Ethics Risk Handbook

Guidelines for
- ethics and risk practitioners
- governing bodies

Editor: Leon van Vuuren
Ethics Risk Handbook

Guidelines for
- ethics and risk practitioners
- governing bodies

Editor: Leon van Vuuren
Other publications in The Ethics Institute's handbook series

The Social and Ethics Committee Handbook (2012)
The Ethics Reporting Handbook (2014)
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>2</td>
</tr>
<tr>
<td>Recognition of sponsorship</td>
<td>4</td>
</tr>
<tr>
<td><strong>PART 1: INTRODUCTION</strong></td>
<td>5</td>
</tr>
<tr>
<td>1.1 The purpose of this handbook</td>
<td>6</td>
</tr>
<tr>
<td>1.2 Target audience</td>
<td>6</td>
</tr>
<tr>
<td>1.3 Standardisation of names of ethics risk management structures and role players</td>
<td>7</td>
</tr>
<tr>
<td><strong>PART 2: RISK MANAGEMENT</strong></td>
<td>9</td>
</tr>
<tr>
<td>2.1 About risk management</td>
<td>10</td>
</tr>
<tr>
<td>2.2 The upside of risk-opportunity management</td>
<td>11</td>
</tr>
<tr>
<td>2.3 The importance and benefits of risk management</td>
<td>11</td>
</tr>
<tr>
<td>2.4 Risk management framework and standards</td>
<td>13</td>
</tr>
<tr>
<td>2.5 Risk management roles and responsibilities</td>
<td>14</td>
</tr>
<tr>
<td>2.6 Risk appetite and risk tolerance</td>
<td>15</td>
</tr>
<tr>
<td>2.7 Risk management in support of organisational strategy</td>
<td>15</td>
</tr>
<tr>
<td>2.8 Risk assessment</td>
<td>16</td>
</tr>
<tr>
<td>2.9 Ethics risk as a dimension of organisational risk</td>
<td>19</td>
</tr>
<tr>
<td><strong>PART 3: ETHICS RISK</strong></td>
<td>20</td>
</tr>
<tr>
<td>3.1 Ethics management</td>
<td>21</td>
</tr>
<tr>
<td>3.2 Understanding ethics risk</td>
<td>26</td>
</tr>
<tr>
<td>3.3 The nature and importance of ethics risk management</td>
<td>26</td>
</tr>
<tr>
<td>3.4 Ethics risk assessment: approach and process</td>
<td>27</td>
</tr>
<tr>
<td>3.4.1 Overview</td>
<td>27</td>
</tr>
<tr>
<td>3.4.2 The risk assessment process</td>
<td>29</td>
</tr>
<tr>
<td>3.4.3 Frequency, scope, and depth of ethics an risk assessment</td>
<td>30</td>
</tr>
<tr>
<td>3.4.4 Risk rating</td>
<td>35</td>
</tr>
<tr>
<td>3.4.5 An ethics management response to risk identification and risk rating</td>
<td>36</td>
</tr>
<tr>
<td>3.5 The ethics of ethics risk assessment</td>
<td>38</td>
</tr>
<tr>
<td><strong>PART 4: GOVERNANCE INTERFACE</strong></td>
<td>40</td>
</tr>
<tr>
<td>4.1 The strategic governance of risk</td>
<td>41</td>
</tr>
<tr>
<td>4.2 Governance oversight of ethics management</td>
<td>43</td>
</tr>
<tr>
<td>4.2.1 Risk committee</td>
<td>44</td>
</tr>
<tr>
<td>4.2.2 Governance of ethics committee</td>
<td>44</td>
</tr>
<tr>
<td>4.3 A reporting structure for the governance of ethics risk</td>
<td>45</td>
</tr>
<tr>
<td><strong>PART 5: KEY SUCCESS FACTORS FOR THE SUCCESSFUL IMPLEMENTATION OF ETHICS RISK MANAGEMENT</strong></td>
<td>48</td>
</tr>
<tr>
<td><strong>PART 6: ETHICS RISK MANAGEMENT TOOLBOX AND CASE STUDY</strong></td>
<td>51</td>
</tr>
<tr>
<td>Terminology</td>
<td>62</td>
</tr>
<tr>
<td>About the institutes</td>
<td>66</td>
</tr>
<tr>
<td>References</td>
<td>67</td>
</tr>
<tr>
<td>About the authors</td>
<td>68</td>
</tr>
<tr>
<td>Contributors</td>
<td>69</td>
</tr>
</tbody>
</table>
Foreword by The Ethics Institute

We have seen a steady increase in the demand for ethics risk assessments over the last five years. One can speculate on the reasons underlying this increase in demand. Amongst the prominent reasons for this increase are the introduction of social and ethics committees through the new Companies Act and the introduction of the Integrity Management Framework in the public sector. Both of these governance reforms have placed the strategic oversight of the ethics performance of organisations on the radar of governance bodies and executive management. It is simply not possible to exercise the governance duty of strategic oversight of ethics management without organisations conducting proper ethics risk assessments.

The Ethics Institute started its Ethics Handbook Series in 2012 with the publication of The Social and Ethics Committee Handbook. This was followed by The Ethics Reporting Handbook in 2014. The choice of making the Ethics Risk Handbook (2016) the next publication in the series was logical in light of the above developments.

Ethics management in an organisation is never an isolated exercise. On the contrary, effective ethics management presupposes close collaboration with governance structures and other management functions in organisations. In the case of ethics risk assessment, the obvious governance structures that come into play are the ethics committee and the risk committee of governing bodies. As far as management functions are concerned, collaboration with the organisational risk management function is not only unavoidable, but of crucial importance in effective ethics risk assessment.

Given the importance of collaboration between the ethics management function and the organisational risk management function, The Ethics Institute partnered with the Institute of Risk Management South Africa (IRMSA) in the preparation of the manuscript of The Ethics Risk Handbook. IRMSA immediately showed enthusiasm for this project, and I would like to thank them for their support and collaboration in producing this book.

The project team was directed by Dr Leon van Vuuren from The Ethics Institute, who was also the principal author of The Ethics Risk Handbook. I would also like to thank him and his team of co-authors for producing this valuable guide for practitioners involved in assessing and managing ethics risk in organisations.

It is our sincere wish that The Ethics Risk Handbook will become a valuable companion to practitioners involved in the governance and management of ethics in organisations. Without organisations that actively and effectively manage ethics, we cannot pursue The Ethics Institute’s vision of “building an ethical society.”

Prof Deon Rossouw
CEO: The Ethics Institute
IRMSA is dedicated to the advancement of the risk management profession. It is important that ethics risk management within an organisation not constitute merely an exercise of ticking boxes, but that it is an embedded and structured process that enables an organisation to operate effectively within strong governance structures.

With the numerous risks currently facing organisations in South Africa, it is imperative that governing bodies and the various committees are adequately equipped to ensure that they are able to not only meet but exceed the deliverables that have been mandated to them. This handbook has been a fantastic opportunity for IRMSA to work with The Ethics Institute to further empower our professionals and member organisations.

The IRMSA Guideline to Risk Management, developed in 2014, has been referenced extensively in The Ethics Risk Handbook, specifically the risk management components. This was done deliberately, to show how we are currently operating in the risk management landscape, and to assist us in creating better frameworks and guidelines for understanding ethics risk management in organisations.

We would like to thank the members of both institutes who assisted in formulating The Ethics Risk Handbook for their expertise and contributions. This handbook will become a valuable tool that will enable organisations to raise the standard of ethics and risk management in South Africa.

Gillian le Cordeur  
CEO: The Institute of Risk Management South Africa
The institutes would like thank the company G4S for its generous sponsorship towards the design and printing of this publication.

G4S is the world's leading global, integrated security company, specialising in the delivery of security and related services to customers across six continents. The group is active in more than 100 countries, and, with over 610 000 employees, is the largest employer listed on the London Stock Exchange, with a secondary stock exchange listing in Copenhagen. G4S is the largest security company in Africa, with operations in more than 29 African countries and more than 119 000 employees on the continent.

Integrity is one of the organisation's core corporate values – it is an integral part of its strategy, and forms the foundation on which it conducts its business and people practices. For G4S, ethical business is not just a solution to the challenges of legal compliance, but a means of doing business that provides customers, employees, partners, and communities with the confidence that they are dealing with an ethical organisation that is not prepared to compromise on its integrity in order to achieve financial objectives. The company's policies and standards on business ethics, whistleblowing, and human rights inform its employees and stakeholders as to how it carries out its business operations in an ethical manner, and what is expected of them reciprocally. Ethics risk assessment is at the heart of the company's ethics management initiatives. Against this backdrop, the company had no reservation in sponsoring *The Ethics Risk Handbook*. 
The institutes would like to thank the company G4S for its generous sponsorship towards the design and printing of this publication. G4S is the world's leading global, integrated security company, specialising in the delivery of security and related services to customers across six continents. The group is active in more than 100 countries, and, with over 610 000 employees, is the largest employer listed on the London Stock Exchange, with a secondary stock exchange listing in Copenhagen. G4S is the largest security company in Africa, with operations in more than 29 African countries and more than 119 000 employees on the continent. Integrity is one of the organisation's core corporate values – it is an integral part of its strategy, and forms the foundation on which it conducts its business and people practices. For G4S, ethical business is not just a solution to the challenges of legal compliance, but a means of doing business that provides customers, employees, partners, and communities with the confidence that they are dealing with an ethical organisation that is not prepared to compromise on its integrity in order to achieve financial objectives. The company's policies and standards on business ethics, whistleblowing, and human rights inform its employees and stakeholders as to how it carries out its business operations in an ethical manner, and what is expected of them reciprocally. Ethics risk assessment is at the heart of the company's ethics management initiatives. Against this backdrop, the company had no reservation in sponsoring The Ethics Risk Handbook.
Part 1: Introduction

1.1 The purpose of this handbook

Best practice governance guidelines suggest that an organisation’s governing body should ensure that ethics risks and opportunities are incorporated in the (enterprise) risk management process. However, to date most organisations have applied risk management and ethics risk management separately and as only somewhat complementary interventions. Since ethics risk is a dimension of risk that is on an equal footing with any other type of risk, it cannot be divorced from organisational risk. In fact, risk management and ethics risk management may be viewed as converging interventions that can be designed and implemented in an integrated manner. Although ethics risk ownership may eventually be proportionally allocated to the organisation’s risk function and ethics risk function respectively, ethics risks need to be integrated, in the form of an ethics risk register, into the organisation’s risk register.

The purpose of The Ethics Risk Handbook, the third in The Ethics Institute’s Ethics Handbook Series, is to create a framework and set of guidelines for understanding ethics risk management in organisations. The purpose of the handbook is not to serve as a substitute for guidelines on risk and/or ethics risk management. The guidelines contained herein will, however, inform organisations’ guidelines.

These guidelines will be contextualised within (a) strategic and standards-driven organisational risk management and (b) ethics risk management, and then integrated into a meaningful interface between risk management and ethics risk management. The interface between, and the respective responsibilities of each, will be indicated. Furthermore, a process flow for organisational governance structures as they relate to ethics risk management oversight and reporting will be provided. The book culminates in key success factors for the successful management of ethics risk. An ethics risk management toolbox and an explanatory case study are also included.

1.2 Target audience

The Ethics Risk Handbook is primarily aimed at those functions in the organisation that bear responsibility for ethics risk management and the practitioners who are involved in these functions. The ethics governance and management structures that could benefit from this handbook include governing bodies of organisations (e.g., boards of directors), social and ethics committees, operational ethics committees, ethics task teams, and ethics offices.

\[1\] The term risk management is preferred over enterprise risk management.
As was alluded to in the introduction, there are also other role players involved in organisational ethics risk management. As such, the handbook could be utilised by, among others, the following complementary functions:

- governance
- risk management
- compliance
- legal
- internal auditing
- forensics
- company secretariat or committees' administrative support
- human resource management
- employment relations
- organisational development
- remuneration
- health and safety
- consumer relations
- investor relations
- social responsibility
- human rights
- information technology

These role players all have a vested interest in being aware of ethics risks, as these may emanate from or directly impact their specific areas of functioning. Also, the governance and management structures within which they are positioned could all meaningfully and substantially contribute to effective ethics risk management. They would therefore benefit from the contents of this book, as it may provide clarity on their respective roles, interfaces, and reporting lines as these pertain to ethics management.

### 1.3 Standardisation of names of ethics risk management structures and role players

Different sectors of the economy employ different structures for the governance of ethics and ethics management. The table below provides an overview of such structures in different sectors (private and public, including national, provincial, and local government) and tertiary institutions.
To avoid unnecessary repetition, the following umbrella terms will be used throughout this handbook:

- governing body (equivalent of a board, ExCo, and council) of the organisation, responsible for the governance of ethics (strategic and oversight role)
- chair of governing body (equivalent of chair of the board, chair of ExCo, Speaker, chancellor, etc.)
- chief executive officer (managing director, DG, HoD, MM, VC, etc.)
- ethics governance committee (equivalent to S&EC or another governing body committee held accountable for the governance of ethics)
- operational ethics committee (operational structure for the management of ethics)
- ethics officer

A list of the terminology used in the book is provided as an appendix at the end of this publication.

<table>
<thead>
<tr>
<th>Private sector</th>
<th>National government</th>
<th>Provincial government</th>
<th>Local government</th>
<th>Tertiary institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board</td>
<td>ExCo</td>
<td>ExCo</td>
<td>Town council/City council</td>
<td>Council</td>
</tr>
<tr>
<td>Chair of the board</td>
<td>Chair of ExCo or accounting officer</td>
<td>Speaker or mayor</td>
<td>Chancellor</td>
<td></td>
</tr>
<tr>
<td>Social and ethics committee (S&amp;EC)</td>
<td>Not required Related structures: parliamentary ethics committee; Municipal councils’ disciplinary committees dealing with issues of elected representatives (politicians)</td>
<td>Council committee responsible for ethics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEO</td>
<td>Director general (DG)</td>
<td>Head of department (HoD)</td>
<td>Municipal manager MM)/City manager</td>
<td>Vice chancellor (VC)</td>
</tr>
<tr>
<td>Operational ethics committee</td>
<td>Ethics committee required by IMF (does not have to be dedicated exclusively to ethics)</td>
<td>Operational ethics committee</td>
<td>Operational ethics committee</td>
<td></td>
</tr>
<tr>
<td>Ethics officer/practitioner</td>
<td>Ethics (Integrity) officer, as required by the IMF, or applicable official as delegated by ExCo</td>
<td>Ethics officer/practitioner</td>
<td>Ethics officer or ombudsman</td>
<td></td>
</tr>
</tbody>
</table>
To avoid unnecessary repetition, the following umbrella terms will be used throughout this handbook:

- governing body (equivalent of a board, ExCo, and council), responsible for the governance of ethics (strategic and oversight role)
- chair of governing body (equivalent of chair of the board, chair of ExCo, Speaker, chancellor, etc.)
- chief executive officer (managing director, DG, HoD, MM, VC, etc.)
- ethics governance committee (equivalent to S&EC or another governing body committee held accountable for the governance of ethics)
- operational ethics committee (operational structure for the management of ethics)
- ethics officer

A list of the terminology used in the book is provided as an appendix at the end of this publication.
Management cannot be expected to deal with unexpected events or opportunities in a structured, planned, and confident manner if such events are not anticipated and planned for. Risk management provides the scaffold for action to address these issues.

Despite best intentions and practices, risk management cannot be an exact science, because it:

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

Risk management should therefore not be perceived as able to provide a perfect vision of future events – it can only ever be an approximation. This does not invalidate risk management – rather, it becomes important to recognise this constraint and implement appropriate responses. This allows decision-makers and risk practitioners to make informed choices about risks.

### 2.1 About risk management

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 that, if it occurs, will have a negative effect on the achievement of objectives
- the possibility of better-than-expected performance

This handbook uses a formal definition of risk that is 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 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 events occurring in the environment in which it functions.

### 2.2 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 may overlook opportunities that provide significant possibilities for innovation and competitive advantage. Missing opportunities may also significantly affect an organisation's overall ability to deliver on its mandate, vision, and goals.

The concept of opportunity in the context of upside risk includes:

- 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 that, if it occurs, will have a positive effect on the achievement of objectives
- favourable circumstances for a positive outcome

### 2.3 The importance and benefits of risk management

**The importance of risk management**

Strategic planning is one of the most crucial means of ensuring that an organisation achieves its vision, mission, and strategic goals. Strategic planning has been defined as “an organisational activity that is used to set priorities, focus energy and resources, strengthen operations, ensuring that employees work towards common goals and establishing agreement around outcomes”, which suggests that organisations use this process to define their vision/mission, set strategic goals (outcomes), identify strategies to achieve these, and develop tools to measure their achievements. Internal and external risks may undermine the achievement of an organisation's strategic goals. By the same token, upside risk may facilitate the achievement of strategic goals.
It has therefore become imperative that organisations adopt a formal risk management process, whereby risks are pro-actively identified, captured in risk registers, and managed. Furthermore, risk management and strategic planning need to be integrated into a single co-ordinated and holistic process.

Risk – opportunity management is important in maximising an organisation's ability to create and protect value. Failing to manage risks may prevent the organisation from achieving its objectives, and ultimately lead to the diminishing of share value, loss of competitive advantage, and 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-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.

**Benefits of risk management**
The ISO 31000 Standards and AS/NZS 4360:2004 Standards highlight the following benefits of risk management:

1. Risk management creates and protects value. It contributes to the demonstrable achievement of objectives and improvement of performance with regard to, for example, health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance, and reputation.
2. Risk management forms an integral part of organisational processes and, if fully integrated, enhances the strategic management process. It is not a stand-alone activity that can be separated from the main activities and processes of an organisation, and should not be managed within functional silos. Risk management is a management responsibility, and forms an integral part of all organisational processes, including strategic planning and project- and change management processes.
3. Risk management is part of decision-making. It assists decision-makers to make informed choices, prioritise actions, and distinguish between alternative courses of action.
4. Risk management addresses uncertainty. It explicitly takes account of uncertainty, the nature of the uncertainty, and how it can be addressed. Even if certain events cannot be avoided, the organisation can achieve a degree of resilience through planning.
5. Risk management must be systematic, structured, and timely. It contributes to efficiency and to consistent, comparable, and reliable results.

6. Risk management is based on the best available information. Since the inputs to the process of managing risk are based on information sources, decision-makers are encouraged to familiarise themselves with valuable information sources, as well as any limitations related to data.

7. Risk management is transparent and inclusive. It therefore encourages organisations to identify internal and external stakeholders, and to consult stakeholders on key policies and decisions that require buy-in and support.

8. Risk management is dynamic, iterative, and responsive to change. It continually senses and responds to change, and allows for more effective planning.

9. Risk management facilitates continual improvement of the organisation. As organisations implement strategies to improve their risk maturity, other aspects of the organisation also benefit.

10. Benefits in economy and efficiency can be achieved in the targeting of resources, protection of assets, and avoidance of costly mistakes.

11. The organisation’s reputation is enhanced, as clients are drawn to organisations that are known to have sound risk management processes.

12. Effective risk management of personal risk (personal wellbeing) generally improves health and wellbeing of self and others.

### 2.4 Risk management framework and standards

The risk management framework 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, where:
2.5 Risk management roles and responsibilities

The organisation should establish 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 controls. This can be facilitated by:

- identifying risk owners who have the accountability and authority to manage risks
- identifying those accountable for the development, implementation, and maintenance of the framework for managing risk
- identifying those responsible for the risk management process at all levels in the organisation
- establishing performance measurement metrics
- establishing external and/or internal reporting and escalation processes

The governing body should specify responsibilities across multiple 'lines of defence' as appropriate to the organisation. These would generally include the executive leadership team, risk practitioners (such as a chief/corporate risk officer), management, and the overall workforce.
2.6 Risk appetite and risk tolerance

**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 taking risks.

It is the responsibility of the governing body of the organisation to determine the various levels of risk appetite. This body 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.).

The governing body is responsible for establishing the overall risk appetite of 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. Project managers may establish their own project risk appetite, within the boundaries agreed upon by the project sponsors.

There should be a range of different appetites defined for different risk types – financial or non-financial – for example, for risks related to the law, finance, operations, ethics, health and safety, and other domains. Risk appetite is dynamic, and fluctuates as various internal and external factors change.

**Risk tolerance**
Risk tolerance reflects an organisation's ability, or readiness, to bear a risk after all responses have been put in place. It is the level of unwanted outcomes that can continually be tolerated. 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. Where the appetite exceeds the tolerance, this should be disclosed to the relevant stakeholders.

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

2.7 Risk management in support of organisational strategy and objectives

The first step in risk management is defining the objectives (strategic goals) that the organisation wants to achieve, how it intends to achieve these (the operating model),
and what might get in the way of such achievement. In establishing the context, the organisation could follow the process below:

- Define an operating model, along with strategic and operational objectives.
- Define the external and internal factors that give rise to the risk that the organisation might not 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 tolerance).

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

While the assessment and evaluation of strategic risks lie within the standard risk management processes, the framework should make specific note of when to apply these processes to strategic risks. This is necessitated by the infrequent nature of strategic risk management, as well as its importance in ensuring the relevance of the risk management system itself.

The executive leadership team should specify a regular interval at 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 conducted more or less frequently, as needed by the organisation.

Strategic risk management should consider the organisation's risk thresholds (risk appetite and risk tolerance).

Functionaries responsible for 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 added to the organisation's calendar, so that appropriate information can be obtained for the executive to make an honest and effective appraisal of the organisation's risk profile.

## 2.8 Risk assessment

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

- quantitative methods (e.g., the accumulation and development of relevant historical or predictive datasets, quantitative surveys/questionnaires)
- qualitative methods (e.g., market research, qualitative surveys/questionnaires, risk workshops)
- a mixed-method approach, which is a combination of quantitative and qualitative methods

In many instances, it is appropriate to use more than one technique or methodology in the risk assessment process. The depth of assessment 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 assessments are conducted 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. Alternatively, a numerical rating scale can be used to estimate the level of risk according to some previously agreed formulae or calculations.

Risk assessment consists of three steps:

1. **Risk identification**
   - identifies specific risks for which the organisation should account
   - identifies how the organisation's objectives could be affected by these risks
   - analyses the risks in terms of their consequences and the probability of their occurrence
   - describes the priority that should be assigned to each risk

2. **Risk analysis needs to be applied subsequent to risk identification.**

Risk analysis involves developing an understanding of the risk. This entails consideration of the causes and sources of the risk, potential positive and negative effects, and what might get in the way of such achievement. In establishing the context, the organisation could follow the process below:

- Define an operating model, along with strategic and operational objectives.
- Define the external and internal factors that give rise to the risk that the organisation might not 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 tolerance).

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

While the assessment and evaluation of strategic risks lie within the standard risk management processes, the framework should make specific note of when to apply these processes to strategic risks. This is necessitated by the infrequent nature of strategic risk management, as well as its importance in ensuring the relevance of the risk management system itself.

The executive leadership team should specify a regular interval at 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 conducted more or less frequently, as needed by the organisation.

Strategic risk management should consider the organisation's risk thresholds (risk appetite and risk tolerance).

Functionaries responsible for 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 added to the organisation's calendar, so that appropriate information can be obtained for the executive to make an honest and effective appraisal of the organisation's risk profile.
consequences, and the likelihood of those consequences occurring. By first analysing risks, the information necessary to undertake the risk evaluation process is obtained. This step is important, as it allows the organisation to prioritise its risks, followed by allocating resources appropriately.

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

The organisation’s existing controls should be factored into the risk analysis process, as these will affect the characteristics of the risk (such as its likelihood and consequences), as well as the extent to which it has been, or could be mitigated.

In some circumstances the probability of a risk may be extremely low; this may skew the risk analysis process such that a risk that can have a significant impact on business continuity is unintentionally accepted. Alternatively, the consequence may be perceived as insignificant, but, in conjunction with other events, could nevertheless lead to a catastrophic outcome (i.e. 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.

Regardless of the type of analysis (e.g., quantitative or qualitative) undertaken, the calculated level of risk remains an estimate, and is influenced by a range of factors. These may include human bias in the evaluation of the risk, or 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, comprehensive data cannot be guaranteed.

In addition, a level of accuracy and detail should not inadvertently be 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. Here, the insight and experience of specialists play an important role in checking the outputs of any modelling process, to make sure they make sense.

A typical risk analysis approach could consist of the following steps:

- assessing current controls
- analysing consequences
- analysing likelihood and estimating probability
  - extrapolation from historical data
  - probability modelling
  - expert judgment
- compiling and populating the contents of the risk register
3. **Risk evaluation is the final step in the risk assessment process.**

This involves comparing the risk against pre-determined criteria, thus specifying the significance of the risk in terms of 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 those with very low probability and impact
- those risks that should be accepted only with the implementation of specific responses
- any immediate decisions that are required to avoid risks that breach specific thresholds

2.9 **Ethics risk as a dimension of organisational risk**

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) describes the role of ethics in risk management as follows:

“An entity's strategy and objectives and the way they are implemented are based on preferences, value judgments, and management styles. Management's integrity and commitment to ethical values influence these preferences and judgments, which are translated into standards of behavior. Because an entity's good reputation is so valuable, the standards of behavior must go beyond mere compliance with the law. Managers of well-run enterprises increasingly have accepted the view that ethics pays and that ethical behavior is good business.”

Risk management emphasises the importance of ethics in enterprise governance, risk, and compliance systems. In addition to COSO, a number of organisations, such as IRMSA, the Ethics Resource Initiative (ERI), and the Open Compliance and Ethics Guidelines (OCEG), have issued frameworks for implementing effective risk management systems.

Ethics risk is a dimension of risk in the same way that legal, operational, IT, finance, and HR risks are. As the non-management of ethics risk could give rise to as many, if not more, reputational and financial costs for an organisation as any other type of risk, it warrants equal attention. As such, ethics risk is a component of the broader organisational risk framework. The risk management processes of an organisation are also highly dependent on the ethical culture of the organisation to enable effective risk management.
3.1 Ethics management

The definition of ethics subscribed to by The Ethics Institute is that ethics concerns itself with what is good or right in human interaction. It revolves around three central concepts: self, good, and other, as depicted in the figure below.

Good
Self
Other


Ethical behaviour results when one does not merely consider what is good for oneself, but also what is good for others. Both the self and the other can refer to an individual, a group, or an organisation. Organisational ethics is about a conception of what good (values and standards) guides the organisation (self) in its interaction with the other (stakeholders) in a sustainable way.

Organisations usually experience two major challenges in regard to ethics:

1. defining the good, i.e. achieving a state where the organisation and (primarily) its internal stakeholders share a common understanding of the good (of course, the larger the organisation and the more numerous and diverse its internal stakeholders, the more difficult it may be to attain a shared meaning of ethics)
2. establishing a sustainable balance between what is good for the self and what is good for others

To ensure that ethics is dealt with in a concerted and structured manner in the organisation, a common understanding of a best-practice approach is desirable. Such an approach – a governance of ethics management framework – that could be utilised by organisations is depicted in the figure below.

Part 3
Ethics Risk
3.1 Ethics management

The definition of ethics subscribed to by The Ethics Institute is that ethics concerns itself with what is good or right in human interaction. It revolves around three central concepts: self, good, and other, as depicted in the figure below.

Ethical behaviour results when one does not merely consider what is good for oneself, but also what is good for others. Both the self and the other can refer to an individual, a group, or an organisation. Organisational ethics is about a conception of what good (values and standards) guides the organisation (self) in its interaction with the other (stakeholders) in a sustainable way.

Organisations usually experience two major challenges in regard to ethics:

1. defining the good, i.e. achieving a state where the organisation and (primarily) its internal stakeholders share a common understanding of the good (of course, the larger the organisation and the more numerous and diverse its internal stakeholders, the more difficult it may be to attain a shared meaning of ethics)
2. establishing a sustainable balance between what is good for the self and what is good for others

To ensure that ethics is dealt with in a concerted and structured manner in the organisation, a common understanding of a best-practice approach is desirable. Such an approach – a governance of ethics management framework – that could be utilised by organisations is depicted in the figure below.

---

Each of the dimensions of the framework is discussed below.

**Leadership commitment**
No ethics management initiative can be successful unless the organisation’s leadership:

- understands the value of ethics in ensuring the organisation's sustainable development
- is fully committed to ethics
- has ethics management competence
- acts ethically (‘walks the talk’)
- acts as an ethical role model for employees and other stakeholders
- sponsors ethics management interventions

Corporate governance best practice guidelines in this regard are the following:

- The organisation’s governing body should provide effective leadership based on an ethical foundation.
- The governing body should ensure that it builds and sustains an ethical corporate culture in the organisation.

Best-practice guidelines for the ethical leadership roles of a number of specific ethics management role players are:
The chair of the governing body should set the ethical tone for the governing body and the organisation.

The chief executive officer should provide ethical leadership and create an ethical culture in the organisation.

**Governance structures**

Since ethics needs to be managed in a structured manner, ethics governance structures dedicated to the ethics-related dimensions of the organisation need to be designed and implemented. Examples of such structures are the board of directors, the ExCo, S&E&Cs, or a board/ExCo committee that assumes responsibility for the governance of ethics, e.g., the audit and/or risk committee(s).

Best-practice guidelines for the ethics committee suggest that it should be a committee of the governing body that provides strategic direction and oversight of the ethics management of the organisation regarding material ethics issues that have been identified.

**Ethics management**

The philosophy of managing ethics is to apply the belief that ethics can indeed be managed in an organisation. Based on this assumption, the following five-step ethics management process could be implemented in organisations:

![](image.png)

Responsibility for the five-step ethics management process (see figure above) could be allocated to one or more of the following: an ethics management committee, an operational ethics committee, an ethics task team, a corporate ethics office staffed with designated ethics (integrity) officers (practitioners), and ethics champions.

The ethics-related roles and responsibilities of other organisational functions that should not only be represented in these structures, but also integrate ethics management activities into their mandates, may include, but not be limited to, the complementary ethics risk management role players mentioned in an earlier section.
Best practice guidelines for activities of the ethics office and its practitioners are:

1. Actively manage ethics in the organisation.
2. Provide ethical guidance to the governing body, senior management, and staff on ethics-related issues.
3. Co-ordinate ethics risk-opportunity assessments.
4. Promote integrity and ethical behaviour in departments.
5. Advise employees on ethical matters.
6. Ensure organisational integrity of policies, procedures, and practices.
7. Manage conflicts of interests, including:
   - financial disclosures related to employees
   - applications for external remunerative work
   - maintaining departmental gift registers
8. Develop and implement ethics awareness- and other ethics training programmes, coupled with sound ethics management- and anti-corruption measures.
9. Identify (through the whistle-blowing hotline and other channels) and report on unethical behaviour and corrupt activities.
10. Keep a register of all employees under investigation and those disciplined for unethical conduct.
11. Provide regular feedback to the governing body and executive management on ethics performance and challenges.

a. **Ethics risk assessment** – An ethics opportunity-risk assessment is the indispensable first step in addressing the challenges of determining the good and striving for an optimal balance between the self and the other. The organisation should assess (in a structured way) what its ethics risks are. An ethics risk assessment (ERA), culminating in an ethics risk profile, provides the organisation with a clear understanding of unethical behaviours and organisational practices that could put the organisation at risk. At the same time, an ethics risk assessment identifies the opportunities related to ethics that can be used by the organisation.

b. **Ethics strategy formulation** – Once an ERA has been conducted, the organisation needs to decide on an ethics management strategy. This would, amongst others, depend on the perceived purpose of bringing ethics into the organisational domain, the current state of the ethics of the organisation, previous reputational damage that was incurred, the magnitude of identified risks, and the desired end-state at a point in the future. Once an organisation has determined its optimal ethics management strategy, it could design an ethics management plan that contains measurable objectives; assigns specific responsibilities, timeframes, and target dates; and allocates the human, financial, and other resources required to implement that strategy.

c. **Code of ethics and policies** – Best practice corporate governance recommends that the governing body in the organisation should (i) ensure that the ethical values
to which the organisation will adhere are expressed in its code of ethics (or conduct) and (ii) ensure that the code of ethics (or conduct) and ethics-related policies are implemented.

Once an organisation knows what its (positive and negative) ethics risks are, it can proceed to formulate (or revise) its code of conduct, code of ethics, and ethics-related policies. The risks identified inform the contents of these aspirational or prescriptive documents.

d. **Institutionalisation of ethics** – A corporate governance directive for the institutionalisation of ethics is that the governing body should ensure that compliance with the code of ethics (conduct) is integrated into the operations of the organisation. Formulating a code of ethics and supporting policies is, however, a necessary but insufficient step in making ethics an integral component of the organisation. Ethics needs to be institutionalised in the organisation – merely being able to demonstrate the existence of the code is not enough. Ethics management systems that complement the formation of an ethical culture, together with an ethics management strategy, need to be designed and implemented. Such systems are usually aimed at making ethics manifest throughout the organisation. Typical ethics management systems, among others, are:

- communication systems (ethics awareness campaigns, ethics help-desks, and safe reporting/whistle-blowing facilities)
- ethics training initiatives (training on ethical standards and decision-making, providing line managers with the ethics competence they require to effectively manage the ethics of their subordinates)
- orientation/induction programmes containing ethics as an important component
- performance assessments including ethics as an indicator
- Human resource management systems that recruit, select, and retain employees with integrity
- disciplinary processes

e. **Monitoring and reporting** – Best practice governance guidelines include a directive that the governing body should ensure that adherence to ethical standards is monitored and measured. The ethics office should monitor the implementation of the ethics management plan, and report to the ethics committee on progress in this regard, as well as on the state of ethics in the organisation.

**Independent assessment and external reporting**

The governance prescript in this regard is that the governing body should ensure that the organisation’s ethics performance is assessed, monitored, reported, and disclosed. There should be independent assessment of the ethics management
processes (e.g., through an internal audit) and of the ethics management reports (e.g., by external auditors). This should then be reported to external stakeholders in integrated sustainability or annual reports.

**Ethical culture**
The desired outcome of any ethics governance and management initiative is a strong ethical culture. Although organisations may survive for many years on laissez-faire approaches to ethics, truly sustainable organisations pro-actively build an organisational culture marked by ethical leadership, ethics awareness, ethical decision-making, and sustained ethical behaviour (ethical action). A truly ethical culture cannot be achieved in the short term, but requires sustained leadership commitment to ensure an ethical culture over time. As with any organisational culture-change exercise, the formation of an ethical culture could take three to seven years to reach maturity.

### 3.2 Understanding ethics risk

Ethics risks are the current or potential organisational beliefs, practices, or behaviours (conduct) that either support (upside risk or opportunities) or are in contravention (downside or negative risk) of organisation-specific standards for desired behaviour, and/or in contravention of legitimate stakeholder rights and expectations. This could negatively impact other key organisational processes and undermine the sustainability of the organisation.

Downside ethics risks, both internal and external, may undermine the achievement of an organisation's strategic goals; by the same token, upside risks may facilitate the achievement of strategic goals.

### 3.3 The nature and importance of ethics risk management

Ethics risk management is the process of planning, organising, directing, and controlling resources and operations to ensure that the organisation's ethics management initiative facilitates the achievement of organisational objectives, despite the uncertainty of events. It is also aimed at preventing ethics risks from undermining the achievement of objectives. Effective ethics risk management enables an organisation to manage the probability of any unforeseen ethics-related events, and, should these occur, to limit the effects of their consequences, along with responding proactively to ethics opportunities (upside ethics risks).

It is thus imperative that organisations adopt a formal ethics risk management process, whereby ethics risks are pro-actively identified, analysed, and captured in an ethics risk
register, and then appropriately addressed. Furthermore, ethics risk management needs to be integrated into organisational strategic planning.

Rossouw and Vuuren (2013) suggest that an ethics risk assessment provides an organisation with the following benefits:

1. Because the organisation's stakeholders' perceptions are polled during an ethics risk assessment intervention, stakeholders feel recognised, and become co-creators of the organisation's future.
2. It affords the organisation the opportunity to distinguish between desirable and undesirable conduct.
3. It assists the organisation in identifying its organisation-specific ethical dilemmas; these can then be pro-actively managed.
4. It culminates in a frame of reference, within which a proper ethics management strategy can be formulated.
5. It provides information on the success of current ethics management systems that were established to promote ethical behaviour or to deal with unethical behaviour. Progress on ethics management systems could include, but is not limited to, information on the appointment of ethics practitioners, the establishment of an ethics committee, and confirming line managers' responsibility for integrating ethics into the activities of their domains of supervision.
6. Specific ethics risks can be accounted for by ensuring that they are adequately covered by the organisation's existing code of ethics and the ethics policies that complement the code. Should the organisation not have a code of ethics or related policies, the ethics risks could be utilised to develop such documents.

3.4 Ethics risk assessment: approach and process

3.4.1 Overview

Ethics risk assessment is a planned and structured assessment process that is applied by obtaining stakeholders' perspectives at regular intervals, with a view to helping the organisation compile its ethics opportunity-risk profile.

The impetus for an organisation to conduct an ethics opportunity-risk assessment could have multiple origins, such as legislation, compliance requirements, corporate governance guidelines, integrated sustainability reporting requirements, stock exchange regulations, business scandals, pressure from internal or external stakeholders, and monetary losses (e.g., through fraud, theft of organisational property, fines for price collusion, etc.).
The purpose of an ethics risk assessment is to identify the beliefs, practices, and behaviours (conduct) that are either (a) counterproductive to the maintenance of the ethical principles and standards that regulate desirable relationships among organisational stakeholders, or (b) enablers of such ethical principles and standards.

When conducting an ethics opportunity-risk assessment, an organisation has to engage with its internal and external stakeholders, to determine (a) stakeholders' perceptions of the organisation's ethics and (b) what they expect of the organisation regarding ethics.

An ethics risk assessment is neither a forensic investigation, nor an ethics audit. It is also not an opportunity to identify transgressors and engage in a witch-hunt to oust them. It is a research intervention to ascertain the ethics perceptions and expectations that stakeholders of the organisation hold.

An ethics risk assessment provides an organisation with a broad frame of reference within which an effective ethics management strategy can be formulated. The ethics risk assessment produces a take on the state of the organisation's ethics; as such, it will provide a general indication if there is a risk of unethical behaviour in the organisation. The ethics risk assessment also culminates in an ethics risk profile, which translates into identification of specific ethics risks, the extent of the prevalence of the perceived ethics risks, and the ethics risks' ratings (high, moderate, or low).

An ethics risk assessment only addresses the first step of the risk assessment process of risk management; that is, the risk identification process (type of ethics risk), the extent (ethics risk prevalence) to which it is perceived to occur, and the risk rating. As such, it considers neither the consequences nor impact of risk events occurring, nor the likelihood that the risk event will occur and the impact it may have on the organisation's objectives. Once the ethics risk assessment has been completed, the ethics office will further analyse and evaluate the ethics risks in conjunction with the organisation's risk management function. Current control mechanisms to deal with ethics risks will be factored into this process, as well as further control mechanisms required to ensure proper ethics risk mitigation. The process culminates in an ethics risk register, which forms an important part of the organisation's overall risk register.

Section 4 of this handbook will provide more clarity on the nature and mitigation of ethics risk identified during an ethics risk assessment and the responsibilities of the respective organisational role players (ethics practitioners and risk practitioners).
3.4.2 The risk assessment process

The consecutive steps in the process by which ethics opportunities and risks are assessed are shown in the figure below.

The ethics risk assessment process

1. Trigger (impetus)
2. Request
3. Planning/budgeting
4. Stakeholder identification and engagement
5. Choice of assessment methodology
6. Data-gathering (application of assessment methodology)
7. Data analysis
8. Data integration
9. Ethics risk profile
10. Written report and feedback

The purpose of an ethics risk assessment is to identify the beliefs, practices, and behaviours (conduct) that are either (a) counterproductive to the maintenance of the ethical principles and standards that regulate desirable relationships among organisational stakeholders, or (b) enablers of such ethical principles and standards.

When conducting an ethics opportunity-risk assessment, an organisation has to engage with its internal and external stakeholders, to determine (a) stakeholders’ perceptions of the organisation’s ethics and (b) what they expect of the organisation regarding ethics.

An ethics risk assessment is neither a forensic investigation, nor an ethics audit. It is also not an opportunity to identify transgressors and engage in a witch-hunt to oust them. It is a research intervention to ascertain the ethics perceptions and expectations that stakeholders of the organisation hold.

An ethics risk assessment provides an organisation with a broad frame of reference within which an effective ethics management strategy can be formulated. The ethics risk assessment produces a take on the state of the organisation’s ethics; as such, it will provide a general indication if there is a risk of unethical behaviour in the organisation. The ethics risk assessment also culminates in an ethics risk profile, which translates into identification of specific ethics risks, the extent of the prevalence of the perceived ethics risks, and the ethics risks’ ratings (high, moderate, or low).

An ethics risk assessment only addresses the first step of the risk assessment process of risk management; that is, the risk identification process (type of ethics risk), the extent (ethics risk prevalence) to which it is perceived to occur, and the risk rating. As such, it considers neither the consequences nor impact of risk events occurring, nor the likelihood that the risk event will occur and the impact it may have on the organisation’s objectives. Once the ethics risk assessment has been completed, the ethics office will further analyse and evaluate the ethics risks in conjunction with the organisation’s risk management function. Current control mechanisms to deal with ethics risks will be factored into this process, as well as further control mechanisms required to ensure proper ethics risk mitigation. The process culminates in an ethics risk register, which forms an important part of the organisation’s overall risk register.

Section 4 of this handbook will provide more clarity on the nature and mitigation of ethics risk identified during an ethics risk assessment and the responsibilities of the respective organisational role players (ethics practitioners and risk practitioners).
As can be seen from the figure, an impetus has to be provided for the ethics risk assessment to be commissioned. This impetus is provided either by a triggering event, at the one extreme (e.g., a corporate scandal - reactive), or an organisational context that is pro-active and seamlessly integrated with the organisation's strategic and sustainability objectives. The instruction to execute an organisational ethics risk assessment usually emanates from the governing body or the committee responsible for ethics governance.

The ethics office then proceeds to formulate the ethics risk assessment intervention - this includes the planning of the process and acquisition of the required financial, human, and other resources. An appropriate risk assessment methodology is selected (qualitative, quantitative, or a combination thereof), according to which will yield the most valid and reliable results.

The intended scope and depth of the assessment then informs the identification and prioritisation of stakeholders (e.g., internal and/or external) to be polled in the assessment intervention. The chosen methodology is then applied and data obtained. Once all the data has been gathered, it is subjected to scientific qualitative and/or quantitative data analyses by expert qualitative and/or quantitative data analysts (the latter being statisticians).

All the data obtained is then integrated in a form that meets the expectations of the intended initial target audience (e.g., ethics governance committee). The integrated data is then included in a comprehensive written report, i.e. the organisation's ethics opportunity-risk profile. The profile is then presented to the source of instruction in written and verbal format.

The duration of an ethics risk assessment could vary from one week for a smaller organisation or one that opted for a dipstick analysis, to several months for a larger organisation or one that opted for a comprehensive assessment. The process is repeated at regular intervals, e.g., a three-year cycle. Continuous monitoring of the ethics risks is imperative - this happens through collaboration with the risk function, and is guided by the organisation's ethics risk register. Unforeseen incidental risks need to be dealt with in an ad hoc manner as they arise.

### 3.4.3 Frequency, scope, and depth of an ethics risk assessment

An ethics risk assessment process differs from organisation risk management, where risk is continuously monitored and mitigated, in that it is a process that is applied at regular intervals. Ethics risk assessments need to be conducted with some regularity, to ensure that new risks that arise as the organisation grows are identified and accounted for.

The factors that determine the frequency with which an organisation should assess its ethics opportunities and risk are: organisation size, number of employees, budget,
ethics management skills levels within the organisation, type of industry, reporting requirements, and the desired scope and depth of assessment. Typically, a comprehensive and in-depth ethics risk assessment is conducted every two to three years.

It should be borne in mind that, depending on the scope and depth of the assessment, e.g., whether both internal and external stakeholders' perceptions and expectations are polled, a risk assessment process, from the time of the request to the feedback of the results, could take between one and six months to complete.

The following three broad approaches to determining an ethics risk assessment project's scope and depth could be utilised:

1. **'Dipstick' assessment**: a limited number of qualitative interviews (e.g., six, with key internal stakeholders, including employees) and a quantitative survey
   
   **Representativity of data**
   - Quantitative: Good
   - Qualitative: Poor

2. **Selective assessment**: approximately 15 qualitative interviews with key internal stakeholders and a quantitative survey
   
   **Representativity of data**
   - Quantitative: Good
   - Qualitative: Acceptable

3. **Comprehensive analysis**: 
   - approximately 40 qualitative interviews with key internal and external stakeholders
   - a quantitative survey
   - document analyses
   - benchmarking (comparing the organisation's opportunities and risks to those of other, similar national or international organisations)
   - The organisation's media exposure, i.e. the quantity and quality of media coverage afforded to the organisation in the recent past, where these reports could either have enhanced or undermined the organisation's ethics reputation
   
   **Representativity of data**
   - Quantitative: Good
   - Qualitative: Good

Similar to the methodology employed to assess organisational risk, the following generic ethics risk identification methods could be utilised during an ethics opportunity-risk assessment:
The most comprehensive results are obtained when using a combined approach of quantitative and qualitative measures. The popular approach is to first conduct a qualitative assessment. The data yielded by qualitative methods is analysed through the application of content analysis methodologies. The major and sub-themes that emerge from the data analyses inform the identification of the types of ethics opportunities and risks that exist, or may occur in the foreseeable future, that could enhance or undermine the ethics dimension of the organisation's reputation.

Three categories of ethics risk are usually assessed:

1. Conduct (behaviour) risk – these are specific types of risk, e.g., supplier relations, nepotism, fraud, bribery, theft, misleading of customers, breaches of confidentiality, and many more.
2. Ethical culture risk – typical risks in this category relate to ethical accountability and responsibility, ethics awareness, the willingness to talk about ethics and ethics challenges, leadership commitment to ethics, and the ethical treatment of employees.
3. Ethics management risks – this category of ethics risk refers to the presence and perceived success of ethics management structures, strategies, and interventions. Examples of related themes include the existence and status of the organisation's code of ethics, the inclusion of ethics in employee induction (on-boarding) interventions, ethics training conducted, conducting integrity assessments of prospective employees, integrity assessment of potential employees, the extent to which ethical behaviour is appraised in performance management systems, and the existence of ethics helpdesks and safe reporting facilities.

Assessment of ethical conduct risk:

Here, a major theme that often emerges is supplier relations. Sub-themes can then be identified, such as the disrespectful treatment of suppliers, late payment of suppliers, irregular fraternising by employees with suppliers, accepting kickbacks from suppliers, and unfair favouring of certain suppliers over others. At this point, the organisation is only aware of the nature of the themes or the types of themes and, at best, a rank order of the themes according to importance. In essence, qualitative measures produce the
What? They do not identify the How much?, i.e. the prevalence or perceived frequency or intensity of occurrence. It also does not yield information on the potential impact or likelihood of occurrence.

A quantitative assessment therefore needs to be applied after the qualitative assessment, where the themes (ethical conduct risks) that emerged from the qualitative assessment inform the contents of the items of a questionnaire or survey. The questionnaire is then used to assist the organisation in determining the extent to which the themes are perceived to occur, or may occur in future. A risk rating exercise is then conducted, which will yield risk ratings of high, moderate, or low.

To further the example used above: supplier relations and its sub-themes as potential risks can now be assessed in quantified terms. See the table below for an example.

<table>
<thead>
<tr>
<th>Conduct (behaviour risk) Types of ethics challenges</th>
<th>To what extent do you agree that this occurs in Organisation X?</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Employees are rude to suppliers</td>
<td>Strongly disagree</td>
</tr>
<tr>
<td></td>
<td>1 2 3 4 5 6 DK</td>
</tr>
<tr>
<td>11 Employees engage in irregular fraternising with suppliers outside of business hours</td>
<td>1 2 3 4 5 6 DK</td>
</tr>
<tr>
<td>18 Suppliers treat employees lavishly during product promotion events</td>
<td>1 2 3 4 5 6 DK</td>
</tr>
<tr>
<td>23 Suppliers have to wait very long to receive payment</td>
<td>1 2 3 4 5 6 DK</td>
</tr>
<tr>
<td>28 Accepting bribes/kickbacks from suppliers/contractors for awarding business</td>
<td>1 2 3 4 5 6 DK</td>
</tr>
<tr>
<td>39 Certain suppliers are used, despite poor products and slow delivery</td>
<td>1 2 3 4 5 6 DK</td>
</tr>
<tr>
<td>43 The process of awarding contracts to suppliers is unfair</td>
<td>1 2 3 4 5 6 DK</td>
</tr>
</tbody>
</table>

The quantitative assessment may also be used to assess the extent to which the organisation is perceived to deal with these risks without delay, should they occur, e.g., the extent to which unethical behaviour (conduct), when it occurs, is encouraged, condoned, ignored (turning a blind eye), discouraged but not dealt with, or discouraged and dealt with effectively. A further use of such a quantitative assessment may be to assess whether the respondents to the survey are familiar with policies that exist in the organisation to deal with such behaviours.
The value of qualitative data obtained through the qualitative dimension of ethics risk assessment interventions should never be negated, as the data reflects the true opinions that respondents offer freely, as opposed to data obtained through surveys, where respondents provide answers only within the parameters of what is offered to them.

Quantitative data is easily interpreted using a risk rating scale. As an example, the scale below utilises agreement scores (in terms of responses to ethics risk surveys), and could be used to present the ethics opportunities and risks (threats) to which an organisation may be exposed.

### 3.4.4 Risk rating

<table>
<thead>
<tr>
<th>Risk category</th>
<th>Agreement score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low risk</td>
<td>0 - 33</td>
</tr>
<tr>
<td>Moderate risk</td>
<td>34 - 66</td>
</tr>
<tr>
<td>High risk</td>
<td>67 - 100</td>
</tr>
</tbody>
</table>

Low risk areas refer to issues (or behaviours) where respondents Disagree or Strongly disagree that these issues are prevalent in (or relevant to) the organisation. Moderate risk areas refer to issues (or behaviours) where respondents only Slightly disagree or Slightly agree that these issues are prevalent in (or relevant to) the organisation. High risk areas refer to issues (or behaviours) where respondents Agree or Strongly agree that these issues are prevalent in (or relevant to) the organisation.

All moderate and high risks should be brought to the attention of the organisation’s risk function, who, in turn, could integrate these risks into the portfolio of organisational risks to be managed. Furthermore, an organisation could, for example, identify its top 5 to 10 high risk areas, and label these material ethics risks, or risks that could undermine the organisation’s efforts to reach its objectives through the implementation of organisational strategies. These material ethics risks will also then resort within the ethics dimension of the ethics committee’s mandate. This process will be clearly illustrated in the case study and ethics risk management toolbox, to be presented in Section 6 of the handbook.

Should the ethics dimension of the organisational culture be weak or underdeveloped, prevailing beliefs, practices, and behaviours become an ethics risk. Ethical culture risks could therefore also be addressed by means of the ethics risk survey. See the table below for an example.

### Ethical culture risk

<table>
<thead>
<tr>
<th>As it relates to Organisation X …</th>
<th>Strongly disagree</th>
<th>Fully agree</th>
<th>I don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Employees know exactly what is expected of them in terms of ethical behaviour</td>
<td>1 2 3 4 5 6 DK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Employees are comfortable approaching superiors with ethical matters/concerns</td>
<td>1 2 3 4 5 6 DK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 Business that violates principles of honest and responsible conduct is turned away</td>
<td>1 2 3 4 5 6 DK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 Organisational leaders set a good example of honest and responsible behaviour</td>
<td>1 2 3 4 5 6 DK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 Employees consider ethical issues/ consequences when making decisions</td>
<td>1 2 3 4 5 6 DK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22 Ethics policies and procedures are applied consistently</td>
<td>1 2 3 4 5 6 DK</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In terms of ethics management risk, a section that could be included in a quantitative ethics risk assessment (survey) is provided in the table below.

### Ethics management risk

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>I don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For example:

- I know who the organisation's ethics champion (or Ethics Officer) is
- The organisation has an ethics committee/task team
- There is a facility in the company where I can get advice on ethics (e.g., whether I can accept a gift from a supplier or not)
- There is a facility in the company where I can safely report (blow the whistle on) unethical behaviour
- I feel equipped to deal with ethical issues
- Ethics/integrity is a dimension of my own performance appraisal
- There are ethics awareness campaigns in the company
- New employees receive ethics training
The value of qualitative data obtained through the qualitative dimension of ethics risk assessment interventions should never be negated, as the data reflects the true opinions that respondents offer freely, as opposed to data obtained through surveys, where respondents provide answers only within the parameters of what is offered to them.

### 3.4.4 Risk rating

Quantitative data is easily interpreted using a risk rating scale. As an example, the scale below utilises agreement scores (in terms of responses to ethics risk surveys), and could be used to present the ethics opportunities and risks (threats) to which an organisation may be exposed.

<table>
<thead>
<tr>
<th>Risk category</th>
<th>Low risk</th>
<th>Moderate risk</th>
<th>High risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement score</td>
<td>0 - 33</td>
<td>34 - 66</td>
<td>67 - 100</td>
</tr>
</tbody>
</table>

Low risk areas refer to issues (or behaviours) where respondents Disagree or Strongly disagree that these issues are prevalent in (or relevant to) the organisation. Moderate risk areas refer to issues (or behaviours) where respondents only Slightly disagree or Slightly agree that these issues are prevalent in (or relevant to) the organisation. High risk areas refer to issues (or behaviours) where respondents Agree or Strongly agree that these issues are prevalent in (or relevant to) the organisation.

All moderate and high risks should be brought to the attention of the organisation's risk function, who, in turn, could integrate these risks into the portfolio of organisational risks to be managed. Furthermore, an organisation could, for example, identify its top 5 to 10 high risk areas, and label these material ethics risks, or risks that could undermine the organisation's efforts to reach its objectives through the implementation of organisational strategies. These material ethics risks will also then resort within the ethics dimension of the ethics committee's mandate. This process will be clearly illustrated in the case study and ethics risk management toolbox, to be presented in Section 6 of the handbook.
3.4.5 An ethics management response to risk identification and risk rating

**Strategy**

Once an organisation has assessed its ethics opportunities and risks, it can proceed to meaningfully utilise, in a structured way, the information obtained. As such, the type of ethics management strategy required to capitalise on opportunities and mitigate negative risks could be informed by the results of the risk assessment.

For example, should an organisation decide on a compliance strategy to deal with the risk supplier relations, it would translate this strategy into an ethics management plan designed to strictly monitor and regulate relations with suppliers. On the other hand, an integrity- or values-based strategy could focus on regular values-based discussions as a component of the organisation's more encompassing stakeholder relations drive, rather than adopting many rules and policies and following a punitive approach.

**Codes and policies**

The organisation should then ensure that the ethics risks identified are sufficiently accounted for in current codes of ethics and ethics-related policies. If not, the codes and policies need to be revised. It may even be necessary to formulate new or additional policies.

It is also then required to link the codes and policies to the ethics management strategy that is deemed appropriate for the organisation at this point in time. For example, a compliance strategy would have at its core a code of ethics with a strong directional/rules-based focus. Such a code will contain clear guidelines on how suppliers should be treated, and how suppliers are expected to act in accordance with organisational prescripts. Moreover, stringent procurement policies and processes that provide specific guidance on how to manage supplier relations need to be formulated. At a micro level, the finance function (creditors) would have very specific rules regarding when suppliers should be paid, e.g., within 25 days of submitting an invoice. Some organisations have specific clauses included in supplier contracts, according to which suppliers are expected to adhere to the organisation's ethics requirements. A gift registry system has to be implemented and closely monitored, to prevent employees from accepting irregular or expensive gifts from suppliers.

Should an integrity- or values-based strategy be followed, the code of ethics would have an aspirational character, whereby values-based guidelines on the treatment of business partners (e.g., suppliers) will be provided in broad terms. In this example, procurement policies that have room for discretion would probably be formulated.
Institutionalising ethics
The formulation of appropriate codes and policies to utilise ethics opportunities and mitigate negative risks is followed by the institutionalisation of ethics guidelines contained in codes and policies. Specific ethics awareness programmes and dedicated ethics training programmes have to be designed and implemented for the organisation's employees, specifically those in the procurement function, and for suppliers/contractors alike.

A critical consideration for ethics practitioners is that ethics has to be strategically incorporated into the existing business processes of the organisation. It is thus imperative that the ethics office form a partnership with the risk managers. Since risk managers are the custodians of all risks in an organisation, they enjoy the respect and co-operation of colleagues. They report to an oversight structure (e.g., risk and/or audit committee(s) of the board). Therefore, an ethics risks register should be compiled after an ethics opportunity-risk assessment has been conducted. This action should be executed through a joint effort of the risk manager and the ethics officer. Through this approach, the ethics risks will be incorporated into the organisation-wide risk management framework (managed by risk managers).

The risk manager will facilitate the identification of ethics risks, and then develop an ethics risk register. The risk owners, typically line managers, will be identified based on the issues that emanate from the ethics risk assessment, and these will be communicated to them. Action plans are then developed (largely ethics programmes that the risk owner will have to implement in conjunction with the ethics officer), and timelines will be allocated. For example, in the case of the supplier relations risk, the risk area gifts from suppliers will be appropriated by the risk manager, while line managers, particularly those in the procurement function, would become the risk owners.

Monitoring and reporting
The implementation of the ethics management strategy and ethics management plan should be monitored. The ethics office would work closely with the organisation's internal audit function at this juncture. Results of such monitoring actions, as well as the current state of ethics of the organisation, should be regularly reported to the management and governance structures that oversee the organisation's ethics management.
3.5 The ethics of ethics risk assessment

Ethics risk assessment is, in essence, similar to many other research interventions in academia and organisations. For this reason, an ethics risk assessment warrants the same rigorous research ethics standards as would be applicable to any other research project. Moreover, any research intervention with ethics as the central theme may be problematic in itself, as the potential research subjects may feel personally threatened or uncomfortable answering ethics-related questions.

The main premise upon which research ethics is based is to avoid harm to subjects. This is irrespective of the research methodology adopted for the assessment process, i.e. qualitative and/or quantitative. In the attempt to avoid harm, the following research ethics principles should be accounted for during an ethics risk assessment process:

Content
Researchers and, in this case, ethics risk assessors have an ethical obligation to ensure that nothing but the organisation's ethics risk is measured. This will result in sound face validity (items/question are perceived by subjects as assessing ethics risks, nothing else) and construct validity (ethics risk as a construct is indeed measured). The questions posed to subjects during an ethics risk assessment intervention, whether in interviews or as items in a quantitative survey, should also be non-invasive. This implies that subjects should not be psychologically uncomfortable responding to questions, nor be hesitant to expose 'their inner selves' during the assessment process. Questions should be formulated in such a way that perceptions are assessed, not personal integrity or propensity for ethical or unethical behaviour. In both quantitative and qualitative ethics risk assessments, subjects should all be asked the same questions, as this will ensure assessment reliability.

Objectivity
For an ethics risk assessment to be objective and to be perceived as objective by the organisation and its participating stakeholders, it is advisable to utilise an independent third-party organisation and its interviewers/facilitators as the assessing entity. Research subjects are less reluctant to share sensitive information pertaining to ethics risks with an objective third party that has no vested interest in the outcome of the risk assessment. Interviewers and facilitators should be properly trained, to ensure a professional and objective assessment.
Informed consent
Research subjects, i.e. participants (the term that applies to qualitative assessment) and respondents (applicable in quantitative assessment), should be informed of:

1. how they were selected to participate in the assessment (preferably through a random selection by, e.g., employee number)
2. what the assessment will entail in terms of process and content
3. how the results will be used by the organisation
4. the fact they will receive feedback once the results of the assessment have been shared with the organisation's senior leadership
5. the voluntary nature of their participation
6. their right to withdraw from the assessment at any time, without consequences
7. the source that they should contact should any item or procedure in the assessment process be unclear
8. the fact that, by participating in the assessment process, they automatically give their informed consent

It is crucial that subjects are informed by the chief executive officer about the imminence and nature of the assessments well prior to commencement.

Anonymity
The cardinal rule is that subjects should never suspect that their identity could be revealed in any way. Demographic information solicited in quantitative surveys should be limited to information that will be essential to decision-makers involved in risk mitigation. Respondents should not be required to surrender personal information such as names or employee numbers. Participants in interviews should be well briefed on their ethical rights. In the case of group interviews, facilitators should clearly communicate that the participants' identities are of no importance, but that obtaining their perceptions of ethics opportunities and risks that occur in the organisation is the true objective of the assessment process. The use of attendance registers should be avoided. As an ethics risk assessment is not a forensic investigation, participants should be discouraged from identifying ethics transgressors, but should rather focus on the type and frequency of ethical transgressions.

Confidentiality
All information obtained, demographic or otherwise, should be kept absolutely confidential at all times. Surveys should be hosted by external, independent data-hosting service providers, and should preferably not be channelled via the organisation's IT function. Trends or patterns of behaviour should be reported in the risk profile documents and during feedback sessions, rather than who did what when.
With risk management, and ethics risk management in particular, being a relatively new development with regard to governance structures dedicated to these functions, there is often a lack of clarity on the interface between the roles, responsibilities, and reporting lines of these functions at governing body level. The purpose of this section of the handbook is to establish a meaningful and unambiguous perspective on the interface between the respective structures that have roles to fulfil in the governance of ethics risk in the organisation.

A number of principles that address an organisation’s accountability for taking responsibility for, identifying, and mitigating risk are presented in the IRMSA Guideline to Risk Management.

The four principles underpinning taking responsibility for risk are:

1. **Principle 1: The governing body should be responsible for the governance of risk.**

   This vests the responsibility for risk in the governing body of an organisation. It tasks the governing body with the responsibility of designing and implementing 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.

2. **Principle 2: The governing body should determine the levels of risk tolerance/appetite.**

   At least once a year, the governing body should set specific limits for the levels of risk the organisation is able to tolerate in pursuit of its objectives. The governing body may also set limits regarding the organisation’s risk appetite, i.e. those risks that the governing body desires or is willing to take. The limits are both financial and non-financial, and instances of the risk appetite limits exceeding or deviating materially from the risk tolerance limits should be disclosed in the integrated annual report.

3. **Principle 3: The risk committee or audit committee should assist the governing body in carrying out its risk responsibilities.**

4. **Principle 4: The risk committee should incorporate independent risk experts.**

   To assist it in the discharge of its duties and responsibilities with regard to risk management, the governing body should appoint a risk committee to review the risk management process and its maturity, 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 it has the capacity. The risk committee may appoint independent risk experts to supplement skills and experience.
With risk management, and ethics risk management in particular, being a relatively new development with regard to governance structures dedicated to these functions, there is often a lack of clarity on the interface between the roles, responsibilities, and reporting lines of these functions at governing body level. The purpose of this section of the handbook is to establish a meaningful and unambiguous perspective on the interface between the respective structures that have roles to fulfil in the governance of ethics risk in the organisation.

4.1 The strategic governance of risk

A number of principles that address an organisation's accountability for taking responsibility for, identifying, and mitigating risk are presented in the IRMSA Guideline to Risk Management. The four principles underpinning taking responsibility for risk are:

**Principle 1: The governing body should be responsible for the governance of risk.**
This vests the responsibility for risk in the governing body of an organisation. It tasks the governing body with the responsibility of designing and implementing 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.

**Principle 2: The governing body should determine the levels of risk tolerance/appetite.**
At least once a year, the governing body should set specific limits for the levels of risk the organisation is able to tolerate in pursuit of its objectives. The governing body may also set limits regarding the organisation's risk appetite, i.e. those risks that the governing body desires or is willing to take. The limits are both financial and non-financial, and instances of the risk appetite limits exceeding or deviating materially from the risk tolerance limits should be disclosed in the integrated annual report.

**Principle 3: The risk committee or audit committee should assist the governing body in carrying out its risk responsibilities.**
To assist it in the discharge of its duties and responsibilities with regard to risk management, the governing body should appoint a risk committee to review the risk management process and its maturity, 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 it has the capacity. The risk committee may appoint independent risk experts to supplement skills and experience.
Principle 4: The governing body should delegate to management the responsibility to design, implement, and monitor the risk management plan. The risk strategy should be executed by management and in accordance with the risk management policy and plan. The roles and responsibilities regarding 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 processes. Rigorous risk management should yield solutions that create the appropriate balance between risk and reward in the organisation.

The three principles in the management of risk are:

Principle 5: The governing body should ensure that risk assessments are performed on a continual basis. The governing body in the organisation should ensure that the organisation has and maintains an effective on-going 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 ensure a focus on the most critical risk responses.

Principle 6: The governing body 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.

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

The three principles that address the monitoring, assurance, and disclosure of risk are:

Principle 8: The governing body should ensure continual risk monitoring by management. The governing body should ensure that the responsibility for monitoring is clearly defined in the risk management plan, and that management monitors the risk management plan effectively and continually.

Principle 9: The governing body should receive assurance regarding the effectiveness of the risk management process.
Management is accountable for providing the governing body with assurance that it has implemented and monitored the risk management plan, and that it is integrated into 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 authority.

**Principle 10: The governing body should ensure that there are processes in place to enable complete, timely, relevant, accurate, and accessible disclosure of risks to stakeholders.**

The governing body 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 thereof, without compromising privileged information. It should disclose any current, imminent, or envisaged risk that may threaten the long-term sustainability of the organisation, as well as its views on the effectiveness of the organisation's risk management processes.

It is the foundational departure point of this handbook that ethics risks are on an equal footing with other organisational risks (e.g., financial, operational, legal, IT-, and HR risk) in terms of the potential monetary and reputational damage they can cause if not managed properly. It therefore stands to reason that the principles discussed above are equally applicable to ethics risk as they are to other categories of risk. The management of ethics risk requires a dedicated:

1. ethics risk assessment approach
2. ethics risk management strategy and plan
3. ethics risk register, to be incorporated into the organisational risk register that, by now, includes all categories of risk
4. governance and management reporting structures to ensure that ethics risk is continually accounted for

### 4.2 Governance oversight of ethics management

Sound corporate governance guidelines stipulate that the governing body is responsible for the governance of risk. The following principles apply to the governance of ethics risk:

- The governing body should provide effective leadership, based on an ethical foundation.
- The governing body should ensure that the organisation is a responsible corporate citizen.
- The governing body should ensure that the organisation's ethics is managed effectively.
The governing body should ensure that ethics risks and opportunities are incorporated into the risk management process. This responsibility is delegated to a sub-committee of the governing body, usually the risk committee or a committee responsible for the governance of ethics (such as an S&EC).

4.2.1 Risk committee

The risk committee (audit and risk committee, or audit committee where there is no dedicated risk committee) assists the governing body in carrying out its risk responsibilities, and reports directly to this entity. This implies that ethics risks are also incorporated into the mandate, activities, and reporting requirements of the risk committee. The risk committee is responsible for oversight of risk management, for ensuring that there is proper co-ordination of risk management, and that the governing body is informed of key risks faced by the company.

4.2.2 Social and ethics committee

The new Companies Act of 2011 stipulates that an S&EC is mandatory in:

- state-owned companies
- listed public companies
- organisations with significant public interests

The mandate of an S&EC is to monitor that the company's activities are adhering to all relevant legislation, other legal requirements, and prevailing codes of best practice with regard to:

(i) social and economic development
(ii) good corporate citizenship
(iii) the environment, health, and public safety
(iv) consumer relationships
(v) labour and employment

Since the Companies Act is silent on the ethics mandate of an S&EC, The Ethics Institute, in its 2012 publication *The Social and Ethics Committee Handbook*, proposed that the mandate of an S&EC be expanded to include an ethics mandate. The expanded mandate was, among others, built upon ethics management guidelines, which, in turn were based on sound governance principles. The ethics dimension of the mandate consists of:

Ensuring that the organisation's ethics is managed effectively, including monitoring activities with regard to:
leadership demonstrating support for ethics throughout the organisation
a strategy for managing ethics that is informed by the negative and positive risks the organisation faces
ethical standards being articulated in a code of ethics and supporting policies
structures, systems, and processes being in place to ensure that the governing body, employees, and supply chains are familiar with and adhere to the organisation’s ethical standards
ethics performance being included in the scope of internal audit and reported on in the organisation’s integrated annual report
ethics being imbedded in the organisational culture

4.3 A reporting structure for the governance of ethics risk

It is important that the organisation has a grasp of the interface between ethics risk and risk management. The reporting channels for each of these entities should also be understood (see figure below).

The above figure illustrates the interface between the risk management function and the ethics management function in the organisation. As previously mentioned, ethics risk is a specific category of risk that ideally needs to be addressed by the risk management function, in co-operation with the ethics office.
The logic underlying this figure is as follows:

1. The identification and prevalence of ethics risk in the organisation is assessed by the organisation's ethics office, using a specific ethics risk assessment methodology.
2. The ethics office reports on the ethics risk profile to the organisation's ethics governance committee (e.g., the S&EC).
3. The ethics office simultaneously liaises with the risk management department, to jointly or separately address the ethics risks identified.
4. The ethics governance committee applies its mind and identifies material ethics risks. This is executed by assessing the impact of those social and ethical issues that may either (a) enhance the implementation of organisational strategy, or (b) seriously undermine the implementation of organisational strategy.
5. The ethics governance committee reports to the audit and/or risk committee(s) and the governing body (e.g., the board) on the ethics risks and how these are being managed.
6. The ethics governance committee (and/or ethics officer) also submits the ethics risk register to the risk committee (and/or chief risk officer), who is responsible for consolidating all risk registers into one corporate risk register. The consolidated corporate risk register consists of various risk registers, e.g., organisational risk, occupational health and safety (OHS) risk, ethics risk, etc.
7. Most organisations have their top 10 risks, often referred to as strategic risks, which are usually determined by the highest regulating authority, who usually give instructions/feedback directly to the risk committee or chief risk officer. These prioritised risks will include material ethics risks. To address these material ethics risks, the risk committee then delegates further ethics risk management activities to the risk management function, which:
   a. appropriates the ethics risks as identified and rated by the ethics office as a category of risk that it has to deal with, among other categories of risk (e.g., operational, IT, legal, HR)
   b. identifies the potential impact of the ethics risk
   c. compiles an ethics risk register
   d. incorporates the ethics risk register into the organisational risk register
   e. reports on all risks to the audit and/or risk committee(s) of the governing body
8. The audit and/or risk committee report(s) to the governing body on all risks identified and managed.
9. The governing body evaluates all organisational risks.
10. The governing body, through the CEO, delegates responsibility for developing/managing/monitoring the risk management plan to management. That is, it instructs the risk management function and/or the ethics office to become the risk owners that deal with the mitigation of risks. The risk owners then report to their respective committees at the end of the next reporting cycle.
11. The ethics officer plays an important role in ensuring that there is a management plan for material ethics risks (the ethics risk management plan is incorporated into the risk management plan).

12. The risk management policy indicates when these plans are submitted to the chief risk officer, and how/when reporting on progress takes place.

13. The ethics officer or chair of the ethics governance committee may be called to report on the progress of the ethics management strategy and plan; presentations are usually also required by the governing body, its sub-committees, e.g., audit and/or risk committee(s) (the same applies to the OHS officer, and the OHS committee.)

14. The risk management function may not be directly involved in the mitigation of ethics risks or drafting of ethics risk response plans, but is involved in the facilitation of the process, and advise on the operationalisation of the frameworks. This is usually the function of the risk owner, which, in the case of ethics risks, could be the ethics officer and/or line management of other organisational functions.

15. Line managers act as the owners of both risks and ethics risks; they deal with the day-to-day management of risks, and are more 'hands-on.'

16. Risk owners also determine the impact of risks, whereas the risk management function is responsible for the monitoring and evaluation of risks.

Should the organisation not have a dedicated ethics office, the ethics risks identified need to be dealt with by the organisational risk management function.
Part 5

Key success factors for the successful implementation of ethics risk management
To ensure that the implementation of ethics risk management activities, as aligned to risk management, is executed in an effective and credible manner, a number of key success factors have been formulated as guidelines. These factors are categorised according to context and planning, assessment, and reporting.

**Context and planning**

1. An in-depth knowledge of the organisation and the legal, social, political, and economic environment in which it operates is essential for those functions involved in ethics risk management.
2. Organisational leadership that is committed to ethics/integrity is a crucial prerequisite for the implementation of the ethics risk management process.
3. The organisation needs to make a firm commitment to account for and manage its ethics risk.
4. The governing body and its relevant committees should provide strategic direction to and oversight of the organisation’s risk management, including ethics risk management.
5. Pragmatic guidelines that empower stakeholders within an organisation by ensuring common understanding of the acceptable principles, behaviours, and practices are an important requirement for the successful implementation of an ethics risk management process.
6. Ethics risk management, when effective, is characterised by the interconnectedness of strategy, operations, and process, in order to achieve organisational objectives.
7. An effective ethics risk management programme ensures the alignment of strategic intent and operational delivery.
8. The risk management function and the ethics management function should collaborate closely in managing the ethics risk of the organisation.
9. The co-ordination of risk and ethics risk management processes allows for the effective use of organisational resources and governance processes.
10. Ethics risk management is a continuous process that supports the organisation’s risk management, and thus guides strategy implementation in organisations.

**Assessment**

1. The organisation should ensure that it has the capacity and competence to identify and manage its ethics risks and opportunities.
2. The ethics risk assessment process should take account of the views of all stakeholders involved in the activity being assessed.
3. An ethics risk assessment process should ensure that all significant risks are identified timeously, and that root causes are comprehensively described and analysed.
4. The ethics risk assessment should be expressed in terms of an ethics risk rating, to
ensure that the subsequent actions of determining risk impact and likelihood can be conducted.

5. The ethics risk assessment should reflect the effectiveness of current controls, and provide sufficient information to assist in improving controls to eliminate or reduce risks to an acceptable level.

**Reporting**

1. The organisation should disclose to its stakeholders how it manages its ethics risks and opportunities.
2. Ethics risk reports need to be accurate and timely.
3. Ethics risk reports need to be sufficiently comprehensive to enable those involved in risk mitigation to make informed decisions – all material and emerging risks need to be included, as well as information relating to risk exposure.
4. Ethics risk reports need to be clear and useful, so as to address the needs of the recipients of the reports.
5. Ethics risk reporting should be done frequently, as determined by the governing body, and will vary according to the type of risk, the purpose of the report, and the needs of the recipients.
6. Ethics risk reports should be distributed to all relevant stakeholders, bearing in mind that confidentiality needs to be maintained.
Part 6
Ethics risk management
Toolbox and case study

5. The ethics risk assessment should reflect the effectiveness of current controls, and provide sufficient information to assist in improving controls to eliminate or reduce risks to an acceptable level.

1. The organisation should disclose to its stakeholders how it manages its ethics risks and opportunities.

2. Ethics risk reports need to be accurate and timely.

3. Ethics risk reports need to be sufficiently comprehensive to enable those involved in risk mitigation to make informed decisions – all material and emerging risks need to be included, as well as information relating to risk exposure.

4. Ethics risk reports need to be clear and useful, so as to address the needs of the recipients of the reports.

5. Ethics risk reporting should be done frequently, as determined by the governing body, and will vary according to the type of risk, the purpose of the report, and the needs of the recipients.

6. Ethics risk reports should be distributed to all relevant stakeholders, bearing in mind that confidentiality needs to be maintained.
The purpose of the case study presented below is to illustrate to users of this handbook how ethics risk is managed in a similar way to other organisational risks. The following chronological process is utilised in the case study:

- **Assessment of ethics risk (identification of types of risk and perceived risk rating)**
  - Risk analysis
    - potential risk impact analysis
    - analysis of risk likelihood
    - rating of inherent risk
    - evaluation of current controls in place
    - rating of residual risk
  - Risk evaluation
    - identification of organisational function that will become the risk owner
    - evaluation of risks in relation to organisation’s risk appetite and risk tolerance
    - identification of mitigating controls that will be established to deal with inherent and residual risk in reducing the residual risk to that which is within the risk appetite of the organisation
    - time lines for implementation of and reporting on mitigation controls

The entire process culminates in a carefully constructed ethics risk register.

### Case study: S Min

#### The organisation
STRP-Mining Pty (Ltd) (“S Min”) is a mining company operating several open-cast and underground mines within the Glorious Republic of Korruptia, a country located on the sub-continent. Korruptia was listed in 143rd position in terms of international perceptions of being corrupt on the most recent Transparency International Corruption Perceptions Index (CPI). The country has one of the lowest GDP distributions per capita in the world. Furthermore, Korruptia is recovering from a recent coup d'état and an 11-year civil war.

The mine recently implemented a female employee empowerment programme, with the purpose of ensuring that more women are employed in entry-level underground mining activities and in leadership roles.

#### Trying to fix things
Due to Korruptia’s local Companies Act requirements, S Min was obligated to establish a separate S&EC, a sub-committee of the company’s board of directors. One of the first instructions of the newly established committee was that the CEO had to appoint a dedicated ethics officer, and, once appointed, that the ethics officer conduct an urgent ethics risk assessment.
Ashley Doright was appointed as S Min's ethics officer, and contracted an independent consultant to conduct a comprehensive ethics risk assessment through both qualitative and quantitative approaches. The focus of this first-ever risk assessment for the company was on ethical conduct risk only, and not ethical culture or ethics management risk. It was decided to engage with both internal and external stakeholders, to assess their perceptions of S Min's ethics risks. The qualitative methodology used consisted of the following group- and one-on-one interviews:

<table>
<thead>
<tr>
<th>Stakeholder category</th>
<th>Stakeholder</th>
<th>Assessment method</th>
<th>Number of interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>1. CEO</td>
<td>Personal interview</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2. Board of directors</td>
<td>Group interview</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>3. Audit and risk committee</td>
<td>Group interview</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>4. ExCo</td>
<td>Group interview</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>5. Senior management</td>
<td>Group interview</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>6. Middle managers</td>
<td>Group interview</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>7. Employees</td>
<td>Group interview</td>
<td>6</td>
</tr>
<tr>
<td>External</td>
<td>1. Regulators</td>
<td>Personal interview</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2. Major shareholders</td>
<td>Personal interview</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>3. Office of the Minister of Mining</td>
<td>Personal interview</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>4. Suppliers (of different organisational size)</td>
<td>Personal interview</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>5. Communities surrounding the mines</td>
<td>Group interview</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>6. The Department of Labour</td>
<td>Personal interview</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>7. Trade unions</td>
<td>Group interview</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>8. External auditor</td>
<td>Personal interview</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td><strong>Total:</strong></td>
<td></td>
<td><strong>37</strong></td>
</tr>
</tbody>
</table>

The themes elicited from the qualitative data analysis were then used to populate the contents (items) of the subsequent quantitative ethics risk survey. The survey was completed by 677 employees.

The qualitative and quantitative data were then integrated and presented in a comprehensive ethics risk profile report.

**Ethics risk assessment**

Below is the output of the ethics risk assessment. The risk rating is noted as perceived risk, as this was obtained through the ethics risk assessment process, and has not yet been evaluated using the broader organisational risk management methodology.
On completion of the ethics risk assessment, the consultancy agency emphasised that the ratings provided were based on a perceived risk rating, and that the company should conduct a formal risk management workshop with the relevant stakeholders, to analyse the above risks in line with the company’s risk appetite and methodology.

Ashley duly followed the advice, and requested Alexis Riskaverse, the company’s Risk Manager, to facilitate a risk workshop with the relevant departmental stakeholders, to formally analyse the ethics risks as per the company’s Risk Management Framework.

Alexis informed Ashley that risk matrixes are used to rate inherent risks (see table below). Further, per the company’s risk appetite, no ethics risks with a moderate risk rating or more can be tolerated.

**Analysis of risk: impact and likelihood assessment**

In analysing the risk in terms of determining risk impact, the following impact- and likelihood risk scales are used by S Min as part of their risk grading methodology:
The table below represents the Risk Rating Heat Map (risk classification table), per the above methodology. The scoring is calculated as a mathematical multiplication of the impact and likelihood axes. For example, a risk rated as Significant (3) in relation to impact and Likely in relation to likelihood, would be scored 12 (3 x 4). The heat map is calculated based on the premise that the organisation has a three-level risk rating scale (High, Moderate, and Low), and that each risk category is equally distributed across the organisation. Thus, the risk classification grading scale is based on the maximum risk score of 25 (per the table below), divided by 3, representing the three risk classification grading scales.

<table>
<thead>
<tr>
<th>Impact assessment</th>
<th>Score</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>Catastrophic</td>
<td>Will result in the company closing down</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Serious</td>
<td>Will result in loss of one year's revenue, loss of employee life, or serious reputational damage to the company (international news coverage)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Significant</td>
<td>Will result in loss of 6 months' revenue, serious injury to employees, or significant reputational damage (national news coverage)</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Minor</td>
<td>Will result in loss of 3 months' revenue, minor injury to employees, or minor reputational damage (local news coverage)</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>None</td>
<td>No effect on the company</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Score</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>Very likely</td>
<td>May occur every day</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Likely</td>
<td>May occur several times a month</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Possible</td>
<td>May occur several times a year</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Rare</td>
<td>May occur once every 2 years</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Unlikely</td>
<td>May occur once in 5 years or more</td>
</tr>
</tbody>
</table>

The table below represents the Risk Rating Heat Map (risk classification table), per the above methodology. The scoring is calculated as a mathematical multiplication of the impact and likelihood axes. For example, a risk rated as Significant (3) in relation to impact and Likely in relation to likelihood, would be scored 12 (3 x 4). The heat map is calculated based on the premise that the organisation has a three-level risk rating scale (High, Moderate, and Low), and that each risk category is equally distributed across the organisation. Thus, the risk classification grading scale is based on the maximum risk score of 25 (per the table below), divided by 3, representing the three risk classification grading scales.
Using the above matrixes, the risk analysis workshop delegates rated the inherent risk of the identified perceived ethics risks occurring within S Min’s environment, i.e. the risk that reflects the aggregate of the risk rating, the perceived impact, and the likelihood of occurrence. This culminated in the following inherent risk ratings (see table below):

<table>
<thead>
<tr>
<th>#</th>
<th>Ethics risk</th>
<th>Risk rating (perceived)</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Inherent risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Use of child labour in mining operations</td>
<td>High</td>
<td>Serious</td>
<td>Very likely</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Use of conflict minerals in supply chain</td>
<td>High</td>
<td>Significant</td>
<td>Possible</td>
<td>Moderate</td>
</tr>
<tr>
<td>3</td>
<td>Illegal mining activities in abandoned mines</td>
<td>High</td>
<td>Serious</td>
<td>Very likely</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Negative environmental impact of mining operations</td>
<td>High</td>
<td>Catastrophic</td>
<td>Very likely</td>
<td>High</td>
</tr>
<tr>
<td>5</td>
<td>Mining operations threatening community safety</td>
<td>High</td>
<td>Significant</td>
<td>Possible</td>
<td>Moderate</td>
</tr>
<tr>
<td>6</td>
<td>Theft of company property</td>
<td>High</td>
<td>Significant</td>
<td>Possible</td>
<td>Moderate</td>
</tr>
<tr>
<td>7</td>
<td>Irregular procurement</td>
<td>High</td>
<td>Significant</td>
<td>Rare</td>
<td>Low</td>
</tr>
<tr>
<td>8</td>
<td>Favouritism in promotions</td>
<td>High</td>
<td>Minor</td>
<td>Rare</td>
<td>Low</td>
</tr>
<tr>
<td>9</td>
<td>Bullying of employees in the workplace</td>
<td>High</td>
<td>Significant</td>
<td>Rare</td>
<td>Low</td>
</tr>
<tr>
<td>10</td>
<td>Bribery of public officials by mining employees</td>
<td>High</td>
<td>Serious</td>
<td>Rare</td>
<td>Low</td>
</tr>
<tr>
<td>11</td>
<td>Employees committing fraud against the company</td>
<td>Moderate</td>
<td>Significant</td>
<td>Possible</td>
<td>Moderate</td>
</tr>
<tr>
<td>12</td>
<td>Intentionally misleading stakeholders</td>
<td>Moderate</td>
<td>Serious</td>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>13</td>
<td>Leaking of confidential information</td>
<td>Moderate</td>
<td>Serious</td>
<td>Rare</td>
<td>Low</td>
</tr>
<tr>
<td>14</td>
<td>Sexual harassment</td>
<td>Moderate</td>
<td>Serious</td>
<td>Very likely</td>
<td>High</td>
</tr>
<tr>
<td>15</td>
<td>Illegal substance use</td>
<td>Moderate</td>
<td>Minor</td>
<td>Very likely</td>
<td>Moderate</td>
</tr>
<tr>
<td>16</td>
<td>Inappropriate gifts and hospitality accepted by employees or given by the company to external stakeholders</td>
<td>Low</td>
<td>Minor</td>
<td>Very likely</td>
<td>Moderate</td>
</tr>
<tr>
<td>17</td>
<td>Nepotism</td>
<td>Low</td>
<td>Minor</td>
<td>Rare</td>
<td>Low</td>
</tr>
<tr>
<td>18</td>
<td>Abuse of company vehicles</td>
<td>Low</td>
<td>Minor</td>
<td>Very likely</td>
<td>Moderate</td>
</tr>
<tr>
<td>19</td>
<td>Extra-marital affairs amongst employees</td>
<td>Low</td>
<td>Minor</td>
<td>Likely</td>
<td>Low</td>
</tr>
<tr>
<td>20</td>
<td>Conflicts of interests</td>
<td>Low</td>
<td>Significant</td>
<td>Likely</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

Further, during the workshop, the delegates were required to determine whether S Min had any controls in place that mitigated the identified risks. Further, the delegates were required to determine if the controls were Satisfactory, Partially satisfactory, or Unsatisfactory in mitigating the identified ethical risks.
Analysis of risk: evaluation of current controls and residual risk rating

Residual risk, which is the risk that reflects the impact of controls on inherent risk, was then determined qualitatively during the same workshop. Desktop research, in the form of the analysis of documents and reports, was also conducted to evaluate the existence of current controls (e.g., policies) to ascertain whether the controls identified satisfactorily mitigate the identified ethics risks. The results were as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Ethics risk</th>
<th>Inherent risk</th>
<th>Current controls</th>
<th>Control effectiveness</th>
<th>Residual risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Use of child labour in mining operations</td>
<td>High</td>
<td>• Group-wide Child Labour Policy</td>
<td>Partially satisfactory</td>
<td>Moderate</td>
</tr>
<tr>
<td>2</td>
<td>Use of conflict minerals in supply chain</td>
<td>Moderate</td>
<td>• Group Policy on Conflict Minerals</td>
<td>Satisfactory</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>Illegal mining activities in abandoned mines</td>
<td>High</td>
<td>• Regulatory and compliance function</td>
<td>Partially satisfactory</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Negative environmental impact of mining operations</td>
<td>High</td>
<td>• Internal environmental impact assessments</td>
<td>Unsatisfactory</td>
<td>Moderate</td>
</tr>
<tr>
<td>5</td>
<td>Mining operations threatening community safety</td>
<td>Moderate</td>
<td>• Health and Safety Forum</td>
<td>Unsatisfactory</td>
<td>Moderate</td>
</tr>
<tr>
<td>6</td>
<td>Theft of company property</td>
<td>Moderate</td>
<td>• CCTV surveillance</td>
<td>Satisfactory</td>
<td>Low</td>
</tr>
<tr>
<td>7</td>
<td>Irregular procurement</td>
<td>Low</td>
<td>• Formal procurement process</td>
<td>Unsatisfactory</td>
<td>Low</td>
</tr>
<tr>
<td>8</td>
<td>Favouritism in promotions</td>
<td>Low</td>
<td>• Recruitment process</td>
<td>Partially satisfactory</td>
<td>Low</td>
</tr>
<tr>
<td>9</td>
<td>Bullying of employees in the workplace</td>
<td>Low</td>
<td>None</td>
<td>Unsatisfactory</td>
<td>Low</td>
</tr>
<tr>
<td>10</td>
<td>Bribery of public officials by mining employees</td>
<td>High</td>
<td>• Anti-bribery and Corruption Policy</td>
<td>Partially satisfactory</td>
<td>High</td>
</tr>
<tr>
<td>11</td>
<td>Employees committing fraud against the company</td>
<td>Moderate</td>
<td>• Fraud Policy</td>
<td>Unsatisfactory</td>
<td>Moderate</td>
</tr>
<tr>
<td>12</td>
<td>Intentionally misleading stakeholders</td>
<td>Low</td>
<td>• Corporate Communication Department</td>
<td>Satisfactory</td>
<td>Low</td>
</tr>
<tr>
<td>13</td>
<td>Leaking of confidential information</td>
<td>Low</td>
<td>• Document Classification Policy</td>
<td>Satisfactory</td>
<td>Low</td>
</tr>
<tr>
<td>14</td>
<td>Sexual harassment</td>
<td>High</td>
<td>None</td>
<td>Unsatisfactory</td>
<td>High</td>
</tr>
</tbody>
</table>
### Evaluation of risk: identification of risk owner, migrating controls and time lines

Finally, during the workshop, the various departments agreed on the mitigating actions required for all ethical risks with a *Risk rating of High* or *Moderate*, together with an implementation date deadline (the company's risk appetite for ethics risks was set at *Low*). Additional mitigating controls for ethics risks with a *Residual risk rating of Low* were deemed unnecessary, as these were within the risk appetite of S Min. The table overleaf illustrates the evaluation of risk.

<table>
<thead>
<tr>
<th>#</th>
<th>Ethics risk</th>
<th>Inherent risk</th>
<th>Current controls</th>
<th>Control effectiveness</th>
<th>Residual risk</th>
</tr>
</thead>
</table>
| 15 | Illegal substance use                                                      | Moderate      | • Employee support programme  
• Random illicit substance screening of employees | Satisfactory    | Low                        |
| 16 | Inappropriate gifts and hospitality accepted by employees or given by the company to external stakeholders | Moderate      | • Gifts Policy                                                                 | Partially satisfactory | Moderate       |
| 17 | Nepotism                                                                   | Low           | • Recruitment process  
• Panel interviews                                                             | Satisfactory        | Low                        |
| 18 | Abuse of company vehicles                                                  | Moderate      | • Fleet Vehicle Policy  
• Vehicle tracking system, monitored independently                               | Satisfactory        | Low                        |
| 19 | Extra-marital affairs amongst employees                                    | Low           | None                                                                              | Unsatisfactory       | Low                        |
| 20 | Conflicts of interests                                                     | Moderate      | • Contractor screening                                                        | Satisfactory        | Low                        |
It is important to note that, at the time of expiry of the target dates for the implementation of the mitigating controls, a follow-up session should have been conducted with the departments identified as risk owners, to ensure that the mitigating actions were, in fact, implemented, and were operating effectively. Consideration should also be given to ensuring that follow-up audits are planned for those ethics risks with a high inherent risk, to ensure that controls are indeed implemented and are effective. An integrated perspective on the entire process described above is provided in the organisation’s ethics risk register (see table overleaf).
<table>
<thead>
<tr>
<th>#</th>
<th>Ethics risk</th>
<th>Risk rating (perceived)</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Inherent risk</th>
<th>Current controls</th>
</tr>
</thead>
</table>
| 1  | Use of child labour in mining operations        | High                    | Serious   | Very likely| High          | • Group-wide Child Labour Policy  
• Vendor screening                                                                   |
| 2  | Use of conflict minerals in supply chain        | High                    | Significant| Possible   | Moderate      | • Group Policy on Conflict Minerals  
• Vendor screening                                                                   |
| 3  | Illegal mining activities in abandoned mines    | High                    | Serious   | Very likely| High          | • Regulatory and compliance function  
• Physical security measures and monitoring                                           |
| 4  | Negative environmental impact of mining operations | High                   | Catastrophic | Very likely| High          | • Internal environmental impact assessments                                        |
| 5  | Mining operations threatening community safety  | High                    | Significant| Possible   | Moderate      | • Health and Safety Forum                                                          |
| 6  | Theft of company property                       | High                    | Significant| Possible   | Moderate      | • CCTV surveillance  
• Body frisks at high-risk areas  
• Security guards at entry and exit points                                           |
| 7  | Irregular procurement                           | High                    | Significant| Rare       | Low           | • Formal procurement process  
• Tender process for high-value spending  
• 3 quotations for lower-level spend                                                  |
| 8  | Favouritism in promotions                       | High                    | Minor     | Rare       | Low           | • Recruitment process  
• Panel interviews                                                                   |
| 9  | Bullying of employees in the workplace          | High                    | Significant| Rare       | Low           | None                                                                              |
| 10 | Bribery of public officials by mine employees   | High                    | Serious   | Likely     | High          | • Anti-bribery and corruption policy                                                |
| 11 | Employees committing fraud against the company  | Moderate                | Significant| Possible   | Moderate      | • Fraud policy  
• Whistle-blowing policy                                                             |
| 12 | Intentionally misleading stakeholders            | Moderate                | Serious   | Unlikely   | Low           | • Corporate Communication Department  
• Media liaison officer                                                               |
| 13 | Leaking of confidential information             | Moderate                | Serious   | Rare       | Low           | • Document classification policy  
• Data leakage software controls                                                     |
| 14 | Sexual harassment                               | Moderate                | Serious   | Very likely| High          | None noted                                                                        |
| 15 | Illegal substance use                           | Moderate                | Minor     | Very likely| Moderate      | • Employee Wellness Programme  
• Random illicit substance screening of employees                                      |
| 16 | Inappropriate gifts and hospitality accepted by employees or given by the company to external stakeholders | Low  | Minor     | Very likely| Moderate      | • Gifts Policy                                                                   |
| 17 | Nepotism                                        | Low                     | Minor     | Rare       | Low           | • Recruitment process  
• Panel interviews                                                                   |
| 18 | Abuse of company vehicles                       | Low                     | Minor     | Very likely| Moderate      | • Fleet vehicle policy  
• Vehicle tracking system, monitored independently                                      |
<p>| 19 | Extra-marital affairs amongst employees         | Low                     | Minor     | Likely     | Low           | None                                                                              |
| 20 | Conflicts of interests                          | Low                     | Significant| Likely     | Moderate      | • Contractor screening                                                            |</p>
<table>
<thead>
<tr>
<th>Control effectiveness</th>
<th>Residual risk</th>
<th>Risk owner</th>
<th>Mitigating controls to be implemented</th>
<th>Target time</th>
</tr>
</thead>
</table>
| Partially satisfactory | Moderate     | Sustainability Department | • Surprise audits  
|                       |              |            | • Employee screening and vetting  
|                       |              |            | • Control of subcontractors  
|                       |              |            | • Vendor screening | 6 months |
| Satisfactory          | Low          | Procurement Department | | |
| Partially satisfactory | High        | Operations and Security | • Additional security measures  
|                       |              |            | at abandoned sites  
|                       |              |            | • Biometric checks at points  
|                       |              |            | of entry to mines | Immediate |
| Unsatisfactory        | Moderate     | Sustainability Department | • Independent environmental  
|                       |              |            | assessments  
|                       |              |            | • Continued environmental  
|                       |              |            | inspections  
|                       |              |            | • Environmental audits | 3 months |
| Unsatisfactory        | Moderate     | Health and Safety Department | • Employee- and community health  
|                       |              |            | safety briefings  
|                       |              |            | • Evacuation planning and training  
|                       |              |            | • Medical Officer appointment  
|                       |              |            | and first-aid training | 3 months |
| Satisfactory          | Low          | Security services | | |
| Unsafe                | Low          | Procurement Department | | |
| Partially satisfactory | Low         | Human Resources Department | | |
| Unsatisfactory        | Low          | Ethics Office | | |
| Partially satisfactory | High        | Forensic services | • Corruption and bribery training  
|                       |              |            | and awareness initiatives in  
|                       |              |            | high-risk areas  
|                       |              |            | • Independent audit of cash payments | Immediate |
| Unsatisfactory        | Moderate     | Forensic services | • Implementation of a formal fraud  
|                       |              |            | prevention strategy | 12 months |
| Satisfactory          | Low          | Customer Care Department | | |
| Satisfactory          | Low          | IT Services | | |
| Unsatisfactory        | High         | Ethics Office | • Sexual harassment counselling  
|                       |              |            | and awareness  
|                       |              |            | • Increased security and patrols in  
|                       |              |            | high-risk areas | Immediate |
| Satisfactory          | Low          | Occupational Health Officer | | |
| Partially satisfactory | Moderate     | Company Secretary | • Implementation of a gifts register  
|                       |              |            | and approval process  
|                       |              |            | • Employee awareness training | 6 months |
| Satisfactory          | Low          | Ethics Office | | |
| Satisfactory          | Low          | Fleet Management Officer | | |
| Unsatisfactory        | Low          | Ethics Office | | |
| Satisfactory          | Low          | Company Secretary | | |
**Terminology**

**Business ethics:** See *organisational ethics*.

**Chief risk officer (CRO):** Title denoting a senior manager tasked with day-to-day oversight of risk management

**Control:** A process effected by the regulating body, management, and other functions, designed to provide reasonable assurance regarding the achievement of objectives relating to identified risks.

**Cost of risk:** The financial impact on an organisation from undertaking activities with an uncertain outcome – the cost of managing risks and incurring losses

**Enterprise risk management (ERM):** See risk management terminology (the term *risk management* is preferred over *enterprise risk management*)

**Ethical culture:** The set of collective ethics beliefs, standards, norms, habits, and taboos that determine the magnitude and quality of ethical behaviour in an organisation.

**Ethics:** What is good or right in human interaction.

**Ethics risk:** The ethics-related opportunities, uncertainties, threats, or barriers to which an organisation must respond in order to achieve its objectives

**Ethics risk assessment (ERA):** An ERA, which culminates in an ethics risk profile, provides the organisation with a clear understanding of unethical behaviours and organisational practices that could put the organisation at risk, as well as the opportunities related to ethics that can be used by the organisation

**Ethics management:** A structured and continuous organisational intervention whereby ethics risk is assessed, mitigated, monitored, and reported – a function of the organisation's ethics office

**Ethics risk profile:** A collation of the results and findings of an ethics risk assessment in a report that describes the organisation's state of ethics or ethics status

**Ethics risk register:** A listing of an organisation's ethics risks, often in table format, which usually includes risk ratings (also called Ethics Risk Portfolio)

**Ethics risk reporting:** Publishing information on ethics risks to internal or external stakeholders

**Governance of ethics:** The process by which strategic direction and oversight of the organisation's ethics are provided by the governing body, mainly through a sub-committee
**Impact:** Result or effect of an event; a range of possible impacts may be associated with an event, which could be positive or negative, relative to the entity's related objectives

**Inherent risk:** The risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or its impact

**Internal environment:** Encompasses the tone of an organisation, and sets the basis for how risk is viewed and addressed by an entity, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which the organisation operates

**Likelihood (probability):** The extent of the possibility that a given event will occur

**Material risk (see also strategic risk):** The uncertainties and untapped opportunities embedded in the organisation's strategic intent and how well they are executed. Such risks are key (material) matters for the governing body and impinge on the whole business, rather than just an isolated unit

**Metrics:** A tool measuring the likelihood and impact of a risk occurring, or the effectiveness and/or success of risk mitigation strategies

**Opportunity:** The possibility that an event will occur and positively affect the achievement of objectives

**Organisational ethics:** A conception of the good (values and standards) that guides the organisation in its interaction with internal and external stakeholders

**Residual risk:** The remaining risk after management has taken action to alter the risk's likelihood or impact

**Risk:** The effect of uncertainty on objectives (ISO 31000), it is the combination of the probability of an event and its consequences; it is inherent in all types of undertaking, and may carry the potential for benefit or be a threat to success (can also be described as the opportunities, uncertainties, threats, or barriers to which an organisation must respond in order to achieve its objectives)

**Risk acceptance:** No action is taken to mitigate risk likelihood or impact

**Risk analysis:** Identifying, describing, and estimating risks, and compiling a risk profile

**Risk appetite:** An organisation's tolerance for risk; the broad-based amount of risk that an organisation is willing to accept in pursuit of its mission (or vision)

**Risk assessment:** Determining the impact or consequence of an identified risk on the organisation (whether inherent and residual)
**Risk assessment tools**: Instruments designed to assist the organisation's risk function in assessing and evaluating risks when making decisions

**Risk avoidance**: Avoiding activities that give rise to risk

**Risk categories**:
- Ethics: Exposure to ethics-related opportunities, uncertainties, threats, or barriers
- External: Exposure to uncertainty affecting the external environment/stakeholders
- Financial: Exposure to uncertainty regarding the management and control of the finances of the organisation
- Hazard: Exposure to loss arising from damage to property or from tortious acts; typically includes the perils covered by insurance
- Human resource: Exposure to uncertainty related to compliance with human resource management policies and procedures, employee morale, and organisational culture
- Legal/Regulatory compliance: Exposure to uncertainty related to laws, statutes, and administrative regulations that govern how an organisation operates
- Operational: Exposure to uncertainty related to day-to-day business activities
- Reputational: Exposure to uncertainty related to brand, perceived value, organisational status, and public perception and trust
- Strategic: Exposure to uncertainty related to long-term policy directions of the organisation (also referred to as *big picture risk* or *material risk*)

**Risk control**: A synonym for loss control in traditional risk management; the technique of minimizing the frequency or severity of losses by employing training, safety, and security measures

**Risk description**: To display the identified risks in a structured format, e.g., in a table

**Risk estimation**: The use of a tool or system (quantitative and/or qualitative) to determine probability of occurrence and consequences or impact of risks

**Risk evaluation**: Comparing the results of risk estimation to established criteria, for the purpose of determining the significance of risks and whether to accept or mitigate them

**Risk financing**: The mechanisms for funding risk mitigation strategies and/or funding the financial consequences of risk (e.g., insurance)

**Risk identification**: The qualitative determination material risks, i.e., those that potentially can impact the achievement of objectives

**Risk management**: An integrated approach to assessing and addressing all risks that threaten achievement of the organisation's strategic objectives; the purpose of risk management is to understand, prioritize, and develop action plans to maximize benefits and mitigate risks; the risk management framework enables management to collaboratively identify, assess, and manage future risks and opportunities individually
and across the organisation (also known as **holistic, strategic, or integrated risk management**).

**Risk management policy:** An organisation's written statement that sets out its approach to an appetite for risk and its approach to risk management

**Risk mapping:** A visual representation of risks (that have been identified through a risk assessment exercise) in a way that allows easy priority ranking; often takes the form of a two-dimensional grid with **Probability** on one axis and **Impact** on the other (risks that fall in the **High probability/High impact** quadrant are given priority)

**Risk mitigation:** Actions that reduce a risk or its consequences/impact

**Risk owner:** The organisational function designated to direct mitigation of a risk

**Risk portfolio:** A list of risks identified and evaluated by an organisation (also referred to as a risk register) that contains an overview of risks at a certain time

**Risk prioritisation:** The ranking of material risks on an appropriate scale, according to frequency and/or severity (see **risk mapping**)

**Risk profile:** The use of a tool or system to rate and/or prioritise a series of risks

**Risk reduction:** Effected through action taken to reduce risk likelihood or impact, or both; measures to reduce the frequency or severity of losses (may include engineering, fire protection, safety inspections, or claims management)

**Risk register:** A listing of an organisation's risks, often in table format, which usually includes risk ratings (also called a risk portfolio)

**Risk response:** Management's selection of the manner in which to respond to risk — avoiding, accepting, reducing or sharing — and developing a set of actions to align risks with the organisation's risk tolerance and risk appetite

**Risk reporting:** Publishing information on risks to internal or external stakeholders

**Risk sharing:** Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk

**Risk tolerance:** The acceptable variation relative to the achievement of an objective

**Risk treatment:** The process of selecting and implementing measures (risk response strategies) to modify the risk

**Strategic risk (see also material risk):** The uncertainties and untapped opportunities embedded in the organisation's strategic intent and how well they are executed. Such risks are key (material) matters for the governing body and impinge on the whole business, rather than just an isolated unit.
The Ethics Institute

The Ethics Institute, a non-profit, public benefit organisation, commenced operations in August 2000. The organisation is governed by a board of directors, consisting of prominent persons committed to promoting ethical responsibility.

The Ethics Institute's vision is: “Building an ethically responsible society.”

We achieve our vision by forming partnerships with the public and private sectors, and the professions. The Ethics Institute serves as a resource through our thought leadership, research, training, support, assessment, and certification activities.

For more information on The Ethics Institute, please refer to our website www.tei.org.za

Thought leadership
The Ethics Institute is committed to stimulating and advancing awareness of ethics in South Africa and in other countries on the African continent where we are active. We regularly participate in public debates in the media, and contribute to standard-setting and policy formulation in respect of business ethics, corruption prevention, and professional ethics.

Services offered
The Ethics Institute offers a wide array of services related to the management of ethics in organisations and professions. These include:

- **Training**: Public and in-house training programmes on a range of ethics-related themes
- **Advisory services**: Consulting to public-sector and private-sector organisations and professional associations on matters related to the management of ethics
- **Assessments**: Assisting organisations to gauge their current state of ethics with a variety of assessment instruments
- **Certification**: Certifying specific ethics-related services and service providers, in order to provide assurance that these meet relevant ethics standards
- **Project management**: Acting as project manager for funder organisations wishing to enhance good governance, prevent corruption, or uphold professional ethics
- **Membership services**: Offering subscription membership to individuals and organisations, with a variety of membership benefits
The Institute of Risk Management South Africa (IRMSA)

IRMSA has been recognised by the South African Qualifications Authority (SAQA) as the only professional body for risk managers in Southern Africa. It is dedicated to the advancement of the risk management profession and accreditation, and is the leading source of information and networking opportunities in the risk management industry.

References


Berenice Francis

Lea Annandale-Dippenaar

Nicholas Harris (ICFP)

Berenice is the group commercial executive of Imperial. Her portfolio includes the development and implementation of frameworks for governance, risk, and compliance. In addition to various governance roles within the Imperial-owned companies, she serves as the chair of National Treasury’s Risk Committee and the IRMSA Education and Technical Committee. She was the recipient of the 2015 IRMSA Risk Manager award.

Lea completed a Master of Philosophy degree in Workplace Ethics at the University of Pretoria, and is currently a doctoral candidate in Applied Leadership and Coaching at UGSM-Monarch Business School in Switzerland. After completing a B.A. degree and Higher Education Diploma at the University of Stellenbosch, she started her career as a teacher. She has over 30 years’ experience working in government, including the Departments of Home Affairs, Defence, and the National Treasury. Lea joined the University of Pretoria as Business Ethics lecturer in 2001. She has since also been teaching business ethics as a contract lecturer at the UNISA School for Business Leadership. She has mainly been involved in the establishment of ethics- and risk management offices for various institutions, and received the IMRSA/Santam award for Best Government Risk Management Initiative shortly after establishing the Ethics Office of the Independent Policy Investigative Directorate (IPID) in 2007.

Nic is a qualified CA. He joined KPMG in 2005 and, after completing his articles, became Manager: Fraud Risk Management. He gained valuable experienced in the fraud risk management field, and joined MTN Group Business Risk Management in July 2010. In July 2011, Nic was promoted to Head of Group Forensics at MTN Management Services. He is responsible for establishing and maintaining the MTN Fraud Risk Management Strategy across all 22 countries in which MTN operates. He conducts extensive high-priority forensic investigations across Africa and the Middle East.

The Ethics Institute contributors

Leon van Vuuren

Leon holds the position of Executive Director: Professional and Business Ethics at the Ethics Institute. Prior to joining the institute in July 2014, he was a professor in Industrial Psychology in the Department of Industrial Psychology and People Management (IPPM) at the University of Johannesburg, where he taught industrial psychology and business- and professional ethics for 26 years. He is professionally registered as an industrial psychologist with the Health Professions Council of South Africa (HPCSA). He serves on the Professional Board for Psychology of the HPCSA, where he is, among other, the chairperson of the Committee for Preliminary Inquiry (Ethics Committee).

Deon Rossouw

Deon Rossouw is the CEO of The Ethics Institute and professor extraordinary in philosophy at the University of Stellenbosch. He was the founding president of the Business Ethics Network of Africa (BEN-Africa), and served as president of the International Society of Business, Economics and Ethics (ISBEE). Deon serves on the fourth King Committee for Corporate Governance in South Africa. He has been recognised as a Chartered Director by the Institute of Directors of South Africa.

Kris Dobie

Kris Dobie is Manager for Organisational Ethics Development at The Ethics Institute. His main focus is on ethics management in the public sector, with a special interest in corruption prevention. He served on the Global Reporting Initiative’s G4 anti-corruption working group, and he also serves on the Gauteng Anti-Corruption Task Team. He holds a degree in landscape architecture from the University of Pretoria, as well as an M.Phil. in Workplace Ethics (cum laude) from the same institution.

IRMSA contributors

Gillian le Cordeur

Gillian has been the CEO of The Institute of Risk Management South Africa (IRMSA) for more than five years. During this time, IRMSA reached new heights, including recognition as the professional body for risk management in South Africa. Gillian became passionate about the strategy and operations of not-for-profit associations during her time as the chief operating officer for an association management company working with many different associations from various industries.
Berenice Francis
Berenice is the group commercial executive of Imperial. Her portfolio includes the development and implementation of frameworks for governance, risk, and compliance. In addition to various governance roles within the Imperial-owned companies, she serves as the chair of National Treasury’s Risk Committee and the IRMSA Education and Technical Committee. She was the recipient of the 2015 IRMSA Risk Manager award.

Lea Annandale-Dippenaar
Lea completed a Master of Philosophy degree in Workplace Ethics at the University of Pretoria, and is currently a doctoral candidate in Applied Leadership and Coaching at UGSM-Monarch Business School in Switzerland. After completing a B.A. degree and Higher Education Diploma at the University of Stellenbosch, she started her career as a teacher. She has over 30 years' experience working in government, including the Departments of Home Affairs, Defence, and the National Treasury. Lea joined the University of Pretoria as Business Ethics lecturer in 2001. She has since also been teaching business ethics as a contract lecturer at the UNISA School for Business Leadership. She has mainly been involved in the establishment of ethics- and risk management offices for various institutions, and received the IMRSA/Santam award for Best Government Risk Management Initiative shortly after establishing the Ethics Office of the Independent Policy Investigative Directorate (IPID) in 2007.

Other contributor
Nicholas Harris (ICFP)
Nic is a qualified CA. He joined KPMG in 2005 and, after completing his articles, became Manager: Fraud Risk Management. He gained valuable experienced in the fraud risk management field, and joined MTN Group Business Risk Management in July 2010. In July 2011, Nic was promoted to Head of Group Forensics at MTN Management Services. He is responsible for establishing and maintaining the MTN Fraud Risk Management Strategy across all 22 countries in which MTN operates. He conducts extensive high-priority forensic investigations across Africa and the Middle East.
Best practice governance guidelines suggest that an organisation's governing body should ensure that ethics risks and opportunities are incorporated in the (enterprise) risk management process. However, to date most organisations have applied risk management and ethics risk management separately and as only somewhat complementary interventions. Since ethics risk is a dimension of risk that is on an equal footing with any other type of risk, it cannot be divorced from organisational risk. In fact, risk management and ethics risk management may be viewed as converging interventions that can be designed and implemented in an integrated manner. Although ethics risk ownership may eventually be proportionally allocated to the organisation's risk function and ethics risk function respectively, ethics risks need to be integrated, in the form of an ethics risk register, into the organisation's risk register.

The purpose of The Ethics Risk Handbook, the third in The Ethics Institute's Ethics Handbook Series, is to create a framework and guidelines for understanding ethics risk management in organisations. The purpose of the handbook is not to serve as a substitute for guidelines on risk and/or ethics risk management. The guidelines contained herein could, however, inform organisations' guidelines.

The Ethics Risk Handbook is primarily aimed at those functions in the organisation that bear responsibility for ethics risk management and the practitioners who are involved in these functions. The ethics governance and management structures that would benefit from this handbook could be governing bodies of organisations (e.g., boards of directors), social and ethics committees, operational ethics committees, ethics task teams, and ethics offices.