

KPMG

MIoD Mauritius Institute of Directors

Mauritius Audit Committee Forum

Position Paper 3

# The Audit Committee's Role in Control and Management of Risk

December 2015

## About the Mauritius Audit Committee Forum

Recognising the importance of Audit Committees as part of good Corporate Governance, the Mauritius Institute of Directors (MIoD) and KPMG have set up the Mauritius Audit Committee Forum (the Forum) in order to help Audit Committees in Mauritius, in both the public and the private sectors, improve their effectiveness.

**The Position Paper 3 deals with the Audit Committee's role in control and management of risk.**

The purpose of the Forum is to serve Audit Committee members and help them adapt to their changing role. Historically, Audit Committees have largely been left on their own to keep pace with rapidly changing information related to governance, risk management, audit issues, accounting, financial reporting, current issues, future changes and international developments.

The Forum provides guidance for Audit Committees based on the latest legislative and regulatory requirements. It also highlights best practice guidance to enable Audit Committee members to carry out their responsibilities effectively. To this end, it provides a valuable source of information to Audit Committee members and acts as a resource to which they can turn for information or to share knowledge.

The Forum's primary objective is thus to communicate with Audit Committee members and enhance their awareness and ability to implement effective Audit Committee processes.

## Position Paper series

The Position Papers, produced periodically by the Mauritius Audit Committee Forum, aim to provide Board directors and specifically Audit Committee members with basic best practice guidance notes in running an effective Audit Committee.

This **Position Paper 3** deals with the Audit Committee's role in control and management of risk.

Previous Position Papers issued:

- **Position Paper 1** (July 2014) sets out the essential requirements that should be complied with by every Audit Committee in accordance with the National Code of Corporate Governance.
- **Position Paper 2** (May 2015) sets out how the Audit Committee can accomplish its duties through a collaborative relationship with two of the Assurance Providers, notably Internal and External Auditors.

### *Current Members of the Forum*

Collectively, the Forum is made up of the following members drawn from diverse professional backgrounds with significant experience in both the private and the public sectors.

| | |
|---|---|
| **Leung Shing** Georges - *Chairman* | **Gujadhur** Anil |
| **Bryce** Alastair | **Halpin** Paul |
| **Chung** John | **Koenig** Fabrice |
| **De Chasteauneuf** Jerome | **Molaye** Sanjay |
| **Dinan** Pierre | **McIlraith** Catherine |
| **Doorgakant** Vidula Darshini | **Ramdin** Madhavi |
| **Enouf** Maurice | **Tse Yuet Cheong** Philise |
| **Felix** Jean-Michel | **Ujoodha** Sheila |
| **Goburdhun** Khoymil | **Valls** Jane |
| *Secretary*: **Bishundat** Varsha | |

## Contents

1. Executive Summary 4
2. Responsibilities for Risk Management 5
3. Risk Identification and Assessment 7
4. Risk Monitoring and Assurance 9
5. Reporting 11

*Appendices*

Appendix 1: Risk indicators 13
Appendix 2: Key questions related to risk identification and assessment 14
Appendix 3: Example Risk Summary and Register 17



# 1. Executive Summary

Risk manifests itself in a range of ways and may have a positive and/or negative outcome for the entity. It is vital that those responsible for the stewardship and management of an entity are aware of the best methods for identifying and subsequently managing such risk.

The governance of risk requires principally the establishment and maintenance of effective systems of internal control. Internal control comprises all the policies, processes, tasks, behaviours and other aspects of an entity that, taken together, ensure, as far as practicable, the orderly and efficient conduct of business. This includes adherence to management policies, compliance with applicable laws including regulations, the safeguarding of assets, the prevention and detection of fraud and error, the accuracy and completeness of accounting records, and the timely preparation of Internal and External Audit reports. The "Internal Control Integrated Framework" (2013) and "Enterprise Risk Management-Integrated Framework" papers published by the Committee of Sponsoring Organisations of the Treadway Commission (COSO) establish the prerequisites for a proper internal control set up.

Apart from internal control, other methods used to manage risk include the transfer of risk to third parties, sharing of risk, contingency planning and the withdrawal from unacceptably risky activities. Entities can accept risk, but need to do so objectively and transparently and within the broad policy regarding risk appetite as approved by the Board.

The risks that entities face are constantly changing and the system of internal control should be responsive to such changes. Effective risk management and internal control depend on a regular evaluation of the nature and extent of risk and taking recommended actions to deal with it effectively.

## Control and Management of Risks

A Company is, in the ordinary course of business, exposed to several types of risk, some of which may have serious adverse consequences. Consequently, it is advisable to ensure that the risks are fully understood and controlled in a sustained and comprehensive manner.

A risk is any event, the consequences of which, should it occur, could be either to prevent an organisation from fulfilling its missions, holding its commitments, achieving its objectives, or to affect its people, assets, environment or reputation. The risk is measured in terms of impact and probability.

The Board is responsible for not only determining the risks that the Company is willing and able to take to achieve its strategic objectives but also ensuring that all the risks are properly identified, evaluated and managed.

In relatively simple businesses, it will be acceptable for risk management to be the direct responsibility of the Board rather than a Board Committee. However, where the scope and complexity of risks faced are significant, companies will, as mentioned in the Code of Corporate Governance for Mauritius, set up a separate Risk Management Committee (RMC) to develop, update, enforce and monitor enterprise-wide risk management. The RMC focuses typically on broad risks at the strategic, operational and management levels, which have potential financial and non-financial consequences. Moreover, by virtue of the Bank of Mauritius regulations, Banks are required to have a separate RMC.

This Paper is aimed towards companies with no separate RMC, i.e., those in which the Audit Committee also assumes the responsibilities of the business risk. The Audit Committee's role is thus expanded from its normal outlook into the Company's historical financial performance, abiding by the existing compliance and control requirements, to a broader consideration of future performance and risk.

The management of risk requires the adoption of the right behaviour (4T) in the face of risk:

- **Take** the risk, when it is tolerable and insignificant
- **Treat** the risk when it can be reduced by internal control
- **Transfer** the risk when it is too high and it can be transferred to say a bank, insurance
- **Terminate** the risk when it is too high, cannot be reduced and is beyond the risk appetite

A Company's risk profile is continually changing due to internal and external circumstances. Effective risk management and internal control are therefore reliant on a regular evaluation of the risk and the adequacy and timeliness of risk management systems in place.

Successful risk management is the process that achieves the most efficient combination of controls necessary to provide *reasonable assurance* that the Company's mission, commitments and objectives can be achieved safely and reliably.



# 2. Responsibilities for Risk Management

Boards are ultimately responsible for maintaining sound risk management and internal control systems. However, the task of establishing, operating and monitoring such systems is, as a matter of course, delegated to Management.

The Board should thus ensure that Management set up appropriate systems that function effectively to manage the risk and so reduce it to an acceptable level.

As it is essential that the right tone is set at the top, the Board should send out a clear message that risk and control responsibilities must be taken seriously. In determining a sound system of risk management and internal control, the Board should consider the:

- Nature and extent of the risk facing the Company;
- Extent and categories of risks acceptable for the Company to bear (risk appetite);
- Impact and likelihood of risk materialising;
- Company's ability to reduce the incidence and impact of materialised risk;
- Cost of control relative to the benefit obtained in managing the related risk.

A template for the assessment of risk is at Appendix 2.

## Oversight

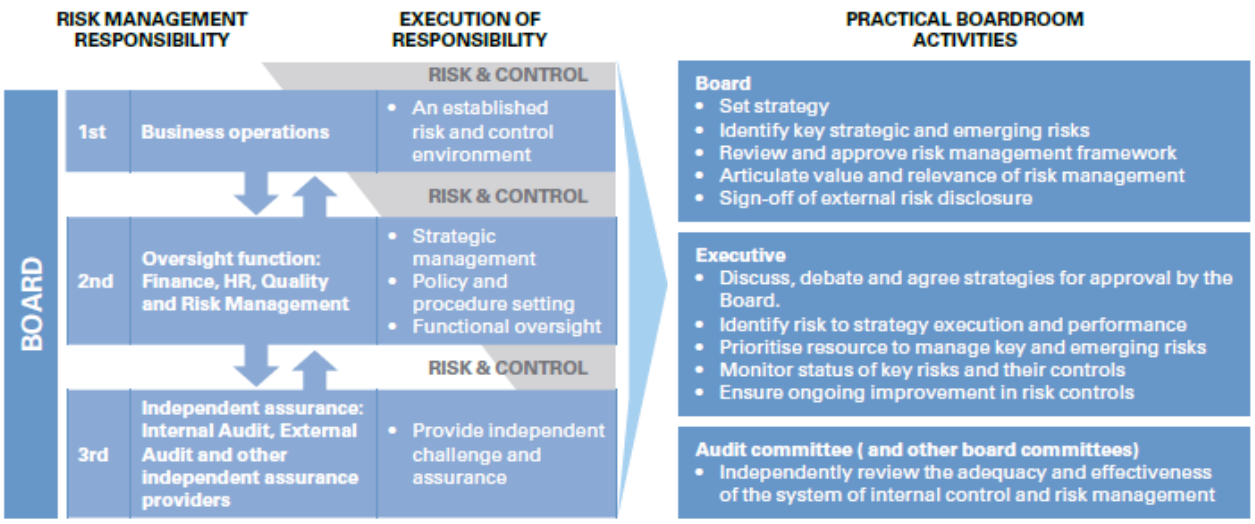
Reviewing the effectiveness of internal control and risk management systems is an essential part of the Board's overall responsibility, with aspects of the review work usually delegated to the Audit Committee.

### Audit Committee versus Board /Board Committee: Who oversees what risks?




This diagram illustrates who is responsible for overseeing which risks in the ordinary course of business. The Audit Committee's traditional responsibility for overseeing financial reporting risks is depicted in the top left triangle. The Board must clarify the responsibilities for non-financial risks, depicted in the lighter blue, deciding whether a dedicated Board committee or the Board itself will oversee these risks. Where the Audit Committee does not oversee all aspects of risk, processes should be put in place, as denoted by the black boxes, to ensure that it is informed of those other risks that may have financial reporting implications.

The precise role of the Audit Committee in the review process should be for the Board to decide and will depend upon factors such as its size, skills-availability and composition; the scale, diversity and complexity of the Company's operations and significant risks.




The Audit Committee's role is a non-executive function that aims to satisfy itself that Management has properly fulfilled its responsibilities, as well as with:

- The degree to which Management has assumed ownership for risk and control;
- How key business risks are identified, evaluated and managed;
- Whether the controls are fit for purpose and are working as intended;
- The rigour and comprehensiveness of the review process.

By asking probing questions, the Audit Committee can help bring clarity to the process used to manage risk, and to the assignment of accountabilities to monitor and react to changes in the Company's risk profile.

Whilst overseeing the risk management functions, the Audit Committee members are expected to demonstrate key attributes such as analytical and creative skills and possession of broader business experience, in addition to financial expertise.

## Management's responsibility for risk management

Management should be delegated the responsibility to design, implement and monitor the risk policy and management plan (the Plan) to be considered and approved by the Board. Thereafter,

- Management executes the Plan, which specifies the roles and responsibilities for risk management.
- Management is accountable for monitoring the systems of the Plan and integrating these into day-to-day activities. The Board should thus ensure that Management has the organisational structures and resources for appropriate execution of risk management processes and the necessary support to perform its duties and responsibilities outlined in the Plan.
- Although a Chief Risk Officer (CRO) may be appointed to assist the Chief Executive Officer (CEO) with the execution of the Plan, accountability to the Board remains with the CEO. Moreover, the carrying out of risk management should be a team-based approach, with all employees having some responsibility in implementing the policies on risk and internal control.

Risk management should be intrusive: its methods and techniques should be entrenched within strategy setting, planning and business processes, to safeguard performance and sustainability. The rigours of risk management should provide responses and interventions that attempt to create an appropriate balance between risk and reward.



# 3. Risk Identification and Assessment

Many different processes and methods are used to identify risk, i.e. risk workshops, interviews, market research and intelligence, control, risk self-assessments, whistle-blowing, and so forth. At a minimum, a risk assessment should result in the:

- Identification of relevant risks involved in the achievement of objectives;
- Prioritisation of risks, which often requires estimating the timing, scale, probability and likely impact of risks occurring.

This involves the following steps:

### Step one: Strategic business objectives

The most important aspect of risk management is the effective identification of the major risks that may influence the entity achieving its strategic business objectives. The risk assessment process should therefore start with the identification of the entity's strategic intent. It is also imperative that its business, operational and management strategies be mapped, since different strategies may expose the entity to different types of risk.

### Step two: Identification

The use of a structured approach for identifying risk comprehensively, and which focuses on the entity's objectives and its chosen strategies while exploring all the areas of its business, is recommended.

To ensure appropriate consideration of all potential threats and opportunities, it is imperative that the process of risk identification is separated from that of its quantification. If this is not done, then potential catastrophic risk events or material opportunities may be discarded before they are adequately considered simply because of their perceived low probability of occurrence. Negative events are often referred to as "black swan" events.

The process of risk management should include all risks that threaten the goals of the entity, irrespective of whether they are controllable or not.

The following should be formally recorded:

- Description of the risk;
- The root causes or factors that shape it;
- A qualitative description of the risk's potential consequences if it occurs.

### Step three: Risk prioritisation

Having identified the risk, the next step is to quantify its potential effects. Each identified risk should be assessed in terms of its impact, as well as the likelihood that the risk will materialise at that level.

It is important to use a methodology that enables risk to be prioritised in terms of 'inherent' risks and 'residual' risk that the entity is exposed to.

**Inherent risks** are those that exist before the effect of mitigating management action is taken into account; i.e. the entity is exposed to those risks by the mere fact of operating its particular business.

**Residual risk** is the level of exposure remaining after the application of controls.

The assessment of the inherent and residual exposure levels allows both Management and Internal Audit to prioritise the risks, and also to focus their attention and resources on those that, should they occur, would have the greatest impact.

In addition, the perspective gained from the analysis of inherent and residual risk will, together with a consideration of the entity's risk appetite and tolerance levels, influence Management's choice of risk response. This is where the entity wishes to direct its efforts and resources to manage risk down to an acceptable level of residual risk.

Failure to anticipate and react to risks can have a catastrophic impact. This includes risks that are systemic (whether local, regional or global), and also risks that are generally considered to be unpredictable. The Board should ensure that the frameworks and processes for anticipating these have the following characteristics:

- **Insight:** the ability to identify the cause of the risk, where there are multiple causes or root causes that are not immediately obvious.
- **Information:** comprehensive information about all aspects of risk and risk sources, especially of financial risk;
- **Incentives:** the ability to separate risk origination and risk ownership to ensure suitable due diligence and accountability;
- **Instinct:** the ability to make a predictable response when there are systemic and pervasive risks;
- **Independence:** the ability to view the entity independently from its environment;
- **Interconnectivity:** the ability to identify and understand how risks are related, especially when their relatedness might exacerbate the risk.

**It should be clear that setting out the correct strategic objectives, comprehensive identification of risks and preventing them from happening, relies extensively on the skills of the members of the Audit Committee, especially where the latter also assumes the responsibilities that normally pertain to the RMC of a company.**

Questions that may lead to the identification of risk are at Appendix 2.

**Review risk assessment process**

The Audit Committee should review the process by which the entity's significant risks are identified and ensure that the Board is fully apprised of these risks. The Audit Committee should clearly scrutinize the risk register that results from the processes for risk identification and assessment.

Risk identification should be carried out in a systematic manner. There are a number of methodologies available to achieve a structured prioritisation of the risks confronting the entity.

**Risk register**

Risk identification should take an enterprise-wide view of the risk spectrum. This implies that the resultant risk register should reflect a balanced, thorough and credible profile of key risks. It should reflect the reality of the company's risk profile with no preconceived bias or weighting towards a particular category of risk. Non-core activities and assets must be included. The risks facing all business units, processes, regions, services, brands, customers, changes, timing issues and suppliers need to be incorporated.

A risk register can take any number of forms but should record at least a description of each risk, the associated business process and objective, along with a description of probable implications. The likelihood of the risk occurring and its potential impact should be quantified on a consistent basis. A risk register should reflect a balanced view of risks across the business spectrum, weighted in ranking according to the degree of threat and likelihood of the risk.

It is important for Management to indicate the current controls and interventions for the identified risks. A desired level of control can be indicated, but invariably an action plan for every key risk is required in order to improve the degree of risk protection or enhance the opportunities arising from the risk in question. A risk register that has a bias towards a particular area of risk, such as insurance of finance, should be questioned.

Appendix 1 lists some of the risk indicators that can help an entity to identify risks and plan better to protect against them.

Appendix 2 provides a number of high level questions that the Board or its committees may wish to consider when framing their discussions with Management in this regard. The list is not exhaustive and will require tailoring based on the particular circumstances of the organisation as well as the terms of reference of the Committee.

Appendix 3 presents an example risk summary and register designed to give Audit Committee members a quick insight into a small number of key risks and the effectiveness of the controls in place. It also includes the quantification criteria for the likelihood of a risk materialising and its impact.



# 4. Risk Monitoring and Assurance

Procedures for monitoring the appropriateness and effectiveness of the identified controls should be embedded within the normal operations of the entity. While effective monitoring throughout is an essential component of a sound system of internal control, the Board cannot rely solely on embedded monitoring processes to discharge its responsibilities. The Board, with the assistance of the Audit Committee, should make it a duty to regularly receive and review reports on internal control and be informed about how the reviews giving rise to the reports have been undertaken.

The Audit Committee should define the process to be adopted for its review of the effectiveness of internal control. As part of its assessment, the Audit Committee should obtain from Management an overview of the risks facing the organisation, together with the policies, procedures and controls in place to mitigate such risks.

The Audit Committee should receive information that is manageable; this should not be so voluminous as to deter a proper understanding of the key risks. It is more important that the Audit Committee gains meaningful insight into the key sources of risk and how effectively such risks are being managed, rather than getting entangled, without adequate focus, with a long list of every imaginable risk facing the business.

### Ongoing review process

**It is essential to have a frank, open dialogue between Management and the Audit Committee on matters of risk and control.**

The reports from Management, and/or others qualified to prepare them in accordance with agreed procedures, should provide a balanced assessment of the significant risks and the effectiveness of the system of internal control in the areas covered. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact they have had, could have had, or may have on the entity, and the actions taken/being taken to rectify them.

When reviewing reports, the Audit Committee should consider:

- What the significant risks are and assess how they have been identified, evaluated and managed. The significant risks threatening the attainment of business objectives should have been identified, assessed and controlled within the Board's defined risk tolerances.
- The effectiveness of the related system of internal control in managing the significant risks, having regard in particular to any significant failings or weaknesses that have been identified, reported or dealt with.
- Whether appropriate action is being taken on a timely basis, as and when risks materialise, to remedy any significant failings or weaknesses. It is not sufficient for the Audit Committee to satisfy itself that weaknesses are being identified; it must also consider the remedial actions taken and whether such steps are appropriate and timely.
- Whether the findings indicate a need for more extensive monitoring or reinforcement of the internal control system. Where a weakness identified in one area of the organisation may be duplicated in other areas, it may be appropriate for the Audit Committee to seek a more comprehensive review.

### Periodic assessment exercise

The assessment review should be performed periodically on a timely and regular basis. It should consider the issues dealt with in the reports, together with additional information necessary to ensure that the Board has taken account of all significant aspects of internal control for the Company's accounting period and the period up to the date of approval of the annual report and financial statements.

### Monitoring special circumstances

The risk profile of any company can also change as a result of its stage in the growth cycle. To illustrate, two very common examples may be highlighted – a fast-growing entrepreneurial company and a company expanding globally through mergers, acquisitions and re-organisations.

*Emerging companies*

Fast-growing entrepreneurial companies often lack a formalised management structure and may not have well-established corporate governance programmes. Policies, procedures, and processes may be evolving haphazardly to meet demands. In addition, the dominant role of an individual executive may overshadow the need to foster a strong control environment and can potentially affect the orderly financial reporting and audit processes. As companies grow, a more standardised corporate governance process becomes a necessity, regardless of the entity's public aspirations.

For companies considering an initial public offering, the need for a formalised structure becomes obvious. While risks represent important issues in today's market place for public companies, they are equally relevant to entrepreneurial and other companies that remain private. Responding to these risks is equally important to companies that wish to deter fraud and improve the quality of their corporate reporting.

Dominant or autocratic Management can also be a cause for concern in an established company. Such leadership can put a strain on the enterprise's controls and corporate governance processes and set the wrong tone from the top. Ensuring that Management fosters an atmosphere that supports a strong control environment is a core Audit Committee responsibility.

*Complex corporate structures*

Mergers, acquisitions and re-organisations often involve melding organisations not only with distinct corporate cultures but also from different industries and different areas of the world. In today's business environment, companies frequently cross borders for every aspect of their business. This environment presents Management and the Audit Committee

with unique oversight challenges. While governance practices in such environments are evolving, the influence of different cultures needs careful consideration.

For the Audit Committee, many questions will need answers:

- How are Management's reporting, control and compliance responsibilities integrated?
- Is there effective global oversight of local boards?
- How should the Committee evaluate domestic and international audit results, both internal and external?
- How does Management determine the Company's compliance with various countries' rules and regulations?

Re-organisation often means downsizing and outsourcing, and downsizing often means that companies remove or weaken controls. As companies focus on core competencies, they often outsource non-core activities and specialised skills to third party providers. The question then arises: have they carefully evaluated the ongoing internal control impact of such decisions?

Audit Committees' responsibilities do not stop at national or organisational boundaries but extend to the organisation as a whole. Audit Committees of parent companies and subsidiaries should coordinate and communicate with one another. They should have a common appreciation of the control frameworks and cultures of the entities, and undertake substantial sharing of information to combat the inherent risk that a single unmonitored risk in one entity or in a particular country can spread out to and affect the entire organisation.



# 5. Reporting

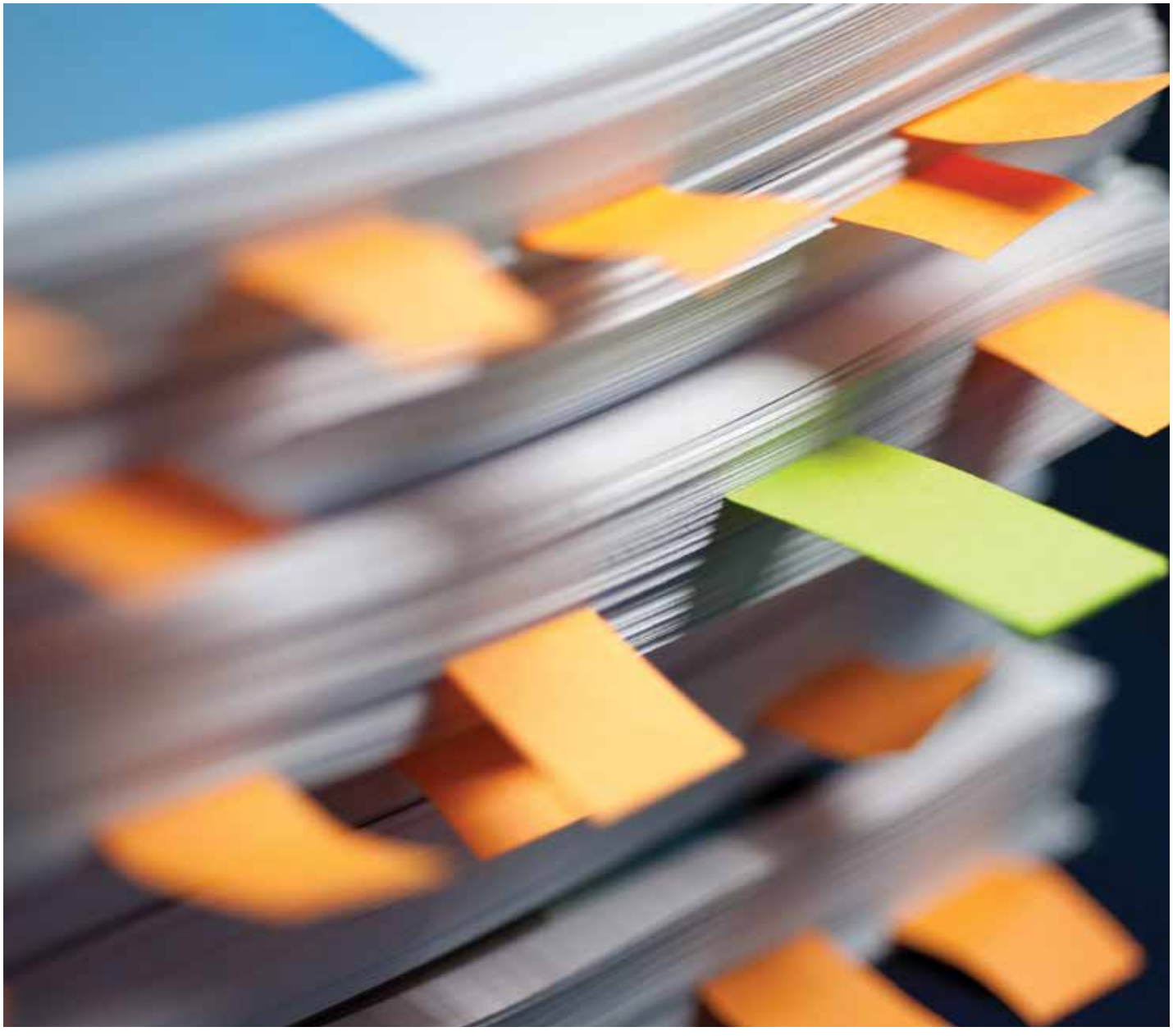
The Audit Committee should report to the Board its deliberations on the monitoring of the effectiveness of internal control and risk management systems. The Board will then need to form its own view on effectiveness based on the information and assurances provided by the Audit Committee, exercising the standard of care generally applicable to directors in the performance of their duties.

### External reporting

The Audit Committee needs to be cognizant of any external reporting requirement relating to risk and control, whether that is private reports to regulators or disclosure in the annual report and financial statements. The Committee should ensure that it is provided with appropriately documented support for any risk and/or internal control statements/reports it (or the Board) is required to make.

"***Audit Committee reports should form part of the conversation between companies and investors building confidence in this important area of governance and showing how it contributes to good financial reporting"***

(Sue Harding, director of the Financial Reporting Lab)



# Appendices

# Appendix 1: Risk indicators

The following are examples of risk indicators:

| | |
|---|---|
| Inappropriate 'tone at the top' | Excessive or inappropriate performance-based remuneration |
| Frequent organisational changes | Over-ambitious growth goals |
| High turnover of senior Management | Lack of transparency in the business model |
| Lack of succession plans | Exposure to rapid technological changes |
| Inexperienced Management | Industry downturns |
| Lack of Management oversight | Interest rate and currency exposures |
| Autocratic Management | Overly complex organisational structures of transactions |
| Untimely reporting and responses to Audit Committee inquiries | Late surprises |
| On-going or prior investigations by regulators and others | Continuous loss-making operations |
| Cash flow problems | Poor financial position |



# Appendix 2: Key questions related to risk identification and assessment

In view of the different approaches Boards may take in referring powers to the Audit Committee in respect of business risk management and the adequacy of the control framework, it is vital that there is an unambiguous understanding of what the Board of Directors, other Board Committees and the Audit Committee are responsible for in this important area of corporate governance. The Audit Committee's responsibilities should be reflected in its terms of reference.

So as to meet its responsibilities under its terms of reference, the Audit Committee needs to assess whether it is receiving appropriate risk management information regularly enough and in a format that meets the needs of members. It needs to evaluate at least annually the adequacy and timeliness of Management reporting on financial, non-financial, current and emerging risk trends. The Audit Committee needs also to discuss risk management with Senior Executives, Internal and External audit. The scope of those discussions should have reference to the Audit Committee terms of reference enhanced by the added responsibility to manage business risk.



The following are high-level questions the Audit Committee may like to consider in framing discussions with Management. The list is not exhaustive and will require tailoring based on the Audit Committee's terms of reference as well as the particular circumstances of the Company.

| Risk management framework | Evaluation of risk management framework |
|---|---|
| **Risk strategy:** the approach for associating and managing risks based on the organisation's strategies and objectives. | • What are the risks inherent in our business strategies and objectives?<br>• How is our risk strategy linked to our business strategy?<br>• Is our risk management policy clearly articulated and communicated to the organisation? If not, why not? If yes, how has this been achieved?<br>• Is our risk appetite (the amount of risk the organisation is willing to take) clear? How is it linked to our objectives?<br>• How has the Board's perspective on risk permeated the organisation and culture? |
| **Risk structure:** the approach for supporting and embedding the risk strategy and accountability. | • Is there a common risk management language / terminology across the organisation? If not, why not and how should the situation be remedied?<br>• Is accountability for risk management transparent at the Management level? If not, why not? If yes, describe how this has been achieved.<br>• Are risk management activities / responsibilities included in job descriptions?<br>• How do our performance management and incentive systems link up to our risk management practices? |
| **Measuring and monitoring:** the establishment of Key Performance Indicators (KPIs) and continuous measuring and improving of performance. | • Are risk owners clearly identified? If not, why not. If yes, how?<br>• Are there systems in place for measuring and monitoring risks?<br>• How are risks, including suspected improprieties, escalated to the appropriate levels within the organisation?<br>• How is the risk management framework linked to the organisation's overall assurance framework? |
| **Portfolio:** the process for identifying, assessing and categorising risks across the organisation. | • Does a comprehensive risk profile exist for the organisation? If not, why not?<br>• Does the risk profile evidence identification and evaluation of non-traditional risk exposures?<br>• Are the interrelationships of risks clearly identified and understood?<br>*Operational Risk*<br>• What are the risks inherent in the processes chosen to implement the strategies?<br>• How does the organisation identify, quantify and manage these risks, given its appetite for risk?<br>• How does the organisation adapt its activities as strategies and processes change?<br>*Reputational Risk*<br>• What are the risks to brand and reputation inherent in the way the organisation executes its strategies?<br>*Regulatory or Contractual Risk*<br>• Which financial and non-financial risks are related to compliance with regulations or contractual arrangements?<br>*Financial Risk*<br>• Have operating processes put financial resources at undue risk?<br>• Has the organisation incurred unreasonable liabilities to support operating processes?<br>• Has the organisation succeeded in meeting measurable business objectives?<br>*Information Technology Risk*<br>• Is our data / information / knowledge reliable, relevant and timely?<br>• Are our information systems reliable and free from external attacks?<br>• Do our security systems reflect our reliance on technology, including our e-business strategy? |

| Risk management framework | Evaluation of risk management framework |
|---|---|
| **Portfolio:** the process for identifying, assessing and categorising risks across the organisation. | *New Risks*<br>• In a business environment that is constantly changing, are there processes in place to identify and deal with emerging risks? If not, why not? If yes, describe.<br>• What risks have yet to develop? These might include risks from new competitors or emerging business models, recession risks, relationship risks, outsourcing risks, political or criminal risks, financial risk such as rogue traders, and other crisis and disaster risks. |
| **Optimisation:** balancing potential risks and opportunities based on the appetite to accept risk. | • Does the risk approach include a regular search for new markets, partnering opportunities and other risk optimisation strategies? If not, why not? If yes, how is this achieved?<br>• Is risk a priority consideration whenever business processes are improved? If not, why not? If yes, describe how this is achieved. |

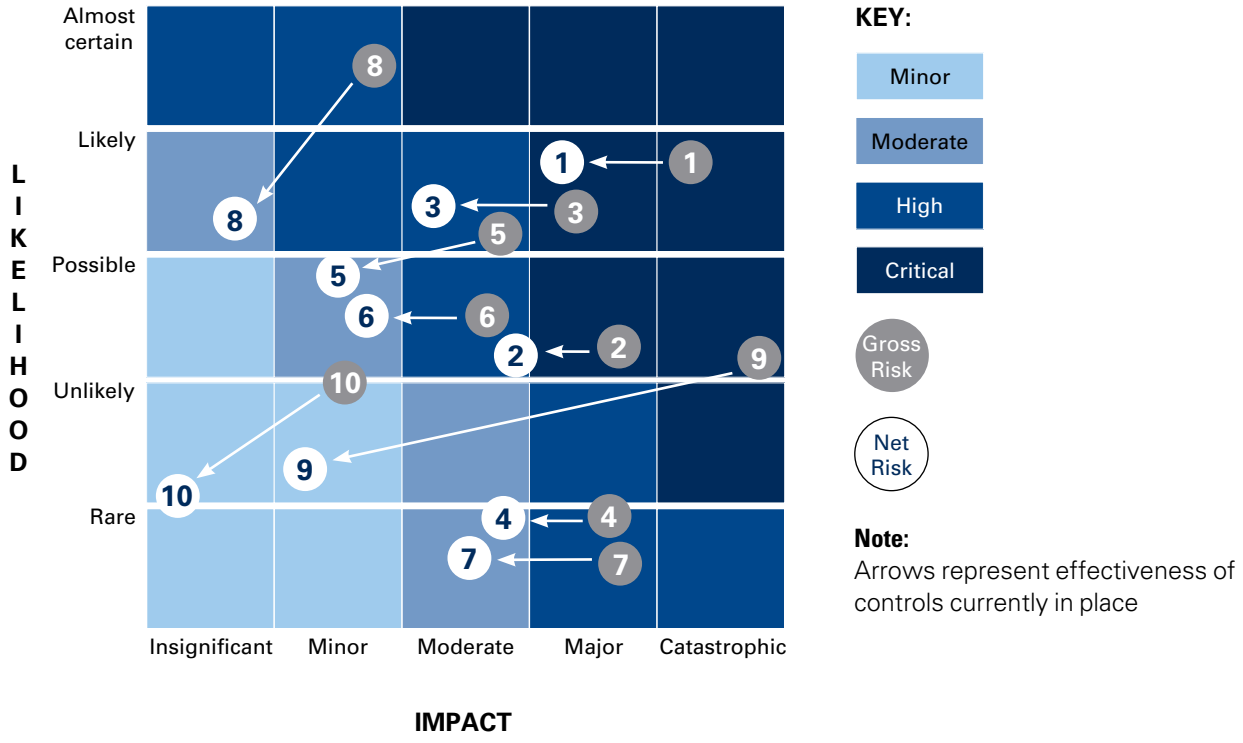


# Appendix 3: Example Risk Summary and Register

The following chart illustrates Management's view of the top 10 risks facing the business. Each of these risks has been assessed in terms of potential impact and likelihood of occurrence, using descriptive scales. The quantification criteria for likelihood and impact are set out on page 18.

The grid below has been used to provide a graphical illustration of the likelihood and impact for each of the organisation's top 10 risks, the arrows representing the influence existing internal controls are thought to have on that risk. The 5*5 matrix is one of the possible matrices that can be used for such analysis.

## Likelihood and Impact for each of the Organisation's Top 10 Risks




**TOP TEN KEY RISKS:**

1. Inappropriate acquisition strategy and process
2. Fall in investor confidence due to media criticism
3. Failure to comply with appropriate regulatory and legal requirements (i.e. cartels)
4. Post implementation IT systems failures
5. Failure to allow current business strategy enough time to develop
6. Failure to manage and respond adequately to economic uncertainty
7. Inadequate business continuity and disaster recovery plans to manage a major IT network failure
8. Inability to protect brand name
9. A key division fail to deliver their expected growth strategy
10. Loss of key staff and inadequate succession planning

## Quantification criteria for likelihood and impact

| LIKELIHOOD | | | | |
|---|---|---|---|---|
| Event is expected to occur in most circumstances | >90% | Almost Certain | 5 | |
| Event will probably occur in most circumstances | 50 - 90% | Likely | 4 | |
| Event should occur at some time | 30 - 50% | Possible | 3 | |
| Event could occur at some time | 10 - 30% | Unlikely | 2 | |
| Event may occur only in exceptional circumstances | <10% | Rare | 1 | |

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| | Insignificant | Minor | Moderate | Major | Catastrophic |
| Time | Resolution would be achieved during normal day to day activity | Resolution would require input from regional management team | Resolution would require input from Executive team | Resolution would require the mobilisation of a dedicated project team | Resolution would require input from the Board |
| Profit | Less than 1% or no impact | 1% to 3% impact | 3% to 10% impact | 10% to 25% impact | Greater than 25% |
| Turnover | Little or no impact | 1% to 3% impact | 3% to 10% impact | 10% to 25% impact | Greater than 25% |
| Environment | On-site environmental exposure immediately contained | On-site environmental exposure contained after prolonged effort | On-site environmental exposure contained with outside assistance | Off-site environmental exposure contained with outside assistance | Environmental exposure off-site with detrimental effects |
| Reputation | Letters to local/ industry press | A series of articles in local/ industry press | Extended negative local/ industry media coverage | Short term national negative media coverage | Extensive negative national coverage |
| Regulatory | Minor breaches by individual staff members | No fine - no disruption to scheduled services | Fine but no disruption to scheduled services | Fine and disruption to scheduled services | Significant disruption to scheduled services over an extended period of time |
| Management effort | An event, the impact of which can be absorbed through normal activity | An event, the consequences of which can be absorbed but management effort is required to minimise the impact | A significant event which can be managed under normal circumstances | A critical event which with proper management can be endured | A disaster with potential to lead to collapse of the business |

**IMPACT**



KPMG
KPMG Centre
31 Cybercity, Ebène, Mauritius
**T:** (230) 406 9999 **F:** (230) 406 9998
**E:** kpmg@kpmg.mu **W:** www.kpmg.mu
Business registration number: F07000189

Mauritius Institute of Directors
1st Floor, Standard Chartered Tower
19 Cybercity, Ebène, Mauritius
**T:** (230) 468 1015 **F:** (230) 468 1017
**E:** miod@miod.mu **W:** www.miod.mu
Business registration number: C08077130

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.

© 2015 KPMG, a Mauritian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. MC14094

The opinions of the authors are not necessarily the opinions of KPMG.