Risk management and internal controls

MCCG Intended Outcome 9.0
Companies make informed decisions about the level of risk they want to take and implement necessary controls to pursue their objectives.

The board is provided with reasonable assurance that adverse impact arising from a foreseeable future event or situation on the company’s objectives is mitigated and managed.

MCCG Practice 9.1
The board should establish an effective risk management and internal control framework.

MCCG Practice 9.2
The board should disclose the features of its risk management and internal control framework, and the adequacy and effectiveness of this framework.

The internalisation and application of the content “Why” and “How” should be read in tandem with the line of sight outlined by the Intended Outcome.

Why
The case for change

Risk management and internal controls are often repeated buzzwords of regulators and corporate governance commentators alike. Although there is widespread agreement that the practice of risk management and internal controls is beneficial, such concepts are often perceived as elements that are disrupting the spirit of entrepreneurship while advocates of risk management and internal controls are often viewed with suspicion by frontline staff, who view them as “wet blankets”.

The diagram on the following page is commonly used to illustrate the relationship between entrepreneurship and risk management, and how they are complementary and not mutually exclusive.

What could go wrong:

- Failure to detect unknown risk exposures or “blind spots”.
- Inability of the company to adapt to changing business circumstances.
- Inability of the company to contain high impact risks in a timely manner, resulting in adverse consequences to the company’s value-creation.
Therefore, running a business with an appropriate risk management and internal control framework can be equated to driving fast whilst equipped with brakes.

Some of the benefits of risk management and internal controls are as follows:

- sharpens corporate strategy and heightens strategic focus;
- frees up capital to be invested in activities with higher returns;
- reduces costs;
- improves the risk finance portfolio;
- improves regulatory and legal compliance; and
- enhances reputation and the company’s attractiveness to investors.

**Point for reflection**

**Is risk management necessary?**

The 9/11 attack caused significant and tragic loss of lives. Beyond that, damage to property and business was immense, with one estimate of US$3.2 billion alone for information technology infrastructure and assets (servers, workstations, storage, hubs and wiring) belonging to securities firms impacted by the attacks.

**Did it:**

American Express Bank: The Bank operated a network of servers on a “hot backup” basis. Although headquartered at the World Trade Centre, it lost neither a transaction nor was its customer service interrupted.

**Did not do it:**

The Pentagon: The Pentagon had a secure server and the back-up of this server was located just down the hall. Needless to say, neither survived the attack.

---

1 Estimate on the Impact of the World Trade Centre Disaster to the Securities Industry’s Technology Infrastructure 2001, TowerGroup
The practice in substance

As with the MCCG, the Companies Act 2016 and Bursa Securities Listing Requirements outline prescriptions on internal controls and risk management.

**Section 246(1) of Companies Act 2016**

The directors of a public company or a subsidiary of a public company shall have in place a system of internal control that will provide reasonable assurance that –

(a) the assets of the company are safeguarded against loss from unauthorized use or disposition and to give a proper account of the assets; and

(b) all transactions are properly authorized and that the transactions are recorded as necessary to enable the preparation of true and fair view of the financial statements of the company.

**Paragraph 15.12(1) of Bursa Securities Listing Requirements**

Without limiting the generality of paragraph 15.11 above, a listed issuer must ensure an audit committee, amongst others, discharges the following functions:

(1) review the following and report the same to the board of directors of the listed issuer:

(b) with the external auditor, his evaluation of the system of internal controls;

e) the adequacy of the scope, competency and resources of the internal audit function and that it has the necessary authority to carry out its work; and

(f) the internal audit plan, processes, the results of the internal audit assessments, investigation undertaken and whether or not appropriate action is taken on the recommendations.

Note: Only requirements pertaining to internal controls and internal audit function are extracted from the said Paragraph.

**Paragraph 15.23 of Bursa Securities Listing Requirements**

A listed issuer must ensure that the external auditors review a statement made by the board of directors of a listed issuer pursuant to subparagraph 15.26(b) below, with regard to the state of risk management and internal control of the listed issuer and report the results thereof to the board of directors of the listed issuer.

---

2 Requirement for audit committee to have written terms of reference
Paragraph 15.26(b) of Bursa Securities Listing Requirements

A listed issuer must ensure that its board of directors makes the following additional statements in its annual report:

(b) a statement about the state of risk management and internal control of the listed issuer as a group.

Note: Only requirements pertaining to disclosure on risk management and internal control are extracted from the said Paragraph.

Enumerations in this regard for financial institutions are encapsulated in Bank Negara Malaysia’s Policy Document on Corporate Governance.

It is helpful to view risk management and internal controls in the context of governance and how each element relates to the other:

The company’s governance framework is always the starting point for its risk management and internal control processes. This is simply because the board will articulate the company’s strategy, set the values and shape its culture.

These elements will influence the company’s risk management appetite and in turn, the risk management appetite will dictate the kind of controls the entity will integrate into its business processes.

As such, risk management and internal controls should not be viewed as “wet blankets” but rather as important lines of defence, as follows:

---

3 Paragraphs 3, 7 and 12 of Appendix 1, Bank Negara Malaysia’s Policy Document on Corporate Governance
A number of methodologies have been developed to help companies approach risk management and internal controls in a systematic manner. Some of these have been widely accepted and include the following:

- ISO 31000 on principles and guidelines for risk management;
- The internal control environment framework suggested by the Committee of Sponsoring Organisations of the Treadway Commission (the “COSO framework” which is now known as “Internal Control – Integrated Framework”); and
- Other globally recognised internal control and risk management frameworks developed by professional organisations (e.g. Criteria of Control Framework developed by the Canadian Institute of Chartered Accountants or widely known as “CoCo Framework” and KPMG’s Risk Management Methodology).

Examples of key aspects contained in a frame of reference to drive the governance of risk management and internal controls in a systematic manner is outlined on the following page.
Corporate Governance Guide
Pull-out II
Guidance on Effective Audit and Risk Management

Risk strategy and appetite
Conscious collective decision to use risk management to support strategic objectives. It includes risk appetite statements and tolerance limits.

Risk governance
A structure through which the company directs, manages and reports its risk management activities. It encompasses clear roles and responsibilities, decision rights, the risk governance operating model, and reporting.

Risk assessment and measurement
Tools and techniques to identify, measure and quantify current and emerging risks. It allows companies to consider the extent to which potential events may have an impact on achievement of objectives.

Risk management and monitoring
Management’s risk strategies and responses to manage risks and improve risk and business performance. Continuous monitoring against established metrics permits proactive and timely response where warranted.

Risk reporting and insights
Reporting of risk information provides insights on significant risks and the strengths and weaknesses in managing them. Disclosure of risk management information to key stakeholders also supports timely decision-making.

Data and technology
Information and associated storage and delivery mechanisms which provide management with a real time view of the key risks and how these are being managed (including risk register).

Risk culture
Values and behaviours that shape risk decisions. Risk culture influences the decisions of management and employees. A strong risk culture helps to encourage strategic decisions and long term value for all stakeholders.

Adequacy and effectiveness review
Internal processes by which management and the Board derive assurance on the overall adequacy and effectiveness of the internal control and risk management systems.

Source: KPMG’s risk management framework
Point for reflection

How much is too much, how little is too little?
Not only are risk management and internal controls important, getting the right balance can be challenging. Examples of real case scenarios are highlighted below:

Example I (Trustee company)

At a trustee company, the board was so risk averse that practically every transaction carried out on behalf of a beneficial owner required the CEO’s signature. As the CEO was frequently away on business, this disrupted day-to-day efficiency and eventually, operational staff resorted to “breaking the law” and proceeding with transactions without the CEO’s authorisation.

Whilst it may seem innocuous, this could have unnecessarily exposed the company to claims by clients if transactions were erroneously carried out.

Example II (Financial institution)

At a major financial institution, the board exercised a high level of controls for investments in equities and debt by the bank’s dealing team, and this has been documented in the bank’s limits of authority matrix. Somewhat inexplicably, the same matrix grants the senior management team with unlimited authority on operational expenses.

Needless to say, the bank was soon caught in a fraud incident amounting to millions of ringgit, perpetrated through the loophole in the matrix.

Whilst the board remains responsible over risk management and internal controls, the task of scrutinising the framework (i.e. its design and effectiveness) is often taken up by a board committee, typically the risk management committee and the audit committee. In some entities, these committees are combined. It is pertinent for the committee members to have sound knowledge of risk management and internal control concepts, and to be able to assess risks in an objective manner – given the elements of self-interest and pressure to achieve returns, representations made by management may not represent the true picture.

Key considerations relating to the application of these Practices (Practices 9.1 and 9.2) are discussed below:

What are the practical ways to embed a risk aware and control optimised culture in companies?

Risk management is often an unwritten process particularly during a company’s start-up phase of its life. As the company progresses along its life cycle and the number of stakeholders increase, risk management and internal controls should receive appropriate consideration and be embedded as part of the company’s culture.
Some guidance are provided below:

- Establishing an effective and well-designed internal control system that takes into account the nature and circumstances of the company. This will support the objective of managing identified risks in the company;

- Designating a section on risk in board papers on proposals, investments, etc. This promotes a culture of risk awareness and can assist directors in identifying “blind spots”;

- Having a well-supported internal audit function. The internal audit function is regarded as a key line of defence after day-to-day management and bolsters the defence provided by the risk management function. Hence, it can greatly benefit the company by way of advising the board on where it can minimise avoidable losses; and

- Taking small steps can help to inculcate a risk aware culture over time. For example, it is customary for construction companies to hold a “toolbox talk” prior to commencement of work. Such talks focus on safe working practices and hazards to look out for.

Examples of questions to be posed to management on controls and compliance are outlined in Appendix V of this Pull-out.

What are the key considerations that should be taken into account in establishing an adequate and effective internal control and risk management framework?

An adequate and effective internal control and risk management framework provides companies with a structured approach to implement, monitor, review and improve internal control and risk management in tandem with the changing business circumstances.

Examples of overarching components and key considerations that should be taken into account in establishing an adequate and effective internal control and risk management framework are outlined on the following page.
Five components of an internal control and risk management framework

Note: The term “objectives” in the explanations below refers to the objectives relating to operations, reporting and compliance.

1. The company demonstrates commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The company demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The company holds individuals accountable for their internal control responsibilities in the pursuit of its objectives.
6. The company specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to its objectives.
7. The company identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.
8. The company considers the potential for fraud in assessing risks to the achievement of its objectives.
9. The company identifies and assesses changes that could significantly impact the system of internal control.
10. The company selects and develops control activities that mitigate risks to acceptable levels.
11. The company selects and develops general control activities over technology to support the achievement of its objectives.
12. The company deploys control activities through policies that establish what is expected and in procedures that put policies into action.
13. The company obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The company internally communicates information, including its objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The company communicates with external parties about matters affecting the functioning of internal control.
16. The company selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The company evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Source: Adapted from the COSO Internal Control – Integrated Framework

COSO is a framework that is developed by the International Committee of Sponsoring Organizations of the Treadway Commission to guide companies in designing, implementing and evaluating internal controls in response to the risks that are being faced by the company.
How can the board assess the adequacy and effectiveness of the risk management and internal control framework?

The board should define the processes to be adopted for its on-going monitoring and review, including specifying the requirements, scope and frequency for reporting and assurance. The board should form its own view on effectiveness and adequacy of the risk management and internal controls, based on the evidence it obtains.

The board’s assessment should, in particular, consider:

- the company’s willingness to take on risks (its “risk appetite”), the desired culture within the company and whether this culture has been embedded;
- the operation of the risk management and internal control systems, covering the design, implementation, monitoring and review, and identification of risks and determination of those which are principal to the company;
- the integration of risk management and internal controls with considerations of strategy and business model, and with business planning processes;
- any changes since the last 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 work of its internal audit and risk management (where applicable) units and other assurance providers;
- the extent and frequency of the communication relating to the results of the monitoring, to the board [or board committee(s)];
- the incidence of significant control failings or weaknesses that were identified at any time during the period and their impact on the company’s performance or condition (financial or otherwise); and
- any events that impacted the achievement of objectives that were not anticipated by management.

---

What are the common pitfalls that should be avoided in the management of risks?

The following are some of the issues the board should be wary of:

**Common pitfalls in risk management:**

- box-ticking rather than business-led assessment of risk approach;
- failure and/or the inability to prioritise principal risks in relation to their mitigating measures leading to unidentified strategic risks turning into emerging risks without a preparedness to respond;
- risks are managed in silos and their impact is not considered across business units and functions;
- inadequate attention is given to the ever changing internal and external market environment;
- merely discussing risk issues without integrating them into the board’s own decision making process, since strategic risks can be difficult to identify;
- general failure to embed risk management in the culture and processes of the company and its workforce, leading to the lack of a sustainable risk identification system in place across business units and functions;
- there is no precise documented accountability for managing risks;
- level of investment is not always a reliable proxy for the level of enterprise risk;
- the board does not have a sense of assurance arising from risk management implementation; and
- bad news is not easily communicated to the top.

**Can internal controls be designed independently outside the risk management process?**

The design of internal controls in silos and without reference to their associated risks can lead to an imbalance and consequently, certain key risk areas may be left unaddressed. For example, too many controls (and thus, resources) are put in place over petty cash, which in the grand scheme of things is hardly material to a company’s survival.

**What are some of the more common ways in which a company’s appetite for risk can be articulated?**

Risk appetite must support a company’s risk management activities. Some companies prefer the distinction between risk tolerance (i.e. maximum risk that can be taken before financial distress) and risk appetite (amount of risk that is actually taken for risk reward benefits). Risk appetite is generally understood to be “how much risk a company is willing to take” as opposed to a maximum threshold before financial sufferings (i.e. risk tolerance). Risk appetite should be a sub-set of risk tolerance.
A company’s risk appetite can be articulated in the following ways:

**Common ways to articulate risk appetite (non-exhaustive):**

- **Setting a boundary on the “impact vs likelihood” grid**
  Established through the use of risk matrices where a risk appetite line is drawn to demarcate the boundary between those risks that are deemed to be “high” and those which are not. Typically identified through an “Enterprise Risk Management” process.

- **Economic capital measures/ balance sheet based expressions**
  Achieved by the ability to absorb losses by holding surplus capital against the desire to invest capital to generate a positive return. The higher the risk premium, the lower the appetite for risk.

- **Changes in credit ratings**
  Based on probability of default by a rating agency, companies with “AA” rating may not wish to take any risks that may cause a downgrade to an “A” rating.

- **Profit and loss measures**
  Profit and loss based expressions, e.g. companies that set maximum loss figures.

- **Value based measures**
  Accomplished by setting limits around the volatility of share price or against a target share price. This allows companies to direct their attention to investments, projects and activities that are likely to achieve these targets/ limits.

- **Develop effective targets or thresholds for key risk indicators**
  The simplest method where the company sets a range of key risk indicators (monitors changes in exposure to a specific risk event), key control indicators (monitors to determine whether specific controls are operating effectively) and key performance indicators (“KPIs”) (monitors to keep track on the financial performance or operational efficiency). Examples of common risk indicators are outlined in Appendix VI of this Pull-out.

- **Qualitative statements**
  Expressions of statements that cannot be articulated numerically. Also applied to areas of risk that are difficult to quantify effectively, such as reputation risks. Often easy to understand and communicate and integrate within the organisation’s culture or statement of values, e.g. “We have zero tolerance for fraud”.

An illustrative non-exhaustive list of risk appetite threshold (quantitative and qualitative) is provided below:

<table>
<thead>
<tr>
<th>Measure</th>
<th>Risk Appetite (Variance Range)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue</td>
<td>1% - 2.5%</td>
</tr>
<tr>
<td>Earnings per share</td>
<td>3% - 5%</td>
</tr>
<tr>
<td>Cash flow</td>
<td>5% - 10%</td>
</tr>
<tr>
<td>Credit rating</td>
<td>To maintain grade of XX</td>
</tr>
</tbody>
</table>
What should be considered from a disclosure perspective?

The state of internal control system of the group (the listed issuer and its subsidiaries) is articulated primarily through the “Statement of Risk Management and Internal Control” within the listed issuer’s annual report. In essence, directors are to comment amongst others on the following:

- What are the features of the risk management process and internal control system – for example, how are risks identified? Were risks flagged during a workshop session or during a board session? How are risks, as they evolve, tracked and managed?
- Did the board assess the design of the risk management process and internal control system and test their effectiveness?
- If weaknesses surfaced during the process, how did the board treat such weaknesses? Were any deficiencies corrected?
- In summary, what does the board think of the risk management process and internal control system?

In making the Risk Management and Internal Control Statement, a listed issuer should be guided by the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers which is issued by the Taskforce on Internal Control (“SORMIC Guidelines”) with the support and endorsement of Bursa Malaysia Securities Berhad.

Paragraphs 41 and 42 of the said document which is reproduced on the following page outline the key elements that a listed issuer should provide in its narrative statement so as to enable stakeholders to make an informed assessment of the main features and adequacy of the listed issuer’s risk management and internal control system.

<table>
<thead>
<tr>
<th>Qualitative Measure</th>
<th>Risk Appetite (Target)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy efficiency</td>
<td>Reduce consumption per unit</td>
</tr>
<tr>
<td>Safety measures e.g. recorded accident rates</td>
<td>To achieve recordable case</td>
</tr>
<tr>
<td>Reputation exposures</td>
<td>Zero tolerance for negative press coverage or customer satisfaction improvements</td>
</tr>
<tr>
<td>Greenhouse gas</td>
<td>X% reduction per tonne</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Qualitative</th>
<th>Risk Appetite (Target)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>Reduce consumption per unit</td>
</tr>
<tr>
<td>Safety</td>
<td>To achieve recordable case</td>
</tr>
<tr>
<td>Reputation</td>
<td>Zero tolerance for negative press coverage or customer satisfaction improvements</td>
</tr>
<tr>
<td>Greenhouse</td>
<td>X% reduction per tonne</td>
</tr>
</tbody>
</table>

Qualitative Measure

- Risk Appetite
  - Energy: Reduce consumption per unit
  - Safety: To achieve recordable case
  - Reputation: Zero tolerance for negative press coverage or customer satisfaction improvements
  - Greenhouse: X% reduction per tonne
### Paragraph 41 of SORMIC Guidelines

In its narrative statement, the board should disclose the following:

- The main features of the company’s risk management and internal control system;
- The ongoing process for identifying, evaluating and managing the significant risks faced by the company in its achievement of objectives and strategies;
- That such process has been in place for the year under review and up to the date of approval of this statement for inclusion in the annual report;
- The process it (or where applicable, through its committees) has applied in reviewing the risk management and internal control system and confirming that necessary actions have been or are being taken to remedy any significant failings or weaknesses identified from that review;
- That a review on the adequacy and effectiveness of the risk management and internal control system has been undertaken;
- Commentary on the adequacy and effectiveness of the risk management and internal control system;
- The process it has applied to deal with material internal control aspects of any significant problems disclosed in the annual report and financial statements; and
- Where material joint ventures and associates have not been dealt with as part of the group for the purposes of applying these guidelines, this should be disclosed.

### Paragraph 42 of SORMIC Guidelines

In its narrative statement, the board should also include whether it has received assurance from the chief executive officer and chief financial officer on whether the company’s risk management and internal control system is operating adequately and effectively, in all material aspects, based on the risk management and internal control system of the company.

It should be noted that **Recommended Practice Guide 5 (Revised 2015)** by the MIA provides guidance for auditors in applying **Malaysian Approved Standard on Assurance Engagements, International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information** in the performance of a limited assurance engagement to report on the Statement on Risk Management and Internal Control.
Regional/international perspectives

Risk management and internal controls are well-established concepts and therefore, as in the case of Malaysia, many jurisdictions have long incorporated them into governance documents.

<table>
<thead>
<tr>
<th>Country</th>
<th>Provision(s)</th>
</tr>
</thead>
</table>
| Singapore      | 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 *(Principle 11)*.  

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 review can be carried out internally or with the assistance of any competent third parties.  

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 *(Guidelines 11.2 and 11.3)*. |
| Australia      | A listed entity should establish a sound risk management framework and periodically review the effectiveness of that framework *(Principle 7)*.  

The board or a committee of the board should:  
(a) review the entity’s risk management framework at least annually to satisfy itself that it continues to be sound; and  
(b) disclose, in relation to each reporting period, whether such a review has taken place. *(Recommendation 7.2)* |
<table>
<thead>
<tr>
<th>Country</th>
<th>Provision(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A listed entity should disclose:</td>
</tr>
<tr>
<td></td>
<td>(a) if it has an internal audit function, how the function is structured and what role it performs; or</td>
</tr>
<tr>
<td></td>
<td>(b) if it does not have an internal audit function, that fact and the processes it employs for evaluating and continually improving the effectiveness of its risk management and internal control processes.</td>
</tr>
<tr>
<td></td>
<td><em>(Recommendation 7.3)</em></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems <em>(Principle C.2).</em></td>
</tr>
<tr>
<td>South Africa</td>
<td>The governing body should exercise ongoing oversight of risk management and, in particular, oversee that it results in the following:</td>
</tr>
<tr>
<td></td>
<td>(a) An assessment of risks and opportunities emanating from the triple context(^6) in which the organisation operates and the capitals that the organisation uses and affects.</td>
</tr>
<tr>
<td></td>
<td>In addition, the following should be disclosed in relation to risk:</td>
</tr>
<tr>
<td></td>
<td>(a) An overview of the arrangements for governing and managing risk.</td>
</tr>
<tr>
<td></td>
<td>(b) Key areas of focus during the reporting period, including objectives, the key risks that the organisation faces, as well as undue, unexpected or unusual risks and risks taken outside of risk tolerance levels.</td>
</tr>
<tr>
<td></td>
<td>(c) Actions taken to monitor the effectiveness of risk management and how the outcomes were addressed.</td>
</tr>
<tr>
<td></td>
<td>(d) Planned areas of future focus. <em>(Recommended Practices 6 and 9 under Principle 11)</em></td>
</tr>
<tr>
<td></td>
<td>The governing body should assume responsibility for assurance by setting the direction concerning the arrangements for assurance services and functions. The governing body should delegate to the audit committee, if in pace, the responsibility for overseeing that those arrangements are effective in achieving the following objectives:</td>
</tr>
<tr>
<td></td>
<td>(a) Enabling an effective internal control environment. <em>(Recommended Practice 40 under Principle 15)</em></td>
</tr>
</tbody>
</table>

\(^6\) Triple context in the Report on Corporate Governance for South Africa 2016 refers to the economy, society and the environment.