The IRMSA Guideline to Risk Management
Acknowledgements

A project like the IRMSA Guideline to Risk Management is never the work of one individual, but rather a communal effort with various contributors. IRMSA would particularly like to thank its membership, the task team who reviewed the guideline, IRMSA’s Executive Committee and its Technical & Education Committee, as well as Marsh and Marsh Risk Consulting for the time spent and contributions made during this venture.

Disclaimer

Although a multitude of sources were consulted in the creation of this guideline, it contains no direct quotations or copies of illustrations from any of the works mentioned. The sources in question were consulted in good faith and are referred to in a manner of fair use. Every effort has been made to acknowledge all sources. Errors and omissions excepted. IRMSA would gratefully accept notification of any corrections to be incorporated in future reprints or subsequent editions.

Acknowledgement of sources from specific companies, products or services do not imply that they are endorsed or recommended by IRMSA in preference to similar companies, products or services not mentioned.
Preamble

All enterprise is the undertaking of risk for reward. It does not matter whether the enterprise is a mega-sized multinational company, a local municipality or a basic healthcare clinic; it takes a continuous series of risks to achieve reward. The reward can be profit, it can be successful service delivery to citizens, or prevention of disease.

Risk is not only negative, but as risk constitutes uncertainty, it also presents opportunity. A missed opportunity is as much of a risk as a building being destroyed by fire.

A risk is therefore not only a bad thing happening, it is also a good thing not happening.

This guideline recognises the importance of the proper management of risk in any organisation, and clearly specifies the recommended roles and responsibilities for risk management of the leadership function in an organisation.

There was a specific decision to align the IRMSA Guideline to Risk Management to the international risk management standard, the ISO 31000: Risk Management - Principles and Guidelines (2009). However, the environment in which many organisations in South Africa find themselves, is also one regulated by the code and principles of the third King Report on Governance for South Africa (King III, 2009). It is therefore important for South African risk practitioners to understand the risk requirements and challenges in the context of King III, to ease compliance of corporate governance systems.

Management cannot be expected to deal in a structured, planned and confident manner with unexpected events or unexpected opportunities, if such events are not planned for. Risk management provides the scaffold to address these issues and informs the bulk of the requirements of King III in terms of the governance of risk.

This guideline to risk management, as developed and published by IRMSA, provides insight into the various activities of risk management, in particular the development of a risk management framework and the process of risk management. Though it is aligned to most major national and international standards, it should ideally be used in conjunction with King III, the ISO 31000 and any additional industry specific standards or legislation.
Contents

About
1. Purpose 6
2. Scope 6
3. Structure 6
   3.1. Underpinning 7
   3.2. Layout 8
   3.3. Terms and definitions 8
   3.4. References 8

Introduction
1. The meaning of risk 10
2. The upside of risk – opportunity management 10
3. Why is managing risk and opportunity important? 10
1. King III’s principles for governance of risk 12
   1.1. Principles addressing the responsibility for risk 12
   1.2. Principles addressing the management of risk 12
   1.3. Principles addressing the monitoring, assurance and disclosure of risk 14
2. General risk management principles 14
3. King III principles vs. general risk management principles 16

Framework
1. Structure of the framework 17
2. The organisation and its context 18
   2.1. Understand the organisation’s operating model 18
       2.1.1. Operational activities 18
       2.1.2. Management systems 19
       2.1.3. Functions 19
       2.1.4. Services and/or products 19
       2.1.5. Strategic partnerships 19
       2.1.6. Supply chain 19
       2.1.7. Relationships with external stakeholders 19
   2.2. Understand the external context 20
       2.2.1. Legal, regulatory and other requirements 20
       2.2.2. Contractual requirements 20
       2.2.3. Implications for society and stakeholders 21
   2.3. Understand the internal context 21
   2.4. Apply the risk management process and determine internal risk thresholds 21
       2.4.1. Risk appetite 21
       2.4.2. Risk tolerance 22
       2.4.3. Risk-bearing capacity 22
3. **Mandate and commitment**  
   3.1. Establishing an effective risk culture  
   3.2. Mandate  
      3.2.1. Risk management policy  
      3.2.2. Roles and responsibilities  
      3.2.3. Role of the internal audit function in risk management  
      3.2.4. Combined assurance model  
   3.3. Commitment  
      3.3.1. Executive commitment  
      3.3.2. Management commitment  
      3.3.3. Risk practitioners  
      3.3.4. Workforce commitment  
4. **Setting up the framework**  
   4.1. Designing the framework (Plan)  
      4.1.1. Common risk language  
      4.1.2. Risk thresholds  
      4.1.3. Risk management process  
      4.1.4. Risk criteria  
      4.1.5. Performance evaluation criteria  
      4.1.6. Consideration of supporting systems  
      4.1.7. Communication procedures  
      4.1.8. Business continuity planning  
      4.1.9. Risk management outputs  
      4.1.10. Resources  
   4.2. Implementing the framework (Do)  
   4.3. Monitor and review performance (Check)  
      4.3.1. Monitoring and review of the framework  
      4.3.2. Management review  
      4.3.3. Documentation and record-keeping  
      4.3.4. Strategic risk management  
   4.4. Continual improvement of the system (Adjust)  
      4.4.1. Continual improvement  
      4.4.2. Non-conformity  

### Process

1. Communication and consultation  
2. Establishing the Context  
   2.1. Internal context  
   2.2. External context  
   2.3. Defining specific risk criteria  
3. Risk assessment  
   3.1. Identifying risk  
      3.1.1. Purpose  
      3.1.2. Approach  
      3.1.3. Tools
3.2. Analysing risk
  3.2.1. Assessing controls
  3.2.2. Analysing consequences
  3.2.3. Analysing likelihood and estimating probability
  3.2.4. Completing the risk register
  3.2.5. Uncertainties and sensitivities
3.3. Evaluating risk
3.4. Opportunity Assessment

4. Risk response
  4.1. Risk responses available
    4.1.1. Accepting or tolerating the risk
    4.1.2. Avoiding the risk
    4.1.3. Removing the source of risk
    4.1.4. Changing the likelihood
    4.1.5. Changing the consequence
    4.1.6. Transferring the risk
    4.1.7. Exploit the opportunity
  4.2. Selection of risk response options
  4.3. Risk controls
    4.3.1. Types of control
    4.3.2. Mechanisms of control
  4.4. Preparing risk response plans
    4.4.1. Preparing and implementing risk response plans

5. Monitoring and review
  5.1. Planning the monitoring and review
  5.2. Examining and evaluating information
  5.3. Recording the risk management process
  5.4. Communicating results
  5.5. Follow-up

Conclusion
1. Maturity measure
  1.1. Risk management culture
  1.2. Risk management framework
  1.3. Risk management practice
Executive **Summary**

Since IRMSA’s Code of Practice was published in 2004, there have been a number of changes in the risk universe as well as in the legislation relating to various areas of risk management. This document replaces that Code of Practice and intends to serve as a practical guideline for those responsible and interested in risk management across all organisations, industries and sectors.

For those who seek to access the overarching principles of risk management (aligned to ISO 31000: Risk Management Principles and Guidelines), as well as the principles set out in the third King Report on Governance, the IRMSA Guideline to Risk Management contains a concise outline of both in its section on risk management principles.

The risk management process on which the IRMSA Guideline to Risk Management focuses, is an adaptation of the centuries-old scientific problem-solving process, where the “problem” is uncertainty. Despite the fact that risk can be either positive or negative, we will be generally discussing risk as a “problem” rather than an “opportunity” because risk management traditionally has dealt only with undesired outcomes, not with unexpectedly positive ones.

*It is important to note that the entire framework and process is equally applicable to the upside of risk.*

Whether already managing risk according to set principles and a fine-tuned framework with its derived actions and processes, or embarking on the formal management of risk for the first time, organisations should ask themselves:

- What are the organisation’s objectives?
- What risks is the organisation accountable for?
- What are the key risk areas that need to be given attention?
- How does the organisation go about clearly defining its risks?
- How should the organisation respond to each risk?
- How does the organisation check that the proper risk responses are in place?
- And how effectively are the organisation’s risks being managed?

This guideline contains information on the various components, arrangements and relationships that would enable the organisation to plan, implement, operate and continuously improve the management of risk and opportunity throughout the organisation.

It also discusses the principles according to which risk management should be executed; the framework pertaining to the accountabilities, processes, systems, policies, behaviours, risk criteria, communication mechanisms, monitoring and reporting; and the risk management processes to be implemented organisation-wide.

This will assist an organisation to be forward looking (through considering emerging and evolving risks), learn from its mistakes (by measuring performance), and exploit opportunities where these exist.

Although not every aspect of risk management as mentioned in this document would apply to every organisation, it remains true that every activity within an organisation involves risk – in other words, there are no risk-free activities. Equally, there are no activities where opportunity for improvement cannot be found. It also remains true that the management of risk and the management of opportunity are linked: preserving, even enhancing, the creation of value, protecting these from the effects of uncertainties, and providing resources essential for grasping opportunities when they arise.

The IRMSA Guideline to Risk Management
The management of risk involves a coordinated effort to control risk, and essentially adopts the following process:

- Understanding the organisation’s objectives.
- Identifying the risks that may influence those objectives.
- Analysing the risks and opportunities to understand how they will influence those objectives.
- Evaluating how to respond to the risks and opportunities to meet the organisation’s risk criteria.

An organisation’s risk criteria and thresholds along with the organisation’s overall intentions, direction and attitude towards risk should be defined by the organisation’s risk policy (which is underpinned by the organisations risk management framework). The most senior management level in the organisation (board of directors, executive committee, etc.) is accountable for establishing and maintaining this policy.

It is important to note that the entire framework and process is equally applicable to the upside of risk.
About

1. Purpose
The purpose of the IRMSA Guideline to Risk Management is to serve as a base document to provide guidance to organisations in the planning, implementing, evaluating and improving of their risk management, no matter the organisation’s size, industry or sector.

There are various ways to achieve an organisation’s risk management objectives, and it would be impossible to name and explore all of these in a single document. The best practice guidelines in this document should thus serve as a starting point from whence risk management practitioners can take their cue.

In addition, the various bulleted lists contained in this document are not intended to be used as final and finite sets of information to be ticked off one by one. However, organisations that follow this guideline would mostly be in a position to reach their risk management objectives and comply with most risk management requirements and international best practice.

2. Scope
As mentioned above, this guideline is intended for all types of organisations, no matter their size, industry or sector. This document is not prescriptive – each company is responsible for applying the appropriate guidelines responsibly and comprehensively to its own needs, and to the requirements of its own stakeholders. To this end, this document is aligned with international and local standards across a variety of industries and sectors. How intensively organisations apply these guidelines will depend on each organisation’s operating environment, its specific industry and the complexity of its operations.

Organisations may use this document to guide the planning, implementation, evaluation and improvement of their risk management frameworks and processes if they wish to do any of the following:

- Establish a new risk management framework where none exists.
- Integrate risk management processes into organisational policies, practices and procedures.
- Adapt and/or improve an existing risk management framework.
- Monitor risk management performance.

Organisations should be aware that this document can neither be used as an exhaustive manual, nor does it describe every element of how risks should be managed. It also cannot serve as replacement for having a risk management practitioner in the organisation.

3. Structure
This guideline follows the shape of the “plan, do, check, adjust” model, also known as the “plan, do, check, act” model, a four-step iterative process that can be applied to any number of processes and systems. The reasoning behind this is that it brings about ease of reference and facilitates a degree of alignment with local and international standards.

By moving through the four steps, an organisation can also identify opportunities to improve its systems and processes, which in turn supports consistent and integrated planning, implementation, operation and evaluation.
3.1. Underpinning

The contents of this guide are informed by specialist, technical, practical and expert experience across industries, sectors and risk management disciplines, as well as by research and industry consultation. It is thus based on a body of knowledge gleaned from a large variety of theoretical as well as practical sources, to include tried and tested, localised solutions and practices, as well as global know-how.

Sources consulted during the compilation of this document include:

- Various risk management standards and codes.
- White papers and discussion documents.
- Writings and submissions by a variety of professional bodies.
- Best practices and standards compiled by risk management practitioners.
- Additions recommended by the IRMSA membership and other stakeholders (this includes public participation).

As the IRMSA Guideline to Risk Management is intended for use by South African companies as well as international companies operating in South Africa, it draws on standards (including ISO 31000), takes codes of governance principles such as King III into account and aligns to South African legislation. Although it has been written primarily for a South African audience, the principles and processes contained in this guideline may also be applicable in other regions.

Figure 1 illustrates the various inputs to the IRMSA Guideline to Risk Management.
3.2. Layout
The IRMSA Guideline to Risk Management comprises three main subsections: the risk management principles, the risk management framework and the risk management process. Figure 2 overleaf illustrates the relationship between the principles, framework and process. From the framework section onwards, each section of the document starts out with the main idea behind it highlighted in blue. These synopses are not definitions, but short descriptions to give the reader quick insight into the content that follows.

3.3. Terms and definitions
The definitions given were mostly sourced from ISO Guide 73: Risk Management – Vocabulary, but some were adapted to reflect recent changes in the domain of risk management. The aim of defining terms is to encourage a mutual and consistent understanding of, and a coherent approach to, the salient aspects relating to the management of risk. The terms and their definitions can also be found in a collated list at the end of this document. The list has been alphabetised for ease of reference. The list of references can be seen at the back of this document.

3.4. References
Two types of reference works were used during compilation of the IRMSA Guideline to Risk Management. The normative references comprise the various legislative requirements applicable to risk management in South Africa, which are indispensable to the planning, application and evaluation of risk management frameworks. The supportive references include other writings on risk management, which are considered practical and contemporary, such as summaries, executive reports and other material on the subject. The list of references can be seen at the back of this document.

Figure 2: Relationship between risk management principles, the risk management framework and the risk management process.
The Guideline
A set of guiding principles

“Risk is the effect of uncertainty on objectives.”

This definition encompasses both the positive and negative consequences of risk, and places it in the context of the organisation’s objectives.
Introduction

1. The meaning of risk
   Understanding the meaning of the term “risk” is the most fundamental prerequisite to developing a risk management programme. Common perceptions include:
   - The possibility of loss, danger or injury.
   - The possibility that the future may be worse or better than what was expected.
   - The possibility of a loss arising from an undesirable future event.
   - An uncertain event or condition which, if it occurs, will have a negative effect on the achievement of objectives.
   - The possibility of better-than-expected performance.

   This document uses a formal definition aligned with ISO 31000, which reads as follows:
   “Risk is the effect of uncertainty on objectives.”

   This definition encompasses both the positive and negative consequences of risk, and places it in the context of the organisation’s objectives.
   Risk management is then the process of planning, organising, directing, and controlling resources and operations to achieve given objectives despite the uncertainty of events. Effective risk management enables an organisation to manage the probability of any unforeseen events that may arise and to limit the effect of the consequences, along with responding proactively to opportunities. This means the organisation will be better able to carry out its plans – in other words, achieve its organisational objectives – despite the uncertainty of the events in the environment in which they function.

2. The upside of risk – opportunity management
   Opportunity management (also known as upside risk) is also an important component of organisational planning and management systems. By focusing on the downside of risk, organisations can overlook opportunities that provide significant possibilities for innovation and competitive advantage. Missing opportunities can also significantly affect an organisation’s overall ability to deliver on its mandate, vision and goals.

   Understandings of opportunity management often include:
   - The possibility that the future may be better than expected.
   - The possibility of a gain arising from a future event.
   - An uncertain event or condition which, if it occurs, has a positive effect on the achievement of objectives.
   - A favourable situation for a positive outcome.

3. Why is managing risk and opportunity important?
   Risk and opportunity management is important for an organisation in maximising its ability to protect and create value. Failing to manage risks may prevent the organisation from achieving its objectives, and ultimately lead to the diminishing of share value and loss of competitive advantage or even closure. Failure to manage risks may also harm stakeholders such as the community in which the organisation operates. Failing to manage opportunities may lead to an organisation becoming less relevant to its stakeholders (including shareholders) or to the beneficiaries of its activities, such as customers, constituents or clients. This is particularly the case where there is competitive pressure to deliver.
   Tangible benefits of risk and opportunity management include projects and activities delivered on time and on budget; not adversely affecting stakeholders (including the workforce, the environment and society) such as through physical and environmental harm, and not exposing the organisation to financial or other penalties.
Principles

The effective implementation of risk management frameworks, plans and processes require those responsible for managing risk to exhibit good sense and sound judgment when approaching the overall challenge of managing the organisation’s risks. A set of guiding principles is indispensable in this case.

Various sets of principles exist, of which two will be discussed here. The first is the principles set forth by the King committee on governance, and the other is a set of general principles for risk management based on the ISO 31000. This section concludes with a comparison of the two for ease of alignment in everyday practice.

Below, we have used the terminology from the King III report, in particular the term ‘board’. This is specifically applicable to private (or privately structured) organisations. Yet it should also be interpreted to mean the highest executive management structure of an organisation, and therefore is also applicable to government departments and municipal entities, where ministerial, executive, or similar committees fulfil this function.
1. King III’s principles for governance of risk

The third King Report on Governance for South Africa, published in 2009, contains certain principles for the governance of risk. A large number of South African companies adhere to these (or to legislation based on or incorporating these), which are structured to address firstly the responsibility for risk, secondly the management of risk (which is mainly the theme and scope of the IRMSA Guideline to Risk Management) and lastly the monitoring, assurance and disclosure of risk.

1.1. Principles addressing the responsibility for risk

**King Principle 1: The board should be responsible for the governance of risk.**
This vests the responsibility for risk in the highest decision-making authority in an organisation. It tasks the highest authority to take responsibility for the design and implement a risk management policy and plan, and to ensure that the processes of risk management are implemented according to accepted risk management frameworks and guidelines.

**King Principle 2: The board should determine the levels of risk tolerance/appetite.**
At least once a year, the board (or highest decision-making authority in the organisation) should set specific limits for the levels of risk the company is able to tolerate in pursuit of its objectives. The board (or equivalent) may also set limits regarding the organisation’s risk appetite, i.e. those risk limits that the board (or equivalent) desires, or is willing, to take. The limits are both financial and non-financial, and where the risk appetite limits exceed or deviate materially from the risk tolerance limits, this should be disclosed in the annual integrated report.

**King Principle 3: The risk committee or audit committee should assist the board in carrying out its risk responsibilities.**
To assist it in the discharge of its duties and responsibilities with regard to risk management, the board (or equivalent) should appoint a risk committee to review the risk management process and maturity of the organisation, the effectiveness of the risk management activities, the key risks facing the company and the responses to those risks. This may be assigned to the audit committee, if the latter has the capacity. The risk committee may appoint independent risk experts to supplement skills and experience.

**King Principle 4: The board should delegate to management the responsibility to design, implement and monitor the risk management plan.**
The risk strategy should be executed by management in accordance with the risk management policy and plan. The roles and responsibilities for risk management should be addressed in the risk policy and plan. Risk management should be intrusive: its methodology and techniques should be embedded within strategy setting, planning and business process. The rigours of risk management should provide responses that strive to create the appropriate balance between risk and reward in the organisation.

1.2. Principles addressing the management of risk

**King Principle 5: The board should ensure that risk assessments are performed on a continual basis.**
The board (or highest decision-making body in the organisation) should ensure that the organisation has and maintains an effective ongoing risk assessment process, consisting of risk identification, risk quantification and risk evaluation. Following the risk assessment process, risks and opportunities should be prioritised and ranked to focus on the most critical risk responses.

1 Please note that King III does not define risk appetite and risk tolerance separately.
King Principle 6: The board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks.
The risk assessment process should be of such a nature that it can help the organisation to anticipate systemic, aggregated, consequential and other unpredictable risks.

King Principle 7: The board should ensure that management considers and implements appropriate risk responses.
Management should identify and consider different ways in which the company can respond to the risks identified during the risk assessment process, and the board should make sure that those responses are in place.

1.3. Principles addressing the monitoring, assurance and disclosure of risk
King Principle 8: The board should ensure continual risk monitoring by management.
The board (or equivalent) should ensure that the responsibilities for monitoring are clearly defined in the risk management plan, and that management monitors the risk management plan effectively and continually.

King Principle 9: The board should receive assurance regarding the effectiveness of the risk management process.
Management is accountable to provide the board (or equivalent) with assurance that it has implemented and monitored the risk management plan and that it is integrated in the organisation's daily activities. Each year, an independent assurance provider should provide a written assessment of the effectiveness of the system of internal control and risk management to the board (or equivalent).

King Principle 10: The board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders.
The board (or equivalent) should disclose in its annual report to stakeholders (such as an integrated report to shareholders or other statutory report) any undue, unexpected or unusual risks the organisation has taken, as well as material losses and the causes there of, without compromising privileged information. It should disclose any current, imminent or envisaged risk that may threaten the long-term sustainability of the organisation and also disclose its views on the effectiveness of the organisation's risk management processes.

2. General risk management principles
The following principles represent best practice concepts to which all levels of an organisation should aspire when managing risk, no matter the legislative and regulatory principles to which the organisation has to adhere to.

2.1. Risk management creates and protects value.
Risk management contributes to the demonstrable achievement of objectives and the improvement of performance in, amongst others, financial performance, health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, project management, production, operations, governance and reputation.

2.2. Risk management should be an integral part of all organisational processes.
Every activity within an organisation carries with it some risk – there are no risk-free activities. Therefore, risk management is not a stand-alone activity, separate from the core activities and processes of the organisation (such as strategic planning, change management, operational activities, IT governance, business continuity and health and safety), but is an integral part of all organisational aspects.
2.3. **Everyone in an organisation is responsible for risk management.**

Every individual member of an organisation, from executive director to the most junior employee, is responsible for managing the elements of risk in their given sphere of influence.

2.4. **Risk management is part of decision-making.**

Understanding risk and the effects of risk is indispensable for decision-makers who want to make informed choices, prioritise actions and distinguish among the various courses of action available. In this view, every individual member of an organisation is a decision-maker in his or her sphere of influence, and therefore risk management principles should be applied across the entire organisation, at every level and opportunity.

2.5. **Risk management considers human, cultural and social factors.**

Risk management recognises the behaviours, capabilities, perceptions and intentions of internal and external individuals and groups who can either facilitate or hinder the organisation in achieving its objectives. The values that people place on different risks influence their decision-making. These values should be investigated and brought to light as explicitly as possible, wherever feasible.

2.6. **Risk management is based on the best available information.**

The inputs to the process of managing risk are based on as much information as can be reasonably obtained in a timely manner. Sources such as historical data, forecasts and models, experience, stakeholder consultation, observation, and expert opinion should be used. However, decision-makers should take note of and consider all data or modelling limitations and the possibility that experts may hold different opinions on a given matter.

2.7. **Risk management is inclusive of all stakeholders.**

Appropriate and timely involvement of external stakeholders ensures that risk management remains relevant, by incorporating external forces that influence the organisation's ability to achieve its objectives, such as considering the impact of local communities, relevant authorities and regulators, customers and suppliers.

2.8. **Risk management explicitly addresses uncertainty.**

Risk management explicitly considers the uncertainty surrounding a decision, activity or event, the possible outcomes of that uncertainty, and how it can be addressed.

2.9. **Risk management is systematic, structured and timely.**

Risk management should be undertaken in a systematic and timely fashion to enable organisational efficiency; by following a standardised, structured approach, it also enables consistent and comparable results.

2.10. **Risk management is tailored to the organisation.**

An organisation’s risk management framework must be aligned with its own unique internal and external context (which includes its objectives, operating model, stakeholders, etc.).

2.11. **Risk management is dynamic, iterative and responsive to change.**

Good risk management is sensitive, and responsive, to changes in the organisation’s context and environment. It should continuously adapt to take account of changing risks, through regular reviews and inclusion of emerging best practices.

2.12. **Risk management facilitates continual improvement of the organisation.**

Effective identification and management of risks allows an organisation to identify systematic improvements to its business and operating model. This is an iterative process in parallel with the maturation of the risk management framework itself.
3. King III principles vs. general risk management principles

The principles enshrined in King III, as discussed in the first half of this section, aim to improve corporate governance and hence performance, in a number of key areas. This is to improve corporate responsibility, to protect and create value, and to ensure that the disclosure expectations of stakeholders (including shareholders) are met effectively.

The principles of risk management as described in the second half of this section detail international best practice for good risk management.

The two sets of principles are therefore complementary: the risk management principles describe what good risk management looks like, while the King III principles help ensure that the organisation applies such good practices. Below is a visual representation of how these two sets of principles align:

Figure 3: King III principles vs. general risk management principles
1. Structure of the framework

The risk management framework adopts the structure as illustrated in figure 4, where:

- **Plan:** is to establish the risk management framework.
- **Do:** is to implement and operate it.
- **Check:** is to monitor and review its effectiveness.
- **Adjust:** is to maintain and continuously improve it.

Figure 4: The risk management framework
2. The organisation and its context

The first step in risk management is defining the objectives that the organisation wants to achieve, how it intends to achieve these objectives (the operating model), and what might get in the way of achieving them.

In establishing the context, the organisation should follow the process below:
- Define its operating model, along with its strategic and operational objectives.
- Define the external and internal factors that give rise to the risk that the organisation cannot meet its objectives.
- Determine externally imposed risk parameters (e.g. regulatory, legal, social, contractual etc.).
- Apply the risk management process to the organisation and define internal parameters (e.g. risk appetite, risk-bearing capacity).

The starting point for understanding the risk profile of any organisation is to specify the objectives and goals of the organisation. These need to be defined as explicitly as possible in order for specific risks to be identified and described in later stages (Section on Risk Assessment, page 35).

2.1. Understand the organisation’s operating model

The starting point in defining a risk management framework should be to articulate what the organisation does, what its objectives are, and how it operates.

The process begins by first describing the overall mission of the organisation, and then progresses to articulating the strategic and operational objectives that facilitate the delivery of that mission. As far as possible, it should describe how the organisation actually reaches these objectives, according to the aspects described below.

2.1.1. Operational activities

All the operational activities the organisation undertakes are part of this aspect, such as:
- Service delivery
- Sales and customer management
- Resource acquisition
- Investment
- Production
- Vendor management
- Project management
- Logistics and stock management
- Innovation, research and development
- Strategy

An accurate articulation of the operating model will help develop a comprehensive and robust risk management framework, and this is therefore strongly recommended.
2.1.2. Management systems
This refers to the various policies, processes and systems that an organisation has in place to manage its activities. These systems are interconnected, and play an important role in driving organisational behaviour.

2.1.3. Functions
This pertains to the compliance, governance and management functions within the organisation, including:
- IT governance, IP and data management
- Security
- Finance
- Health and safety
- Human resources
- Risk governance
- Compliance and assurance (including internal audit)
- Operations.

2.1.4. Services and/or products
The current and potential products and/or services that the organisation offers to its customers should be considered when designing the risk management framework. It should include information pertaining to:
- Market information
- Competitors
- User profiles of the target market
- Economic and behavioural trends.

2.1.5. Strategic partnerships
This refers to all the strategic partnerships that the organisation has in place and which are critical to the operational success of the business. It includes, for example:
- Trade unions
- Technology development partners
- Maintenance and service partners
- Joint venture partners
- Financiers
- Communities

2.1.6. Supply chain
This comprises the organisation’s entire supply chain, with a particular focus on critical supply chain dependencies up and down the chain (including the management of contracts).

2.1.7. Relationships with external stakeholders
The external parties who can influence the organisation’s ability to operate also have to be considered, and may include:
- Government bodies
- Licensing authorities
- International regulatory organisations
- Certification authorities
- Rating agencies.
2.2. Understand the external context

The external context entails the external environment in which the organisation seeks to achieve its objectives, and over which it has no direct influence. Describing the external context is important in order to understand the market forces (e.g. political, technological, legal, economic, etc.) and the social and environmental forces that will affect the organisation’s operating and strategic capabilities.

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

- The sociocultural, economic, political, legal and regulatory, natural and competitive environment, whether international, national, regional or local.
- Key drivers and trends that influence the objectives of the organisation.
- Relationships with, and the perceptions and values of external stakeholders.

2.2.1. Legal, regulatory and other requirements

As part of the operating model, an organisation will have to meet certain legal and regulatory requirements to continue operating. The organisation should articulate:

- The legal, regulatory or other requirements to which it must adhere.
- The penalties the organisation will face if it breaches these (intentionally or unintentionally).
- In the South African context, key legal, regulatory and other requirements include for example the following:
  - The South African Constitution
  - The Companies Act
  - The Public Finance Management Act
  - The Municipal Finance Management Act
  - Requirements such as the third King Report on Governance in South Africa (King III) and the JSE rules
  - The Occupational Health and Safety Act
  - Acts on short and long-term insurance
  - Money laundering regulations
  - The Income Tax Act
  - FAIS regulations
  - The Financial Intelligence Centre Act (FICA)
  - The Labour Relations Act
  - Competition laws
  - The Protection of Personal Information Act
  - The Consumer Protection Act
  - The National Environmental Management Act (NEMA)
  - Industry or sector-specific legislation, such as The Mining Act, Financial Services Act, and Mining and Petroleum Resource Development Act.

Organisations in other geographies may need to consult local equivalents.

2.2.2. Contractual requirements

The organisation may enter into specific contractual agreements, within certain parameters or constraints. These contracts will have specific risk thresholds and operational requirements, and these should be considered when developing the framework. This may include, amongst others:

- Service level agreements
- Key resource/utility arrangements
- Counter-party risk and insurance.
2.2.3. Implications for society and stakeholders

Effective external communication and consultation should take place throughout the risk management process to ensure that the organisation understands:

- Which stakeholders it exposes to risk.
- How these stakeholders could influence the organisation’s operational capability.

Stakeholders make different value judgements regarding risk, based on their perceptions of risk. These perceptions can vary due to differences in values, needs, and assumptions, as well as individuals’ concerns about, and concepts of, risk.

2.3. Understand the internal context

The internal context is the internal environment in which the organisation seeks to achieve its objectives. These factors lie wholly or mostly within the organisation’s decision-making capacity, and the organisation can thus influence it directly.

Specifying the internal context is critical in understanding the internal drivers that shape the organisation’s ability and capacity to reach its objectives. This can include, but is not limited to:

- Governance, organisational structure, roles and accountabilities.
- Executive mandate for risk function – sign-off on project contingencies, escalation on exposures beyond appetite.
- Risk calibration / quantification.
- Policies, objectives, and the strategies in place to achieve them.
- The inter-dependencies of the various management systems, functions and activities of the organisation.
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies).
- The relationship with, and perceptions and values of internal stakeholders.
- The organisation’s culture, including its risk management culture, attitudes and behaviours.
- Information systems, information flows and decision-making processes (both formal and informal).
- Standards, guidelines and models adopted by the organisation.
- The nature and extent of contractual relationships.

2.4. Apply the risk management process and determine internal risk thresholds

The final component of developing or enhancing the risk management framework is to apply the organisation’s risk management processes. This will identify the various risks that the organisation must address, and allows the executive leadership team to establish the appropriate internal risk parameters the organisation should follow. These concepts are discussed below.

2.4.1. Risk appetite

An organisation’s risk appetite reflects the level of risk it is willing to accept in all spheres in order to achieve its stated objectives. It is an organisation’s propensity for risk. It is the responsibility of the highest level of management with authority for the organisation to determine the various levels of risk appetite. They should take into account the views and requirements of internal and external stakeholders (e.g. shareholders, regulators, local communities, customers, the organisation’s own workforce, etc.).

For example, the executive is responsible for establishing the overall risk appetite for the organisation within the limits of legal and regulatory requirements. A business unit general manager may be responsible for establishing the risk appetite of that particular unit, within the broader constraints imposed by the overall organisation. A project manager may further establish their own project risk appetite, within the boundaries agreed by the project sponsors.
There should be a range of different appetites defined for different risk types whether it be financial or nonfinancial – for example, for risks related to finances, operations, health and safety and other domains. Risk appetite is dynamic and it fluctuates as various internal and external factors change.

2.4.2. Risk tolerance

Risk tolerance reflects an organisation’s ability or readiness to bear a risk, after all responses have been put in place. This means it indicates the level of unwanted outcomes that can continually be tolerated or aspired to, based on internal and external requirements. Risk tolerance may refer to financial (e.g. profit), quasi-financial (e.g. gearing), or non-financial (e.g. staff turnover) aspects of risk. The organisation’s risk tolerance, however, should always be higher than its appetite for risk – and where the appetite exceeds risk tolerance, this should be disclosed to the relevant stakeholders.

Public sector organisations should recognise that their risk tolerances should be defined differently to private organisations, particularly as there are legislated service commitments that must be maintained, irrespective of financial constraints.

2.4.3. Risk-bearing capacity

In simplest terms, risk-bearing capacity is the maximum financial loss that can be borne in the medium term without the organisation having to change its strategic plans or financing requirements. Risk-bearing capacity is traditionally a purely financial concept, used mostly in the insurance and financial service provider arenas. However, the idea itself refers to the ability to absorb additional risk-based volatility in an organisation’s performance without detrimental effect to key plans and strategies, operational status and financial resources in any given year, over approximately a three-year static time horizon.

Public sector organisations, or other service delivery organisations with social responsibilities, will have a different view of risk-bearing capacity. Being ultimately supported by government, they cannot become ‘bankrupt’ (although these organisations can default on debt). However, this does not change the fact that events may lead to allocated resources becoming inadequate for service delivery if no significant changes are made to the operational model or strategic plan, or without material injection of resources. In this sense, risk-bearing capacity remains a relevant concept for public sector organisations.

3. Mandate and commitment

The board or equivalent is responsible for the governance of risk throughout the organisation, and for delegation of authority, but managing risks itself is the responsibility of every individual in the organisation. The authority and mandate regarding risk management within an organisation will differ from individual to individual.

Given the range of organisations that may use this document, three levels of responsibility are distinguished:

- Executive level – the highest management structure in an organisation. This would mean the board of directors, executive management, government ministers, municipal mayoral committees, executive committees and other similar groups.
- Management level – this includes functional management, and includes general managers, business unit managers, director generals, deputy director generals and all others who have management authority within an organisation.
- Workforce – the employees of an organisation who do not specifically fall in one of the first two categories.

In addition, specific responsibilities have been identified for risk practitioners and risk specialists, who may be involved at different levels of the organisational hierarchy.
3.1. Establishing an effective risk culture

The risk culture of the organisation describes the overall behaviour of every member in how they view, handle, manage and communicate about risk. Establishing an effective risk culture is vital to ensure that risk management creates genuine value for the organisation, rather than being simply a ‘tick-the-box exercise’.

It is the behaviour of those at the top that has the most significant influence on how effective the organisation’s risks will be managed. An organisation with an effective risk culture will respect not only the letter of the legislation and standards it has to adhere to, but also to the spirit of such regulations. In addition to this, an effective risk culture gives individuals and groups the right means to manage and respond to risks in an informed manner.

The following are signs of healthy and effective organisational risk culture:

- The executive and senior management maintain a distinct and consistent tone when conveying information about risk-taking and avoidance (and consider their tone as appropriate for different levels).
- Organisation-wide commitment to ethical principles, evident right through the organisation, from the actions of individuals to the consideration of stakeholders when making decisions.
- All members of the organisation accept that risk should be managed without pause; it includes being accountable and taking ownership of specific risks and risk areas.
- Information pertaining to risk is disseminated in a timely and transparent manner through the entire organisation; negative risk and related events are communicated swiftly. A transparent and integrated reporting is adopted in the organisation’s annual reporting to stakeholders.
- Risk-event reporting and whistle blowing is encouraged, as the organisation actively seeks to learn from mistakes and near-misses.
- The organisation sees no process or activity as too large, too complex or too obscure for thorough risk management.
- Appropriate risk-taking behaviours are rewarded and encouraged; inappropriate behaviours are discouraged and rectified.
- The organisation values, encourages and develops risk management skills, resources its risk management function properly and is a member of various professional bodies.
- The organisation’s members are encouraged to obtain professional risk management qualifications and are given the opportunity for technical training.
- The organisation accepts diverse perspectives, values and beliefs as it means the status quo will be consistently and rigorously challenged.
- The risk culture is managed in conjunction with employee engagement and people strategy to ensure that people are supportive socially but also strongly focused on the task in hand.

3.2. Mandate

Different parts of the organisation are mandated to fulfil certain roles, and ensure that different aspects of good risk management are applied. The mandate begins with the executive leadership team, who are responsible for both allocating all other responsibilities, and ensuring the effective governance of risk throughout the organisation.

3.2.1. Risk management policy

The executive leadership team has the mandate to develop the risk management framework, systems and structures within the organisation. They are accountable, though not necessarily responsible, for the development of all risk management systems, beginning with the overarching policy for risk management.
This policy should clearly state the organisation's objectives for and commitment to risk management. It will typically include the following:

- The organisation's rationale for managing risk.
- Links between the organisation's objectives and policies and the risk management policy.
- The overall criteria according to which risks will be managed.
- Accountabilities and responsibilities for managing risk.
- The way in which conflicts of interest are dealt with.
- Commitment to make the necessary resources available to assist those accountable and responsible for managing risk.
- The way in which risk management performance will be measured and reported.
- A commitment to review and improve the risk management system periodically.

3.2.2. Roles and responsibilities

The organisation should ensure that there is accountability, authority and appropriate competence for managing risk throughout the organisation. This includes designing, implementing and maintaining the risk management process, along with ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:

- Identifying risk owners that have the accountability and authority to manage risks.
- Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk.
- Identifying other responsibilities of people at all levels in the organisation for the risk management process.
- Establishing performance measurement metrics.
- Establishing external and/or internal reporting and escalation processes.

The executive should specify responsibilities across multiple 'lines of defence', as appropriate to the organisation. This would generally include the executive leadership team, risk practitioners (such as a chief or corporate risk officer), management, and the overall workforce.

3.2.3. Role of the internal audit function in risk management

The organisation's internal audit and compliance functions or processes should complement the risk management system. Internal audit should further provide independent assurance on the integrity and robustness of the risk management function/process. The specific audit roles and responsibilities should be noted within the framework. This should also take note of any risk management self-assessment processes that the organisation has put in place.

Where a risk or audit committee exists, they should assist the executive leadership team in carrying out its risk responsibilities, through appropriate oversight, reporting and governance. There should be a strong and effective communication channel between the internal audit function and the risk management function. This should be specified as part of the risk management framework (i.e. the manner and medium in which the risk management and internal audit teams communicate). The various risk profiles developed should form a key input in the internal audit process.
3.2.4. Combined assurance model

Using a combined assurance model helps coordinate and optimise the extent of assurance coverage obtained from different providers regarding the various risk areas that might affect the company. The audit committee (or equivalent structure) has the mandate to ensure the appropriateness of the combined assurance model, and should balance the appropriate use of internal and external assurance providers.

3.3. Commitment

*Each individual in the organisation should understand and commit to meeting the specific responsibilities that go hand in hand with their position in the organisation.*

3.3.1. Executive commitment

Those in executive management should demonstrate leadership with respect to the risk management framework, and ensure a consistent application of risk culture to limit behavioural risk. The executive should:

- Be responsible for the governance of risk throughout the organisation.
- Ensure that the organisation has in place a robust framework that describes the policies, processes, systems, resources, and performance criteria, and which remains relevant to the goals of the organisation.
- Ensure that risk assessments are undertaken on a continual basis.
- Be responsible for setting the overall risk policy for the organisation, and defining key risk thresholds – in particular, the organisation’s risk appetite and risk tolerance.
- Be responsible for evaluating the effectiveness of the risk management framework. This should be done continuously, based on the development of new information and advice regarding best practice risk management.
- Ensure a regular formal, independent review of the risk management performance of the organisation. This should be done at a frequency that is reasonable concerning the pace at which different risks evolve.
- Be responsible for ensuring that the risk management framework remains aligned to the strategic objectives of the organisation.
- Ensure there are processes in place that enable complete, timely, relevant, accurate and accessible risk disclosure to stakeholders.
- Establish performance criteria for risk management that are linked to incentive compensation.

More information about the responsibilities of executive leaders, where risk is concerned, can be found in the third King report on governance.
3.3.2. **Management commitment**

Management should demonstrate leadership and commitment with respect to the risk management framework by:

- Ensuring that risk management frameworks and strategies are developed that ensure the organisation operates within the risk thresholds defined by the executive.
- Ensuring the integration of the risk management framework into the organisation’s operating processes.
- Ensuring that the resources are available to let the risk management framework function efficiently, including people, skills and finances.
- Building a culture of sincere risk management throughout the organisation, supported through a common risk language.
- Conforming to the risk management framework in all their decision-making.
- Supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility.
- Identifying and determining responsibility and accountability for each element of the risk management framework.
- Reviewing the appropriateness of the risk management strategy against the policy established by the executive.
- Appointing a specific person to be responsible for risk management activities within the organisation.
- Communicating appropriate risk criteria, thresholds and behaviours to different levels of the organisation.
- Ensuring that all relevant external stakeholders are consulted and appropriately included in the risk management framework.
- Ensuring that the risk management process is applied consistently and appropriately in both business-as-usual and areas of development at the organisation.
- Ensuring that appropriate data and systems are in place to support the risk management function.
- Seeking the input of relevant specialists to enhance risk management capabilities.
- Communicating the benefits of risk management to all stakeholders and shareholders within the organisation.
- Ensuring that audit functions are appropriately integrated into the overall risk management system.
- Ensuring that the workforce is suitably educated and trained to apply and meet the risk management requirements for their role in the organisation.
- Ensuring that the workforce is appropriately informed, considered and consulted regarding the risk management framework at all times.

3.3.3. **Risk practitioners**

Risk practitioners at all levels of the organisation will have very specific responsibilities within the risk management framework. At the highest level of the organisation, it may be the corporate risk officer; at other levels of management, it may involve risk specialists.

Risk practitioners are responsible for:

- Ensuring that the risk management function is designed appropriately to the needs of the organisation.
- Implementing the risk management processes to assess and respond to risks.
- Supporting the effective usage of risk management processes.
- Providing advice and guidance to the organisation regarding risk management.
- Monitoring and reviewing the performance of the risk management framework.
- Providing information to relevant management structures as and where required.

3.3.4. **Workforce commitment**

The general workforce should demonstrate commitment to risk management by continuously applying and conforming to the risk management framework, policies and processes.
4. Setting up the framework

Successful risk management requires that the foundation, components and arrangements within which risk management is undertaken, are institutionalised within the organisation and adhered to by the entire workforce, including managerial and non-managerial staff.

The framework therefore describes:
- Why the organisation manages risk.
- Who manages risks.
- How risks are managed.
- How relevant information about risk is communicated.
- How assurance is provided.

The following sections describe the design, implementation, review and improvement of the risk management framework.

4.1. Designing the framework (Plan)

The organisation should understand the overall context and objectives it is trying to achieve, and carefully plan how risk management can help achieve these. It should describe the people, processes, systems, accountabilities, limits and resources required to achieve good risk management.

The risk management framework should be designed with the organisational context in mind. The framework should then consider or include:
- A risk management policy, outlining the organisation’s approach to managing risk (See Risk management policy, page 22).
- A description of responsibilities for managing risk, at each level of the organisation (See Roles and responsibilities, page 23).
- A set of guidelines or standards on how to manage risk across all the relevant areas of the business, including:
  - A common risk language
  - (Ensuring everyone understands the same thing.)
  - Risk thresholds
  - (Ensuring everyone knows what is acceptable and what is not.)
  - The risk management process
  - (Such as how to identify, assess and treat risk.)
  - Risk criteria
  - Performance evaluation criteria.
  - Assurance of the process.
- Integration with supporting systems, including:
  - IT
  - Engineering
  - Governance
  - Health and safety
  - Environment
  - Quality
  - Legal
  - Communication procedures, i.e. how and with whom information about risk will be communicated.
- Business continuity planning – even where this is specified separately, references should be made to this the business continuity system.
The outputs of the risk management framework, including for reporting purposes.

The resources required to implement the framework, in terms of people, capital, technology, relationships and others as appropriate (see Resources, page 29).

Relevant details about the risk management framework should be made available to all employees, with specific guidance provided to those employees with specific responsibilities.

4.1.1. Common risk language

The risk management framework should define specific terms and language for risks across the organisation. Wherever possible, these should refer back to nationally and internationally accepted terminology (e.g. ISO Guide 73; see References), but specific local definitions should take preference.

4.1.2. Risk thresholds

The framework should specify the different thresholds (i.e. risk appetite, risk tolerance, risk-bearing capacity) of risk the organisation is willing to accept. (See the section on Internal Risk Thresholds on page 20 for more detail).

4.1.3. Risk management process

The framework should define the overall process by which risks are identified, assessed and treated. Although the specifics will be different for different areas of risk management (such as strategic, operational, safety), the overall process remains comparable. See the section on Process on page 33 for a best practice approach towards the risk management process.

4.1.4. Risk criteria

An important component of the risk management process is the criteria used to evaluate the significance, value and impact of different risks.

Certain risks have evaluation criteria that are mandated by regulatory or other bodies. The organisation must adhere to these criteria wherever applicable. The externally imposed constraints – identified in Understand the external context, on page 19 – have relevance here.

Other evaluation criteria will reflect the organisation’s values, objectives, resources and individual risk preferences. Wherever possible, the organisation should take all reasonable steps to define these ‘subjective’ criteria as explicitly as possible. This is to ensure that individual risk preferences do not unintentionally bias the organisation’s risk scoring process, for example, the pre-selection of experts who are known to support a particular perspective.

Risk criteria should be consistent with the organisation’s risk management policy, as established by the executive. They should be defined at the beginning of any risk management process and reviewed on a regular basis.

When defining risk criteria, factors to be considered should include the following:

- The nature and types of causes and consequences that can occur and how they will be measured.
- How likelihood will be defined.
- The timeframe(s) of the likelihood and consequence(s).
- Timeframe of exposure.
- How the level of risk is to be determined.
- The views of stakeholders.
- The level at which risk becomes acceptable or tolerable.
- How and which combinations of multiple risks should be taken into account.
4.1.5. Performance evaluation criteria

The framework should include a description of how and when the framework itself will be reviewed. The organisation should therefore define performance metrics for the framework, including:

- The effectiveness with which risks are being managed, i.e. whether the organisation is operating within the approved risk thresholds.
- The costs and effort involved in the operation of the various risk management activities defined by the framework.
- How well the framework is aligned to the organisation’s objectives and context.
- Responses to changes in risk exposure on capital allocation / pricing and on allocation models for risk management costs.

4.1.6. Consideration of supporting systems

The framework should also note the various systems that need to be implemented to enable the risk management processes to function effectively. These systems will be unique to the organisation, and will include, but is not limited to, health and safety, financial control, information governance, information technology, and asset and property maintenance. It is also important to consider how the integration of these systems across the organisation.

4.1.7. Communication procedures

Communication and consultation with external and internal stakeholders should take place during all stages of risk management. Therefore, a communication or consultation strategy should be designed into the risk management framework from the beginning, and include the following:

- What information it needs to communicate, in terms of sensitivity, internal requirements, or legislation.
- The medium of communication, such as e-mail, posters.
- When it will communicate this.
- With whom it will communicate.
- Conditions of deviation from the communication procedure in respect of the frequency and chain of command.

4.1.8. Business continuity planning

Business continuity planning is an important aspect of organisation-wide risk management, as it allows pro-active action for those risks that result in the disruption of key business activities. Whatever the organisation’s attitude towards business continuity planning – considering it a separate function or seeing it as part of their risk management programme – it should make sure that any business continuity plans complement and are integrated into the risk management programme.

4.1.9. Risk management outputs

Different organisations have different reporting requirements, depending on their size, industry or sector. The risk management system should support the reporting requirements, ensuring that relevant information is provided in the correct manner, and to the correct level of detail, as per those requirements.
4.1.10. Resources

The organisation should determine and allocate the resources needed for the establishment, implementation, maintenance and continual improvement of the risk management framework and process. If the necessary resources to implement and manage risks are not identified and allocated efficiently, the system will not perform adequately.

Consideration should be given to the following:
- People, skills, experience and competence.
- Resources needed for each step of the risk management process, including resources for implementing controls.
- The organisation’s processes, methods and tools to be used for managing risk.
- Documented processes and procedures.
- Information (and Information Technology tools) and knowledge management systems.
- Training programmes.

4.2. Implementing the framework (Do)

Implementation of the framework throughout the organisation should be done as professionally and with as little disruption as possible.

The implementation of any organisation-wide system is a significant undertaking, and should be undertaken by experienced change management practitioners wherever possible and appropriate. Therefore, the implementation of the risk management framework should be done in accordance with established project management and change management processes, such as those found in ISO 21500. Proper implementation will help achieve the following objectives:
- Ensuring that the risk management framework is capable of achieving its objectives.
- Identifying any risks inherent in the risk management framework itself.
- Identifying any risks that may arise in the rest of the organisation as a result of implementing the risk management framework.
- Facilitate continuous learning about and improvement of the risk management system.

The organisation should also plan:
- Change management actions to control or manage the implementation risks identified.
- Monitoring and evaluation criteria to ensure the effectiveness of these controls.

4.3. Monitor and review performance (Check)

Based on the performance criteria for risk management, those responsible for risk management should continually obtain data about the performance of the risk management system and identify areas for improvement.

4.3.1. Monitoring and review of the framework

To ensure that risk management is effective and continues to support organisational performance, the organisation should:
- Regularly measure the performance of the risk management system against previously defined metrics.
- Regularly consider whether the system enables appropriate management responses to mitigate risk.
- Periodically review whether the risk management framework, policy and plan are still appropriate, given the organisation’s external and internal context.
4.3.2. Management review

Management should review the organisation's risk management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The management review should consider:
· The status of actions from previous management reviews.
· Changes in external and internal issues that are relevant to the risk management system.
· Information on the risk management performance, including trends in:
   · Non-conformities and corrective actions, with related risk exposures quantified in terms of risk appetite or risk tolerance.
   · Evaluation results.
   · Audit results.
· Opportunities for continual improvement.

The outputs of the management review should include decisions related to continual improvement opportunities and the possible need for changes to the risk management framework or process, and include the following:
· Variations to the scope of the risk management framework.
· Improvement of the effectiveness of the risk management system.
· Update of the risk assessment, business impact analysis, risk management plans and related procedures.
· Status of risk appetite and tolerance against updated risk exposures and resources
· Modification of procedures and controls to respond to internal or external events that may impact on the risk management framework, including changes to:
   · Business and operational requirements
   · Risk reduction and security requirements
   · Operational conditions and processes
   · Legal and regulatory requirements
   · Contractual or project obligations
   · Levels of risk and/or criteria for accepting risks
   · Resource needs
   · Funding and budget requirements.
· How the effectiveness of controls are measured.

4.3.3. Documentation and record-keeping

The risk management framework and performance should be documented and/or recorded as far as reasonable (preferably in both electronic and hard copy formats).

Various organisations have specific reporting and documentation requirements (e.g. financial requirements for listed companies, government requirements through the National Archives), and these should always inform the record-keeping activities of the organisation, in respect to risk management.

Within these constraints, a number of factors should be taken into consideration when creating this documentation, including:
· The organisation's needs for continuous learning.
· Legal, regulatory and operational needs for records.
· Potential benefits of re-using information for management purposes.
· Costs and efforts involved in creating and maintaining records.
· Method of access, ease of retrieval and storage media.
· Retention period.
· Sensitivity of information.
· Which information should be available to external stakeholders.
4.3.4. **Strategic risk management**

Strategic risk management helps an organisation to consider the various uncertainties that affect its strategy and strategy execution, and then act on it. It should not only consider the ‘stumbling-blocks’ that may prevent the successful execution and implementation of its strategies, but also the risks that the implementation of such strategies may bring on.

While the assessment and evaluation of strategic risks falls within the standard risk management processes described later, the framework should make specific note of when to apply these processes to strategic risks. This is because of the infrequent nature of strategic risk management, and its importance in ensuring the relevance of the risk management system itself.

The executive leadership team should specify a regular interval in which strategic risks are to be identified, assessed and treated. This is often a yearlong cycle, depending on the nature and complexity of the organisation, and often starts and concludes during an annual strategy planning session. It can be done more or less frequently as needed by the organisation.

Strategic risk management should consider the organisation’s risk thresholds (risk appetite, risk tolerance and risk-bearing capacity).

This process should be cognisant of the financial and other reporting deadlines to which the organisation must adhere. Therefore, strategic risk management activities should be planned into the organisation's calendar such that appropriate information can be obtained for the executive to make an honest and effective appraisal of the organisation's risk profile.

4.4. **Continual improvement of the system (Adjust)**

*Based on the performance evaluation, the necessary changes should continually be made to improve the performance of the risk management system.*

4.4.1. **Continual improvement**

The organisation should continually improve the suitability, adequacy and effectiveness of the risk management system.

Based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and process can be improved. These decisions should lead to improvements in the organisation's management of risk and its risk management culture.

4.4.2. **Non-conformity**

Non-conformity exists when there is a gap between the expected and actual performance of the risk management framework. This may occur for several reasons:

- Flaws in the design or implementation of the risk management framework mean that it is not addressing risks in the way that it was intended.
- The behaviour of people does not follow the risk management framework’s intention, thus bypassing controls.
- People misinterpreting or manipulating the risk management process (often to enable the achievement of other objectives, e.g. production targets, service delivery, sales, etc.).
- The context in which the organisation operates has changed, and therefore the framework is not fully relevant.
- Incidents or events occurring that were not reflected in the risk management framework.
- The external and internal contexts evolve over time, hence reducing the relevance of the risk management framework.
The ability of the organisation to respond to these reflects its overall maturity. The generic process an organisation should follow to address these non-conformities is as follows:

- Identify the gap, or ‘non-conformity’.
- React to the deviation, as applicable, to:
  - Take action to control and correct it.
  - Deal with the consequences.
- Evaluate the need for action to eliminate the causes of the non-conformity, in order that it does not recur or occur elsewhere, by:
  - Reviewing the non-conformity.
  - Determining the causes of the non-conformity.
  - Determining if similar non-conformities exist, or could potentially occur.
- Determining and implementing corrective actions as needed. Any corrective action should be appropriate for the effects of the non-conformities encountered.
- Reviewing the effectiveness of any corrective action taken and making changes to the risk management framework or process, if necessary.
- Implement any action needed.
- Review the effectiveness of any corrective action taken.
- Make changes to the risk management framework and process, if necessary.

The organisation should retain documented information as evidence of the nature of the non-conformities and any subsequent actions taken, and the results of any corrective action.

Based on the performance evaluation, the necessary changes should continually be made to improve the performance of the risk management system.
1. Communication and consultation

To successfully achieve any risk management activity, it is critical that the right people have access to the right information, at the right time. The communication process should be structured to identify who (internally and externally) should receive what information, to generate the information required and to communicate it on time and in an effective manner.

An organisation should develop its risk communication and consultation strategy at the very beginning of the risk management process. The reason for this is that its leadership and management team are supposed to communicate and consult with external and internal stakeholders every step along the way. It is important to communicate and consult with stakeholders, as they make decisions based on what their perceptions of the risk involved may be. Such perceptions are wide and varied, as individuals and organisations all have different values, needs, assumptions, concepts and concerns.

The communication and consultation taking place should be truthful, relevant, accurate and understandable, taking into account confidentiality and personal integrity.

An effective external and internal risk communication and consultation strategy will ensure that all the role-players who are responsible for the risk management process, as well as all the other stakeholders, understand the reasons for and the actions required by risk-related decisions. To this end, a consultative team approach may:

- Help describe the context properly.
- Ensure that stakeholders’ interests are understood and taken into consideration.
- Ensure that risks are thoroughly and appropriately identified.
- Lead to cross-functional cohesion during the analysis of risks.
- Ensure that different viewpoints are considered while defining the risk criteria, and evaluating the risks.
- Help obtain backing from leadership and other stakeholders for the risk response plan.
- Support change management actions if the risk management process recommends any organisational changes.
- Lead to improvement of the external and internal risk communication and consultation strategy over time.

2. Establishing the Context

The process of risk management starts by defining the objectives that the organisation wants to achieve, how it intends to achieve these objectives (the operating model), and which factors (both internal and external) may get in the way of achieving those goals.

Determining the context of a specific risk should be based on the context of the organisation itself – its internal operations and external environment.

Many of these elements are similar to what was described for the risk management framework itself. They will differ in the level of detail and specificity of a particular objective and risk – i.e. the framework provides the overall structure, but this is a very specific application of that structure to a particular objective and risk.
2.1. Internal context

Whereas an organisation often has little or no control over its external context, its internal context is that over which it has direct control and influence. Controlling and influencing the internal context enables the organisation to achieve its objectives. Internally, the risk management process should be aligned with the organisation’s culture, processes, structure and strategy. Ascertaining the organisation’s own particular internal context is necessary to conduct effective risk management, because:

- Risk management as a process takes place in the context of the organisation’s objectives.
- Good risk management should consider how a specific risk may impact on the objectives of the overall organisation through secondary effects.
- In some instances, an organisation could fail to grasp an opportunity to achieve its strategic, project-related or operational objectives (‘carpe diem failures’), which in turn affects stakeholders’ continual commitment to the organisation, as well as the credibility, trust and value ascribed to it.

The internal context encompasses the following organisation-related aspects, amongst others:
- The objectives of the organisation, and the strategies and policies to comply to or achieve these.
- Organisational structure and governance.
- Leadership and senior management’s roles and accountabilities.
- Resource and knowledge capabilities (i.e. capital, time, people, processes, systems and technology).
- The organisation’s relationship with internal stakeholders, its perception of these stakeholders and the value it attaches to them.
- The organisational culture.
- Formal and informal systems for the acquisition, dissemination and retrieval of information.
- Decision-making processes and strategies.
- Adopted standards, guidelines and models.
- The structure and scope of contractual relationships.
- Environmental issues (i.e. internal physical environment, including space, ergonomics, and office layout).

2.2. External context

The entire environment outside the operational control of the organisation makes up the external context of that organisation. It is crucial to understand this external context, as it influences the organisation and the forces exerted upon it by its particular market, society and setting. All of this should be taken into account, along with the external stakeholders’ objectives and concerns when considering risks.

The external context includes the following, amongst others:
- The sociocultural, natural, political, legal and regulatory, financial and economic, technological and market environments – on an international, national, regional and local scale.
- The key drivers and trends that influence the organisation’s objectives.
- The organisation’s external stakeholders and their relationship with the organisation, as well as how they perceive and value the organisation, its objectives and related risks.

2.3. Defining specific risk criteria

It may be necessary for the objectives being evaluated that additional, or different, risk criteria should be established. This should always be done in consideration of the broader criteria established in the framework itself.
3. Risk assessment

It is important to identify what could cause an organisation to deviate from its objectives, to determine how likely it is to happen, as well as what the consequences could be if it does happen. Subsequent to this, the organisation needs to determine which risks need to be addressed first, which risks are less urgent and which risks do not warrant intervention.

Risk assessment is a structured process that:
- Identifies how an organisation’s objectives could be affected by risks.
- Analyses the risk in terms of its consequences and probabilities of occurrence, along with what type of risk it is.
- Describes the priority that should be assigned to each risk.

These aspects are covered by the sections on identifying risk, analysing risk and evaluating risk that follow. In addition, the importance and process behind evaluating opportunities are also discussed. Identifying, analysing and evaluating opportunities essentially follows the same process as for risk, and as such will not be discussed, but some important concepts related to opportunity management will specifically be dealt with.

3.1. Identifying risk

3.1.1. Purpose
Risk identification endeavours to provide reasonable assurance that all key risks are discovered for assessment. Organisations should make all reasonable efforts to identify risks, yet remain aware that unpredictable events do exist that cannot be identified from the outset. For these situations, the organisation should have effective business continuity plans in place.

3.1.2. Approach
Risk identification proceeds through three stages: the finding, diagnosing and then documenting of risks.

Risks can only be efficiently responded to if they are appropriately and accurately identified, as early as possible. The process of identifying risks focuses on looking for the root causes and sources of those situations, trends, events or circumstances that could have an effect on the organisation’s objectives. It is also important to understand what kind of effect it will be, whether positive or negative (although not calculated in detail at this stage).

In the case of on-going risk management, the organisation may have already chosen various responses to manage the risk; these could include engineering, management and administrative controls (Mechanisms of control, page 44).

The organisation should apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. All risk identification should be based on the most reliable and robust data available. It should also be undertaken by people with the appropriate knowledge and skills to identify risk.

Three basic approaches can be adopted:
- Quantitative methods (e.g.: the accumulation and development of relevant historical or predictive data sets).
- Qualitative methods (e.g.: market research, surveys, questionnaires, risk workshops).
- Semi-quantitative methods, which are a combination of quantitative and qualitative methods.
3.1.3. Tools

There is a range of methods that can be used to identify risks at the various levels of an organisation, for example:

- Strategic (e.g.: strategic risk registers, competitor analysis, market trend research, PESTEL / SWOT analysis).
- Operational (e.g.: risk registers, audits, internally generated questionnaires, sales performance reports, accounting information).
- Activity or project level (e.g.: task-based risk assessments, project risk registers, project plans, and Gantt charts).

The above list is not exhaustive. A range of suggested techniques to complement internally developed risk identification processes can also be found in ISO 31010.

It should also be noted that underlying risk preferences, values and perceptions may bias the identification of risks by individuals. Therefore, wherever possible, it is preferable for more than one person to be involved in this stage of the process.

3.2. Analysing risk

Risk analysis involves developing an understanding of the risk. It involves consideration of the causes and sources of the risk, their positive and negative consequences, and the likelihood that those consequences can occur. By first analysing risks, the information necessary to undertake the risk evaluation process (Evaluating risk, page 40) is obtained. This step is important as it allows the organisation to prioritise its risks, and thereby allocate resources appropriately.

It is important to understand that an event or situation can have multiple causes or multiple consequences. A single event or situation can also affect multiple objectives. In such cases, risks can be described using a range of probabilities, across a range of circumstances.

The organisation's existing controls should be included in the risk analysis process, as these will affect the characteristics of the risk (such as its likelihood or consequence).

In some circumstances, the probability of a risk may be extremely low; this may skew the risk analysis process such that a risk is unintentionally accepted that can have significant impacts on business continuity. Alternatively, the consequence may be perceived as insignificant by itself, but in conjunction with other events, it could nevertheless lead to catastrophic outcomes for the organisation (since the combination of risks exceeds the risk tolerance). Both of these situations require sound judgment and insightful appraisal of the risk, acknowledgement of any personal or cultural bias towards risk, and a rigorous application of minimum risk thresholds.

A wide range of techniques to analyse risk exists, such as the ones described below. In many instances, it is appropriate to use more than one technique or methodology during the risk analysis process. The depth of analysis depends entirely on the context, and will be determined by the specific risk(s) in question, the availability of reliable data and the organisation's decision-making criteria. In addition, some methods and the inclusion of certain details are prescribed by legislation.

Not all analyses are conducted by using purely quantitative, numerical methods. Qualitative and semi-quantitative methodologies can also be used, in which case rating scales and significance levels deliver results.
For example, a risk can be assessed by combining its probability and consequences according to established criteria and categorising it as a 'high', 'medium' or 'low' level risk; or a numerical rating scale can be used to estimate the level of risk according to some previously agreed formulae or calculations.

Regardless of the type of analysis undertaken, the calculated levels of risk remain an estimate and are influenced by a range of factors. These may include human bias in the valuation of the risk, or even biases in the design of the risk scoring criteria of automated systems. Sample sizes are rarely exhaustive, and while relevant statistical techniques should be applied where appropriate, this cannot guarantee comprehensive data.

In addition, a level of accuracy and detail should not be inadvertently ascribed to the results. Throughout the process, good sense and sound judgment must be applied to the models used, and a rational decision must be made based on the information available. In such circumstances, the insight and experience of specialists plays an important role in checking the outputs of any modelling process to make sure they make sense.

The risk valuation criteria – for quantitative, semi-quantitative and qualitative approaches – should always be established before the process starts, preferably during the development of the organisation’s risk management framework (Risk criteria, page 27). In addition, there should be clearly defined risk-related terms, and these should be used consistently across the entire risk management framework.

3.2.1. Assessing controls

Although new risks do emerge over time, most organisations will already be managing previously identified risks by means of preventative, detective and corrective controls (see Types of controls, page 43), which are one type of response available to the organisation.

Part of the risk assessment process is to evaluate the effectiveness and adequacy of these controls to determine the residual risk. This ensures that controls remain relevant whenever there are changes in the internal and external context of the organisation, or to the risk itself. The control assessment should ask:

- Which preventative, detective and corrective controls apply to the risk?
- Can these controls treat the risk to an acceptable level of probability and consequence? (Acceptability being defined by both the risk framework itself and any risk-specific criteria established earlier.)
- Are the controls functioning as they are set up to, in other words, are they working in practice to achieve their objective?

Appropriate information and data regarding the performance of controls are absolutely necessary to answer these questions. Therefore, it is important that assurance and documentation processes are in place to track this information.

In addition, the same different types of analysis – quantitative, semi-quantitative and qualitative – can be applied to judge the suitability of these controls.
3.2.2. Analysing consequences

The second major component of a risk is the consequences it holds for the organisation. It is important to note that a given risk may have a number of different impacts, of varying magnitude, across a range of different objectives. In addition, there are likely to be downstream or indirect consequences that should also be considered.

These consequences may also affect those outside the organisation and this should be taken into consideration, as external stakeholders can have a significant impact on the organisation’s ability to operate.

Depending on the context of the risk, describing the consequences can range from simplistic descriptive outcomes to the detailed mathematical quantification of specific impacts. The level of detail should be established before the consequence analysis is begun (often, this is defined in the risk management framework itself).

When analysing the consequences of a risk, the organisation should consider the severity of its effects, where appropriate, on at least the following:

- Human and environmental well-being
- Financial stability of the organisation/activity
- Operational performance
- Governance and compliance
- Security, including financial, physical and IT
- Preservation of assets

3.2.3. Analysing likelihood and estimating probability

There are several broad approaches to estimate the probability (quantitative) or likelihood (qualitative) of an event. It is very rare for a single approach to be followed in this process, and approaches can be applied in concert or consequentially. In particular, obtaining expert judgment is vital, to ensure that the outputs of any modelling or extrapolative process are reasonable and robust.

The various tools or techniques described can be classified according to the following types:

3.2.3.1. Extrapolation from historical data

The use of historical data can be a powerful approach to identify the root causes of events or situations that occurred in the past. The fundamental assumption is that events will re-occur under similar circumstances, and can therefore be reliably predicted.

There are many situations in which this assumption is valid, often in operational situations such as where the failure rate of a particular device leads to downtime, or in insurance situations such as where unprecedented hailstorms lead to an increase in claims.

However, there are many situations in which the assumption is not valid, or is perceived to be valid when it is in fact not valid. It is imperative that any assumptions regarding the suitability of historical data be clearly articulated by the organisation and the usage of such data be individually agreed on. This is particularly the case for situations with a very low likelihood or probability, or for which there is very little historical data (it has not happened very often).

The data used should be relevant to the organisation, system or activity being considered, and should be sufficiently detailed to meet the organisation’s risk analysis criteria.
3.2.3.2. Probability modelling

In a number of circumstances, direct relevant information regarding a particular risk or situation may be inadequate or may simply not exist. For example, when planning a new activity there may not be historical data (although there may be historical information for a similar activity).

Appropriate models can be created, based on the theoretical behaviour of the system, to predict future events and situations. Often, these can be calibrated using data from similar systems, organisations, technologies, other operational experience or externally published or available data. Appropriate modelling techniques are noted in various documents, such as ISO 31010.

A concern when using predictive models is that they may not fully incorporate system-wide influences (as the entire system is unlikely to be modelled). This should be taken into account when evaluating risk.

3.2.3.3. Expert judgment

Beyond the development of quantitative or qualitative models (such as those described above), the opinion of industry experts and specialists can be invaluable in estimating the likelihood of an event. It is recommended that the organisation provides the maximum amount of relevant information to their appointed experts; such information includes, wherever appropriate, historical information, the outputs from various predictive models, and the organisational, operational and other information that is deemed necessary to make an effective assessment.

3.2.4. Completing the risk register

Once the risk has been fully described, it should be documented in an appropriate register or similar structure. The risk responses that have been enacted (including any controls that have been implemented) to manage the risk should also be included.

This step enables the risk evaluation process, (page 40) and helps track risks over time.

3.2.5. Uncertainties and sensitivities

Despite best intentions and practices, risk management cannot be an exact science. This is because:

- It relates to an uncertain future event
- It is based on data sets that may not fully describe a potential event.
- It depends on predictive models that cannot fully specify reality.
- It relies on the judgment of people throughout the entire process – not just experts, but the people that obtain the data, the people that create the models, and the people that interpret the output.

Risk management should therefore not be perceived to describe a perfect vision of future events – it can only ever be an approximation, however accurate. This does not invalidate risk management – rather, it becomes important to recognise this constraint and put appropriate responses in place. This allows decision-makers and risk practitioners to make informed choices about the risk. Recognising these flaws in the process therefore revolves around the uncertainty of the inputs and assessment process. Uncertainty analysis helps determine the level of variation or imprecision in the results. These may arise from variations in the data sets available, or the assumptions used in the modelling process.
Essentially it asks the question: “If we say the risk is 80%, how sure are we that it is not in fact 90%, or 70%?; or if one uses a qualitative approach – if we believe the risk is ‘medium’ how likely is it to actually be ‘high’ or ‘low’?

Sensitivity analysis is a closely related area, and helps define how easily a given risk changes, if one of its underlying causes or contexts change. For example, if one were measuring how the total fleet costs of a company affected its operating margin, then one could look at incremental changes in the price of fuel: how much difference does a price increase of one rand make? or two rand? and so forth.

Sensitivity analysis further allows an organisation to determine those variables that have a large knock-on effect on a risk, in comparison to those to which the risk is relatively immune. This can help to direct resources to understand those ‘sensitive’ risk factors in detail.

Wherever possible, risk models or methods should specify their sources and levels of uncertainty. These models or methods should also state and describe the variables or parameters to which the analysis is sensitive, including the degree of sensitivity.

### 3.3. Evaluating risk

The final step in the risk assessment process is to evaluate the risk. This involves comparing the risk against pre-determined criteria, thus specifying the significance of the risk to the organisation’s objectives.

All available information should be used in the evaluation stage, including the relevant risk thresholds the organisation has specified in terms of legal, ethical, financial or other constraints. The decision that should be taken at this point should consider the following:

- The priority of a risk, and hence the urgency with which it should be addressed.
- Any risks that can be accepted without further action, such as very low probability and very low impact.
- Those risks which should be accepted only with the implementation of specific responses, (Risk response, page 43).
- Any immediate decisions to avoid risks that breach specific thresholds.
- The decision-making criteria should have been specified at the beginning of the risk management process, usually in the overall risk management framework. There may also be specific criteria mandated by legislation or regulation.
- Where risks are accepted ‘as is’ it is important to note any factors that may escalate them upwards, and hence require a response. These should be documented and tracked so that the risk does not escalate without an appropriate response.

The decision-making criteria should have been specified at the beginning of the risk management process, usually in the overall risk management framework. There may also be specific criteria mandated by legislation or regulation.

Where risks are accepted ‘as is’ it is important to note any factors that may escalate them upwards, and hence require a response. These should be documented and tracked so that the risk does not escalate without an appropriate response.
3.4. **Opportunity Assessment**

The same methodology used to identify, analyse and evaluate risks is used to collect business insights regarding opportunities. This assessment process should not be limited to identifying positive aspects related to threats. At the end, changing business environments create both risks and opportunities to innovate or adapt the organisation to the new playing field.

Opportunities identified by top management should be communicated, validated and responded to by all the employees across the organization (top-down). It is also important that employees are empowered to communicate their ideas for improvement, adaptation and innovation upwards through the management structure of the organisation (bottom-up).

An organisation should therefore consider a wide range of opportunities, including but not limited to those that:

- Create a new process, product or service.
- Improve existing processes, products or services.
- Broaden the range of products or services (geography, target).
- Use excess resources.
- Generated from changing stakeholder demands (e.g. Freeing up capital).
- Reduce the use of various resources, including financial or natural.
- Improve the reputation and trust which stakeholders have in the organisation.
- Improve health and safety performance.
- Build or strengthen alliances, partnerships and relationships with both new and existing stakeholders.

Several of these can be related to risk, such as reputational risk that is linked to opportunities to improve the organisation’s public image.

*It is important to identify what could cause an organisation to deviate from its objectives, to determine how likely it is to happen, as well as what the consequences could be if it does happen. Subsequent to this, the organisation needs to determine which risks need to be addressed first, which risks are less urgent and which risks do not warrant intervention.*
4. Risk response

The organisation has to decide on, develop and pro-actively implement the various actions needed to prevent its activities from being derailed.

Once risks have been identified, assessed and evaluated there will be enough information to begin the process of responding to the risks. This involves selecting the options for modifying and/or mitigating the identified risks, and implementing these options. It should be remembered that different response options often institute new risk controls or modify existing ones.

Responding to risks is a cyclical process that begins with assessing a current or proposed risk response for suitability and effectiveness. When choosing, evaluating or re-evaluating how to respond to a risk, one should determine whether the residual risk levels are acceptable, and if not, consider what additional responses may be required. This will ensure that risks are managed within the risk tolerance and risk appetite thresholds established earlier.

4.1. Risk responses available

Different risk response options are not necessarily mutually exclusive. Neither are they all suitable in all circumstances.

Some of the standard responses include:

4.1.1. Accepting or tolerating the risk

The organisation may decide to accept the level of risk inherent to an event and continue to pursue its objectives. This may occur if or when the management team believes that the costs of responding to the risk do not create or protect sufficient value to justify additional effort. In this case, it may be better to simply accept the positive or negative consequences, integrate the risk into existing processes and incorporate the learning into future decisions.

4.1.2. Avoiding the risk

The organisation may decide to completely avoid this specific risk by deciding not to pursue or continue the activity that gives rise to the risk exposure. This means that the organisation will not suffer the consequences but will also not have the opportunity to benefit from the activity.

4.1.3. Removing the source of risk

It may be possible under particular circumstances to remove the source of risk from the activity. This is particularly the case if it is a technology or asset that can be disposed of, substituted or replaced. This option can be applied in other ways as well, for example by changing (an aspect of) the operating model of the organisation.
4.1.4. Changing the likelihood

It may be possible to influence the likelihood of an event. This option usually adjusts either the operating processes or human behaviour that give rise to a particular risk. An example would be introducing mandatory rest breaks for long-distance drivers (thus reducing the likelihood of accidents), or increasing the acceptance criteria for issuing short-term debt (thereby improving the quality of debtor, and hence decreasing the likelihood of default). These are also known as preventative controls.

4.1.5. Changing the consequence

A variety of techniques can affect the severity of a particular risk. These involve a detailed understanding of the consequences, and who experiences them. This can range from the provision of fire-fighting equipment as a measure of last resort to maintaining an effective emergency response plan for certain catastrophic operational events. These are often known as corrective controls.

4.1.6. Transferring the risk

A final option is to transfer the risk (at a price) to another party or parties; this usually focuses on the financial consequences of a risk (e.g. loss of income, unexpected expenditure). This may include contractual agreements, outsourcing, risk financing and insurance. Risk transfer is a risk management technique whereby risk of loss is transferred to another party through a contract (e.g., a hold harmless clause) or to a professional risk bearer (i.e., an insurance company) normally at a fee or premium. Risks that are transferred normally refer to activities with low probability of occurring, but with a large financial impact. The best response is to transfer a portion or all of the risk to a third party by purchasing insurance, hedging, outsourcing, or entering into partnerships. Alternative Risk Transfer (often referred to as ART) is the use of techniques other than traditional insurance and reinsurance to provide risk bearing entities with coverage or protection. Most of these techniques permit investors in the capital markets to take a more direct role in providing insurance and reinsurance protection.

4.1.7. Exploit the opportunity

For positive risks, the organisation may wish to allocate additional resources to exploit and benefit from the uncertainty. This is often the case when external trends or factors move in the organisations favour (such as movements in the exchange rate, relaxation of legislation, or actions of competitors).

4.2. Selection of risk response options

As mentioned, there are several factors to consider when selecting the risk response:

- What the residual risk would be after responding to the risk, and whether this residual risk is acceptable.
- The cost-to-benefit ratio – balancing the effort and expenditure required with the benefits.
- Legal and/or regulatory requirements (e.g.: social responsibility initiatives, environmental laws, occupational health and safety advisory standards, and sustainability imperatives).
- Risk response that may not be economically viable, but still warranted (e.g.: high-impact, small likelihood risks).
- Has sufficient investigation and resource been applied to the development of new risk response capabilities (i.e. reducing impact and / or likelihood)
Solitary response options or combinations of responses (e.g.: a mixture of preventative and corrective measures; organisations generally benefit from using a combination and variety of risk response options).

- The values and perceptions of stakeholders – though equally effective, some risk responses are more acceptable to some stakeholders than to others.
- Inter-dependencies – where risk response options can affect risk elsewhere in the organisation, in which case the stakeholders involved in those areas also need to be consulted.
- Secondary risks arising from the choice of response – these knock-on risks should also be assessed (identified, analysed and evaluated) and incorporated into the same response plan as the original risk (not treated as a new risk) – the relationship between the two risks should be identified and maintained.

The response plan should clearly identify the order in which individual responses should be implemented. Monitoring needs to be an integral part of the risk response plan to ensure that the measures remain effective.

4.3. Risk controls

A risk response is essentially a control that influences the likelihood or severity of the risk. Risk controls can be defined according to two dimensions – the types of control describe how they influence a risk, while the mechanism of control talks about how they achieve this.

4.3.1. Types of control

Controls can be divided into three groups according to how they influence risk – preventing, detecting or correcting – as below:

4.3.1.1. Preventative controls

These affect the likelihood of a particular risk occurring.

The primary advantage of a preventative control is that the effort required to prevent a risk from occurring can be significantly lower than dealing with the consequences. For example, regular maintenance in a manufacturing plant is much more efficient than allowing equipment to break down, which incurs both replacement costs, along with operational downtime.

Regular pre-emptive maintenance, training and skills development, separation of duties, and credit-worthiness checks are examples of preventative controls.

4.3.1.2. Detective controls

Detective controls identify events that have already happened, but which have not necessarily affected the operational ability of the organisation (and hence may have gone unnoticed).

They are useful as they allow the organisation to institute corrective or mitigating actions early enough so that further deviation from objectives might be prevented. They also help ensure that corrective controls are being implemented properly.

Inspection of equipment or facilities, regular internal and external audits and the use of leading and lagging safety indicators are examples of detective controls.
4.3.1.3. Corrective controls
These affect the severity or consequences of a risk, either minimising harm or optimising benefits.

The main advantage of corrective controls is that they enable the continued operation of the organisation or activity, helping to maintain continuity in delivering services or products to the organisation's stakeholders, and value to its shareholders.

Examples of corrective controls include insurance, product stockpiles, emergency response plans and teams, force majeure contracts and back-up power generators.

4.3.2. Mechanisms of control
Controls can also be categorised according to the mechanism by which they achieve the desired effect, whether through physical control of the risk, modifying human behaviour, or a combination of both. There are three types of controls – engineering, management and administrative. These are arranged in terms of the strength of the control influencing the risk – engineering controls being the strongest, then management controls, then administrative controls.

4.3.2.1. Engineering controls
Engineering controls are physical systems in place that are designed to act or function within specific constraints. They can be designed with fail-safe principles, such that when operating conditions are exceeded, the physical processes cease.

Engineering controls can also be used for non-physical systems – generally IT platforms – in which specific operating constraints can automatically start or stop activities (such as stop-limit orders in financial trading).

Engineering controls generally operate without human intervention after they have been set up and started. They are reliant on effective design to ensure adherence to the operating parameters set.

4.3.2.2. Management controls
Management controls relate to the systems, processes and policies in place that assist an organisation to function according to its operating model. They include the organisation's commitments to legal and regulatory constraints, and include, amongst others:

· Information systems technology
· Financial reporting
· Risk management
· Operating procedures (including health and safety)
· Governance and compliance.

Management controls rely on effective system design, delegation of authority, appropriate skills and organisational capacity. They are most effective when the organisational culture is strongly aligned with the overall management style and culture, as they depend on a combination of human implementation and engineering systems (such as IT).
4.3.2.3. Administrative controls

Administrative systems are a monitoring control that ensures that policies, processes and systems are being implemented effectively, often enough and strictly enough.

Administrative controls are the weakest, as they rely on (relatively) infrequent manual analysis of performance, which can often only identify a problem after it has occurred.

Administrative controls can be used in risk prediction if they are captured effectively; however, engineering solutions can often be developed that are more reliable and efficient. Administrative controls rely on people for implementation and continuation.

4.4. Preparing risk response plans

As with all systems, once established, it is essential to document the chosen response options and how and by whom these will be implemented. The information in such a risk response plan should include:

- The response(s) chosen.
- The reason for the choice of response.
- The secondary risks, possible benefits and effects on stakeholders associated with each response.
- The individuals and groups responsible for implementing the plan, as well as who approved the plan.
- The proposed actions.
- The resources required.
- Contingencies, performance measures and constraints.
- Reporting and monitoring requirements.
- Timing and schedule.

The response plans should also be integrated with the organisation's management processes and communicated with the various relevant stakeholders.

All stakeholders should appreciate that risk management is not aimed at eliminating risk, but rather to manage it to keep within the acceptable risk thresholds. As such, there always remains residual risk for an activity or decision, even after responding to the risk. This residual risk should be noted, documented and subjected to the risk management process as far as is reasonable.

4.4.1. Preparing and implementing risk response plans

Risk response plans are developed to document and describe how a specific response will be implemented. The plan should include the following information:

- A description of the risk, including its likelihood and severity.
- Any other controls already in place.
- The option that has been selected, along with an appropriate and practical cost-benefit analysis justifying the selection of that particular option.
- Accountabilities and responsibilities of who will implement and monitor the option throughout its life cycle (including implementation and operation).
- The proposed actions to implement the option.
- A description of resources required to implement the option, including financial and human resources, etc. The plan should also contain the contingency resources required.
- The performance monitoring and performance evaluation criteria for the option.
- The reporting process and reporting system, including frequency of reporting.

The response plan should be developed by considering the overall risk management framework, and from there on it should be integrated with other relevant management systems in the organisation, such as financial reporting, health and safety monitoring, and IT governance.
5. Monitoring and review

Monitoring and review are the activities undertaken to ensure that the risk management process actually works as set out according to the organisation's risk management framework, and that it happens at the appropriate level of cost and effort.

Another important part of the risk management process that should be planned beforehand, is how risks will be monitored and reviewed. This should entail regular checking or observation, whether impromptu, at set intervals or continuously.

The risk management plan should specify who is responsible for monitoring and evaluating which risk, the extent to which it should be monitored and the factors that should be taken into account when reviewing the risk. This will enable those responsible for risk management to reach the following goals:
- Designing and implementing effective (method-wise) and efficient (cost-wise and time-wise) risk responses.
- Improving the organisation's risk assessment over time as new information comes to light.
- Analysing events as they happen (close calls as well) and learning from these events.
- Identifying changes, trends, successes and failures.
- Detecting changes in the organisation's external and internal contexts, which includes changes to the risk criteria and the risk itself, leading to the revision of risk responses and priorities.
- Identifying any new or previously unrecognised risks.

In this regard, performance can be measured by evaluating the progress made by implementing the organisation's chosen risk response plans. These progress results can be incorporated into the organisation's overall performance management, its performance measurement and its external and internal reporting activities.

Monitoring and review work must include planning, examining and evaluating, recording, communicating results and following up.

5.1. Planning the monitoring and review

Each monitoring activity must be properly planned before it starts. The planning must be documented and should include:
- Establishing monitoring objectives and scope of work.
- Obtaining background information about the activities to be monitored.
- Determining the resources (people and time) necessary to perform the monitoring.
- Identifying and documenting specific risks relating to the area concerned.
- Identifying and documenting existing controls in place to mitigate identified risks.
- Writing a monitoring program that responds to the risks identified or updating existing monitoring programs.
- Obtaining approval of the monitoring work plan.

5.2. Examining and evaluating information

Those responsible for monitoring and review have to collect, document, analyse and interpret the information gathered. The process of examining and evaluating information is as follows:
- Performing a walkthrough of the activity and collecting information on all matters related to the monitoring objectives and scope of work.
- Information should be sufficient, competent, relevant and useful to provide a sound basis for monitoring findings and recommendations.
- Conducting control operating effectiveness testing.
- Documenting monitoring issues with ratings.
- Holding a close-out meeting with management.
5.3. Recording the risk management process

The results of monitoring and reviewing risk should be recorded and reported on (externally and internally) in an appropriate manner. It should also serve as input during the cyclical review of the risk management framework.

Activities undertaken as part of risk management should by their very nature be traceable, and noted, so that these records can serve as a foundation for improvement in methods and tools, as well as in the overall process.

When deciding how risk management activities should be recorded, the following aspects should be taken into account:
· The cost and effort that creating and maintaining such records would entail.
· The legal, regulatory and operational requirements where records are concerned.
· How records would be accessed, how easy retrieval needs to be (backups included) and the type of storage media required.
· How long records should be retained.
· How sensitive is the information contained in the records.
· How reusing information would benefit management purposes.
· How the analysis of records could aid the organisation in its learning process.

5.4. Communicating results

Responsible persons shall communicate their results through the issuing of monitoring reports as follows:
· Preparing and issuing a draft report.
· Documenting the agreed management action plans.
· Preparing and issuing a final report.

5.5. Follow-up

Those responsible for risk management must follow up on reports to ascertain that appropriate action is taken after the findings and recommendations. It is vital to ensure that corrective action is taken and achieves the desired results, or that management has assumed the risk of not taking corrective action on reported findings.
Conclusion

1. Maturity measure

After all has been said and done, closing the cycle by returning to some basic questions would serve the organisation well. The questions that follow would help an organisation understand how mature it is in regards to risk management.

Answering these questions would help highlighting areas for immediate attention, and identify which elements of the risk management framework, culture and behaviour should be improved. The questions do not make up a scorecard according to which performance should be measured; instead, the answers to these questions should inform the executive about the overall state of risk management in the organisation. Certain questions could also be evident to the application of a minimum standard. This can assist the executive and management to establish realistic and achievable improvement targets against which performance should be managed.

1.1. Risk management culture

Is there buy-in to risk management at the highest level of the organisation?

Is the organisation able to demonstrate that the executive accepts its responsibilities for risk management, reflected in its mandate or charter? Is risk on the agenda of the executive committees, or included in the strategic intent of the organisation (i.e. the organisation aspires to good risk management practices)? Does the organisation release an annual risk strategy approved by the executive?

Do all managers have a consistent understanding of what is acceptable and unacceptable risk to the organisation?

Have risk-bearing capacity, risk appetite and risk tolerance criteria been determined by the appropriate management structure?

The principle issue here is one of ‘shared risk management values’. Achieving this involves using common methods to measure risk, an organisation-wide approach to prioritising risk mitigation and consistent internal communication and training about risk. Consistency will be evident in such things as reports to directors, selection of insurance deductibles, capital expenditure guidelines and standard operating practices. Are the risk thresholds critiqued for consistency and application of present practices to continue developing and introducing improvements to the present practice?

Do managers have specific risk management responsibilities in their key performance indicators?

Position descriptions, key performance indicators, and formal delegations are all ways in which organisations provide direction to the management team. If these documents do not include risk management responsibilities it is unlikely that there will be a shared understanding of risk management expectations. It can also signal that risk management is not very important. Integrating risk management responsibilities into managers’ key performance indicators will ensure there is both direction and accountability for risk management performance.
Do you have a current (up to date) inventory of risks for the organisation?

A risk inventory (often called a risk register) provides a central source of risk information that can be used to plan, review and monitor the success of risk action plans and other risk management activity. It also helps risk information to be factored into day to day management decision-making and so contributes to good governance. Risk inventories that are not kept current are unreliable and can result in unsound decision-making. Spreadsheets and other programs are available that may assist in maintaining and giving managers access to the risk inventory. Is your organisation making consistent improvements to your risk inventory and considering suitable evaluation, quantification and software tools?

Is a transparent, integrated approach taken to risk management reporting?

Are the management mandates appropriate to the risk management delegations and performance measures?

Different decision-making authority will be delegated to management structures; part of this will be an explicit or implicit limit of authority as regards the risk associated with the decision. It is important that the limits of authority are connected to the risk thresholds and risk performance for which they can reasonably be held accountable.

Are the response measures for critical risks observed consistently at all levels of the organisation?

Critical risks warrant continual and consistent attention across the entire organisation. Deeds need to consistently match words. For example, there is no point in having a risk policy that says “safety is our first priority” if managers walk past unsafe work place situations. An external perspective is important to reviewing consistency of the controls for critical risks and, where there is no consistency, devising an appropriate mix of improvements.

1.2. Risk management framework

Do you have a risk management policy that includes all forms of risk?

A formal risk management policy is intended to set out the organisation’s approach to risk. It introduces a common language and understanding of risk, demonstrates management ownership and endorsement of an approach and helps ensure that all employees have a sound basis for risk management decision-making and application. This policy needs to be worded in a way that contemplates all forms of risk. The policy should reflect the organisation’s overall goals and operating environment.

Do you have documented procedures to respond to the various types of risk?

If risk responses are not documented, it is impossible to take a proactive approach to managing risks or to formally delegate responsibility for implementation or train employees, and it is unlikely that there will be consistent application of the responses. The process of documenting the responses provides an opportunity to seek employees’ input to ensure that responses are practical. Organisations should consistently devise and document responses, recording these in either paper or user-friendly electronic manuals, and develop associated training and auditing protocols.
Do you routinely capture, analyse and report on incidents, close calls and loss-producing events to senior management or directors?

Information and data in relation to incidents (including near misses) provides both insight into the causes and prevention of events, and provides governance data including an understanding of associated costs. It is important to design methods to capture this information, analyse it and then report against appropriate criteria.

Do you have documented procedures in place to protect the security of people, assets, intellectual property and financial assets of the organisation?

Every country and industry has specific issues in respect of its security environment. This can extend to such issues as employee security and their families both at home and overseas, theft of intellectual property of an organisation, personal information of employees and customers, and the political landscape. The procedures need to be formulated, bearing in mind the specifics of both the country and industries. It is important to critically assess the organisation’s vulnerabilities and procedures, and to devise a framework or improve the existing one to align to the organisation’s overall goals and operating environment.

1.3. Risk management practice

Does your organisation routinely/regularly identify and measure its risks?

Every decision or management action has the effect of in some way changing risks. To manage risks proactively, it is preferable to routinely identify and measure risks at the time the decisions are made. Additionally, it is prudent to review risks periodically, particularly if there have been changes in the external or internal environment or if the company has changed its strategic focus. It is important to devise risk assessment practices, identify key decision-making points at which to apply standard assessment practices, and provide periodic external review of existing risks.

Do you regularly report to the executive on key risks?

The executive cannot fulfil responsibilities for good governance unless they are aware of the organisations’ key risks. Risk information should be included in regular reports as well as those concerning major projects or to inform other key decisions. This will obviously include high or extreme risks, as well as those controls on lower risks for which the controls are critical. It is important to develop reporting regimes and by providing periodic external audit by way of independent confirmation to senior management and directors.

Are employees regularly trained in a range of risk management issues?

As with any other aspect of the business, required levels of risk management performance are unlikely to be achieved unless employees are appropriately trained and there is consistent and regular reinforcement of the training. It is important to develop training material, source in-house trainers and directly deliver training at all levels of the organisation.
Do you consistently use advice of professionals to make decisions with significant exposure to liability, environment, brand and safety risks?

Managing these risks effectively will usually require at least some skill sets which are not available within the organisation. It is important to engage well qualified and experienced risk consultants who offer a wide range of professional expertise and experience in your industry sector to help ensure that risk factors are fully considered in major decision-making. Where appropriate, you should expect to work closely with in-house or external legal counsel, financiers or other professional advisers.

Do you have the performance of most of your risk management framework independently and externally tested?

An external audit provides an independent evaluation and perspective of performance and can therefore help drive improvement. The fact that such reviews occur also helps stakeholders form a positive view of risk management practice. It is important to undertake these assessments across the spectrum of risk issues ranging from property, liability, safety, environmental, product/brand and contingency planning.

Does your capital expenditure or project development authorisation process include a specific requirement to identify and document associated risks?

Capital expenditure inevitably introduces new or changed risks. The formal process for capital expenditure approval that occurs in most companies provides an opportunity to ensure that risks associated with new projects or expenditures are foreseen. This further embeds good risk management practice. It is important to design a suitable risk assessment model for incorporation into the capital expenditure and project development approval processes.

Does the organisation have a plan to deal with business disruptions?

A key risk for all companies is that they may be unable to operate as usual due to an event that either directly disrupts their operations or disrupts the interruptions of one of their supply chain partners. By fully analysing this risk, and preparing suitable plans to deal with the event should it occur, the impacts of the event could be much reduced. Such plans are also useful to demonstrate to insurers that business interruption risk and product liability risk are being effectively controlled. It is important that companies in all industries prepare plans, tailored to the company’s needs, to deal with the various aspects of business disruption risk.

Have you estimated how much uninsured, unbudgeted loss you could withstand this year (what is the organisation’s risk-bearing capacity)?

Insurance is a suitable method of funding losses that you do not have the capacity to fund within the organisation. Most premiums are, however, expensive. By formally considering what capacity your organisation has to fund unbudgeted losses without insurance, premium expenditure can be better targeted.

Can you provide assurance and objectively prove to the executive that the management of your key risks is better this year than last year?

Continuous improvement of both effectiveness and efficiency of risk management practice is fundamental to achieving best practice. As with other areas of business improvement, risk management efforts need to be planned and measured using consistent metrics in order to evaluate year on year progress. It is important to develop planning templates and appropriate risk management metrics. Improvement data is useful in demonstrating an improving risk profile to insurers.
The first step in risk management is defining the objectives that the organisation wants to achieve, how it intends to achieve these objectives (the operating model), and what might get in the way of achieving them.

The board or equivalent is responsible for the governance of risk throughout the organisation, and for delegation of authority, but managing risks itself is the responsibility of every individual in the organisation.

The risk culture of the organisation describes the overall behaviour of every member in how they view, handle, manage and communicate about risk.

The mandate begins with the executive leadership team, who are responsible for both allocating all other responsibilities, and ensuring the effective governance of risk throughout the organisation.

Each individual in the organisation should understand and commit to meeting the specific responsibilities that go hand in hand with their position in the organisation.

The organisation should understand the overall context and objectives it is trying to achieve, and carefully plan how risk management can help achieve these.

Implementation of the framework throughout the organisation should be done as professionally and with as little disruption as possible.
Appendices

C
communication and consultation
continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk

NOTE 1 The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organisation and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:
  · a process which has an effect on a decision through influence rather than power.
  · an input to decision-making, not joint decision-making.

consequence
outcome of an event affecting objectives

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

control
measure that is modifying risk

NOTE 1 Controls include any process, policy, device, practice or other action that modifies risk.

NOTE 2 Controls may not always exert the intended or assumed modifying effect.

E
establishing the context
defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy

event
occurrence or change of a particular set of circumstances

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an “incident” or “accident”.

NOTE 4 An event without consequences can also be referred to as a “near miss”, an “incident”, a “near hit” or a “close call”.

exposure
extent to which an organisation and/or stakeholder is subject to an event

external context
the environment outside of the organisation in which it seeks to achieve its objectives

F
frequency
number of events or outcomes per defined unit of time

NOTE Frequency can be applied to past events or to potential future events, where it can be used as a measure of likelihood/probability.

H
hazard
source of potential harm

NOTE Hazard can be a risk source.
**I**

inherent risk

risk that exists before any risk response

internal context

internal environment in which the organisation seeks to achieve its objectives

**L**

level of risk

magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood

likelihood

chance of something happening

**R**

residual risk

risk remaining after risk response

**P**

probability

measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

**M**

monitoring

continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

**N**

NOTE 1 In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as a probability or a frequency over a given time period].

NOTE 2 The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

**N**

NOTE Monitoring can be applied to a risk management framework, risk management process, risk or control.

**N**

NOTE Review can be applied to a risk management framework, risk management process, risk or control.

**N**

NOTE Risk acceptance can occur without risk response or during the process of risk response.

NOTE Accepted risks are subject to monitoring and review.

**N**

NOTE Risk appetite includes risk estimation.

**N**

NOTE Risk analysis provides the basis for risk evaluation and decisions about risk response.

**N**

NOTE Risk analysis includes risk estimation.

**N**

NOTE Risk appetite amount and type of risk that an organisation is willing to pursue or retain
risk assessment
overall process of risk identification, risk analysis and risk evaluation

risk attitude
organisation’s approach to assess and eventually pursue, retain, take or turn away from risk

risk aversion
attitude to turn away from risk

risk avoidance
informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk

NOTE Risk avoidance can be based on the result of risk evaluation and/or legal and regulatory obligations.

risk criteria
terms of reference against which the significance of a risk is evaluated

NOTE 1 Risk criteria are based on organisational objectives, and external and internal context.
NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements.

risk description
structured statement of risk usually containing four elements: sources, events, causes and consequences

risk evaluation
process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

NOTE Risk evaluation assists in the decision about risk response.

risk financing
form of risk response involving contingent arrangements for the provision of funds to meet or modify the financial consequences should they occur

risk identification
process of finding, recognising and describing risks

NOTE 1 Risk identification involves the identification of risk sources, events, their causes and their potential consequences.
NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder’s needs.

risk management framework
set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation

NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage risk.
NOTE 2 The organisational arrangements include plans, relationships, accountabilities, resources, processes and activities.
NOTE 3 The risk management framework is embedded within the organisation’s overall strategic and operational policies and practices.

risk management plan
scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk

NOTE 1 Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.
NOTE 2 The risk management plan can be applied to a particular product, process and project, and part or whole of the organisation.

risk management policy
statement of the overall intentions and direction of an organisation related to risk management

risk management process
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk
risk management
coordinated activities to direct and control an organisation with regard to risk

NOTE 2 The level of risk retained can depend on risk criteria.

risk management audit
systematic, independent and documented process for obtaining evidence and evaluating it objectively in order to determine the extent to which the risk management framework, or any selected part of it, is adequate and effective

risk matrix
tool for ranking and displaying risks by defining ranges for consequence and likelihood

risk owner
person or entity with the accountability and authority to manage a risk

risk perception
stakeholder's view on a risk
NOTE Risk perception reflects the stakeholder's needs, issues, knowledge, belief and values.

risk profile
description of any set of risks
NOTE The set of risks can contain those that relate to the whole organisation, part of the organisation, or as otherwise defined.

risk register
record of information about identified risks
NOTE The term "risk log" is sometimes used instead of "risk register".

risk reporting
form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management

risk retention
acceptance of the potential benefit of gain, or burden of loss, from a particular risk
NOTE 1 Risk retention includes the acceptance of residual risks.
NOTE 2 Risk responses that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".
NOTE 3 Risk response can create new risks or modify existing risks.

NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate risk sharing.
NOTE 2 Risk sharing can be carried out through insurance or other forms of contract.
NOTE 3 The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.
NOTE 4 Risk transfer is a form of risk sharing.

risk source
element which alone or in combination has the intrinsic potential to give rise to risk
NOTE A risk source can be tangible or intangible.

risk tolerance
organisation's or stakeholder's readiness to bear the risk after risk response in order to achieve its objectives
NOTE Risk tolerance can be influenced by legal or regulatory requirements.

risk response
process to modify risk
NOTE 1 Risk response can involve:
- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk.
- taking or increasing risk in order to pursue an opportunity.
- removing the risk source.
- changing the likelihood.
- changing the consequences.
- sharing the risk with another party or parties (including contracts and risk financing).
- retaining the risk by informed decision.
NOTE 2 Risk responses that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".
NOTE 3 Risk response can create new risks or modify existing risks.
risk

effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected – positive and/or negative.
NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process).
NOTE 3 Risk is often characterised by reference to potential events and consequences, or a combination of these.
NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

S

stakeholder

person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity

NOTE A decision-maker can be a stakeholder.

V

vulnerability

intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence

To successfully achieve any risk management activity, it is critical that the right people have access to the right information, at the right time. The communication process should be structured to identify who (internally and externally) should receive what information, to generate the information required and to communicate it on time and in an effective manner.
References

Normative references


Department of Professional Practice KPMG, 2009, *King III Summary*, KPMG, Johannesburg, South Africa.


King Committee on Corporate Governance, 2009, *King Report on Governance for South Africa*, Institute of Directors, Johannesburg, South Africa.


Supportive references


Mitchell, S. & Switzer, C., 2012, GRC Capability Model V.2.1, OCEG, Scottsdale, USA.


PricewaterhouseCoopers, 2009, King’s Counsel*: King III at a Glance: Steering Point, pwc, Johannesburg, South Africa. *connectedthinking

PricewaterhouseCoopers, 2009, King’s Counsel*: Understanding and Unlocking the Benefits of Sound Corporate Governance, pwc, Johannesburg, South Africa. *connectedthinking


The Risk Management Society, 2011, RIMS SRM Definition, RIMS, Altamonte Springs, Florida, USA.

Contact Us

PostNet Suite 616
Private Bag X43
Sunninghill, 2157

First Floor, A Block
Grayston Ridge Office Park
144 Katherine Street, Sandton
www.irmsa.org.za  | 011 555 1800