have the right to attend committee meetings. However, other individuals such as the chairman of the Board, directors, the chief executive officer, and representatives of the risk function, compliance, and internal and external audit, may be invited to attend all or part of any meeting as and when appropriate and necessary.

2.3 The Board shall appoint the committee chairman who shall be an independent non-executive director. In the absence of the committee chairman, the remaining members present shall elect one of themselves to chair the meeting.

3. Quorum

3.1 The quorum necessary for the transaction of business shall be [insert appropriate number] members. A duly convened meeting of the committee at which a quorum is present shall be competent to exercise all or any of the authorities, powers and discretions vested in or exercisable by the committee.

4. Frequency of meetings

4.1 The committee shall meet at least [twice a year[4]], or as and when circumstances or events merit it.

[3] Or such other number as is appropriate.
[4] Or such other number as is appropriate.

5. Notice of meetings

5.1 Meetings of the committee shall be called by the secretary of the committee at the request of any of its members.

5.2 Unless otherwise agreed, notice of each meeting confirming the venue, time and date together with an agenda of items to be discussed, shall be forwarded to each member of the committee, any other person required to attend and all other non-executive directors, no later than [insert appropriate number] working days before the date of the meeting. Supporting papers shall be sent to committee members and to other attendees as appropriate, at the same time.

6. Minutes of meetings

6.1 The secretary shall minute the proceedings of all meetings of the committee, including recording the names of those present and in attendance.

6.2 Draft minutes of committee meetings shall be circulated promptly to all members of the committee. Once approved, minutes should be circulated to all other members of the Board.

7. Annual General Meeting

7.1 The committee chairman should attend the general meeting of shareholders to answer shareholder questions on the committee's activities, role and scope of responsibilities.

8. Reporting responsibilities

8.1 The committee chairman shall report to the Board on the committee's proceedings after each committee meeting.

8.2 The committee shall make whatever recommendations to the Board it deems appropriate on any area within its remit where action or improvement is needed.

8.3 Taking into account the company's reporting obligations (pursuant to, as applicable, relevant rules and regulations, including for instance the SGX-ST's Listing Rules), the committee shall produce a report of its activities and the company's risk management and strategy to be included in the company's annual report.

9. Other matters

9.1 The committee shall:

9.1.1 have access to sufficient resources in order to carry out its duties, including access to the company secretary for assistance as required;

9.1.2 be provided with appropriate and timely training, in particular in respect of risk management expertise, both in the form of an induction programme for new members and on an ongoing basis for all members;

9.1.3 give due consideration to laws and regulations, the provisions of the Singapore Code of Corporate Governance, the requirements of the SGX-ST's Listing Rules and any other applicable rules, as appropriate;

9.1.4 oversee any investigation of activities which is within its terms of reference; and

9.1.5 arrange for periodic reviews of its own performance and, at least annually, review its constitution and terms of reference to ensure it is operating at optimal effectiveness and recommend any changes it considers necessary to the Board for approval.

10. Authority

10.1 The committee is authorised to:

10.1.1 seek any information it requires from any employee of the company in order to perform its duties;

10.1.2 obtain, at the company's expense, outside legal or other professional advice on any matter within its terms of reference; and

10.1.3 require any employee to be in attendance at a meeting of the committee as and when required, and to respond to the committee's questions and/or to provide the committee with any other assistance.

Appendix C – Understanding What Constitutes a Sound System of Risk Management and Internal Controls

1. A sound system of risk management and internal controls contributes to the safeguarding of the company's assets and consequently shareholders' investment. It is the Board's oversight responsibility to ensure that risks relevant to the company are adequately addressed and mitigated.

2. There is a need to recognise that the pursuit of any opportunity in business always encompasses risk, and that a sound system of risk management and internal controls does not eliminate risk, but rather optimises risk-taking such that the company understands the risk-reward trade-off and makes a decision that is commensurate with its risk tolerance.

3. A company's objectives, its organisational structure and the environment in which it operates are continually evolving, and as a result, the risks it faces are continually changing. A sound system of risk management and internal controls therefore depends on a thorough and regular evaluation of the nature and extent of risks to which the company is exposed.

4. The Board should set appropriate policies on the company's system of risk management and internal controls. It should seek regular assurance so that it can be satisfied that the system is functioning effectively. The Board must further review the system of risk management and internal controls for adequacy and effectiveness.

5. As many companies' financial and operational processes are highly computerised, the Board should pay special attention to risks relating to IT. Some measures that the Board should undertake include: periodic IT audit, penetration test on the IT system, etc. Some of the key risks that the Board should be aware of are set out in **Appendix F** – Information Technology Risks that Boards should be aware of.

6. In determining the company's risk management and internal control policies, and thereby assessing what constitutes a suitable sound system of risk management and internal controls while having regard to the particular circumstances of the company, the Board's deliberations should include consideration of the following factors:

    - the nature and extent of the risks facing the company;
    - the extent and categories of risk which it regards as acceptable for the company to bear;
    - the likelihood of the risks concerned materialising;
    - in respect of risks that do materialise, the company's ability to reduce the incidence and impact on its business;
    - the risk-reward trade-off, i.e. the costs of operating particular controls relative to the benefit thereby obtained in managing the related risks; and
    - the adequacy of resources and availability of requisite experience to manage risks.

7. A sound system of risk management and internal controls provides reasonable, but not absolute, assurance that a company will not be hindered in achieving its business objectives, or in the orderly and legitimate conduct of its business, by circumstances which may reasonably be foreseen.

8. The ERM policy helps establish a structured and disciplined approach towards managing risk into the organisation's core business processes and decision-making activities.

9. A **risk management policy** should contain the following[5]:

    - Risk management and internal control objectives (governance)
    - Statement of the attitude of the organisation to risk (risk strategy)
    - Description of the risk awareness culture or control environment
    - Level and nature of risk that is acceptable (risk tolerance)
    - Risk management organisation and arrangements (risk architecture)
    - Details of procedures for risk recognition and ranking (risk assessment)
    - List of documentation for analysing and reporting risk (risk protocols)
    - Risk mitigation requirements and control mechanisms (risk response)
    - Allocation of risk management roles and responsibilities
    - Risk management training topics and priorities
    - Criteria for monitoring and benchmarking of risks
    - Allocation of appropriate resources to risk management
    - Risk activities and risk priorities for the coming year
    - Frequency of review of the risk management systems in place

10. The risk management process is an integral part of good management practices and should be embedded into the organisation's core business activities. Examples of the application of the risk management process in daily routines include the strategy setting process, investment decisions, health and safety policies, project management and change management practices.

11. The risk management process can also be undertaken at the project-level, e.g. mergers and acquisitions, joint ventures, etc.

[5] A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000, Institute of Risk Management, 2010.

Appendix D – Setting Risk Tolerance

1 Risk Tolerance

1.1 Risk tolerance[6] is defined as the boundaries of risk-taking outside of which the organisation is not prepared to venture in the pursuit of long term business objectives.

1.2 Risk tolerance may vary according to the various categories of risks the company may face. Boards should therefore recognise that risk tolerance levels have to be capable of being expressed differently for different classes of risk and at different levels of the organisational structure. There is no single risk tolerance level applicable across the company, but rather, a range of levels for different types of risks. This range needs to be aligned and consistent with an overall risk tolerance framework.

1.3 The design of a risk tolerance framework should encompass the following features:

- the risk tolerance framework should be established in the context of the organisation's risk capacity: its ability to carry risks and manage them;
- the risk tolerance is set at not just at the strategic level, but also at the tactical and operating levels; and
- both the organisation's propensity to take risk and the propensity to exercise control are considered in tandem.

1.4 The key drivers of risk tolerance within the organisation may include credit rating, analyst expectations and shareholder expectations. Risk tolerance is shaped with reference to the expectations and risk preferences of major stakeholders who have an interest in the strategy and strategic objectives of the organisation, such as:

- Providers of capital (debt and equity)
- Governments and regulators
- The Board
- Management
- Staff
- Business partners
- Customers
- The communities within which the organisation operates

1.5 Setting risk tolerance is ultimately a Board decision. The risk management policy should describe the tolerance for various classes of risk and how much of each type of risk can be taken without endangering the organisation.

[6] Risk Appetite and Tolerance Guidance Paper, Institute of Risk Management, September 2011.

2 Examples of Risk Tolerance Statements[7]

2.1 Some examples of risk tolerance statements are set out below:

- While we expect a return of 18% on this investment, we are not willing to take more than a 25% chance that the investment leads to a loss of more than 50% of our existing capital.

- We will not accept more than a 5% risk that a new line of business will reduce our operating earnings by more than 5% over the next ten years.

- We strive to treat all emergency room patients within two hours and critically ill patients within 15 minutes. However, management accepts that in rare situations (5% of the time) patients in need of non-life-threatening attention may not receive that attention for up to four hours.

- For purchasing agents, the risk tolerance is set at near zero for procuring products that do not meet the organization's quality and sourcing requirements.

- The company has set a target for production defects of one flaw per 1,000 board feet. Production staff may accept defect rates up to 50% above this target (i.e. 1.5 flaws per 1,000 board feet) if the cost saving from using lower-cost materials is at least 10%.

[7] Understanding and Communicating Risk Appetite, Dr. Larry Rittenberg and Frank Martens, COSO, January 2012.

Appendix E – Understanding the Risk Management Process

The Risk Management Process

A generic risk management process looks like this:

A. Establish Context

1 This step involves defining the internal and external parameters that need to be taken into account when managing risk, and setting the scope and risk criteria for the remaining process.

External Context

2 Understanding the external context (or external environment) in which the organisation seeks to achieve its objectives is important in ensuring that external stakeholders, their objectives and concerns are considered when developing risk criteria.

3 The external context can include, but is not limited to:

- the cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organisation; and
- perceptions and values of external stakeholders.

Internal Context

4 Internal context is the internal environment in which the organisation seeks to achieve its objectives. The risk management process should be aligned with the organisation's culture, processes and structure.

5 Internal context is anything within the organisation that can influence the way in which the organisation will manage risk. It should be established because:

- risk management takes place in the context of the objectives of the organisation;
- objectives and criteria of a particular project or activity should be considered in the light of objectives of the organisation as a whole; and
- a major risk may be the failure to achieve a strategic, project or business objective, and this risk affects ongoing organisational commitment, credibility, trust and value.

6 It is necessary to understand the internal context in terms of, for example:

- the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- information systems, information flows, and decision making processes (both formal and informal);
- internal stakeholders;
- policies, objectives, and the strategies that are in place to achieve them;
- perceptions, values and culture;
- standards and reference models adopted by the organisation; and
- structures (e.g. governance, roles and accountabilities).

B. Risk Identification

7 The aim of this step is to generate a comprehensive list of risks based on those events that might enhance, prevent, degrade or delay the achievement of the objectives. It is also important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis. Identification should include risks whether or not their source is under control of the organisation.

8 Relevant and up-to-date information is important in identifying risks. This should include suitable background information where possible. People with appropriate knowledge should be involved in identifying risks. After identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes should be considered.

9 Risk identification can apply to both inherent and residual risks:

- **Inherent Risks** are the risks that an event may occur assuming that no controls or risk treatment measures are implemented.
- **Residual Risks** are the risks that an event will occur after having taken into account any actual or proposed actions to mitigate the risk.

10 An important aspect of the identification process is to be clear in the description of the risk and where possible, to categorise similar risks together.

11 Clear descriptions of risks using a structured format, will promote improved understanding of the risk and increase the possibility that an appropriate risk treatment will be selected. Categorising similar risks enables a clearer picture of the impact of similar risks across the organisation and enables a more holistic view to be taken of the importance of a risk and the determination of alternative strategies to address the risk.

12 There are many possible techniques that can be applied to help in the identification of

risks affecting the organisation.

13 Risk identification techniques include:

- Brainstorming (sometimes called Risk Storming) with colleagues
- Questionnaires
- Business studies (i.e. looking at business processes and describing both the internal and the external factors influencing them)
- Industry benchmarking
- Scenario analysis
- Risk assessment workshops
- Past incident reports or investigations

C. Risk Analysis & Evaluation

14 Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated and on the most appropriate risk treatment strategies and methods.

15 Risk analysis involves consideration of:

- the causes and sources of risk;
- their potential positive and negative impact or consequence; and
- the likelihood that those consequences can occur.

16 Factors that affect consequences and likelihood should be identified. An event can have multiple consequences and can affect multiple objectives. Existing risk controls and their effectiveness should be taken into account.

17 Considering the impact and likelihood of each risk makes it possible to prioritise risks and highlight those that need to be analysed in further detail. Risk analysis can be undertaken with varying degrees of detail depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances. In practice at the organisation, qualitative analysis will typically be used first to obtain a general indication of the level of risk and to reveal the major risks. When appropriate, more specific and quantitative analysis of the risks can be undertaken as a following step.

18 Consequences can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data. Consequences can be expressed in terms of tangible and intangible impacts. In some cases, more than one numerical value or descriptor is required to specify consequences for different times,

places, groups or situations.

Risk Evaluation

19 Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. If the level of risk is not consistent with the risk criteria, the risk should be treated.

20 Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organisation that benefit from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

21 In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing risk controls. This decision will be influenced by the organisation's risk tolerance or risk attitude and the risk criteria that have been established. Such criteria might include costs and benefits, legal requirements, socioeconomic and environmental factors, concerns of stakeholders, etc.

Risk Analysis Techniques

22 Risk analysis techniques are needed to clearly identify the manner in which incidents or issues occurred, in order to minimise the risk of reoccurrence. In addition, risk analysis techniques should be used to determine why positive variances have occurred. A major portion of risk management engagements involves an analysis or assessment of one or more of the organisation's risks. A range of qualitative and quantitative risk analysis techniques is available, with varying degrees of suitability in different circumstances.

23 A range of techniques that can be used to analyse risks includes:

- Risk Analysis Techniques
- Dependency modelling
- SWOT analysis (Strengths, Weaknesses, Opportunities, Threats)
- Fault and event tree analysis
- BPEST (Business, Political, Economic, Social, Technological) analysis
- Decision-taking under conditions of risk and uncertainty
- Statistical inference
- Measures of central tendency and dispersion
- PESTLE (Political Economic Social Technical Legal Environmental)
- Threat analysis

- FMEA (Failure Mode & Effect Analysis)
- Near-Miss Programme

24 Often a combination of two or more complementary techniques is used. An illustration outlining the degree of sophistication in various risk analysis techniques is shown below:

24.1 Individual qualitative self-assessment

The most basic form of risk assessment is a qualitative assessment, which may use nominal or ordinal scales to provide categorisation of items based on similarities. External validation should be obtained to guard against potential management biases.

24.2 Group-facilitated qualitative prioritisation

This prioritisation can be done in a number of ways, but brainstorming is a popular technique. Brainstorming involves a serial or iterative expression of thoughts and ideas between two or more knowledgeable individuals that leads to augmented thinking by all those involved, with the objective of working towards a commonly shared view. Brainstorming as a structured technique requires a facilitated approach, where the facilitator provides a structure or straw man to trigger the desired train of thought and to capture the outcomes.

The prioritisation can take place either in a group workshop setting or in a structured interview setting. In both instances, a facilitator (interviewer) provides a structure to unlock specific knowledge of the attendee(s).

Brainstorming is a technique used in most engagements, often in combination with other techniques. All of the other risk analysis techniques discussed in this building block involve some sort of brainstorming to get the required inputs.

When brainstorming risks, a typical structure or straw man for the brainstorm is a set of risk categories, sources or drivers. These can include the Political, Economic, Social, Technological, Legal, Environmental (PESTLE) factors and the organisation's value chain components.

Quantitative Risk Analysis and Risk Modelling

25 Quantitative risk analysis provides greater insight into the risks an organisation is facing. The approach has the ability — in contrast to qualitative risk analysis — to capture stochastic variability of risks (i.e. the distribution of possible outcomes, rather than a single point on a likelihood/consequence matrix), the dynamics of risks over time and the interdependencies between risks (correlation). This ability provides a better understanding of the individual risks and also how the portfolio of risks affects selected business parameters / strategic goals / key performance indicators (KPIs) (e.g. sales, EBITA).

26 Risk Modelling is the statistical and financial analysis of risks that provides quantitative measures of risks and enables integration of risk analysis in the company's existing business parameters/strategic goals / KPIs .

D. Risk Treatment

27 Risk treatment is a cyclical process. A treatment is identified and determined as to whether or not it reduces the residual risk to an acceptable level. If not, further treatments are considered until the effect of the treatment is to reduce the residual risk to an acceptable level.

28 Risk treatment options are often described using the following four terms:

28.1 **Transfer** – Transfer or share the risk with another party through such means as insurance, joint ventures and outsourcing contracts. This usually involves a cost or risk premium such as an insurance premium.

28.2 **Avoidance** – Avoiding the risk by deciding not to start or continue with an activity that gives rise to the risk.

28.3 **Reduction** – Eliminate the source of the risk; reduce the likelihood of its occurrence (e.g. quality assurance procedures, preventative maintenance, day to day procedural and management controls); or minimise the consequence of risks (e.g. contingency planning, crisis management, contract terms and conditions).

28.4 **Accept** – Accept the risk.

29 A further treatment may be to seek an opportunity by deciding to start or continue with an activity likely to create or enhance the risk.

Selecting a Risk Treatment Option

30 Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived having regard to legal, regulatory, and other requirements, social responsibility and the protection of the natural environment. Decisions should also take into account risks that can warrant risk treatment actions that are not justifiable on economic grounds e.g. severe (high negative consequence) but rare (low likelihood) risks. A number of treatment options can be considered and applied either individually or in combination. The organisation can benefit from the adoption of a combination of treatment options.

31 Where risk treatment options can impact on risk elsewhere in the organisation, these areas should be involved in the decision. Though equally effective, some risk treatments can be more acceptable to stakeholders than others.

32 If the resources for risk treatment are limited, the treatment plan should clearly identify the priority order in which individual risk treatments should be implemented.

33 In defining risk treatment plans, it is useful to address the following questions:

- Do we already have natural offsets for a risk somewhere in the organisation?
- Do we have superior capabilities for managing the risk or are we disadvantaged?
- Are the accessible risk-transfer markets reasonably efficient?

34 It is fundamental to identify those risks for which the organisation has a competitive advantage (natural risks) and which the organisation should retain rather than transferring them to an external party.

E. Monitoring and Reporting

35 Monitoring the risks within an organisation is a crucial task of risk management. To understand how risks are behaving and are interlinked with one another it is essential to identify, design, and monitor Key Risk Indicators (KRIs) within defined parameters. An assessment of the existing KRIs and the identification of KRI needs within the organisation is the basis for addressing risk monitoring improvements and identifying current and desired future levels of maturity.

36 The basis for risk monitoring and reporting is to provide transparency to relevant stakeholders regarding:

- The achievement of business objectives and strategy
- The satisfaction of the organisation's obligations
- The effectiveness of business processes including risk management

37 Effective monitoring and reporting frameworks support an organisation in achieving its business objectives by enabling informed and effective risk management and business decision making.

38 Once an appropriate risk treatment has been determined, the organisation’s monitoring and review processes should look into:

- ensuring that the risk control and treatment measures are effective in both design and operation;
- analysing emerging risks;
- analysing and learning lessons from events, changes and trends; and
- detecting changes in the external and internal context including changes to the risk itself which require revision of risk treatments and priorities.

39 Actual progress made in implementing risk treatment plans provides a performance measure and should be included in the performance management and reporting activities.

Appendix F – Information Technology ("IT") Risks that Boards should be aware of

The following are some of the IT risks which the Board should be concerned about and ensure that management take appropriate action to mitigate them:

1. **IT Governance & Oversight**

   Inadequate IT governance and oversight lead to lack of tone at the top and accountability for securing the confidentiality, integrity and availability of the underlying information assets. Clearly defined and implemented IT management controls, including identified persons, functions or business units responsible for managing and co-ordinating the relevant controls and security requirements, are critical.

2. **Information Security Policy and Standards**

   Lack of or inadequately drafted IT Security Policies and Standards. These are foundation stones upon which to build, risk-manage and sustain a secured IT environment. Sound IT Security Policies and Standards provide a basis to implement 'best practice' security controls and ensure a high level of security awareness at all times by users of IT systems.

3. **Compliance**

   Inadequate knowledge of regulations and standards in countries in which the organisation operates, results in regulatory compliance failures. Hefty penalties and sanctions can undermine customer confidence and loss of business. Organisations with large regional or global footprints should ensure that a well-resourced and competent compliance function exists.

4. **Data Loss Protection**

   Information assets that need to be protected, have not been identified, inventorised and classified according their levels of sensitivity and criticality. Security breaches can make headline news and expose an organisation to costly financial and reputational damage. Data Loss Protection policies and controls are needed to address these risks to protect the organisation's customer data, intellectual property assets and other sensitive information.

5. Cyber security

No network is safe from cyber security threats and the concept of a closed network (to the internet) no longer exists. Today's corporate networks are exposed to the internet in many ways though direct connection to the internet and/or through the introduction of portable thumb drive and storage devices, none of which can be absolutely secured against external and internal cyber attacks. IT Management needs to ensure it is up to date on technology risks, perform annual IT risk assessments as a minimum and implement a robust programme to continually manage risk and strengthen its information security controls to mitigate against the threats of increasingly sophisticated cyber criminals.

6. Data Privacy

With the impending introduction of Singapore's Data Protection legislation, policies and controls relating to how data can and cannot be used come into focus. Management needs to understand the impact of this new legislation, communicate the policies and controls clearly to everyone in the organisation and implement suitable controls to manage the risk of data privacy breaches.

7. New Generation Technologies

Much is still unknown about the security risks associated with new generation technologies such as open source, cloud computing, mobile technology and virtualisation. The IT industry is still at an early stage in understanding and developing security standards and related technologies to adequately secure these systems. Management should embrace new generation technologies "with caution".

8. Outsourcing

Outsourcing business and IT processes to third parties (vendors, business partners, contract staff, etc), and with it, responsibility for security and controls as well. Organisations can outsource the process but not responsibility for the confidentiality, integrity and security of systems and data outsourced. Adequate due diligence should be performed on assessing the suitability of outsourced service providers before selecting them and adequate monitoring controls should be implemented to ensure that they comply with the organisation's information security policies and standards, and meet performance standards.

9. Incident Management & Business Continuity Planning

Incidents, disasters and catastrophes do happen and usually unexpectedly, and the impact on the organisation and its heavy reliance on IT systems to support the business recovery processes may be underestimated. Attention should be paid to developing Crisis Management Plans to respond quickly to such contingency events and robust and well-tested business continuity plans to recover critical business functions.

Appendix G – Reviewing Adequacy and Effectiveness

1 Effective monitoring on a continuous basis is an essential component of a sound system of risk management and internal controls. The Board cannot, however, rely solely on the embedded monitoring processes within the company to discharge its responsibilities. It should regularly receive and review reports on risks and internal controls.

2 Reviewing the adequacy and effectiveness of risk management and internal control systems is an essential part of the Board's responsibilities. The Board will need to form its own view on effectiveness and adequacy after due and careful enquiry based on the information and assurances provided to it.

3 A risk management and internal controls system is considered **adequate** and **effective** if it provides reasonable assurance for the managing of the company's risks, the safeguarding of its assets, the reliability of financial information, and the compliance with laws and regulations.

4 Reasonable assurance is a concept that acknowledges that the systems should be developed and implemented to provide Management with the appropriate balance between risks of a certain business practice and the level of control required to ensure business objectives are met. The cost of a control should not exceed the benefit to be derived from it.

5 Management is accountable to the Board for the design, implementation and monitoring the company's risk management and internal control systems and for providing assurance to the Board that it has done so.

6 The Board should define the process to be adopted for its review of the effectiveness and adequacy of risk management and internal controls. This should encompass both the scope and frequency of the reports it receives and reviews during the year, and also the process for its annual assessment, such that it will be provided with sound, appropriately documented, support for its statement on risk management and internal controls in the company's annual report and accounts.

7 The reports from Management to the Board should provide a balanced assessment of the significant risks and the effectiveness and adequacy of the system of internal controls in managing those risks. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact that they have had, could have had, or may have, on the company and the actions being taken to rectify them. It is essential that there be openness of communication between Management and the Board on matters relating to risk and internal controls.

8 When reviewing reports during the year, the Board should:

- consider what are the significant risks and assess how they have been identified, evaluated and managed;
- assess the effectiveness of the related system of internal controls in managing the significant risks, having regard, in particular, to any significant failings or

weaknesses in internal controls that have been reported;

- consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and

- consider whether the findings indicate a need for more extensive monitoring of the system of internal controls.

9 Sample questions to ask when reviewing risk management and internal control systems are set out in **Appendix L**.

Appendix H - Risk Assurance and the Annual Assessment

1 The Board should undertake an annual assessment for the purpose of making its public statement in the annual report on the adequacy and effectiveness of the company's risk management and internal control systems. [8] The assessment should consider issues dealt with in reports reviewed by the Board during the year together with any additional information necessary to ensure that the Board has taken account of all significant aspects of risks and internal controls for the company for the year under review and up to the date of approval of the annual report and accounts.

2 The Board's annual assessment should in particular consider:

- the changes since the last annual assessment in the nature and extent of significant risks, and the company's ability to respond to changes in its business and the external environment;
- the scope and quality of management's ongoing monitoring of risks and of the system of internal controls, and, where applicable, the work of its internal audit function and other providers of assurance;
- the extent and frequency of the communication of the results of the monitoring to the Board (or Board committee(s)) which enables it to build up a cumulative assessment of the state of internal controls in the company and the effectiveness with which risk is being managed;
- the incidence of significant internal controls failings or weaknesses that have been identified at any time during the period and the extent to which they have resulted in unforeseen outcomes or contingencies that have had, could have had, or may in the future have, a material impact on the company's financial performance or condition; and
- the effectiveness of the company's public reporting processes.

3 In order to obtain assurance that the company's risks are managed adequately and effectively, it is necessary to have an overview of the risks which the company is exposed to, as well as an understanding of what mechanisms are in place to manage them. Management's role is to assist the Board in developing this understanding. The following two tables in **Appendix I and J** provide an illustration of what can be done in terms of documentation to support this.

4 The Board (or appropriate committee) may commission an independent audit for its assurance, or where it is not satisfied with the company's system of risk management or internal controls.

[8] Other than Principle 11 of the Code and its accompanying guidelines, the SGX-ST Listing Manual also contains provisions regarding the Board's reporting obligations in respect of the adequacy of internal controls (addressing financial, operational and compliance risks). In this regard, reference may be made to SGX-ST's advisory note dated 16 April 2012, whereby SGX-ST issued guidance to issuers' boards on compliance with such reporting requirements.

Appendix I - The Enterprise Summary ("Helicopter View")

Critical Risk Areas		Risk owner	Critical SOP Frameworks are: •Updated •Acceptable	Timely escalations of compliance issues in line with SOPs in year	Any unacceptable breaches of compliance noted in year	Detailed comfort matrix view of key inherent risks exists	Assurance				Overall view of controls (Acceptable / Not acceptable / NA (not applicable)
Level 1 risk	**Level 2 risk**						**Internal Audit**	**CSA**	**External Audit**	**Other**	
Financial	**Credit**	CFO	✓	✓	No	✓	=	✓	=	✓	Acceptable
	etc										
Operational	**People**	VP HR	✓	✓	No	✓	x	✓		✓	Acceptable
	Safety & Health	VP S&H	✓	✓	Yes	✓	x	x	x	x	Needs more focus
	etc										
Compliance	**Regulatory**	Legal	✓	✓	No	✓	✓	✓		=	Acceptable
	etc										

Key	Full compliance	✓
	Concerns addressed	=
	Concerns to address	x

Appendix J - Comfort Matrix View of Key Inherent Risks

Area: _____ **Owner:** _____

Inherent Risk Category	Strategy and Policy	People and Structure	Process	IT systems	Assurance Coverage	Reports to: Management & Management Committees	Reports to: Board & Board Committees
	Description of strategy and policies adopted for managing the risk	*Description of key responsibilities, organisation structure, centralised controls etc*	*Description of core processes instituted to manage key risks*	*Description of systems / major applications to manage risk*	*What Assurance processes cover the risk*	*Description of information or reports received and reviewed by management, the various management and board committees and ultimately the Board.*	
Level 2 Risks e.g. Safety & Health							
Source or evidence							

Appendix K – Setting and Instilling the Right Culture

1 Boards should not overlook the importance of embedding the right culture throughout the organisation, alongside any improvements in techniques and processes. For risk management to be effective, there is a need for openness throughout the organisation. This will enable Management and staff to escalate concerns in a timely manner without fear. Good culture results in better judgement, which reduces the reliance on process and provides greater comfort to the Board and Management.

2 It is also essential that Boards lead by example and set the right tone at the top in order to influence the behaviour of Management and staff. Thus, the leaders, in particular the Chairman and the CEO, should be seen to live the values they espouse.

3 Some practices that may help create a risk-aware organisation include:

- establishing values statements and codes of conduct;
- clear communication about any risks or practices for which there is zero tolerance;
- clear communication of the boundaries within which employees can operate;
- periodic risk reports to the Board and/or the appropriate Board committee;
- periodic discussions of risk and risk issues with Management;
- clear allocation of responsibility for managing specific risks ; and
- review and evaluation of performance against rewards.

4 The company's remuneration framework and policy should include a component on risk management. There must be alignment with the risk tolerance and overall risk strategy of the company to encourage the desired behaviour of staff. The Remuneration Committee should conduct periodic reviews of the framework to ensure relevance and consistency.

Appendix L – Sample Questions to Ask when Reviewing Risk Management and Internal Control Systems

Risk assessment:

1. Does the company have clear objectives and have they been communicated so as to provide effective direction to employees on risk assessment and control issues? For example, do objectives and related plans include measurable performance targets and indicators?

2. Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis? (Significant risks may, for example, include those related to market, credit, liquidity, technological, legal, health, safety and environmental, reputation, and business probity issues.)

3. Is there a clear understanding by Management and others within the company of what risks are acceptable to the Board?

Control environment and control activities:

4. Does the Board have clear strategies for dealing with the significant risks that have been identified? Is there a policy on how to manage these risks?

5. Does the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control system?

6. Does Management demonstrate, through its actions as well as its policies, the necessary commitment to competence, integrity and fostering a climate of trust within the company?

7. Are authority, responsibility and accountability defined clearly such that decisions are made and actions taken by the appropriate people? Are the decisions and actions of different parts of the company appropriately co-ordinated?

8. Does the company communicate to its employees what is expected of them and the scope of their freedom to act? This may apply to areas such as customer relations; service levels for both internal and outsourced activities; health, safety and environmental protection; security of tangible and intangible assets; business continuity issues; expenditure matters; accounting; and financial and other reporting.

9. Do people in the company (and in its providers of outsourced services) have the knowledge, skills and tools to support the achievement of the company's objectives and to manage effectively risks to their achievement?

10. How are processes/controls adjusted to reflect new or changing risks, or operational deficiencies?

Information and communication:

11. Do Management and the Board receive timely, relevant and reliable reports on progress against business objectives and the related risks that provide them with the information, from inside and outside the company, needed for decision-making and management review purposes? This could include performance reports and indicators of change, together with qualitative information such as on customer satisfaction, employee attitudes etc.

12. Are information needs and related information systems reassessed as objectives and related risks change or as reporting deficiencies are identified?

13. Are periodic reporting procedures, including quarterly, half-yearly and annual reporting, effective in communicating a balanced and understandable account of the company's position and prospects?

14. Are there established channels of communication for individuals to report suspected breaches of laws, regulations or policies, or other improprieties?

Monitoring:

15. Are there ongoing processes embedded within the company's overall business operations, and addressed by Management, which monitor the effective application of the policies, processes and activities related to internal controls and risk management? (Such processes may include control self-assessment, confirmation by personnel of compliance with policies and codes of conduct, internal audit reviews or other management reviews.)

16. Do these processes monitor the company's ability to re-evaluate risks and adjust controls effectively in response to changes in its objectives, its business, and its external environment?

17. Are there effective follow-up procedures to ensure that appropriate change or action occurs in response to changes in risk and control assessments?

18. Is there appropriate communication to the Board (or the appropriate Board committee) on the effectiveness of the ongoing monitoring processes on risk and control matters? This should include reporting any significant failings or weaknesses on a timely basis.

19. Are there specific arrangements for Management to monitor and report to the Board (or the appropriate Board committee) on risk and control matters of particular importance? These could include, for example, actual or suspected fraud and other illegal or irregular acts, or matters that could adversely affect the company's reputation or financial position.

Appendix M – Providing Commentary on Risk Management and Internal Controls

1. The commentary relating to the application of Principle 11 of the Code and its accompanying guidelines[9] should include an acknowledgement by the Board that it has the responsibility of overseeing the company's system of risk management and internal controls and for reviewing its adequacy and effectiveness. It should further elaborate that such a system is designed to manage rather than eliminate the risk of failure to achieve business objectives, and can only provide reasonable and not absolute assurance against material misstatement or loss.

2. The Board should summarise the process (where applicable, through the appropriate Board committee) which it has applied in reviewing the adequacy and effectiveness of the system of risk management and internal controls. It should also disclose the process it has applied to deal with material internal control aspects of any significant problems disclosed in the annual report and accounts.

3. The Board should ensure that its disclosures provide meaningful, high-level and accurate information that allows relevant stakeholders to make an informed decision on how well the company is managing its risks. The Board may also wish to provide additional information in the annual report and accounts to assist understanding of the company's risk management processes and system of internal controls.

4. Companies should keep the commentary concise and focussed, with appropriate references to the supporting description of the company's internal control framework and risk management systems.

Receiving Assurance from the CEO and CFO

5. The Audit Committee Guidance Committee[10] (ACGC) guidebook already advocates that the CEO and CFO should sign an undertaking confirming their responsibilities for internal controls, as follows:

    - establishing and maintaining internal controls;
    - designing the internal controls to ensure that material information relating to the company is disclosed on a timely basis for the purposes of preparing financial statements; and
    - evaluating the effectiveness of the company's internal controls as at the end of the financial year and reporting the conclusion to the Audit Committee.

[9] Other than the provisions of Principle 11 of the Code and its accompanying guidelines, the SGX-ST Listing Manual also contains provisions regarding the Board's reporting obligations in respect of the adequacy of internal controls (addressing financial, operational and compliance risks). In this regard, reference may be made to SGX-ST's advisory note dated 16 April 2012, whereby SGX-ST issued guidance to issuers' boards on compliance with such reporting requirements.

[10] Audit Committee Guidance Committee Guidebook for Audit Committees in Singapore, October 2008.

6. In this regard, Guideline 11.3 of the Code also provides that the Board should comment on whether the CEO and CFO have provided the Board with assurance on the integrity of the financial records / statements, as well the effectiveness of the company's risk management and internal control systems.

Risk Governance Guidance for Listed Boards