NATIONAL TREASURY

DRAFT REVISED

ENTERPRISE RISK MANAGEMENT FRAMEWORK

23 July 2017
Contents

Introduction to the Framework ........................................................................................................... 9

Chapter 1: Risk management principles .......................................................................................... 11

Chapter 2: What is risk management? .............................................................................................. 13

1. Introduction ................................................................................................................................. 13

2. Best practices ............................................................................................................................... 13

3. Overview ..................................................................................................................................... 15

4. Glossary of terms ......................................................................................................................... 15

5. Purpose ....................................................................................................................................... 19

6. Applicability ............................................................................................................................... 20

7. Background .................................................................................................................................. 20

8. Why municipalities need risk management ............................................................................... 21

9. Five lines of assurance ................................................................................................................ 24

   Diagram 1: Layers of the five lines of assurance ........................................................................ 24

10. Combined assurance .................................................................................................................. 30

   Diagram 2: Combined assurance ................................................................................................. 30

11. Responsibilities of the role players ............................................................................................ 31

   Table 1: Responsibilities of the RM role players ......................................................................... 38

Chapter 3: Risk Maturity Matrix ................................................................................................... 39

12. Capacity in the risk management function .................................................................................. 39

   Template 1: Assessment for skills, capacity and budget .............................................................. 40

13. Maturity matrix to assess maturity of a municipality ................................................................. 40

   Diagram 3: Components of the maturity assessment .................................................................. 40
Table 2: The five lines of assurance in the maturity assessment

14. Maturity index (rating scale)

Table 3: Rating scale for maturity index

Diagram 4: Maturity status

Diagram 5: Calculation of maturity

Table 4: Table for the maturity assessment – risk governance

Table 5: Table for the maturity assessment – risk systems

Table 6: Table for the maturity assessment – risk processes

Chapter 4: Risk Assurance

15. Introduction

16. Applicability

17. Benefits of combined assurance

18. Audit Committee responsibilities in terms of combined assurance

19. Requirements to qualify as an assurance provider

20. Risk universe

Diagram 6: Example of a public sector risk universe

21. Combined assurance template

Template 2: Combined assurance

22. Guidelines for implementing an effective combined assurance model

23. Drafting an assurance plan

Example 1: Combined Assurance Plan

Chapter 5: Control environment and tone at the top

24. Introduction

25. Applicability
Chapter 6: Aligning risk management to strategic planning processes..............91

31. Introduction........................................................................................................91

32. Defining risk management strategy..................................................................91

33. Alignment between risk management and municipal objectives.....................91

34. Tools and mechanisms....................................................................................92

35. Strategic risk assessment (SRA) ......................................................................94

Table 14: Strategic risk register layout.................................................................96

Example 2: Linking strategic objectives with strategic risks...............................97

Chapter 7: Risk management strategy..................................................................100

36. Introduction.......................................................................................................100

37. Developing a risk management strategy..........................................................100
54. The risk identification process ................................................................. 128
55. Risk workshops and interviews .............................................................. 128
56. Focus points of risk identification ........................................................... 129
57. How to perform risk identification .......................................................... 130
58. Understand what to consider when identifying risks ................................. 130
59. Gather information from different sources to identify risks ....................... 131
60. Apply risk identification tools and techniques .......................................... 131
61. Document the risks identified ................................................................. 132
62. Document your risk identification process .............................................. 132
63. The outputs of risk identification ............................................................ 133
64. Risk Analysis ....................................................................................... 134
65. Risk Analysis Methods ......................................................................... 134
66. Risk analysis techniques ....................................................................... 135
67. Risk assessment .................................................................................... 136

Table 16: Inherent risk ratings ................................................................. 138

Table 17: Likelihood ratings ..................................................................... 138

68. Determine the inherent risk rating ......................................................... 139

Table 18: Heatmap – risk rating ............................................................. 140

69. Identify and evaluate existing control effectiveness ............................... 140

Table 19: Effectiveness ratings ................................................................. 141

70. Reference to the maturity index ............................................................. 141

Table 20: Risk assessment per risk maturity index .................................... 142

71. Assessing of risk – fragmented risk maturity ........................................ 142
Table 21: Operational risk register – fragmented status............................................. 143
72. Assessing of likelihood and consequence – integrated risk management .......... 144

Table 22: Operational risk register – integrated status.......................................... 145
73. Assessing of likelihood and consequence – risk intelligent management ........ 145

Table 23: Operational risk register – risk intelligent status .................................. 146
74. Document risk assessment process ................................................................. 147
75. Risk assessment considerations .................................................................... 147
76. Outputs ........................................................................................................ 148
77. Risk evaluation .............................................................................................. 148

Table 24: Risk index ........................................................................................... 148
78. Treat the risk - risk response ......................................................................... 149
79. Developing a risk response strategy .............................................................. 150
80. How to respond to risks? ............................................................................. 150

Template 3: Treatment of risk ........................................................................... 152
81. Opportunities versus threats ........................................................................ 153

Diagram 10: A Sample Value Map .................................................................... 154

Chapter 11: Risk Appetite and Risk Tolerance .................................................. 155
82. Introduction .................................................................................................. 155
83. Approach ...................................................................................................... 156
84. Calculating risk appetite .............................................................................. 159

Table 25: Risk tolerance .................................................................................... 160
85. Risk tolerance statements ............................................................................ 160
86. Graphical depiction of risk appetite ............................................................ 161

Diagram 11: Graphical depiction of risk appetite and risk tolerance .......... 161
Table 26: Risk rating parameters ................................................................. 162
87. Communication of risk appetite ............................................................ 162
88. Risk targets ......................................................................................... 163

Chapter 12: Communication and Reporting .............................................. 164
89. Introduction ......................................................................................... 164
90. Implementing an efficient and effective risk management reporting system ........................................................................... 164
91. Information systems for risk reporting .................................................. 165

Table 27: Considerations for implementing effective risk reporting Risk index .... 167
92. Types of risk management reports ....................................................... 167

Table 28: Types of reports to be generated .............................................. 173
93. Risk report formats ............................................................................. 174

Report 1: Inherent vs residual rating ....................................................... 174
Report 2: Risk matrix ............................................................................... 174
Report 3: Individual risk summary .......................................................... 175
Report 4: Pie charts ................................................................................. 176
Example 5: Risk Profile Report ................................................................. 179
94. Incident reporting system ................................................................. 190

Table 29: Incident report .......................................................................... 191
95. Emerging risk warning system ........................................................... 191

Table 30: Emerging risks ......................................................................... 192
96. Principles for effective risk data aggregation and risk reporting .......... 192

Chapter 13: Disaster recovery and business continuity ............................... 197
97. Business Continuity ........................................................................... 197

Table 31: Disaster recovery assessment ................................................ 198
Table 32: Back-up and recovery assessment .......................................... 199
Introduction to the Framework

This Revised National Treasury Draft Risk Management Framework is based on the most widely adopted international standards and guidelines for Enterprise Risk Management, the most recent King codes on Corporate Governance, the prescripts of the Municipal Financial Management Act (MFMA), as well as the combined knowledge of a number of experts in risk management, having decades of experience in both the private and public sectors, and more specifically local government.

It has been written comprehensively for application at the most mature and risk intelligent municipality, thus setting a benchmark for all municipalities across South Africa to strive for.

However, municipalities across South Africa differ greatly in terms of their size, their provincial and regional contexts, their threat and exposure profiles, as well as their Financial Management Capability Maturity, and capacity, skill levels and budget for implementing sound risk management.

This framework forms part of a revised toolkit, the design of which has taken into consideration that not all municipalities are ready to implement all the principles and practices discussed in this framework. It caters for three distinct levels of risk management maturity, namely fragmented, integrated and risk intelligent. Before using the toolkit, a municipality needs to determine its current level of risk management maturity using the maturity assessment matrix in this framework.

Reference to the different levels of municipal maturity is provided throughout this framework, indicating, where relevant, the applicability of the various sections, principles, practices and templates to the relevant maturity level.

There are some significant changes made to the original framework and toolkit, with a wide range of examples and templates added to simplify the applicability and ease of use of the toolkit. Although many more leading practice and sophisticated principles and practices have been introduced in this revised version, such as the concepts of 5 Lines of Assurance (5LOA), and Combined Assurance, these should facilitate rather than complicate the process of becoming an integrated or risk intelligent municipality.

It is important, however, that each municipality, irrespective of its level of maturity, can minimally apply a basic set of risk management principles and practices, to enable the identification, assessment, treatment and reporting of key risks affecting the achievement of municipal objectives. Also to enable the collecting and aggregation of risk and risk management performance information across all municipalities in South Africa.

This framework comprises 13 Chapters, including examples of tables, templates, and reports that can be adopted and adapted for application by a municipality. It forms part of a toolkit which also includes a supporting on-line website to enable ease of use of the toolkit.
The website version of the model allows for a rating mechanism, where a municipality can determine their maturity status. The following links allows the user to access one of two supporting websites that applies to their risk maturity status.

Basic/fragmented risk management maturity status:

http://munirate.wixsite.com/ntrmf-fragmented

Compliant/Integrated risk management maturity status:

http://munirate.wixsite.com/ntrmf-integrated
Chapter 1: Risk management principles

A set of guiding principles is indispensable for risk management to be effective in a municipality. According to the ISO 31000 Standards for Risk Management, these would include:

a. **Risk management creates and protects value**

Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, at all levels in the municipality, and across all functions and processes, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

b. **Risk management is an integral part of all municipal processes**

Risk management is not a stand-alone activity that is separate from the main activities and processes of the municipality. Risk management is part of the responsibilities of, not only management, but of all municipal personnel and an integral part of all municipal processes, including strategic planning and all project and change management processes.

c. **Risk management is part of decision making**

Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action, especially where there is a level of uncertainty associated with the achievement of objectives, and projected outcomes, and the risk reward ratios vary for the different decision options.

d. **Risk management explicitly addresses uncertainty**

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can best addressed, to either optimise value creation or minimise value destruction.

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

A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

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

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should consider the level of reliability and accuracy due to the methods of data gathering used, or difference of opinion between experts.

g. **Risk management is tailored**

Risk management is aligned with the municipality’s external and internal context and risk profile.
h. **Risk management takes human and cultural factors into account**

Risk management recognises the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the municipality's objectives.

i. **Risk management is transparent and inclusive**

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the municipality, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

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

Due to the dynamic character of risk, risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some risk change and others disappear.

k. **Risk management facilitates continual improvement of the organization**

Municipalities should develop and implement strategies to improve their risk management maturity alongside all other growth and performance activities of their municipality.
Chapter 2: What is risk management?

1. Introduction

The term 'risk management' is currently being utilised very liberally within municipalities. Safety, security, disaster management, business continuity, insurance, internal audit and even compliance are often referred to as 'risk management'. It is certainly true that these functions form part of the wider subject of risk management. The term 'risk management' however means a deliberate focus on, and on-going management of both risks and opportunities of a municipality.

The term 'enterprise risk management' (ERM) has become a popular way of describing application of risk management throughout a municipality rather than only in selected business processes or disciplines.

Risk management is a management discipline with its own set of techniques and principles. It is a recognised management science and has been formalised by international and national codes of practice, standards, regulations and legislation.

Risk management forms part of management's core responsibilities and is an integral part of the internal processes of a municipality. Worldwide managers are simplifying the processes and practices of to optimise the cost-benefit thereof, with a greater shift away from compliance for the sake of compliance, to a greater focus on the pursuit of value creation opportunities, the achievement of objectives, and the mitigation of potential value destruction.

2. Best practices

Risk management is a systematic process to identify, evaluate and address risks pro-actively and continuously before such risks can impact negatively on the municipality's service delivery.

When properly executed, risk management provides reasonable, although not absolute assurance, that the municipality will be successful in achieving its goals and objectives.

The ISO 31000\(^1\) standards and COSO\(^2\) risk management frameworks are recognised as providing the best available practice guidance on risk management - this framework is based on many of the principles contained in these frameworks.


Locally the South African King codes on corporate governance\(^3\) has been breaking ground in this space, and is observed as one of the leading governance codes competing favourably with other international codes, also regarding its reference to risk management and how it should be dealt with within municipalities.

King III principles address the responsibility of risk, mostly as these pertain to the municipal councils and its subcommittees. Councils should:

a. Be responsible for the governance of risk;
b. Determine the levels of risk tolerance/appetite;
c. Establish a risk committee or audit committee to assist the council in carrying out its risk responsibilities; and
d. Delegate to management the responsibility to design, implement and monitor the risk management plan.

King III principles also address the management of risk, whereby the Municipal Council should ensure that:

a. Risk assessments are performed on a continual basis;
b. Frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks; and
c. Management considers and implements appropriate risk responses.

King III principles address the monitoring, assurance and disclosure of risk, whereby the Municipal Council should:

a. Ensure continuous risk monitoring by management;
b. Receive assurance regarding the effectiveness of risk management processes; and
c. Ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders.

In addition King IV recommends that the council should appreciate that the core purpose of the municipality, its risks and opportunities, strategy, business model, performance and sustainable development are all inseparable elements of the value creation process. Council should:

a. Assume responsibility for municipal performance by steering and setting the direction for the realisation of the core purpose and values through its strategy;
b. Delegate the formulation and development of short, medium and long term strategy to management;
c. Approve the strategy by considering:
   i. The timelines and parameters of the short, medium and long term;
   ii. The risks and opportunities relating to the municipal environment; and
   iii. The various forms of capital supporting the strategy.

---

\(^3\)The King Code of Corporate Governance, chapter 6, Institute of Directors of Southern Africa, 2009.
d. Oversee whether the municipality frequently and continuously assess the negative consequences of its activities and outputs; and

e. Be alert to the general viability of the municipality with regard to its capital resources, its solvency and liquidity and its status as a going concern.

3. Overview

Many managers have justifiably asked why 'risk' needs a separate focus, and why it cannot be managed as before. The main reason is that the service delivery environment and the public sector's interface with stakeholders have become far more demanding and volatile than before. Historical ways of doing things are no longer effective as evidenced by a number of service delivery and general governance failures. In response to this, the principles of corporate governance and associated legislation require public sector municipalities to be more transparent and structured about the ways in which they manage and report on risk.

Risk management addresses strategic risks that will prevent the achievement of the objectives of the municipality.

The ISO 31000 standards broadly define ‘risk’ as the effect of uncertainty on objectives.

There should not be a bias towards any particular risk control function. Risk management must address all parts of the municipality and no part of the municipality is excluded from its processes. Risk management eventually works its way through the entire municipality so that all levels of management participate in its processes.

Existing risk-related functions such as security risk management, insurance, health and safety risk management etcetera must also align their activities with the municipality’s risk management plan. This alignment of activities then allows for risk management to reconfigure as ERM. This broad approach has been designed in terms of the five lines of assurance model under heading 9 in this chapter (see Diagram1: Layers of the five lines of assurance).

Stakeholders need to observe that the municipality has a proactive and systematic approach to managing municipality risks.

Risk management is recognised by the public sector as an appropriate way of managing risk. Different municipalities may have different existing responses to risk, ranging from safety management and insurance to internal control and public relations. It is important that different types of risk receive appropriate attention at an operational or process level. For the municipality as a whole, however, stakeholders want to see a single coherent strategy for managing the municipality's wide range of strategic and operational risks.

4. Glossary of terms

<table>
<thead>
<tr>
<th>Accounting Officer</th>
<th>The Municipal Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGSA</td>
<td>The Auditor General of South Africa</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Audit Committee</td>
<td>An independent committee constituted to review the effectiveness of control, governance and risk management within the municipality, established in terms of section 166 of the MFMA.</td>
</tr>
<tr>
<td>Chief Audit Executive</td>
<td>A senior official within the municipality responsible for internal audit activities (where internal audit activities are sourced from external service providers, the Chief Audit Executive is the person responsible for overseeing the service contract and the overall quality of the services provided).</td>
</tr>
<tr>
<td>Chief Risk Officer</td>
<td>A senior official who is the head of the risk management unit.</td>
</tr>
<tr>
<td>Cobit</td>
<td>Framework for the Control Objectives for Information Technology – leading framework for governance and managing the IT environment.</td>
</tr>
<tr>
<td>Combined assurance</td>
<td>Integrating and optimising all assurance services and functions, so that taken as a whole, these enable an effective control environment, support the integrity of the information used for decision-making by management, the municipal council and it’s committees to maximise risk and governance oversight and control efficiencies, and optimise overall assurance to the audit and risk committee, within the municipality's risk appetite.</td>
</tr>
<tr>
<td>CAP</td>
<td>Combined Assurance Plan</td>
</tr>
<tr>
<td>Compliance risks</td>
<td>Compliance risks include the risk that laws, regulations, policies, procedures and contractual obligations will be breached. This would typically include risks associated with legal and regulatory obligations.</td>
</tr>
<tr>
<td>ERM</td>
<td>Enterprise Risk Management.</td>
</tr>
<tr>
<td>Executive Authority</td>
<td>The Municipal Council.</td>
</tr>
<tr>
<td>External risks</td>
<td>External risks are related to requirements or forces imposed on a municipality from outside. The municipality cannot control the likelihood they will occur; it can only prepare for and respond to them. It includes legal/regulatory, natural hazard, economic, technological, social and demographic risks.</td>
</tr>
<tr>
<td>Financial risks</td>
<td>Financial risks include the risk of loss of revenue and / or earnings as a result of price volatility, the inability to secure funding capital, increase in bad debts, etc. This would typically include risks associated with the market, credit; liquidity, solvency and capital availability.</td>
</tr>
<tr>
<td>Framework</td>
<td>The Local Government Risk Management Framework.</td>
</tr>
<tr>
<td>Governance</td>
<td>The act of directing, controlling and evaluating the culture, policies, processes, laws, and mechanisms that define the structure by which municipalities are directed and managed.</td>
</tr>
<tr>
<td>IIA</td>
<td>The Institute of Internal Auditors</td>
</tr>
<tr>
<td>Inherent Risk</td>
<td>The exposure arising from risk factors in the absence of...</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>deliberate management intervention(s) to exercise control over such factors.</td>
<td></td>
</tr>
<tr>
<td>Integrated assurance</td>
<td>An integrated coordinated approach by two or more assurance providers, for the purpose of providing the most effective and complete independent assessment on risk management, control, and governance processes for their municipality.</td>
</tr>
<tr>
<td>IDP</td>
<td>The Integrated Development Plan (IDP) of the municipality is an elaborate and collaborative planning process which produces a strategic plan designed to guide municipality to systematically eradicate backlogs of service delivery, encourage socio economic development, address spatial disparities of development, and deliver on agreed priorities with clearly defined outputs and targets within an agreed timeframe.</td>
</tr>
<tr>
<td>Integrated risk management</td>
<td>A continuous, pro-active and systematic process to understand, manage and communicate risk from a municipal-wide perspective in a cohesive and consistent manner. It requires an ongoing assessment at every level and in every sector of the municipality, aggregating these results at the executive level, communicating them and ensuring adequate monitoring and review.</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>An independent, objective assurance and advisory activity designed to add value and improve a municipality's operations. It helps a municipality accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.</td>
</tr>
<tr>
<td>Municipality(s)</td>
<td>A local municipality is governed by a municipal council elected by voters resident in the area. There are three different systems by which the executive government of the municipality may be structured. In the plenary system, executive powers are vested in the full council, and the mayor is chairperson of the council. The Constitution defines the areas and topics for which municipal governments are responsible. National legislation divides this responsibility between the district municipalities and the local municipalities.</td>
</tr>
<tr>
<td>Municipal Council</td>
<td>Council of a municipality as referred to in Section 18 of the Municipal Structures Act, as defined in Section 1 of the MFMA.</td>
</tr>
<tr>
<td>Management</td>
<td>All officials of the municipality except for the Chief Risk Officer and officials reporting to him/her.</td>
</tr>
<tr>
<td>MFMA</td>
<td>Municipal Finance Management Act (Act No. 56 of 2003), as amended.</td>
</tr>
<tr>
<td>Operational risks</td>
<td><strong>Operational risks</strong> could include the risk of loss resulting from inadequate or failed internal processes, people and systems,</td>
</tr>
</tbody>
</table>
or from external events. This would typically include risks associated with business continuity; fraud; people; processes and systems.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residual Risk</td>
<td>The remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (the remaining risk after management has put in place measures to control the inherent risk). However risk can also be reduced by transferring (outsourcing, sharing) of the management of that risk. This is extremely important in the public sector environment where outsourcing is a viable alternative to poor service delivery.</td>
</tr>
<tr>
<td>Risk</td>
<td>Risk is about the uncertainty of events, including the likelihood of such events occurring and its effects, both positive and negative, on the achievement of the municipality’s objectives. Risks include uncertain events with a potential positive effect on the municipality (i.e. value creation opportunity) not being captured or not materialising.</td>
</tr>
<tr>
<td>Risk Appetite</td>
<td>Risk appetite can be defined as the amount and type of risk that a municipality is willing to take in order to meet their strategic objectives. Municipalities will have different risk appetites depending on their maturity, location, culture and objectives. A range of appetites exist for different risks and these may change over time.</td>
</tr>
<tr>
<td>Risk Champion</td>
<td>A person who by virtue of his/her expertise or authority champions a particular aspect of the risk management process, but who is not the risk owner.</td>
</tr>
<tr>
<td>Risk Factor</td>
<td>Any threat or event which creates, or has the potential to create risk.</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Systematic and formalised processes to identify, assess, manage and monitor risks.</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Committee appointed by the Municipal Manager to govern (guide, monitor and review) the municipality’s system of risk management.</td>
</tr>
<tr>
<td>Risk Management Unit</td>
<td>A business unit responsible for coordinating and supporting the overall municipal risk management process, but which does not assume the responsibilities of management for identifying, assessing and managing risk.</td>
</tr>
<tr>
<td>Risk Owner</td>
<td>The person accountable for managing a particular risk.</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Philosophy</td>
</tr>
<tr>
<td></td>
<td>Set of shared beliefs and attitudes that characterises how the entity considers risk in everything it does, from strategy development and implementation to its day-to-day activities. It reflects the entity’s values, influencing its culture and operating style, and affects how enterprise risk management components are applied, including how risks are identified, the kind of risks accepted, and how they are managed.</td>
</tr>
<tr>
<td>Risk Policy</td>
<td>The statement of the overall intentions and direction of a</td>
</tr>
</tbody>
</table>
municipality related to risk management.

<table>
<thead>
<tr>
<th>Risk Tolerance</th>
<th>The amount of risk the municipality is capable of bearing (as opposed to the amount of risk it is willing to take)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic risk</td>
<td><strong>Strategic risks</strong> are those internal and external events and scenarios that can inhibit a municipality’s ability to achieve its strategic objectives. This would typically include risks associated with governance, the business model and the industry/ economic environment.</td>
</tr>
<tr>
<td>Technology</td>
<td>Comprises the infrastructure, devices, systems and software that is used to record, analyse, report and maintain risk management information, to enable risk management decision-making.</td>
</tr>
</tbody>
</table>

5. **Purpose**

a. The Framework has been developed in terms of the following prescripts:

- Sections 62(1)(c)(i) and 95(c)(i) of the MFMA, which require the Accounting Officers to ensure that their municipalities and municipal entities have and maintain effective, efficient and transparent systems of risk management; and
- Section 20(1)(b)(iv) of the MFMA, which empowers the Minister of Finance to prescribe uniform norms and standards in terms of this Act.

b. The Framework also incorporates the requirements of the Batho-Pele principles and King III and King IV insofar as they concern risk management. King IV has specific guidance for municipalities, included in Part 6.2 – Supplement for municipalities. These include that Municipal Councils should:

- Lead ethically and effectively;
- Ensure that the municipality is seen as a responsible corporate citizen;
- Ensure that the municipality’s core purpose, its risks and responsibilities, strategy, business model, performance and sustainable development is all inseparable elements of the value creation process;
- Serve as the custodian of corporate governance of the municipality;
- Govern in such a way that support the municipality in setting and managing the achievement of their objectives; and
- Ensure that assurance services enable an effective control environment and that these support the integrity of information for decision-making purposes.

---

\(^4\) No. 56 of 2003: Local Government: Municipal Finance Management Act,
c. The framework aims to support municipalities to improve and sustain their performance by enhancing their systems of risk management to protect against adverse outcomes and optimise opportunities.

6. **Applicability**
   
a. The Framework recognises that municipalities are not homogenous hence it is not possible to produce a blueprint that can be generically replicated across all municipalities. To this extent the maturity of a municipality in terms of their risk assessment will guide their application of this framework.

b. The Framework is thus “principles” rather than “prescripts” based and adopts the approach of elucidating the principles, standards, models and practices proven to support and sustain effective risk management. However, if a municipality has a low maturity rating, the framework allows for appropriate templates and examples to assist a municipality to be compliant with the legislative requirements.

c. Municipalities are expected to develop their systems of risk management by adopting the said principles and standards, and adapting the models and operational practices to match their specific municipal requirements.

7. **Background**
   
a. Municipalities are bound by their Constitutional mandate to provide services or products in the interest of the public good. No municipality has the luxury of functioning in a risk-free environment and municipalities are especially vulnerable to risks associated with fulfilling their mandates.

b. The public sector environment is fraught with unique challenges such as inadequate capacity, excessive bureaucracy and silo mentality, limited resources, competing priorities and infrastructure backlogs to mention a few. Such dynamics increase the risk profile of the public sector as a whole and place an extra duty of care on public sector managers to contain risks within acceptable limits.

c. Risk management is a valuable management tool which increases a municipality’s prospects of success through minimising negative outcomes and optimising opportunities. Local and international trends confirm that risk management is a strategic imperative rather than an option within high performing municipalities.

c. High performing municipalities set clear and realistic objectives, develop appropriate strategies aligned to the objectives, understand the intrinsic risks associated therewith and direct resources towards managing such risks on the basis of cost-benefit principles.
d. Municipalities must, in accordance with the previously mentioned prescripts under 5(a), implement and maintain effective, efficient and transparent systems of risk management and internal control.

e. The underlying intention of (d) above is that municipalities should through the risk management process achieve, among other things, the following outcomes needed to underpin and enhance performance:

- More sustainable and reliable delivery of services;
- Informed decisions underpinned by appropriate rigour and analysis;
- Innovation;
- Reduced waste;
- Prevention of fraud and corruption, unauthorised, fruitless and irregular expenditure;
- Better value for money through more efficient and effective use of resources; and
- Better outputs and outcomes through improved project and program management.

d. Risk management enables a municipality to:

- Increase the likelihood of achieving service delivery objectives;
- Encourage proactive management;
- Be continuously aware of the need to identify and treat risk throughout the municipality;
- Improve the identification of both opportunities and threats;
- Comply with relevant legislative and regulatory requirements;
- Improve mandatory and voluntary reporting to all stakeholders;
- Improve stakeholder confidence and trust;
- Improve governance on municipal council, municipal manager and senior management level by:
  a. Establishing a reliable basis for strategic and operational decision making and planning;
  b. Efficiently allocating and using resources for risk treatment;
  c. Improving operational effectiveness and efficiency;

- Enhance health and safety performance, as well as environmental protection;
- Improve controls and loss prevention and incident management; and
- Improve municipal learning.

8. Why municipalities need risk management

Risk management provides a dedicated focus on risk for the following reasons:

8.1 Corporate governance
Legislation such as the MFMA\(^5\) together with corporate governance codes such as King III and IV expect a municipality to implement a risk management plan. As a result of municipality failures in the past, stakeholders do not want to be caught unawares by risk events. They expect that internal control and other risk mitigation mechanisms to be based on a thorough assessment of municipality wide risks.

Stakeholders require assurance that management has taken the necessary steps to protect their interests. Councillors, Municipal Managers and stakeholders now want to know more about the risks facing a municipality. This is understandable in an environment of complex and challenging service delivery expectations.

### 8.2 Planning and organisation

The value of risk management is best leveraged when its principles and techniques are applied during municipal planning processes and organisation. Given the increased levels of volatility and uncertainty, it is vital that plans, particularly multiple year plans, take into consideration a thorough assessment of risks and mitigation strategies.

For this purpose, existing tools and methodologies such as SWOT analysis, PESTLE analysis and Porters Model, amongst others, can be utilised to supplement the municipality’s risk management model, to better understand risk drivers in the internal and external contexts of the municipality. Hence, it becomes clear that planning and risk management are inter-dependent.

### 8.3 Continuous risk assessment

The risk profile of a municipality is changing on an on-going basis. Some risks are created by changes initiated by the municipality. An example would be where a new CFO has been appointed or where the supplier master-file has been centralised. Other risks are the result of changes in society, business, legislation or communities. An example is where the credit rating of the country deteriorates, which has a significant impact on the interest rates, and eventually on the cost of servicing debt. A once a year risk assessment will not elevate this to the decision-making level.

Even the best management teams will struggle to keep an accurate perspective of changing risks when risk management is approached on an informal basis.

The risk management plan must provide the municipality with the ability to systematically identify new and emerging risks, and the assurance that existing risks are being addressed in the best possible way given current resource constraints and other challenges.

Change is often beyond the control of management, however, the risks it creates need to be managed as effectively as possible.

### 8.4 Evolution of risk management

\(^5\)Municipal Finance Management Act (MFMA) No 56 of 2003
Risk management has evolved over recent years. We have seen the integration of risk management techniques with fraud prevention, internal control and corporate governance. There has also been an integration of operational risk management functions into the broader umbrella of risk management. Aspects such as internal control, safety management, sustainability and environmental management, for example, have increased in importance in recent times. The broadening of risk management has seen a change in emphasis from risks as individual hazards to risks as uncertainties around key objectives.

Risk management has also seen the introduction of new participants into the process. The function is no longer confined to insurance, internal auditors, and loss prevention functions. The wider approach to risk management has brought the function into the view of human resources officers, compliance officers, financial managers, ICT specialists and other functional managers.

**8.5 Risk-based internal audit plans**

Internal audit plans are now based on the outcomes of risk assessments. Internal auditors are increasingly basing their priorities on the risk management plan and give priority to high-risk assets and processes.

Internal audit is well-placed to independently evaluate the adequacy and effectiveness of key controls. The frameworks of internal control used by auditors are useful contributions to the risk management plan.

Internal audit is a key role player in providing assurance with regards to the effectiveness of risk management.

**8.6 Cultural adjustment**

The essential behaviours of officials charged with responsibility for various activities of risk management must change. This requires a shift in the cultural dynamics insofar as it concerns risk management, which can be achieved through awareness and advocacy, communication, coaching, training and linking risk management to performance measures. Risk management must be a catalyst for change in behaviour of managers. Managers need to develop competencies to ensure that they make conscious risk-based decisions. Rather than viewing risk management and its associated activities as mere bureaucracy, managers need to look at it as a powerful driver of service delivery excellence.

There is a danger that risks that fall outside traditional functions may go unmanaged and have serious consequences on municipal objectives. The need for broad-based risk management is thus critical as it will also ensure that risks that were not previously given adequate attention are now properly managed. Risk management processes that are integrated within the municipality's existing structures are likely to be more effective in producing the desired service delivery and other objectives.
9. Five lines of assurance

Every municipality has objectives it strives to achieve. In pursuit of these objectives, the municipality will encounter events and circumstances which may threaten the achievement of these objectives. These potential events and circumstances create risks a municipality must identify, analyse, assess, and treat. Some risks may be accepted (in whole or in part) and some may be fully or partially mitigated to a point where they are at a level acceptable to the municipality.

The Five lines of Assurance (5 LOA)⁶, as illustrated below, addresses how specific duties related to risk and control could be assigned and coordinated within a municipality, regardless of its size or complexity. Councillors and management should understand the critical differences in roles and responsibilities of these duties and how they should be optimally assigned for the municipality to have an increased likelihood of achieving its objectives. In particular, 5 LOA clarifies the difference and relationship between municipalities’ assurance and other monitoring activities - activities which can be misunderstood if not clearly defined.

Diagram 1: Layers of the five lines of assurance

5 LOA enhances the understanding of risk management and control by clarifying roles and duties. Its underlying premise is that, under the oversight and direction of council and the municipal manager, three separate groups (or lines of assurance) within the municipality are necessary for effective management of risk and control. The responsibilities of each of the groups (or ‘lines’) are:

a. The Municipal Council who should steer and set strategic direction, approve policy and planning, oversee, monitor and ensure accountability;
b. The Municipal Manager who executes the strategic direction, policies and oversight responsibilities;

⁶www.riskoversightsolutions.com
c. **Risk Owners** who manage risk and control (front line operating management);
d. **Risk Management** who monitors risk and control in support of management (risk, control, and compliance functions put in place by management); and
e. **Independent assurance provided by Internal and External Audit** to the Council through its Audit Committee and senior management concerning the effectiveness of the management of risk and control.

Each of the five lines plays a distinct role within the municipality’s wider governance framework. When each performs its assigned role effectively, it is more likely the municipality will be successful in achieving its overall objectives. Everyone in a municipality has some responsibility for internal control, but to help assure that essential duties regarding risk management are performed as intended, 5 LOA brings clarity to specific roles and responsibilities. When a municipality has properly structured its 5 LOA, and they operate effectively, there should be:

- No gaps in risk and control coverage;
- No unnecessary duplication of effort; and
- A higher probably of risks and controls being effectively managed.

The council will have increased opportunity to receive unbiased information about the municipality’s most significant risks and about how management is responding to those risks.

5 LOA provides a flexible structure that can be implemented in support of the Framework. Functions within each of the lines of assurance will vary from municipality to municipality, and some functions may be combined or split across the lines of assurance. For example, in some municipalities, parts of a compliance function in the second line may be involved in designing controls for the first line, while other parts of the second line focus primarily on monitoring these controls.

Regardless of how a particular municipality structures its five lines of assurance, there are a few critical principles implicit in 5 LOA:

**a. The first line of assurance** lies with the process and risk owners whose activities create and/or manage the risks that can facilitate or prevent a municipality’s objectives from being achieved. This includes taking the right risks. The first line owns the risk, as well as the design and execution of the municipality’s controls to respond to those risks.

The first line of assurance is primarily handled by front-line and mid-line managers who have day-to-day ownership and management of risk and control. Operational managers develop and implement the municipality’s control and risk management processes.

These include internal control processes designed to identify and assess significant risks,
execute activities as intended, highlight inadequate processes, address control breakdowns, and communicate to key stakeholders of the activity. Operational managers must be adequately skilled to perform these tasks within their area of operations. Senior management has overall responsibility for all first line activities. For certain high-risk areas, senior management may also provide direct oversight of front-line and mid-line management, even to the extent of performing some of the first line responsibilities themselves.

b. **The second line** is established to support management through particular expertise and process excellence, and management monitoring alongside the first line to help ensure that risks and controls are effectively managed.

These second line of assurance support functions are essentially advisory and oversight functions of their expertise applied to management processes, for example Risk Management ‘owns’ the Risk Management process methodology, and provides both guidance and oversight to management (Risk Owners).

The second line of assurance includes various risk management and compliance functions put in place by the Municipal Manager to help ensure controls and risk management processes implemented by the first line of assurance are designed appropriately and operating as intended. These are management functions, separate from first-line operating management, but still under the control and direction of senior management.

Functions in the second line are typically responsible for ongoing monitoring of risk and control. They often work closely with operating management to help define risk management implementation strategy, provide expertise in risk management, guide the implementation of policies and procedures, and collate information to create an enterprise-wide view of risk and control.

The composition of the second line can vary significantly depending on the municipality’s size. In metropolitan municipalities, these functions may be separate and distinct. In B1 and C graded municipalities, some of the second-line functions may be combined or non-existent. For example, some municipalities may combine the legal and compliance functions into a single department or may combine a health and safety department with an environmental function.

Some or all of the duties of the second line may also be retained by managers within the first line of assurance in smaller municipalities. Typical second-line functions include specialised groups such as risk management, information security, financial control, physical security, quality, health and safety, inspection, compliance, and legal and
environmental experts.

Under the oversight of senior management, second-line specialists monitor specific controls to determine whether the controls are functioning as intended. Monitoring activities performed by the second line typically cover all three categories of objectives, namely operational, reporting, and compliance.

The responsibilities of individuals within the second line of assurance vary widely but typically include:

- Assisting management in design and development of processes and controls to manage risks;
- Defining activities on how to monitor and measure success as compared to management expectations;
- Monitoring the adequacy and effectiveness of internal control activities;
- Escalating critical issues, emerging risks and outliers;
- Providing risk management frameworks;
- Identifying and monitoring known and emerging issues affecting the municipality’s risks and controls;
- Identifying shifts in the municipality’s implicit risk appetite and risk tolerance; and
- Providing guidance and training related to risk management and control processes.

c. **The third line** provides assurance to senior management and council (represented in this model by the Municipal Manager and the Municipal Council respectively) over both the first and second lines’ efforts consistent with the expectations of council and senior management. The third line of assurance is typically not permitted to perform management functions to protect its objectivity and municipal independence.

In addition, the third line has a primary reporting line to the council by reporting to the audit committee. As such, the third line is purely an assurance function and not a management function, which separates it from the second line of assurance. Internal auditors serve as a municipality’s third line of assurance.

The IIA defines internal auditing as “an independent, objective assurance and consulting activity designed to add value and improve a municipality’s operations. It helps a municipality accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.” Among other roles, internal audit provides assurance
regarding the efficiency and effectiveness of governance, risk management, and internal control.

The scope of internal audit work can encompass all aspects of a municipality's operations and activities. What distinguishes internal audit from the other two lines of assurance is its high level of independence and objectivity. Internal auditors do not design or implement controls as part of their normal responsibilities and are not responsible for the municipality's operations. In most municipalities, internal audit's independence is further strengthened by a direct reporting relationship between the chief audit executive (CAE) and the Council through the audit committee. Because of this high level of municipal independence, internal auditors are optimally positioned for providing reliable and objective assurance to the council and senior management regarding governance, risk, and control. Internal audit actively contributes to effective municipal governance providing certain conditions fostering its independence and professionalism are met.

Establishing a professional internal audit activity should therefore be a priority for all municipalities. This is important not just for larger municipalities but also for smaller entities. Smaller municipalities may face equally complex environments with a less formal, robust municipal structure to ensure the effectiveness of governance and risk management processes, and may lack an effective second line of assurance. Every municipality should establish and maintain an independent, adequate, and a competent internal audit function; reporting to a sufficiently high level in the municipality to be able to perform its duties independently; and operating in accordance with a suitable globally recognized set of standards (The IIA's International Standards for the Professional Practice of Internal Auditing).

d. In the fourth line of assurance senior management (represented in this model by the Municipal Manager) is accountable for the selection, development, and evaluation of the system of internal control with oversight by the council (Municipal Council). Senior management must fully support strong governance, risk management and control. In addition, they have ultimate responsibility for the activities of the first and second lines of assurance. Their engagement is critical for success of the overall model.

COSO clearly identifies the responsibilities of the senior management to design and implement processes that:

i. Demonstrate commitment to integrity and ethical values;
ii. Exercise oversight responsibility;
iii. Establish structure, authority and responsibility;
iv. Demonstrate commitment to competence; and
v. Enforce accountability.

e. **Fifth line of assurance** The Municipal Council and the Audit Committee fulfils the fifth line of assurance. Senior management and the council collectively have responsibility for establishing a municipality’s objectives, defining high-level strategies to achieve those objectives, and establishing governance structures to best manage risk. They are also the parties best positioned to ascertain the optimal municipal structure for roles and responsibilities related to risk and control.

King IV outlines the key principles that Municipal Councils should endorse, namely:

i. Councils should lead ethically and effectively;
ii. Councils should govern the ethics of a municipality in a way that supports an ethical culture;
iii. The Council should ensure that the municipality is and seen to be a responsible corporate citizen;
iv. The Council should appreciate that the municipality’s core purpose, its risks and opportunities, strategy, business model, performance and sustainable development are all inseparable elements of the value creation process;
v. The Council should ensure that reports issued by the municipality enable stakeholders to make informed assessments of the municipality’s performance and its short, medium and long term prospects;
vi. The Council should serve as a focal point of and custodian of good governance in the municipality;

vii. The Council should comprise an appropriate balance of knowledge, skills and experience, diversity and independence to discharge it governance role and responsibilities objectively and effectively;

viii. The Council should ensure that its arrangement for delegation within its own structures promote independent judgment, and assist with the balance of power and the effective discharge of its duties;
ix. The Council should ensure that the evaluation of its own performance and that of its committees. Its speaker and its individual councillors, support continued improvement in its performance and effectiveness;
x. The Council should ensure that the appointment of, and delegation to, management contribute to role clarity and the effective exercise of authority and responsibilities;

xi. The Council should govern risk in such a way to support the municipality in setting and achieving its strategic objectives;

xii. The Council should govern technology and information in a way that supports the municipality in setting and achieving its strategic objectives;
xiii. The Council should govern compliance with applicable laws and adopted non-binding rules, codes and standards in a way that supports the municipality being ethical and a good corporate citizen;

xiv. The Council should ensure that the municipality remunerates fairly, responsibly and transparently so as to promote the achievement of strategic objectives and positive outcomes in the short, medium and long term;

xv. The Council should ensure that assurance services and functions enable an effective control environment, and that these support the integrity of information for internal decision-making and of the municipality’s external reports; and

xvi. In execution of its governance role and responsibilities, the council should adopt a stakeholder inclusive approach that balances the needs, interests and expectation of material stakeholders in the best interest of the municipality over time.

The goal for any municipality is to achieve its objectives. Pursuit of these objectives involves embracing opportunities, pursuing growth, taking risks, and managing those risks – all to advance the municipality. Failure to take the appropriate risks, and failure to properly manage and control risks taken, can prevent a municipality from accomplishing its objectives. There is, and always will be, tension between activities to create value and activities to protect value. The COSO Framework provides a structure to consider risk and control to ensure they are appropriate and properly managed. 5 LOA provides guidance as to a municipal structure to be implemented, assigning roles and responsibilities to parties that will increase the success of effective management of risk and control.

10. Combined assurance

The first three lines of assurance each have the same ultimate objective: - to assist the municipality to achieve its objectives with effective management of risk. They serve the same ultimate stakeholders, and they often deal with the same risk and control issues. Senior management and council should clearly communicate the expectation that information be shared and activities coordinated among each of the three lines where this supports the overall effectiveness of the effort and does not diminish any of the line’s key functions.

While they have the same objective, each line has its own unique roles and responsibilities. They are separate lines but should not operate in silos. They should share information and coordinate efforts regarding governance, risk and control. In many situations there could be a shared perspective regarding risk and control. Careful coordination is essential to avoid unnecessary duplication of efforts while assuring that all significant risks are addressed appropriately.

The first line of assurance (risk owners) has primary ownership of risks and the risk
response strategies and treatment mechanisms used to manage those risks. The second line (risk management) provides expertise in risk, helps to determine the risk management implementation strategy, and assists in the implementation of related policies and procedures.

The second line should ensure that all risk owners (the first line) apply a common risk language and consistent set of risk management processes and tools, to enable the monitoring, review and reporting on risks and risk management performance across the municipality.

11. Responsibilities of the role players

The responsibilities of the different role players have been documented in the following table. The table also clearly indicates the 5 lines of assurance in the headings, and also the role players participating in the combined assurance model.
### Combined assurance

<table>
<thead>
<tr>
<th>1st line of assurance</th>
<th>2nd line of assurance</th>
<th>3rd line of assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>RM = Risk management, RMP = Risk management policy, RMF = Risk management framework</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MC = Municipal Council, MM = Municipal Manager, AC = Audit Committee, IA = Internal audit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Key business risk universe

<table>
<thead>
<tr>
<th>5th line of assurance</th>
<th>4th line of assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Municipal Council (MC)</td>
<td>Audit Committee (AC)</td>
</tr>
<tr>
<td>Municipal Manager (MM)</td>
<td>Risk committee (RC)</td>
</tr>
<tr>
<td>Senior management (SM)</td>
<td>Risk owners (RO)</td>
</tr>
<tr>
<td>Risk management (RM)</td>
<td>Internal audit (IA)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1st line of assurance</th>
<th>2nd line of assurance</th>
<th>3rd line of assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>RM = Risk management, RMP = Risk management policy, RMF = Risk management framework</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MC = Municipal Council, MM = Municipal Manager, AC = Audit Committee, IA = Internal audit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Strong definition - Risk appetite and tolerance

<table>
<thead>
<tr>
<th>1st line of assurance</th>
<th>2nd line of assurance</th>
<th>3rd line of assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve risk appetite and tolerance</td>
<td>Advise MC on approval of risk appetite</td>
<td>Understand, determine and set the risk appetite and tolerance</td>
</tr>
<tr>
<td>Evaluate relevance / appropriateness of risk appetite</td>
<td>Determine risk tolerance levels in line with risk appetite and tolerances</td>
<td>Provide guidance on determining risk appetite and tolerances</td>
</tr>
<tr>
<td>Facilitate and tolerance design with business unites</td>
<td>Advise MM</td>
<td>Independent assurance on risk appetite and tolerance levels assessment</td>
</tr>
<tr>
<td>Risk culture throughout municipality</td>
<td>Oversight on development of risk culture and the control environment</td>
<td>Establish effective control environment for effective RM</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Risk maturity model</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strong definition - Risk appetite and tolerance</td>
<td>Approve and do oversight on risk maturity status of municipality</td>
<td>Review the maturity assessment</td>
</tr>
<tr>
<td></td>
<td>Approve risk appetite and tolerance</td>
<td>Advise MC on approval of risk appetite</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strong methodology</td>
<td>Fraud prevention policy and plan (FPP)</td>
<td>Approve FPP</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Strong methodology</td>
<td>Risk management policy and framework (RMP and RMF)</td>
<td>Approve RMP</td>
</tr>
<tr>
<td>Risk management strategy (RMS)</td>
<td>Approve risk management strategy</td>
<td>Approve risk management strategy</td>
</tr>
<tr>
<td>Risk management implementation plan (RMIP)</td>
<td>Approve risk management implementation plan</td>
<td>Approve risk management implementation plan</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Capacity, skills and budget</td>
<td>Oversight on performance management process through risk reports</td>
<td>Provide sufficient capacity, skills and budget for effective RM</td>
</tr>
</tbody>
</table>

**Strong methodology continued**

<table>
<thead>
<tr>
<th>Assign risk management responsibilities to operational managers</th>
<th>Empower operational managers to execute their risk responsibilities</th>
<th>Operational management execute their risk management responsibilities</th>
<th>Provide guidance and training to RO on risk management responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold operational managers accountable for risk management failures</td>
<td>Hold staff accountable for risk management failures</td>
<td>Identification of risks</td>
<td>Identification of risks</td>
</tr>
</tbody>
</table>

**Robust GRC system**

<table>
<thead>
<tr>
<th>Risk identification</th>
<th>Risk assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide guidance to MC, MM and senior management on how to manage risk to an acceptable level, within the</td>
<td>Identification of risks</td>
</tr>
<tr>
<td>Assessment + risk response</td>
<td>Assessment + control / risk</td>
</tr>
</tbody>
</table>

**Assurance on risk management process**

<p>| Assurance on adequacy |</p>
<table>
<thead>
<tr>
<th>Risk Appetite and Tolerance Levels and Risk Management Maturity</th>
<th>Strategy Design</th>
<th>Treatment Design</th>
<th>Processes and Effectiveness of Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor and report on the effectiveness of risk management</td>
<td></td>
<td></td>
<td>Where necessary, facilitate the risk management workshops with RO on risk identification, assessment and treatment</td>
</tr>
</tbody>
</table>

**Issues Tracking**

<table>
<thead>
<tr>
<th>Monitoring</th>
<th>Oversight on assurance provided by AC</th>
<th>Review of combined assurance approach</th>
<th>Continuously evaluate the added value of IA and RM (combined assurance)</th>
<th>Assess the state of operational effectiveness of the RM process</th>
<th>Manage risks associated with operational activities and apply effective oversight on the effectiveness of those activities</th>
<th>Make risk registers available to RM</th>
<th>Custodian of combined assurance model (in absence of separately appointed Combined Assurance Champion)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nature of risks</td>
<td>Financial</td>
<td>Disclose in the annual</td>
<td>Measure and report to</td>
<td>Measure and report overall</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>------------------------</td>
<td>-----------------------</td>
<td>---------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting</td>
<td>Oversight on RM – review of reports</td>
<td>Report to MC and MM on effectiveness of combined assurance</td>
<td>Ensure appropriate action of recommendations by AC, IA and RM committee.</td>
<td>Provide regular reports to municipal manager on state of risk management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Provide information on risk exposures to the AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicate the results of combined assurance to the MC for their oversight</td>
<td>Recommend key performance indicators to MM regarding risk management</td>
<td>consolidated risk registers available to RM</td>
<td>Measure and report overall exposure to fraud and corruption</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Continuously monitor RM activities within areas of responsibilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Make consolidated risk registers available to IA on request</td>
<td>Continuousl monitor all RM activities across the municipality and provide remedial advice where necessary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Prepare a risk based audit plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Provide assurance on adequacy and effectiveness of the controls / risk treatment solutions mitigating risks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Report on the effectiveness of the risk management in own area of responsibility: 1. risk and control matrix (effectiveness of risk profile improvement) 2. implementatio n of RM processes 3. compliance with RM policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Consolida te all RM performance reports from Risk Owners</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Report on adequacy and effectiveness of the controls / risk treatment solutions mitigating risks (effectiveness of CSA and RM performance)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Ensure that all the risks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Provide assurance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td>report that risk assessment, management and intervention are effective</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic</td>
<td>and MM overall exposure to fraud and corruption, and instances where actual risk &gt; risk appetite</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory</td>
<td>municipal council overall exposure to fraud and corruption, and instances where actual risk &gt; risk appetite</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Municipal health and safety</td>
<td>Ensure implementation of recommendations made by the AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Technology</td>
<td>exposure to fraud and corruption, information technology design and operational effectiveness, and risk exposure beyond acceptable boundaries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance and ethics</td>
<td>Continuous management of risk profiles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Emerging</th>
<th>Disclose in the annual report that emerging risks identified, assessed and managed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Report in the annual report an opinion on effectiveness of governance, risk and control processes</td>
</tr>
<tr>
<td></td>
<td>Measure and report to municipal council overall exposure to new emerging risks</td>
</tr>
<tr>
<td></td>
<td>Measure and report to municipal council overall exposure to new emerging risks</td>
</tr>
</tbody>
</table>

| Continuous | Continuously scan both the internal and external municipal environment and measure and report to municipal manager incidents of exposure to new emerging risks |
|            | Measure and report to senior management incidents of exposure to new emerging risks related to the environment under their responsibility |
|            | Ensure that all the risks, including emerging risks, have been considered in the risk identification and assessment processes |
|            | Provide guidance on the identification and process of dealing with emerging risks |

| Senior Management | Ensure that all the risks, including emerging risks, have been considered in the risk identification and assessment processes |

| Exceeding | have been considered in the risk identification and assessment processes and are reported appropriately |

| on the adequacy and effectiveness of the controls mitigating risks |

| Table 1: Responsibilities of the RM role players |  |
Chapter 3: Risk Maturity Matrix

12. Capacity in the risk management function

Risk management needs time and resources to ensure its effective application. Many local municipalities do not have the budget and/or skills to implement risk management in its full context. To this extent municipalities are required to complete a risk management capacity assessment. The results will influence the extent to which risk assessment is implemented. To this extent municipalities should evaluate their capacity, skills and budget, and the following template could be used to inform the municipal manager’s decision-making process. It is strongly recommended that the first three lines of assurance (Risk Owners, Risk Management, and Internal Audit) complete the assessment to allow the municipal manager to make an informed decision during strategic and operational planning. It also forms the basis of combined assurance. This assessment should be completed irrespective of the maturity status of a municipality.

<table>
<thead>
<tr>
<th>Capacity, skills and budget – risk management</th>
<th>1 LOA</th>
<th>2 LOA</th>
<th>3 LOA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes/ no</td>
<td>Yes/ no</td>
<td>Yes/ no</td>
<td>Yes/ no</td>
</tr>
<tr>
<td>Capacity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1  The risk management structure is appropriate for the size and complexity of the functions within municipality.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2  Job descriptions and performance agreements define tasks required to accomplish particular jobs/fill the various positions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3  Specific lines of authority and responsibility are established to ensure compliance with legislation and regulations relating to risk management.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skills</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3  High-level analyses are performed on an annual basis of the knowledge, skills, and abilities needed to perform risk management responsibilities appropriately.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5  Demonstrated risk management ability in general management and extensive practical risk management experience in operating departments.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6  Council understands the importance of internal controls, including the division of responsibility/delegation of authority.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
7 Regular risk management employee evaluations are documented and shared with employees.

8 The municipality continuously provides mentoring and training opportunities needed to attract, develop, and retain sufficient and competent staff.

9 The municipality checks credentials, references, and past work experience of potential new employees. Background checks are conducted on candidates for employment.

10 Effective policies and procedures for hiring, orienting, training, evaluating, counselling, promoting, compensating, disciplining, and terminating risk management employees.

Budget

12 The risk management function has sufficient budget to perform their responsibilities.

Template 1: Assessment for skills, capacity and budget

13. Maturity matrix to assess maturity of a municipality

A maturity matrix should be simplistic and easy to apply. The following model serves the purpose of simplicity, and is widely used to assess risk management maturity⁷.

The maturity assessment forms the basis of this framework. The extent to which risk management will be implemented in a municipality is directly aligned with its culture, capacity and capability to do so, and therefore aligned with its risk management maturity.

Diagram 3: Components of the maturity assessment

In this model maturity of risk management can be evaluated on three levels, as depicted in the table below. The model differentiates between:
a. Risk oversight;
b. Risk systems; and
c. Risk processes.

The following table reflects some of the roles of the different lines of assurance, which is then used to assess the maturity of the municipality by applying a maturity index.

\[\text{\textsuperscript{7}Deloitte: Enterprise risk management – A risk intelligent approach. Deloitte Advisory August 2015.}\]
### Three levels of risk maturity assessment

| Risk governance  
(assessment A) | Risk infrastructure and management  
(assessment B) | Risk ownership  
(assessment C) |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Five lines of assurance</strong></td>
<td>Municipal Council and the Audit Committee</td>
<td></td>
</tr>
</tbody>
</table>
- Foster a risk intelligent culture;  
- Approve the risk appetite;  
- Ratify key components of the integrated risk management program; and  
- Routinely discuss municipal risks with executive management. |
| **Executive management:** | **Senior management:** | **Risk management:** |
| o Defines the risk appetite;  
o Evaluate proposed strategies against the risk appetite;  
o Provide timely risk related information by:  
  ▪ Aggregating risk information;  
  ▪ Identifying and assessing municipal risks;  
  ▪ Determining risk response strategies; and  
  ▪ Monitoring risks and risk response plans. | o Aggregate risk information  
o Identify and assess risks  
o Determine risk response strategies  
o Monitor risks and risk response plans. | o Creates a risk methodology;  
o Provide direction and training on the use of the methodology;  
o Implement and manage technology systems for risk assessment; and  
  
| **Internal audit:** | **Technology** |  
- Provides assurance on the risk management process, the risk response plan for critical risks, and the risk and control matrix. |  
- Information technology on a pervasive basis:  
  - Provides dashboards to oversee risks on a real-time basis;  
  - Improve monitoring and reporting of risks;  
  - Support timely maintenance and pre-empt potential problems; and  
  - Facilitate risk escalations. |

Table 2: The five lines of assurance in the maturity assessment
### Maturity index (rating scale)

Each of the elements above is then measured on a five point scale:

<table>
<thead>
<tr>
<th>Maturity rating</th>
<th>Basic risk management</th>
<th>Comments</th>
</tr>
</thead>
</table>
| 1               | Basic risk management | • Response to ad-hoc, high incidences of liquidity problems, irregular expenditure, high levels of wastage, increased vacancy in key positions, lack of consequence management;  
• Continual “fire fighting”; and  
• Risk identification depends on individual capabilities and verbal wisdom. |
| 2               | Fragmented risk management | • Independent risk management activities;  
• Limited focus on linkages between risks;  
• Limited alignment of risks to strategies; and  
• Disparate monitoring and reporting functions. |
| 3               | Compliant risk management | • Implemented risk management framework, policies and training programs;  
• Routine risk assessments with a dedicated risk manager;  
• Communication of top strategic risks to Council; and  
• Knowledge sharing across risk activities. |
| 4               | Integrated risk management | • Coordinated risk management across different silo's;  
• Risk appetite is fully defined;  
• Municipal-wide monitoring, measuring and reporting;  
• Technology designed and implemented for real-time measurement; and  
• High correlation between risk assessment and audit activities. |
| 5               | Risk intelligent | • Risk management embedded in strategic planning, capital and budget allocations, resource planning;  
• Application of risk bearing capacity principles in planning;  
• Balance between risk taking (value creation) and risk mitigation (for potential value destruction);  
• Linkage to performance measures and performance bonuses;  
• Risk modelling and what-if analysis;  
• Risk management applied in all decision-making;  
• Early warning indicators used; and  
• Industry benchmarking |

*Table 3: Rating scale for maturity index*
The assessment methodology applied in the following table illustrates three levels of assessment (Assessment A: Oversight; Assessment B: Systems, and Assessment C: Processes) to assist in determining a municipality's maturity. For ease of application, the five risk maturity ratings have been condensed into three, namely Fragmented (Basic/Fragmented), Integrated (Compliant/Integrated); and Risk Intelligent. The rating should be applied as follows:

i. Use the risk elements in column 1 and measure the current status of the municipality by comparing their own risk management to the descriptions under the heading of fragmented, integrated and risk intelligent.

ii. Award 1 mark for a fragmented rating, 2 marks for an integrated rating, and three marks for a risk intelligent rating.

iii. Aggregate the marks once all the ratings have been completed. Note that there are 22 elements that should be rated.

If the total score is between 22 and 33, the risk management within your municipality is rated as fragmented. If the score is between 34 and 48, your risk management is rated as integrated, and if the score is between 49 and 66, the risk management has a status of risk intelligent.

The diagram below illustrates the calculation of the maturity.

Diagram 4: Maturity status

Diagram 5: Calculation of maturity
**Assessment A: Risk governance**

The key driver for a municipality’s risk management maturity is the attitude that the municipal council, its audit committee and senior management take towards the role of risk management, assessed as follows:

<table>
<thead>
<tr>
<th>Risk culture</th>
<th>Fragmented</th>
<th>Integrated</th>
<th>Risk intelligent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness of risks</td>
<td>Beyond a common understanding of health/safety risks, individuals only understand their own specific risks.</td>
<td>Centralised risk register covering risks across the municipality, updated annually.</td>
<td>Decisions are made based on risk perspectives, risk appetite and cost-benefit.</td>
</tr>
<tr>
<td>Willingness to raise risks</td>
<td>Apart from whistle-blowing for extreme events, there is an ingrained cultural resistance to report risks.</td>
<td>Processes designed and implemented to report on failing procedures and individuals.</td>
<td>Employees rewarded for reporting on risks/making recommendations, failure to report breached are penalised.</td>
</tr>
<tr>
<td>Ownership of risks</td>
<td>Risk is assumed to be managed by the municipality and not included in</td>
<td>Employees are aware of risk reporting processes and escalating reporting if</td>
<td>Employees understand responsibility to report risks, its consequences if not</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inclusion of risks in decision making</th>
<th>Risk management is separate from decision making, and risks are dealt with after the event.</th>
<th>Risks inform strategic planning and budget forecasting, re-assessed annually.</th>
<th>Risk is part of key decisions, day-to-day operational activities and strategic decisions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk strategy and appetite</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk appetite statements</td>
<td>Any guidance on risk is general and of little operational use.</td>
<td>Qualitative risk appetite calculations are done for processes and are used in decision making.</td>
<td>Risk appetite statements formulated for robust measurement of KRI’s around impacts/ exposure limits and for risk-based decision making.</td>
</tr>
<tr>
<td>Awareness of risk appetite</td>
<td>There are no limits set for risk, apart from zero tolerance for accidents.</td>
<td>Employees understands how much risk they can expose the municipality to when making decisions.</td>
<td>Acceptable limits are part of the decision making processes and measured accordingly, i.e. risk tolerance levels defined and applied to facilitate decision-making.</td>
</tr>
<tr>
<td>Inclusion of risk appetite in decision-making</td>
<td>Decision-making generally seen as a go/no-go with risks addressed afterwards.</td>
<td>Risks inform strategic planning and budget forecasting, re-assessed at least annually.</td>
<td>Risk is part of key decisions, day-to-day operational activities and strategic decisions.</td>
</tr>
<tr>
<td>Risk governance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delegation of authority</td>
<td>Delegation of authority for risk management is not defined, inefficient or incomplete.</td>
<td>Formal delegations of authority for risk decisions and management, with consequence management for non-compliance.</td>
<td>Delegations have been aligned to service delivery demands of the municipality without compromising on risk.</td>
</tr>
<tr>
<td>Risk monitoring and mitigation</td>
<td>Risks identified are escalated to management on an ad-hoc basis.</td>
<td>Risks are identified on a routine basis, and reporting tracks the risks and its consequences.</td>
<td>Issues are resolved on lowest level of the municipality to maximize efficiency without compromising on risk appetite.</td>
</tr>
<tr>
<td>Risk and control assurance</td>
<td>Limited liaison between risk</td>
<td>Some alignment of risks and controls</td>
<td>Combined assurance roles and</td>
</tr>
</tbody>
</table>
management and internal audit regarding risks and control.

between risk management, internal audit and line management - control self-assessment and principles of combined assurance applied.

responsibilities clearly defined and applied amongst all assurance providers regarding risks and risk responses.

Table 4: Table for the maturity assessment – risk governance
Assessment B: Risk systems

Risk management resources and infrastructure often determine the effectiveness of the risk management process.

<table>
<thead>
<tr>
<th>Resources/Infra-structure</th>
<th>Fragmented</th>
<th>Integrated</th>
<th>Risk intelligent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management official</td>
<td>Lower level delegation, not taken seriously, or too little time devoted to risk management.</td>
<td>Nominated risk management official with appropriate time and resources.</td>
<td>Risk management is supported by the Municipal Manager, Council and the Audit Committee.</td>
</tr>
<tr>
<td>Reliability and integrity of data</td>
<td>Risk information is frequently incomplete, inaccurate and untimely.</td>
<td>Both qualitative and quantitative, reliable and relevant information available.</td>
<td>KRI's and KPI's are aligned with assurance on the integrity of all data and information.</td>
</tr>
<tr>
<td>Automation</td>
<td>Compiling risk information is manual and time-intensive. Multiple IT systems are incompatible with each other, reporting occurs on Excel.</td>
<td>Standardised information that are completed manually and reported to management meetings.</td>
<td>Risk information reported on a real-time, automated, continuous basis to management - used for decision making on a preventative basis.</td>
</tr>
<tr>
<td>Risk management strategy</td>
<td>Mostly around gut feel and without sufficient data.</td>
<td>Full range of strategies (accept, avoid, transfer and mitigate) considered.</td>
<td>Full range of strategies (accept, avoid, transfer and mitigate) considered as well as a cost-benefit analysis.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Monitoring and reporting</td>
<td>Frequency</td>
<td>Risk monitoring and reporting is done to the Exco and the Municipal Council in a risk reporting pack, and ad-hoc if requested.</td>
<td>Risk monitoring is largely automated and therefore done on a continuous basis, and reports can be generated when requested.</td>
</tr>
<tr>
<td></td>
<td>Link to KPI’s</td>
<td>Risks are reported on a bottom-up basis, and grouped together according to their impact on top down municipal KPI’s for more meaningful reporting.</td>
<td>Risks are reported on a bottom-up basis, and then quantified with respect to municipal KPI’s, in terms of probabilities, impacts and correlations.</td>
</tr>
<tr>
<td>Link to strategic objectives</td>
<td>Risks are reported on a bottom-up basis, with large risk registers, with no or indirect link to the municipal strategic objectives</td>
<td>Risks reported on a bottom-up basis, and grouped together according to their impact on municipal strategic objectives for more meaningful reporting.</td>
<td>Risks are reported on a bottom-up basis, and then quantified with respect to municipal strategic objectives, in terms of probabilities, impacts and correlations.</td>
</tr>
</tbody>
</table>

Table 5: Table for the maturity assessment – risk systems
### Assessment C: Risk ownership and the risk management process

#### Risk identification

- **Approach**
  - The only risks reported are those from a bottom-up perspective and reported in a risk register.
  - Bottom-up operating risks are complemented by management’s top-down view of principle risks, as well as other municipal wide risks.
  - Focus is on the effort to anticipate those risks that can have a material adverse impact on the municipal business or its achievement of strategic objectives in advance.

- **Types of risks**
  - Financial and human resource risks
  - Financial, human resource and operational (service delivery) risks, with some assessment of information technology risks.
  - Financial and operational risks with a specific focus on potential legal impacts and contingent liabilities if failing to deliver services. Risks relating to information technology embedded in all processes.

#### Risk assessment

- **Oversight**
  - Risk culture
  - Risk strategy and appetite
  - Risk governance

- **Systems**
  - Risk resources and infrastructure
  - Risk monitoring and reporting

- **Processes**
  - Risk identification
  - Risk assessment
  - Risk management

**Integrated**

**Risk intelligent**
<table>
<thead>
<tr>
<th>Measurement</th>
<th>Aggregation</th>
<th>Risk management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks are measured in green, yellow and red.</td>
<td>Risks are aggregated and only measured on the worst case scenario.</td>
<td>Quantitative probabilities and impacts are estimated, using ranges for uncertainty.</td>
</tr>
<tr>
<td></td>
<td>Risks are measured on a colour scale, and ranked with a consistent metric such as likelihood and impact.</td>
<td>Quantified probabilities and impacts allows for easy aggregation of risks across different dimensions and at any level of confidence using statistics.</td>
</tr>
<tr>
<td></td>
<td>Risks are measured and aggregated per business process and risk universe categories for municipal level reporting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
<td></td>
</tr>
<tr>
<td>Risk response</td>
<td>Little data available to respond to risk, normally done on gut feel.</td>
<td>Different options are identified and cost-benefit analysis is performed on a qualitative and quantitative basis where possible.</td>
</tr>
<tr>
<td>Subsequent monitoring</td>
<td>Risk is added to the risk register, which is updated infrequently.</td>
<td>Key risks are discussed as part of management meetings, until they have been resolved to management’s satisfaction.</td>
</tr>
</tbody>
</table>

Table 6: Table for the maturity assessment – risk processes
At different levels of municipal maturity, municipalities will be at different levels of risk management maturity. Municipalities with lower levels of maturity regarding capacity, skills and budget, therefore will most likely not be able to yet perform at integrated or risk intelligent levels of risk management maturity. However, a municipality should determine its current level of maturity and then strive to move to a higher level of maturity over a period of time, i.e. a municipality should determine a strategy to move to higher levels of maturity in a progressive manner over a pre-determined period of one to five years. For example, if the municipality is at a Basic/Fragmented level, it should move to a Compliant/Integrated level over one or two years, and then strive to move to a Risk Intelligent level if their culture, capacity and capability would allow it in another two to three years.

A municipality at the lowest level of municipal and risk management maturity should do at least a minimal number of risk management activities as a start and report this in their annual report, together with their strategy and plan together with a budget and resource specification to move to the next level.

For this purpose, and to enable this in municipalities, the toolkit has two versions, namely one for municipalities at the Basic/Fragmented level, and one for municipalities at the Compliant/Integrated level.

The toolkit and supporting website do not specifically cater for the Risk Intelligent level, as Risk Intelligent municipalities would use the principles of Compliant/Integrated as their basis and point of departure, and would have the capability to move, at their own discretion, to higher levels of maturity, such as Risk Intelligence.

The website version of the model therefore allows for a rating mechanism (as discussed in table 6 above), where a municipality can determine their maturity status. The following links allows the user to access the specific website that applies to their risk maturity status.

Basic/Fragmented status:  http://munirate.wixsite.com/ntrmf-fragmented

Compliant/Integrated status:  http://munirate.wixsite.com/ntrmf-integrated
Chapter 4: Risk Assurance

15. Introduction

The term 'assurance' refers to the verification of risk mitigation and internal control. It embraces the tasks of internal audit, management reviews and specialised audits that test and validate the control environment.

Combined assurance is, simply, ensuring that a co-ordinated (combined) approach is applied in receiving assurance on whether key risks are being managed appropriately within a municipality.

Firstly, the backbone of a combined assurance model is a commonly accepted view of the risks facing the municipality. A municipality looking to apply this model effectively and efficiently is setting itself up for failure if it does not have a robust, mature risk management process. Conversely, a municipality that has a risk management process, but no combined assurance model, is missing a vital piece of this puzzle.

Combined assurance seeks to reduce duplications in audit processes and prevent any key controls from being missed by assurance providers. This approach to assurance normally has a risk foundation. The contents of risk registers are used to design the annual assurance plans. An assurance plan is one of the primary means by which the Municipal Manager receives confirmation that risk responses and internal controls are appropriately designed and implemented. A risk-based assurance plan follows the outputs of the risk identification, assessment and control evaluation processes.

It is commonly accepted that assurance should be designed on an integrated basis. This means that there is a coordinated plan to provide a spread of assurance providers for the key controls. The principle of integration lies in the arranging of specialist assurance providers based on a rational allocation of resources.

Assurance providers usually have an existing assurance role, for example internal auditors, insurance surveyors, safety auditors, environmental surveyors, quality auditors, stakeholder satisfaction surveys, credit auditors, etc.

The International Standards for Professional Practice of Internal Auditing (Standard 2050) prescribes that the Chief Audit Executive should share information and co-ordinate activities with other internal and external providers of relevant assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

King IV suggests that the Municipal Council should assume responsibility for assurance by setting the direction concerning the arrangements for assurance services. It should also oversee that a combined assurance model is designed and implemented to effectively cover the significant risks and material matters of the municipality through a combination of assurance providers.
King IV further recommends that the Municipal Council should delegate the responsibility to the Audit Committee to establish a combined assurance model to achieve the following objectives of:

- The adequacy and effectiveness of the internal control environment; and
- The integrity of information used in decision-making.

16. **Applicability**

Combined assurance can only effectively be applied to integrated risk management and in risk intelligent municipalities. It requires a solid understanding of risk, the roles of the first three lines of assurance, and correlation between the different assurance providers. Municipalities with a fragmented status will use the independent assurance provided by internal and external auditors.

Internal audit specifically should also provide assurance on the **effectiveness of the risk management process**. In some instances, where municipalities are lacking the necessary skills and resources as assessed in chapter 3, internal auditors might actually also perform the risk assessment. In such cases, the independence of the internal auditors might be under scrutiny.

External auditors will provide assurance on financial and compliance risks, by auditing the reliability and integrity of the financial statements, and the compliance with relevant laws, regulations, policies, procedures and contractual obligations.

17. **Benefits of combined assurance**

By effectively implementing combined assurance, a number of tangible benefits will be derived, including:

a. Greater coordination of relevant assurance efforts focusing on key risk exposures;
b. Assistance with closure of assurance gaps;
c. Minimised operational disruptions;
d. A comprehensive and prioritised approach in tracking of remedial actions;
e. Improved reporting to the Municipal Council and committees, including reducing the duplication of reports being reviewed by different committees;
f. Greater ease of information sharing and action;
g. A possible reduction in assurance costs; and
h. Support of the Municipal Council and Audit Committee in making their control
   statements in the integrated report.

Combined Assurance will add value to the municipality by:

   a. Providing an understanding who all the assurance providers are;
   b. Providing a realisation of what is actually assured;
   c. Providing information that is reported within the governance structures;
   d. Allowing alignment of assurance to the critical risk exposures;
   e. Ensuring coordination of the assurance activities;
   f. Ensuring consolidation of the risk and assurance profile.

18. Audit Committee responsibilities in terms of combined assurance

The audit committee is an independent committee responsible for oversight of the
municipality’s governance, risk management and control, and should provide an independent
and objective view of the municipality’s risk management effectiveness. Responsibilities should
include reviewing and recommending disclosures on risk in the annual report, providing
feedback on the adequacy and effectiveness of risk management, including recommendations
for improvement, ensuring internal and external plans are aligned to the municipality’s risk
profile, and satisfying itself that financial reporting risks, internal financial control and
information technology risks are appropriately addressed.

Chapter 3 Principle 3.5 of King III states that the audit committee should ensure that a
combined assurance model is applied to provide a coordinated approach to all assurance
activities, and that it includes as recommended practice the principle that the audit committee
should ensure that combined assurance is appropriate to address all the significant risks facing
the municipality, and furthermore, should monitor the relationship between the external
assurance providers and the municipality.

It should be reiterated that the audit committee’s responsibilities for combined assurance have
now been expanded to include all significant risks and is not limited to financial and information
technology risks only. With combined assurance the audit committee will be able to fulfil the
oversight function much more effectively and efficiently. Combined assurance can be used to
provide the audit committee with the comfort that significant risks, including strategic risks, and
the actions to mitigate the risks, have been subjected to assurance procedures.

In the absence of clear guidelines to audit committees on their roles and responsibilities
relating to combined assurance, the following are some suggested minimum generic steps that
audit committees could consider taking:

   a. Ensure that the responsibilities of the audit committee for combined assurance are
      appropriately reflected in the audit committee charter.
   b. Review, provide input and adopt the developed combined assurance framework or the
      combined assurance plan.
c. Review the combined assurance framework/plan and ensure that the framework/plan can be clearly linked to the risk analysis, and that all the high risk areas identified in the risk analysis are covered in the combined assurance plan. This would include ensuring that when the risk profiles change, the combined assurance plan is updated. Risk analysis should include the strategic risks as well as the significant risks within the different assurance areas, including for example, but not limited to, forensics, legal, financial, environmental, occupational health and safety. The combined assurance plan should link the risks to the activities/mitigating actions and the responsible assurance providers, with an indication of the frequency of the actions.

d. Where internal audit has been identified in the combined assurance plan as responsible for co-coordinating the inputs received from the different assurance providers on the execution of the plan, the audit committee needs to review quarterly reports from internal audit that reflect actual performance by the different assurance providers and compare this with the combined assurance plan. The audit committee should also review the corrective actions taken where identified risks are not being covered by assurance activities.

e. Where internal audit has been identified in the combined assurance plan as one of the assurance providers, the audit committee needs to ensure that the activities allocated to internal audit in terms of the combined assurance plan are included in the scope of coverage and in the internal audit plan.

f. Where external audit has been identified in the combined assurance plan as one of the assurance providers, the audit committee needs to confirm with external audit that the work performed by them will warrant such reliance.

g. The audit committee should consider the extent to which they were able to fulfil their combined assurance responsibilities and reflect that appropriately in the audit committee report.

19. Requirements to qualify as an assurance provider

Assurance providers play a pivotal role in effective risk management. The following table provides guidance on the requirements to qualify as an assurance provider.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independence and objectivity</td>
<td>Independent reporting lines, no recent direct involvement and/or work done in the area/aspects to provide assurance on/be audited.</td>
</tr>
<tr>
<td>Conflict of interest</td>
<td>In the areas/aspects in which assurance is to be provided, there should not be any conflict of interest (could require a declaration in this regard).</td>
</tr>
<tr>
<td>Skills and experience</td>
<td>The assurance provider should have the appropriate skills and experience to effectively conduct the assignment.</td>
</tr>
<tr>
<td>Qualifications</td>
<td>The assurance provider should hold appropriate qualification(s).</td>
</tr>
<tr>
<td>Assurance methodology</td>
<td>A sound audit/review methodology should be adopted by the assurance provider. Ideally, a risk-based approach should be followed. The reported findings and opinions should be supported by adequately documented working papers/audit trails.</td>
</tr>
</tbody>
</table>

The assurance providers relevant to the first three lines of assurance of the Combined Assurance model as discussed in this framework, are:

- **Risk owners**: overseeing risks and controls of the people and activities under their area of responsibility (partially independent) – i.e. *management based assurance*.
- **Risk management officials** (also sometimes called risk custodians): overseeing the implementation of the risk management methodology (semi-independent) – i.e. *risk and compliance based assurance*.
- **Internal Audit**: overseeing the effectiveness of the implementation of the risk management methodology (fully independent) – i.e. *independent assurance*.

### 20. Risk universe

Effective application of the combined assurance model is reliant on an accurate population of the risk universe. To make sure that a municipality does not miss any potential risks in its structured process of risk identification, assessment, and reporting, it is important that a so-called risk universe with an exhaustive list of risk categories, as far as possible, is drafted.

Several risk universe models are available. The following risk universe is an example of a risk universe for the public sector. It can be adopted to accommodate the unique environment of individual municipalities. The example is tailored towards the integrated and risk intelligent municipalities.

Creating a universe for fragmented risk maturity, will exclude many of these elements, and would rather include the critical processes, i.e. supply chain management, human resources, asset management, etc., and/or where operational processes are aligned with their strategy through the implementation of programs and projects. Where external regulation greatly influences the strategic and operational decisions, the categories of project risks and regulatory risks could typically be added in relation to the other categories of risk.

It is important to note that these categories are not rigid boxes that ring-fence risks exclusively, but that categories of risk can overlap, for example a project risk would typically also include operational and financial risks. Categories of risk should be used as a guideline for risk identification, assessment and reporting. However, the principle of risk scenarios, which may cut across the different categories of risk, could very effectively be applied to further analyse risks and coming up with useful and appropriate risk response measures. One example of a risk universe is displayed on the next page.
Diagram 6: Example of a public sector risk universe
21. Combined assurance template

The main output from this wide focus on assurance is a spreadsheet that details all the key controls of the municipality and indicates which assurance provider will validate them. An assurance plan should indicate how often a control will be validated. Certain key controls may be validated and reviewed more than once by different parties. The allocation of control validation by internal and independent parties is a fundamental principle of structuring a good assurance plan.

Once again the level of maturity should determine the extent to which combined assurance is implemented. An approach of combined assurance might not be effective for a municipality that is operating on the fragmented risk assessment level. The template clearly allows for integration of risk and for supplementary assurance from a range of assurance providers. The table indicates a minimum layout for combined assurance.

<table>
<thead>
<tr>
<th>#</th>
<th>Key risk as identified in the risk universe</th>
<th>Combined assurance – integrated and risk intelligent municipalities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1st line of assurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management – Risk owners</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management processes and controls</td>
</tr>
<tr>
<td>1</td>
<td>Financial</td>
<td>Liquidity</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>Budget</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Grants</td>
</tr>
</tbody>
</table>

Template 2: Combined assurance
22. Guidelines for implementing an effective combined assurance model

a. Identifying Role Players

Step One entails the Municipal Manager identifying and appointing a combined assurance champion. The champion will coordinate the process and ensure process continuity. This executive must be appointed to provide the authority, oversee the process and ensure that cooperation is provided throughout the initiative.

b. Assess potential for combined assurance

The second step entails establishing a high level understanding of who the assurance providers are for the risk exposures facing the municipality. Ideally, assurance providers should be separated in terms of first, second and third line of assurance i.e. management-based assurance, risk and compliance-based assurance and independent assurance respectively.

The first line of assurance (Management based assurance):

Managers, the risk owners, are responsible for ensuring the managing of the risk and are termed “first line” assurance providers. The first line of assurance is best suited to offer broader assurance coverage.

The second line of assurance (Risk and compliance based assurance):

The second line of assurance comprises corporate functions such as risk management, compliance officers, occupational health and safety, legal services and internal control units. It is recommended that the combined assurance champion be selected from the second line of assurance.

The third line of assurance (Independent assurance):

The third line of assurance may be categorized in terms of audit and oversight. Internal audit and the Auditor-General are examples of independent assurance providers that form the third line of assurance. During step 2 of the process an assurance profile should be documented.

c. Test Coverage of Assurance

The third step in the process is to test the coverage of assurance provided through interaction with recipients and assessment of reports to establish what is being done and for what reasons. This test will ensure coordination of efforts and eradicate duplication. The IIA Standard 2110 states that the internal audit activity must coordinate the activities of and communicate information among the council, external and internal auditors and management. Unless a combined assurance champion has
been appointed out of the second line of assurance, the third stage in the process could be assigned to the internal audit activity.

d. Risk Focus

In the **fourth step** a full understanding is established of what assurance is currently being provided and what needs to be provided based on the strategic and operational risk profiles of the municipality. This step will allow a detailed gap analysis to be developed, which will also inform the next step in the process. Here the different lines of assurance will be mapped to the identified risks and detail work actually performed to provide the expected assurance.

It becomes imperative for the risk profile to be relevant to the business that is managed on a consistent basis. Risk information should be regularly and centrally maintained. It might not feasible to consider all identified risks in the Combined Assurance Model. It is recommended that the limit is set in terms of risk severity (which should be in line with the risk appetite and tolerance levels of the municipality). The risk rating will therefore be the criteria for incorporation in the Combined Assurance Model. This approach will simultaneously ensure that the assurance is worth the cost.

e. Combined Assurance Application

The **final step** requires stakeholder acceptance of the approach and respective responsibilities through identifying the recommended areas of assurance and articulating the nature of the assurance activities. The detailed gap analysis should highlight four areas of assurance, i.e. *extensive assurance, moderate assurance, inadequate assurance, or no assurance*. In this instance the municipality must apply its discretion in defining extensive, moderate and inadequate assurance.

Inadequate assurance coverage must be addressed by the Combined Assurance Champion in conjunction with the Municipal Manager. The third line of assurance will then be responsible for reporting on the adequacy of assurance provided by the implementation of combined assurance. Lastly, the assurance provided must be credible. It is recommended that Executive management and Council ensure that both internal and external assurance providers are appropriately skilled and experienced to follow an adequate approach.

### 23. Drafting an assurance plan

A risk-based assurance plan encourages an allocation of assurance resources based on risk priorities. Risk owners have a key role to play in selecting assurance activities for their respective risks.

The co-ordinated approach requires the municipality to provide a spread of assurance providers for each risk, balanced between management, independent functions and external parties.
The assurance template is completed by listing the key risks and their respective controls in the indicated column. The risk owner will then indicate which assurance providers currently review or monitor the controls listed.

This can be indicated by means of a code which indicates the frequency of the particular assurance activity, e.g. 'M' for 'monthly'. Gaps in the assurance program are then considered with input from assurance providers themselves, such as the internal audit function. The desired additional assurance activities, with preferred frequency of activity, are then inserted into the selected template (see template 2, as a basic template example which can be extended to include such information).
Example 1: Combined Assurance Plan

1. Introduction

The combined assurance plan has been compiled from the risk analysis performed by the XYZ Municipality. This will enable management to assign resources priority efficiently to mitigate the risks to an acceptable level and to identify who is responsible for each risk.

1. Objectives

The objectives of the combined assurance plan are mainly to:

a. Identify and specify the sources of assurance over the municipality’s key risks (where the risk exceeds the risk appetite);

b. Provide the Risk Management Committee, the Municipal Manager (MM) and Executive Management with a framework of the various assurance parties;

c. Link risk management activities with assurance activities. This will also assist the MM to review the effectiveness of the risk management system; and

d. Provide a basis for identifying any areas of potential assurance gaps.

2. Approach

The combined assurance plan has been designed to highlight the relevant high-risk areas and the assurance to be provided by management, external audit, internal audit and other consultants or service providers in order for the Council to be appraised of the risk management efforts undertaken to manage the risks to an acceptable level. The risk analyses performed during the XXX financial year formed the basis for determining the combined assurance plan for the Municipality.

The combined assurance plan was developed through:

a. Analysis of the risk assessment; and

b. Discussion and agreement regarding assurance priorities.
4. Role and Responsibilities

4.1 Role of Internal Audit in terms of Combined Assurance

International Standards for the Professional Practice of Internal Auditing (ISPPIA) and its associate Practice Advisories (PA) state that the Chief Audit Executive (CAE) should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts. The Internal Audit Activity (IAA) has access to the work of other internal and external assurance providers. The IAA will provide assurance over the entire municipality, including:

a. Assurance on the design and adequacy of the risk management processes;
b. Management of the top risks including the effectiveness of the controls and other responses; and
c. Verification of the reliability and appropriateness of the risk assessment and reporting of the risk and control status.

In instances that the head of Internal Audit (CAE) is hiring an assurance provider, the CAE will document engagement expectations in a contract or agreement. The following minimum expectations will be set to ensure that work is adequate and reporting requirements are fulfilled:

a. The nature and ownership of deliverables;
b. Methods / techniques;
c. The nature of procedures and data / information to be used; and
d. Progress reports / supervision.

The IAA will consider the following to conclude whether to rely on the work of the assurance provider:

a. Independence and objectivity; and
b. Competencies and qualifications, through verification of:

   I. appropriate professional experience and qualifications;
   II. current registration with relevant professional body or institute;
   III. reputation for competency and integrity in the sector;
   IV. elements of practice to have reasonable assurance that the findings are based on sufficient, reliable, relevant and useful information; and
   V. that the work of the assurance provider is appropriately planned, supervised, documented and reviewed.

When management require an overall opinion from the CAE, the CAE should understand the nature, scope and extent of the integrated assurance map to consider the work of other assurance providers, rely on it as appropriate, before presenting an overall opinion on the municipality’s governance, risk and control processes.
The IAA should include reference to other assurance providers where reports rely on such information. Instances where the municipality does not expect an overall opinion, the CAE can act as the coordinator of assurance providers. The CAE should report on any lack of input by other assurance providers. If the CAE believes that the assurance is inadequate or ineffective, the Municipal Manager and Audit Committee will be advised accordingly.

The IAA will follow up on recommendations made by other assurance providers and should determine whether management has implemented the recommendations or accepted the risk of not taking action. It should become common practice that internal and external audit rely on the work of the other to increase efficiencies. In this case, sufficient information should be provided to enable the other party to understand the techniques, methods and terminology to facilitate reliance on the work performed.

Planned audit activities of internal and external auditors need to be discussed to ensure that audit coverage is coordinated and duplicate efforts are minimized where possible.

Sufficient meetings are to be scheduled during the audit process to ensure coordination of audit work and efficient and timely completion of audit activities and to determine whether observations and recommendations from work performed to date require that the scope of planned work be adjusted.

4.2 Role of the Audit- and Performance Audit Committee in terms of Combined Assurance (APAC)

The APAC should ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities. This role emanates in the following primary tasks:

a. Ensure that the responsibilities for combined assurance are appropriately reflected in the AC Charter;
b. Encourage cooperation between internal and external audit;
c. Review coverage and scope between internal and external audit to avoid duplication and allow for possible cost savings from the integration of the two functions. Timing of internal audits and the months during the financial period that the audit scope will cover must be aligned;
d. Review, provide input and adopt the Combined Assurance Plan (CAP);
e. Ensure that the CAP can be clearly linked to the risk assessment;
f. Ensure that all high risk areas are included in the plan;
g. Review quarterly reports that reflect actual performance by the different assurance providers and compare with the CAP; and
h. Review corrective action taken when identified risks are not being covered by assurance activities.
5. Combined Assurance Plan (CAP)

5.1 Results - Assurance providers

Based on the results of the risk assessment and discussions with Management as well as our experience and understanding of the underlying risk of its occurrence, certain of the risks identified may require additional independent assurance. These have been included in the combined assurance plan in point 5.2 of the report.

The Municipal Manager will ultimately decide on the most appropriate assurance provider for the identified risks. Where internal audit is identified as the most appropriate assurance provider, the Audit Committee must approve the scope of coverage and audit plan. Similarly, if external audit is to be relied upon for assurance, the Municipal Manager should inform them of this reliance to determine from the external auditors whether or not such reliance is appropriate from their work performed or to be performed.

Executive Management may be engaged as assurance providers as part of its ongoing activities or as part of an identified special project.

5.2 Combined assurance plan

The facilitated risk assessment has identified risks, which if they materialise, may have a negative impact on the Municipality as a whole. In order to ensure that this exposure is appropriately mitigated, a combined assurance plan has been developed to allocate responsibility and accountability for the risks to Executive Management, External Audit, Internal Audit, or a combination thereof.

Due to the nature of risk management, Executive Management is ultimately responsible for all risks within the Municipality and hence assumes overall responsibility and accountability for all the identified strategic risks. The Combined Assurance Plan details the Residual Risks above the Risk Appetite, identified during the Risk Assessment process.

Although, the mitigation and management of the said risks is the responsibility of management, Internal Audit has used the results of the risk assessment to develop its risk-based plan and accordingly focus its efforts on HIGH risk areas to determine whether actions taken by management to mitigate such risks has achieved the desired outcome. The Combined Assurance Plan (CAP) based upon the key business risks is documented in a table that engages the roles of all the role players.
Chapter 5: Control environment and tone at the top

24. Introduction

A municipality is as strong as its tone at the top, and as such the control environment should be evaluated as the first step.

King IV recommends 16 principles that should embody the aspirations towards good governance. King IV has specific guidance for municipalities, included in Part 6.2 – Supplement for municipalities which includes that the council should ensure that assurance services enable an effective control environment and that these support the integrity of information for decision-making purposes.

25. Applicability

Evaluating the control environment can only effectively be applied to integrated risk management and in risk intelligent municipalities. It requires a solid understanding of risk, the roles of the first three lines of assurance, and correlation between the different assurance providers. Municipalities with a fragmented status will use the independent assurance provided by internal and external auditors.

The COSO ERM framework defined the elements of a strong tone at the top. It comprises elements that should be implemented and applied to ensure that risk and controls are managed effectively.

Implementing COSO is a daunting task, and the following diagrams, tables and assessment matrixes should assist in the process.

COSO has five elements which are supported by 17 principles. Compliance with the principles is tested by assessing supporting guidelines for these principles.

As with most assessments, a matrix is applied to perform the assessment, which in line with this framework, is published as a control environment risk assessment.

The five elements are discussed below.

Diagram 7: Assessing the control environment

7 Leveraging COSO across the three lines of defence – IIA-INC – July 2015
26. **Assessment process**

The assessment process should be completed by the first three lines of assurance. A red rating will indicate areas where management can improve the control environment. It is absolutely essential to allow the three lines of assurance to provide independent answers.

Combined assurance requires that management designs and implements controls (1st LOA), risk management provides ongoing monitoring (2nd LOA), and that internal audit provides assurance on the adequacy and effectiveness of the processes in place (3rd LOA).

The result of the three-way measurement might, for example, illustrate that management believes that they have designed adequate systems, but risk management has no ability to monitor residual risk against the risk appetite, or alternatively that internal audit assesses the process to be full of loopholes.
27. 17 principles

The application of the 17 principles of COSO across the lines of assurance can be explained in the diagram below:

<table>
<thead>
<tr>
<th>COSO elements</th>
<th>COSO principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 LOA – Senior management</td>
<td></td>
</tr>
<tr>
<td>Control environment</td>
<td>1 Demonstrates commitment to integrity, ethical values</td>
</tr>
<tr>
<td></td>
<td>2 Exercise oversight responsibility</td>
</tr>
<tr>
<td></td>
<td>3 Establishes structure, authority, responsibility</td>
</tr>
<tr>
<td></td>
<td>4 Demonstrates commitment to competence</td>
</tr>
<tr>
<td></td>
<td>5 Enforces accountability</td>
</tr>
<tr>
<td>1 LOA – Risk owners - design and implement management and internal controls</td>
<td></td>
</tr>
<tr>
<td>Risk assessment</td>
<td>6 Specifies suitable objectives</td>
</tr>
<tr>
<td></td>
<td>7 Identifies and analyses risk</td>
</tr>
<tr>
<td></td>
<td>8 Assesses fraud risk</td>
</tr>
<tr>
<td>Control activities</td>
<td>9 Identifies and analyses significant change</td>
</tr>
<tr>
<td></td>
<td>10 Selects and develops control activities</td>
</tr>
<tr>
<td></td>
<td>11 Selects and develops general controls over IT</td>
</tr>
</tbody>
</table>

2 LOA – Risk management

Provide appropriate and specific expert guidance for implementation

3 LOA – Internal Audit

Provide independent assurance regarding the design and implementation of all 17 principles
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Deploys through policies and procedures</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Uses relevant information</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Communicates internally</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Communicates externally</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Conducts ongoing and/or separate evaluations</td>
<td>Ongoing monitoring and reporting</td>
</tr>
<tr>
<td>17</td>
<td>Evaluates and communicates deficiencies</td>
<td></td>
</tr>
</tbody>
</table>

**Table 7: 17 principles of the COSO framework**
28. Guidelines to assess the control environment within a municipality

Effective risk management is based on a very strong control environment. The guideline questions below provide an understanding of the 17 principles to enable an evaluation of the control environment by the three lines of assurance.

<table>
<thead>
<tr>
<th>Control environment</th>
<th>1 LOA</th>
<th>2 LOA</th>
<th>3 LOA</th>
<th>Self-assessment of policies, procedures and processes – see matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1: The municipality demonstrates a commitment to integrity and ethical values.</td>
<td></td>
<td></td>
<td></td>
<td>Combined score</td>
</tr>
<tr>
<td>1 Management expectations translate into a statement of beliefs, values, and standards of conduct that the staff exhibit daily. Formal *code of conduct/*policies communicates appropriate ethical/moral behavioural standards, addressing acceptable operational practices, conflicts of interest.</td>
<td></td>
<td></td>
<td></td>
<td>Sum (1 LOD +2 LOD + 3 LOD)</td>
</tr>
<tr>
<td></td>
<td>1-4</td>
<td>5-7</td>
<td>8-11</td>
<td>12-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2</td>
<td>Management communicated a clear view as to how risk management is integral to the municipality's business and value creation objectives so that employees at all levels can understand. These communications are focused on the municipality's progress in implementing its risk management strategies and achieving risk management goals and objectives.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Processes are in place to ensure that the Municipality’s standards of conduct are communicated and reinforced to all levels of the municipality and to outsource service providers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Processes are in place to ensure that employees regularly state explicitly whether they comply with the code of conduct or similar pronouncements of expected employee behaviour. Senior management action implemented processes that appropriately address intervention or overriding internal control.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>The municipality has a continuous improvement philosophy, i.e., obtain an understanding of the risk assessment, control and monitoring process, measure risk against risk tolerances to “manage by fact,” evaluate risk control process performance against management’s risk tolerance or standard, and improve processes to close gaps.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 6 | Senior management and the Municipal Council have approved a formal control policy that is widely distributed and clearly understood by managers at all levels of the municipality. The policy addresses:  
- The objectives of assessing and controlling business risk and its importance to the municipality's objectives and strategies;  
- The framework for evaluating risk;  
- Who is responsible for implementing the policy for key risks;  
- The strategies for managing different types of risks, including management's “risk tolerance,” i.e., how much risk the municipality is willing to accept/tolerate; and  
- Risk authorities, i.e., who are authorized to commit firm resources in conjunction with high risk activities and execute risk |
management strategies.

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Processes in place to define, maintain, and periodically evaluate the skills and expertise needed among its members to enable them to question and scrutinize management’s activities and present alternate views.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>The criteria for promotion and advancement within the municipality is clearly communicated, incentive and bonus plans are based upon specified performance criteria for each key risk management position and the relationship of these plans to established performance measures and to the performance evaluation process is clearly defined and communicated. There is evidence that the municipality is successful in retaining exceptional staff with the knowledge and skills needed to support the municipality’s risk management objectives and strategies.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Principles 2 and 3:**
Management establishes, with Council oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Processes are in place to evaluate whether the municipal structure is appropriate for the size and complexity of the functions within the municipality.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Processes are implemented whereby job descriptions and performance agreements define tasks required to accomplish particular jobs/fill the various positions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>High-level analyses are performed on an annual basis of the knowledge, skills, and abilities needed to perform jobs appropriately.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Specific lines of authority and responsibility are established to ensure compliance with legislation and regulations. Managers and process/activity owners obtain an understanding of the risk assessment, control and</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
monitoring process, measure risk against risk tolerances to “manage by fact,” evaluate risk control process performance against management’s risk tolerance or standard, and improve the processes to close the gaps. Once improvements have been identified, they are implemented in accordance with management’s priorities.

14 Appropriate mechanisms are used to discipline the implementation of recommendations in risk assessment, control and monitoring processes resulting from any audit activity, broadly defined (i.e., external financial statement audits, or regulatory audits, internal audits, etc.), including timetables for action, establishing accountability with appropriate responsible process/activity owners, etc.

15 Council understands the importance of internal controls, including the division of responsibility/delegation of authority. Appropriate restrictions are placed on uncontrollable business activities and communicated to appropriate risk managers and process/activity owners.

**Principle 4:**
The municipality demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

16 Processes are in place to ensure that regular employee evaluations are documented and shared with employees.

17 Tasks that comprise specific risk management activities are defined in writing. The Human Resources function works with process/activity owners to determine that key employees assigned to important risk management tasks are selected based on the experience, knowledge and skills required to perform each task and the extent to which employees must exercise judgment in performing the task. Selection and hiring processes are linked to specifically identified knowledge and skill requirements.
Processes are in place to ensure that the municipality checks credentials, references, and past work experience of potential new employees.

Principle 5:
The municipality holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Effective policies and procedures are designed and implemented for hiring, orienting, training, evaluating, counselling, promoting, compensating, disciplining, and terminating employees. Processes in place to ensure that background checks are conducted on candidates for employment.

Risk measurement and performance reporting so that process/activity owners are accountable for implementation. Written policies exist that clearly specify management’s risk tolerances, limits on transactions and asset exposures, boundaries on behaviour, etc.

Accountabilities for implementing improvements are clearly defined, including what is the task, who is responsible, when is it to be completed, how much resources are needed, etc. Discipline is established through tracking progress against established timetables.

Table 8: Internal control environment of the COSO framework
<table>
<thead>
<tr>
<th>Risk assessment</th>
<th>1 LOA</th>
<th>2 LOA</th>
<th>3 LOA</th>
<th>Self-assessment of policies, procedures and processes – see matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 6 and 7: The municipality specifies, with sufficient clarity, processes to enable the identification and assessment of risks relating to supply chain objectives.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Processes are in place to ensure that the municipality specifies objectives with sufficient clarity enabling the identification and assessment of risks that threaten the achievement of the supply chain objectives.

2. Processes are in place to ensure that the strategic plan has established objectives and key measurable indicators that are aligned with the local government mandate.

3. Processes are in place to ensure that an effective integrated management strategy and risk assessment plan is in place that considers the objectives and sources of risk from internal and external factors and establishes a control structure to address those risks.

4. Objectives are aligned with the municipality’s risk appetite, which drives risk tolerance levels for the municipality’s activities. Resources are allocated within the municipality with consideration to the risk appetite and strategies for growth and return.

5. Processes are in place to ensure that the municipality sets entity-wide financial reporting controls and assesses the risks that those controls will not prevent material misstatements, errors, or omissions in the financial statements. Risk acceptance or avoidance is limited to instances where
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6</strong></td>
<td>Senior management establishes risk tolerances relative to the importance of the related objectives and aligns risk tolerances with risk appetite. These risk tolerances are measurable and provides management with greater assurance that the municipality is operating within its risk appetite and provides higher degrees of comfort that the objectives will be achieved.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>7</strong></td>
<td>Processes are in place to ensure that risk identification considers both internal and external factors as well as their impact on the achievement of objectives.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>8</strong></td>
<td>Management groups the potential events into categories by aggregating horizontally across the municipality and vertically within operating units which reinforces a municipality – level portfolio view of events across the municipality.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>9</strong></td>
<td>Management categorizes events between those that potentially have a negative impact (risks) and those events that potentially have a positive impact (opportunities). Negative events are then considered by management for assessment and response. Potential events are channelled back into management’s strategy or objective-setting process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>10</strong></td>
<td>Management uses a common risk language when considering risks in terms of inherent risk and residual risk. Within its risk framework, the municipality considers risks in terms of likelihood of occurring and impact to the municipality. Management uses techniques like sensitivity analysis and scenario analysis to assess the impact of new or changed risks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>11</strong></td>
<td>The municipality's risk management policy requires participation in assessing, monitoring and controlling risk at all levels of the business. The policy documents in writing the objectives of assessing, monitoring and controlling business risks and identifies who within the municipality is</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
primarily responsible for achieving these objectives. The policy sends a clear message throughout the municipality that risk assessment and control is everyone’s job.

12 A cost-effective risk assessment process is in place, i.e., risk/control self-assessment techniques.

13 Senior management leads and is involved with the municipality’s risk assessment processes. Management takes appropriate action on results of risk assessment at process/activity level and monitors the actions taken.

14 Managers and process/activity owners throughout the municipality develop both effective early-warning systems to monitor changes in risk factors and support the continuous assessment of risk management strategies.

15 Appropriate risk management options are considered for significant risk, including risk avoidance (AVOID), risk transfer (e.g. insure, hedge, strategic alliances, joint ventures, contractual risk sharing provisions, etc.) (TRANSFER), risk reduction to an acceptable level (MITIGATE) or risk acceptance at present level (i.e., self-insure risk) (ACCEPT).

16 Policies for managing significant risks are approved by the Municipal Council and implemented under the direction of an executive committee and/or a senior executive reporting directly to the Municipal Manager. Risk responsible owners are allocated to new risks or changes in risks significant to the municipality on a timely basis.

17 Performance accountability is established at all levels for continuously improving risk controls. Performance appraisals and appropriate oversight and supervision reinforce significant entity-level risk management priorities and strategies. Performance expectations and measures are linked to the reward system.

Principle 8:
The municipality considers the potential for fraud in assessing risks to the achievement of objectives.

<table>
<thead>
<tr>
<th></th>
<th>Processes are in place to ensure that the municipality periodically performs an assessment of its exposure to fraudulent activity and how the operations could be impacted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Processes are in place to ensure that the municipality periodically performs an assessment of each of its operating locations potential exposure to fraudulent activity and how the operations could be impacted.</td>
</tr>
<tr>
<td>20</td>
<td>Processes are in place to ensure that the assessment of fraud risks considers opportunities for unauthorized acquisition, use, disposal of assets, altering the reporting records or committing other inappropriate acts.</td>
</tr>
</tbody>
</table>

Table 9: Risk assessment and management - COSO framework
<table>
<thead>
<tr>
<th>Control activities</th>
<th>1 LOA</th>
<th>2 LOA</th>
<th>3 LOA</th>
<th>Self-assessment of policies, procedures and processes – see matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 10:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The municipality selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Management determines which relevant business processes require control activities.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Control activities are well defined in the form of clearly articulated policies and documented procedures and processes. There is an appropriate balance of preventive and detective controls in place, with emphasis on preventive controls when appropriate. In addition, there is an appropriate balance between automated and manual controls, with emphasis on automated controls when appropriate.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Senior management involves appropriate risk/process owners in the design of new or improved risk control processes in accordance with the specifications inherent in management’s risk tolerances and risk management strategies.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Risk owners are required to report to senior management the status of risk control process design activities for significant risks to provide assurance that the specifications of defined risk tolerances and strategies are addressed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 People with sufficient relevant knowledge and skills are assigned to work on development of risk control processes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
For significant risks, senior management receives status reports on the risk control design process. Management takes appropriate action on the results of risk control design activities and monitors the actions taken.

| Principle 6: | Processes in place to ensure effective, economic and efficient use of all resources. |
| Principle 7: | Management segregates incompatible duties, and where such segregation is not practical, management selects and develops alternative controls. |

**Principle 11:**
The municipality selects and develops general control activities over technology to support the achievement of objectives.

| Principle 8: | Management selects and develops control activities that are designed and implemented to restrict access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats. |
| Principle 9: | Effective risk assessment is done for the criticality and sensitivity of computerized operations and identification of supporting resources. |
| Principle 10: | Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives. |
| Principle 11: | Effective data and program procedures are in place to prevent and minimize potential damage and interruption, including off-site storage of backup data as well as staff training, and hardware maintenance and management. |
| Principle 12: | The municipality has a process that requires regular back-up of computer files and testing of the back-up files to ensure proper functionality. |
The municipality deploys control activities through policies that establish what is expected and in procedures that put policies into action.

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>The municipality has policies and procedures addressing proper segregation of duties between the authorization, custody, and record keeping.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Management performs periodic review of policies and procedures to determine their continued relevance, and refreshes them when necessary.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>The municipality maintains policies and procedures to facilitate the recording and accounting of transactions in compliance with laws, regulations, and provisions of contracts and grant agreements.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 10: Control activities - COSO framework
<table>
<thead>
<tr>
<th>Information and communication</th>
<th>1 LOA</th>
<th>2 LOA</th>
<th>3 LOA</th>
<th>Self-assessment of policies, procedures and processes – see matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 13: The municipality internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Appropriate information is identified and captured to identify, assess and respond to risks and manage the business – this information is:
   i. Obtained from appropriate internal and external sources
   ii. Generated manually and electronically
   iii. Both formal and informal.

2. Knowledge and information about performance, opportunities, risk and risk management and control processes flow across functions, departments or divisions, as well as up and down the various levels of the municipality, e.g.:
   i. Environmental risks, strategy and municipal performance from senior management downwards
   ii. Process performance, risks and improvement opportunities from lower levels upwards
   iii. Continuous improvement and risk control information across business processes

3. Management establishes reports and acts on metrics of risk management process performance. For example:
   i. Defined metrics are linked to risks and risk control process performance;
   ii. Thresholds of values are decided for management attention
to guide reporting;

iii. Risk management reports are collected and aggregate risk data is analyzed by a risk management function;

iv. Results are communicated to senior management and the Municipal Council in response to the thresholds determined by management,

v. Conflicts on the implementation of risk management strategies are reported to senior management (i.e., the Municipal Manager and the Council) for resolution, and

vi. The status of corrective action to improve risk assessment and control processes is monitored.

4 Information quality is evaluated by management in terms of:
   i. Level of detail of the content – Is it at the right level of detail?
   ii. Timeliness – Is it there when needed?
   iii. Currency – Is it the latest information available?
   iv. Reliability – Is it accurate?
   v. Accessibility – Is it easy to obtain by those who need it?

5 Management accesses its information systems and ensures that they are designed and used to support business strategy. In addition, information systems are fully integrated into most aspects of the municipality’s operations.

6 Management uses information systems to improve the ability of the municipality to measure and monitor performance and present analytical information at the municipal-wide level.

Principle 14:

The municipality communicates with external parties regarding matters affecting the functioning of other components of internal control.
<table>
<thead>
<tr>
<th></th>
<th>Limits on risk taking are defined and communicated to appropriate risk managers and process/activity owners for significant risk areas, i.e., prudent limits are defined for transaction origination, decision making and/or risk taking authority in high risk areas to focus those business activities and establish a ceiling on the level of risk-taking.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Managers and key employees fully understand their respective responsibilities, including those relating to managing risk. All stakeholders in the business risk management process (e.g., the Municipal Council, senior management, risk management owners and business process owners) are able to freely communicate about risk issues.</td>
</tr>
<tr>
<td>9</td>
<td>There are processes in place to ensure that reported problems regarding products, services or other matters are addressed timely. Responsive staff process customer complaints, and the appropriate managers and process/activity owners are made aware of the nature of the reported concerns and actions taken to satisfy the customer.</td>
</tr>
</tbody>
</table>

Table 11: Information and communication - COSO framework
### Principle 16:

The municipality selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of risk and internal control are present and functioning.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>1 LOA</th>
<th>2 LOA</th>
<th>3 LOA</th>
<th>Self-assessment of policies, procedures and processes – see matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>There are processes in place to monitor the environment and internal business processes for new risks, i.e., management periodically assesses performance of processes for identifying, sourcing and measuring new risks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>There is a process for monitoring changes in municipality’s risk profile, i.e., management and process/activity owners periodically evaluates changes in the external environment (e.g., using industry analysis, market analysis, competitor analysis) and changes in business operations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Management sets targets for growth, and liquidity, and measures against them. Budgets are used as a risk management tool.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Municipal measures of value and performance (i.e., cost, quality and time) are linked to process-level performance measures for business processes that are critical to execution of value creation strategies.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Senior management monitors the performance of risk controls it has implemented in conjunction with business processes it has assumed responsibility to control, i.e., resource allocation process, municipality performance measurement process, shareholders communications process, etc. The objective of the monitoring process is to determine that the risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
control processes are operating as intended.

6 Defined boundaries and limits are enforced and monitored continuously through independent oversight, i.e., business processes/activities that are critical to the municipality as a whole are monitored to ensure compliance with limits are established for the municipality.

7 Senior management communicates on an ongoing basis the vital importance of effective risk management to all levels of the municipality. Managers and key employees understand that it is their job to develop effective risk management processes to reduce significant risks to acceptable levels. In this context, benchmarking risk management processes against best practices is encouraged and expected.

**Principle 17:**

The municipality evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the First Line of Assurance, as appropriate.

8 The municipality periodically evaluates internal controls, tests for compliance with Treasury requirements, and communicates the results of those evaluations to the 4th and 5th line of assurance.

9 Internal audit provides recommendations for improvements in internal control with management taking appropriate follow-up action.

10 Key managers and process/activity owners perform periodic self-assessments (surveys, facilitated meetings, etc.) and report the results to senior management if there are significant municipality-wide issues.

11 Internal audit activities are driven by a top-down risk assessment and are approved by senior management and the Municipal Council. The internal
audit function possesses the competence to assess risk management processes at the entity, business process and activity levels.

| 12 | Management takes appropriate action on the results of audit activities focused on the risk management process and monitors the actions taken. Management takes appropriate action on results of continuous improvement activities and monitors the actions taken. |

Table 12: Ongoing monitoring - COSO framework
29. **Assessment matrix for the control environment**

The template contains an abbreviated format of the control environment assessment, and should be completed by the first three lines of assurance. Each of the three lines of assurance needs to complete the three columns with a rating of between 1 and 5 using the maturity assessment below. Each line of assurance needs to complete their rating separately. When the total is aggregated, the aggregation will indicate the level of risk.

Maturity is assessed on the following scale:

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No formal processes in place</td>
</tr>
<tr>
<td>2</td>
<td>Process is documented, but not aligned with job descriptions and performance management</td>
</tr>
<tr>
<td>3</td>
<td>Process is documented, staff trained on process, job descriptions aligned with process responsibilities</td>
</tr>
<tr>
<td>4</td>
<td>Process has the ability to detect and report failures of the controls</td>
</tr>
<tr>
<td>5</td>
<td>Continuous monitoring and improving of the process</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key questions for the completion of the control environment analysis</th>
<th>Score the COSO guidelines according to the assessment matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First Line of assurance</strong> Did management design and implement processes to achieve the objectives?</td>
<td>1</td>
</tr>
<tr>
<td><strong>Second line of assurance</strong> Does the risk management function identify incidents of non-compliance and is it reported to the first line of assurance?</td>
<td>1</td>
</tr>
<tr>
<td><strong>Third line of assurance</strong> Did Internal Audit evaluate the design, implementation, and effectiveness of the processes implemented by management, as well as the effectiveness of risk management?</td>
<td>1</td>
</tr>
</tbody>
</table>

*Table 13: Assessment matrix - 17 principles of the COSO framework*
30. **Control environment risk assessment process**

Instructions

1. Distribute the assessment to the first three lines of assurance.
2. Each of the lines should then evaluate the standard against the assessment index, and complete the column under 1 LOA, 2 LOA or 3 LOA.
3. The Combined Assurance Champion will then aggregate the scores.
4. The aggregated score will be applied against the heat map to determine the risk.
5. The process should be repeated for the full questionnaire.

<table>
<thead>
<tr>
<th>Control environment</th>
<th>1 LOA</th>
<th>2 LOA</th>
<th>3 LOA</th>
<th>Self-assessment of policies, procedures and processes – see matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle:</td>
<td></td>
<td></td>
<td></td>
<td>Combined score</td>
</tr>
<tr>
<td>The municipality demonstrates a commitment to integrity and ethical values.</td>
<td>Rating is read from the assessment matrix above</td>
<td>Sum ( 1 LOD + 2 LOD + 3LOD)</td>
<td>1-4</td>
<td>5-7</td>
</tr>
<tr>
<td>1</td>
<td>Management expectations translate into a statement of beliefs, values, and standards of conduct that the staff exhibit daily. Formal code of conduct/policies communicate appropriate ethical/moral behavioural standards, addressing acceptable operational practices, conflicts of interest.</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

The heat map below indicates the relevant risk attached to the standard.

<table>
<thead>
<tr>
<th>Aggregate score</th>
<th>Colour coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 4</td>
<td></td>
</tr>
<tr>
<td>5 – 7</td>
<td></td>
</tr>
<tr>
<td>8 – 11</td>
<td></td>
</tr>
<tr>
<td>12 - 15</td>
<td></td>
</tr>
</tbody>
</table>
31. Introduction

In municipal strategy, whether defined in terms of a mission, vision and/or purpose, management sets out (with Municipal Council oversight) what the municipality aspires to achieve – explicitly establishing the municipality’s broad-based reason for being.

Management then sets strategic objectives, formulates strategy, and establishes related operational implications, performance criteria, compliance requirements and reporting objectives for the municipality.

While a municipality’s mission and strategic objectives are generally stable, its strategy and many related objectives are more dynamic and adjusted for changing internal and external conditions, and emerging risk scenarios. As they change, strategy and related objectives are realigned with strategic objectives.

Strategic objectives reflect management’s choice as to how the municipality will seek to create value for its stakeholders. In considering alternative ways to achieve its strategic objectives, management identifies and assesses risks associated with a range of strategy choices and consideration of their implications. This would be more evident in risk intelligent municipalities.

32. Defining risk management strategy

The right place for a municipality to start the design of its risk management strategy is to focus on the identification and management of strategic risks - those risks that are most consequential to a municipal’s ability to execute its strategy, achieve its operational objectives, and build and protect value.

33. Alignment between risk management and municipal objectives

Considering the definition above, an appropriate process of objective setting is a critical component of risk management. Risk management focuses primarily on:

a. Developing consistency of objectives and goals throughout the municipality;
b. Identifying key success factors and associated key risk indicators and risks;
c. Assessing the risks and making informed responses;
d. Implementing appropriate risk responses, and establishing needed controls; and
e. Timely reporting of performance and expectation.
Effective risk management provides reasonable assurance that a municipality’s reporting objectives are being achieved. Achieving reporting and compliance objectives is largely within the municipality’s control. But there is a difference when it comes to strategic and operational objectives, because their achievement is not solely within the municipality’s control. It is exposed to external events – such as change in government, mother of nature conditions, exchange rate fluctuations and oil prices – where an occurrence is beyond its control.

For strategic and operational objectives, risk management can provide reasonable assurance that management and, in its oversight role, the Municipal Council are made aware, in a timely manner, of the extent to which the municipality is moving toward achievement of these objectives.

Management must ensure that the municipality’s objectives align with the municipality’s risk appetite. Misalignment could result in not accepting enough risk to achieve the objectives, or conversely, putting the municipality’s survival at risk by accepting too much risk. Effective risk management does not dictate which objectives management chooses, but that management has a process that aligns strategic objectives with the municipality’s mission and that ensures the chosen strategic and related objectives are consistent with the municipality’s risk appetite, and risk bearing capacity.

See table 14 for an example of the alignment between the strategic plan and the risks.

The starting point is a Strategic Risk Assessment designed to identify a municipality’s strategic risks and related action plans to address those risks.

34. Tools and mechanisms

Effective good practice strategic risk assessment and management tools and mechanisms would include:

A return driven strategy methodology

The methodology is used to analyse the elements of a municipality’s strategy. It provides a systematic way and a common language for articulating and clarifying the municipality’s strategy and drive value creation. It also offers perspective on identifying risk areas in the strategy.

The municipal strategy is communicated in its annual Integrated Development Plan (IDP). Integrated Development Planning is an elaborate and collaborative planning process which produces a strategic plan designed to guide municipality to systematically eradicate backlogs of service delivery, encourage socio economic development, address spatial disparities of development, and deliver on agreed priorities with clearly defined outputs and targets within an agreed timeframe.
Key performance areas are fairly standardized across municipalities. See example 2 in this chapter for an example of how strategic objectives can be linked to key performance indicators, and how strategic objectives can be linked to strategic risks.

**Strategic risk management methodology**

This methodology is used to assess strategic risk and should be approved by the municipal manager, senior management and measured against best practices in risk management.

It provides a way to identify, link, and prioritize a municipality’s strategic risks, which can encompass a broad spectrum, including customer risk, innovation risk, operations risk, brand and reputation risk, partnering risk, supply chain risk, employee engagement risk, fraud risk, governance risk, financial markets risk, financial reporting risk and sustainability risk.

**Strategic risk maturity assessment**

This assessment is based on several streams of leading practices in risk management and provides a way to assess the maturity and development of risk management processes and capabilities in a municipality. It includes diagnostic questions for self-assessment. The risk maturity assessment could typically include matters relating to risk culture, risk strategy and appetite, risk governance and risk capacity and infrastructure measured over three categories of maturity:

**Strategic risk management alignment matrix**

This matrix provides a way to determine how well risk management is covered within a municipality allowing for identifying where gaps and redundancies exist. A strategic risk management alignment matrix could typically include the following:

<table>
<thead>
<tr>
<th>Risk category</th>
<th>Risk owner</th>
<th>Risk appetite metrics</th>
<th>Risk monitoring and reporting</th>
<th>Combined assurance</th>
<th>Council oversight</th>
<th>Audit Committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial risk - liquidity</td>
<td>Chief Financial Officer</td>
<td>Approved by Council</td>
<td>Ongoing monitoring and reporting</td>
<td>Quarterly reporting to Municipal Council</td>
<td>Continuous measurement of liquidity risks &gt; risk appetite</td>
<td>Oversight on effectiveness of risk and control processes</td>
</tr>
</tbody>
</table>

**Strategic GRC methodology**

A strategic GRC (Governance, Risk and Compliance) methodology provides an overview for aligning risk and control units in a municipality. CROs, CFOs and management teams have a great opportunity to help Municipal Councils and senior management build a municipality’s risk management processes that focuses on strategic risks and on aligning risk management and GRC initiatives based on an ongoing assessment of those risks.
35. Strategic risk assessment (SRA)

SRA is a systematic and continual process for assessing significant risks facing an organisation. In drafting a risk management strategy and implementation methodology, the right place to start is to focus on the identification and management of strategic risks – those risks that are most consequential to a municipality’s ability to execute its strategy, achieve its business objectives, and build and protect value.

This focus on strategic risk will also reinforce the direct relationship and critical link connecting the municipality’s strategy, strategy execution, and risk management processes. Strategic risk assessment is an important forerunner to determine the focus of operational and project risk assessments in the broader municipality. It will assist in determining the amount of resource to be allocated to further risk assessment and risk management effort, and where to allocate such resources.

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

During this process, the municipality’s risk appetite and risk bearing capacity should be considered. A key Council responsibility is to understand a municipality’s strategies and associated risks and to ensure that management’s risk management practices are appropriate and conducted to ensure the risk profile of the municipality remains within its risk thresholds. CFOs and management teams have a great opportunity to help council and senior management build risk management processes so that these are focused on strategic risks and on aligning risk management and GRC (Governance, Risk and Compliance) initiatives based on an ongoing assessment of those risks. SRA can provide a valuable foundation and first step for risk management and governance that will clarify and define the path to developing risk management capabilities for how risk is assessed, monitored, and managed.

The six steps for conducting a Strategic Risk Assessment can be summarised as follows:

a. Achieve a deep understanding of the strategic direction of the municipality;
b. Gather views and data on strategic risks;
c. Prepare a preliminary risk strategy;
d. Validate and finalise the risk strategy;
e. Develop a Strategic Risk Management Implementation plan; and
f. Communicate and implement the risk strategy and strategic risk implementation plan.
The following table provides one layout of a strategic risk register. Strategic risk registers should rather be produced on excel spreadsheet in a horizontal format (fragmented risk management units). If a municipality is already using software tools like BarnOwl or Teammate, it will be easier as the templates are part of the standardised design of the risk management software.

<table>
<thead>
<tr>
<th>Elements of strategic risk register</th>
<th>Strategic risk 1</th>
<th>Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic outcome</td>
<td>Financially sustainable municipality, well maintained assets</td>
<td>Obtained from the strategic plan</td>
</tr>
<tr>
<td>Risk description</td>
<td>Irregular expenditure</td>
<td></td>
</tr>
<tr>
<td>Risk category</td>
<td>Financial</td>
<td>Financial, operational or compliance - risk categories under the risk identification module</td>
</tr>
<tr>
<td>Root causes – internal</td>
<td>Over-riding of financial controls No second line of assurance No internal audit unit</td>
<td>Use the fishbone diagram to determine the potential root causes for the risk</td>
</tr>
<tr>
<td>Root causes – external</td>
<td>Political interference</td>
<td>Use the fishbone diagram to determine the potential root causes for the risk</td>
</tr>
<tr>
<td>Consequence</td>
<td>Cash flow pressure Weak current ratio Inability to borrow</td>
<td>Brainstorm the consequences should the risk materialise</td>
</tr>
<tr>
<td>Likelihood</td>
<td>5</td>
<td>Rate the likelihood of risk materialising on a level of 1 - 5</td>
</tr>
<tr>
<td>Impact</td>
<td>4</td>
<td>Rate the impact if risk materialises on a level of 1 - 5</td>
</tr>
<tr>
<td>Rating</td>
<td>20</td>
<td>Multiply likelihood and impact and rate risk according to the assessment scale</td>
</tr>
<tr>
<td>Risk response</td>
<td>Mitigation</td>
<td>Identify risk response – mitigate, avoid, accept or transfer</td>
</tr>
<tr>
<td>Control processes</td>
<td>Bid evaluation and adjudication processes.</td>
<td>Identify current processes in place</td>
</tr>
<tr>
<td>Control effectiveness</td>
<td>Ineffective</td>
<td>Rate the effectiveness of the risk</td>
</tr>
<tr>
<td>Residual risk</td>
<td>20</td>
<td>Calculate the remaining risk</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>Zero tolerance for irregular expenditure</td>
<td>Measure the residual risk against the risk appetite</td>
</tr>
</tbody>
</table>
Table 14: Strategic risk register layout

The example below is an indication of the different elements that should be included in the layout.

<table>
<thead>
<tr>
<th>Action plan</th>
<th>Implement accountability controls Allocate budget towards establishing risk management/ internal audit unit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible official</td>
<td>Municipal Manager</td>
</tr>
<tr>
<td>Due date</td>
<td>June 2017</td>
</tr>
</tbody>
</table>
Example 2: Linking strategic objectives with strategic risks

Strategic goal 5: Sufficient, affordable and well-run services

(a) Current state of affairs

Assess the current state of affairs for the basic services as it will inform the strategic plans for the new financial year.

<table>
<thead>
<tr>
<th>Basic Service</th>
<th>Minimum service level (% achieved)</th>
<th>Higher level service (% achieved)</th>
<th>Below minimum level services %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Water</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electricity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sanitation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Refuse removal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roads</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(b) Alignment with national and provincial plans and policies

Strategic Goal 5 aligns with the:

National Development Plan -
  - Chapter 4 (Economic infrastructure)

Integrated Urban Development Framework: 2016 -
  - Policy lever 2 (Integrated transport and mobility)
  - Policy lever 4 (Integrated urban infrastructure)

Medium-Term Strategic Framework: 2014-2019 -
  - An efficient, competitive and responsive economic infrastructure network

Western Cape's Provincial Strategic Plan -
  - Strategic Goal 4 (Enable a resilient, sustainable, quality and inclusive living environment)

(c) Applicable sector plan(s)

- Water Services Development Plan, March 2016
- Water Master Plan, 2008
- Pavement Management System, 2014
- Electricity Master Plan, 2015
(d) Results chain

**STRATEGIC OBJECTIVES**

4.1 A redesigned municipality structure that can effectively facilitate the long term strategy

4.2 Proactive succession and talent management that ensures consistent high levels of employee performance

4.4 More informed and effective ward councillors and ward committees

4.7 Sound long-term financial planning including making the right investment decisions

4.8 Sound financial management, budgeting and expenditure control

5.1 Secure sufficient long term bulk water provision

5.2 Maintenance and upgrading that sustain and improve the current condition of surfaced roads

5.3 Ensure sufficient civil services capacity for planned developments

5.4 Maintenance and upgrading that sustain and improve current condition of civil infrastructure

5.5 Ensure sufficient electricity capacity for planned developments

5.6 Maintenance and upgrading that sustain and improve the current condition of electrical infrastructure

5.7 Provide electricity cost effectively

2.2 Well located, serviced sites and premises available for commercial & industrial investors

**TARGET GROUPS**

Corporate Services

Financial Plan

Civil Engineering Services

Electrical Engineering Services

LED strategy

**MAIN BENEFITS**

Municipality

Increased value added and reduced exposure to risks, given the resources available

Development partners incl. public investors

The benefits of public investment / developments for society are maximised.

All business

Business utilise advantages to grow

Business investors (new)

More businesses invest & locate here to utilise opportunities

Home investors & new local consumers

More rate paying citizens re-locate to live here, to benefit from the citizen advantages.

**STRAEGIC GOAL**

RELIABLE, AFFORDABLE AND WELL-RUN SERVICES
### (e) Action Plan

<table>
<thead>
<tr>
<th>Strategic Objectives</th>
<th>Strategic Initiatives</th>
<th>Key Performance Indicators</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### (f) Strategic Risks linked to Strategic Goal 5

<table>
<thead>
<tr>
<th>Strategic Risk Description</th>
<th>Likelihood Impact</th>
<th>Inherent Risk Rating</th>
<th>Current Control Processes</th>
<th>Confirm process design and implementation</th>
<th>Rate control Effectiveness</th>
<th>Residual Risk exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ageing and poorly maintained infrastructure</td>
<td></td>
<td></td>
<td></td>
<td>Yes/ No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19 - 25</td>
<td>19 - 25</td>
<td>Annual Budget provision for maintenance, renewal, upgrading and refurbishment of existing obsolete networks and equipment;</td>
<td>19 - 25</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12 - 18</td>
<td></td>
<td>Monthly monitoring of losses;</td>
<td>12 - 18</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7 - 11</td>
<td></td>
<td>Indigent household incidents are monitored and addressed within a specific time period;</td>
<td>7 - 11</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 - 6</td>
<td></td>
<td>Maintenance plans for major infrastructure</td>
<td>1 - 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Updated and relevant master plans.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Availability or reliable and specialised equipment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Scheduled inspections</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Continuous monitoring of infrastructure capacity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Insurance of assets</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 7: Risk management strategy

36. Introduction

The implementation of the municipality’s risk management policy should be guided by a risk management strategy approved by the Municipal Council.

The risk management strategy is informed by the risk management policy and the municipality’s risk profile. For example, a risk profile with a high level of threat to objectives will require a more rigorous commitment to risk management. It is ironic, however, that those municipalities with a lower capacity and budget to deal with service delivery issues, also then have a higher threat of failure and risk. And therefore would not have the capacity to apply a more rigorous level of risk management. Such municipalities may need a sharply focused risk management strategy to assist the MM to deal with the most critical issues until such capacity is built.

A risk management strategy must be aligned with the municipality’s business strategy to outline a high-level plan on how risk management will be implemented, and it must be implemented by senior management and the executive demonstrating their buy-in and commitment. The risk management strategy should give an overview of the following to ensure sound and sustainable implementation of risk management at the appropriate level of complexity for the municipality:

a. The structure of risk management in the municipality regarding risk management components to be included in the risk management framework and towards what level of detail and maturity the municipality is striving;
b. The roles and responsibilities for risk management throughout all levels within the municipality;
c. The risk management process, methodologies, reporting and monitoring activities that will give effect to the risk management policy and strategy;
d. The monitoring and review of the risk management policy, processes and activities. Key milestones and outcomes must be included as well as the means in which these will be monitored and evaluated, such as key performance measures.

37. Developing a risk management strategy

When facilitating the development of the risk management strategy, the following should be considered:

a. Assessment of existing or possible future strengths and weaknesses affecting the implementation of risk management. Strength could be high-level commitment from the Council or the Municipal Manager, and a
weakness could be a lack of capacity or skilled resources for risk management.

b. A clear picture on what it entails to become a municipality with effective, efficient risk management, defined in terms of the vision and mission of a municipality in two to five years' time in terms of where it wants to be in the risk management space, how it proposes to get there and what can interfere with progress.

c. The goals and objectives that need to be achieved to give purpose to the vision and mission for risk management, and associated strategic actions in specific measurable, achievable detail – specific steps detailing resources and timeframes, taking into consideration where the a municipality finds itself as a point of departure.

d. Key strategies for different functional areas or business units to implement risk management. Having different business unit involved in the strategy development will improve buy-in and embedding risk management during implementation. Strategies must build on strengths and resolve weaknesses if they are to be achievable and effective.

e. Current and past performance of risk management in a municipality, both formal and informal, must be reviewed and taken into account when developing the risk management strategy to determine the direction, scope and areas of priority focus of risk management – i.e. clear understanding of the point of departure on this journey towards risk management excellence.

f. Perspectives of employees, investigating what employees feel the requirements for risk management include, how risk management can work for them, and what is required to ensure transparency and good communication of risk management.

g. The process of regularly reviewing and redefining the risk management strategy to ensure objectives are re-evaluated and possibly redefined in light of municipal changes.

h. The risk management strategy should include the following elements:

i. A plan of action to improve the municipality’s risk management maturity;
ii. A focus on the prevention of fraud and corruption;
iii. The municipality’s risk management architecture (structure and arrangements) and reporting lines;
iv. A description of the risk management methods and procedures;
v. User guidelines; and
vi. Details of review and assurance of the risk management process.

Documenting the risk management implementation plan also overcomes problems with changes in staff and is a good way of creating risk awareness and promoting a culture of risk management.

A risk management strategy should be facilitated by the Risk Management official (in larger municipalities fulfilling the role of Chief Risk Officer), and could ideally be
developed in a workshop format with Council and/or senior management. The following considerations may improve the efficiency and effectiveness of the workshop:

a. Buy in and commitment from all the role players;
b. Participation by all members of council and senior management and any staff responsible for risk management development and/or specialist risk areas in the municipality;
c. Focus on matters of strategic importance and not operational detail;
d. The discussion and planning must be realistic, relevant and proactive;
e. The current risk profile and management thereof must be considered;
f. Industry best practice must be discussed for the strategy to be aligned therewith; and
g. All decisions and strategic information must be recorded.

The risk management strategy should be documented comprehensively, made available and communicated to all employees – ideally as a one-page document, signed by the municipal manager. The development and implementation of a municipality’s risk management policy should be guided by a risk management strategy. As the risk management strategy gives high-level direction and commitment to risk management, the risk management policy contains further detail and infrastructure required for good risk management and support for the risk management strategy.

The risk management strategy should include a risk management implementation plan, in the form of a project plan and record the tasks, names of responsible persons and target dates.

38. Developing a risk management implementation plan

A municipal-wide risk management implementation plan, based on the risk management strategy and policy, should drive the integration of the management of risk at strategic, program and operational level, so that the levels of activity support each other. This plan is a well sequenced range of date-linked steps towards implementing the requirements specified in the risk management strategy and to some extent those contained in the fraud prevention plan. The risk management implementation plan is drafted once the risk management strategy and fraud prevention documents have been approved.

The following key steps need to be taken when developing the risk management implementation plan:

- Determine the risk management activities to be performed taking into account the risk profile and related costs versus the benefits;
- Determine the resourcing requirements, describing the capacity and competence of staff and the strategy to address capacity gaps, as well as the
technology and funding requirements to give effect to the risk management strategy;

- Determine the sequence of activities and the target implementation dates
- Assign ownership for and communicate risk management activities; and
- Agree on frequency and format of reporting - consensus should be obtained regarding the frequency, content and responsibility for reporting. (See Chapter 12 on risk management reporting).

The competition for management attention and resources requires that the sequence of activities should be founded on the principles of urgency, quick wins and sustainability of implemented risk mitigation strategies.

See example 3 for a typical example of a risk management implementation plan.

39. Conclusion

The risk management strategy and risk management implementation plan should ideally be developed together to ensure alignment and continuity. Both documents should be approved by the Municipal Manager and reviewed on an annual basis.
Example 3: Risk Management Implementation Plan

Purpose of this document

This document sets out the annual risk management implementation plan.

Objective

The primary objective of risk management implementation plan is to facilitate the execution of risk management. The risk management implementation plan for the municipality was prepared to give effect to the implementation of the risk management policy and strategy and sets out all risk management activities planned for the XXX financial year.

Approach

The development of the risk management implementation plan has taken into consideration:

- the risk management policy;
- the risk management strategy;
- available resources;
- urgency, quick wins and sustainability.

Detailed risk management implementation plan

<table>
<thead>
<tr>
<th>Planned Action</th>
<th>Detailed Actions</th>
<th>Outputs</th>
<th>Due date and responsible person</th>
<th>Progress to date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop a risk management policy</td>
<td>Risk Management Committee (RMC) to review the policy and recommend to the Municipal Manager and Municipal Council for approval.</td>
<td>Approved risk management policy</td>
<td>Chief Risk Officer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>dd/mm/yy</td>
<td></td>
</tr>
<tr>
<td>Planned Action</td>
<td>Detailed Actions</td>
<td>Outputs</td>
<td>Due date and responsible person</td>
<td>Progress to date</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------</td>
<td>---------</td>
<td>---------------------------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| Develop/ review risk management strategy | Develop ERM Implementation Framework  
Develop guidelines on roles and responsibilities for risk management  
Review Fraud Prevention Plan  
RMC to review the strategy and recommend to the Municipal Manager and Municipal Council for approval  
The CRO to develop the risk management unit structure and present it to the RMC to review and recommend for approval by the Municipal Manager and Municipal Council | Approved risk management strategy | Chief Risk Officer | dd/mm/yy |
<p>| Structures and responsibilities | | | | |
| Publication of Risk Management Policy | Publicise the policy on the intranet | Communicated risk management policy to | Chief Risk Officer | dd/mm/yy |</p>
<table>
<thead>
<tr>
<th>Planned Action</th>
<th>Detailed Actions</th>
<th>Outputs</th>
<th>Due date and responsible person</th>
<th>Progress to date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raising awareness and risk management training</td>
<td>Develop and formalise detailed training program/plan for all officials and any cost implications.</td>
<td>all officials in the municipality</td>
<td>Chief Risk Officer dd/mm/yy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Develop risk orientation program for new employees.</td>
<td>Completed orientation for all officials, RMC and Audit Committee members. All new employees orientated on risk management. Make presentations on risk management at management forums.</td>
<td>Chief Risk Officer dd/mm/yy</td>
<td></td>
</tr>
<tr>
<td>Terms of reference for the Risk Management Committee</td>
<td>Review existing RMC’s Terms of Reference and align to the RM strategy.</td>
<td>Approved risk management committee charter</td>
<td>Chief Risk Officer dd/mm/yy</td>
<td></td>
</tr>
<tr>
<td>Develop/ review risk management methodologies and processes</td>
<td>Development of a risk assessment protocol which includes risk quantification and risk ranking.</td>
<td>Approved risk assessment methodologies and processes</td>
<td>Chief Risk Officer dd/mm/yy</td>
<td></td>
</tr>
<tr>
<td>Facilitate enterprise-wide risk</td>
<td>Information gathering.</td>
<td>Approved strategic risk</td>
<td>Chief Risk Officer</td>
<td></td>
</tr>
<tr>
<td>Planned Action</td>
<td>Detailed Actions</td>
<td>Outputs</td>
<td>Due date and responsible person</td>
<td>Progress to date</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Development of risk response strategies</td>
<td>Drafting action plans for all gaps identified in addressing the top risks.</td>
<td>Action plans implemented per agreed milestone</td>
<td>Chief Risk Officer and each functional manager</td>
<td>Risk Owner dd/mm/yy</td>
</tr>
<tr>
<td>Drafting of individual key risk indicators for the top risks</td>
<td></td>
<td>Analysis report of key risk indicators per agreed frequency</td>
<td>Risk Owner dd/mm/yy</td>
<td></td>
</tr>
<tr>
<td>Assess risks controls effectiveness</td>
<td>Assign assurance providers to assess the controls of medium and low risks identified (monitored risks).</td>
<td>Combined assurance plan Report on risks controls assessed</td>
<td>Internal Audit dd/mm/yy</td>
<td></td>
</tr>
<tr>
<td>Ensure risk management processes and methodologies are reviewed independently.</td>
<td>Audit of risk management effectiveness.</td>
<td>Performance audit report Status reports on risk management</td>
<td>Internal / External Audits dd/mm/yy</td>
<td></td>
</tr>
<tr>
<td>Planned Action</td>
<td>Detailed Actions</td>
<td>Outputs</td>
<td>Due date and responsible person</td>
<td>Progress to date</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------</td>
<td>---------</td>
<td>--------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Facilitate the execution of ERM processes and infrastructure.</td>
<td>Implement appropriate risk reporting to the Municipal Manager, Exco, Audit Committee, RMC and Senior Management.</td>
<td>Approved progress reports: present progress reports to various stakeholders at various intervals.</td>
<td>Chief Risk Officer dd/mm/yy</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 8: Risk Management Policy

40. Introduction

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

It is important that the Municipal Manager sets the right tone for risk management in the municipality. Although all staff will be aware of the need to prevent loss and to safeguard stakeholders' interests, they may not be quite so clear about the municipality's standpoint on risk.

The municipality should operate within the terms of a risk management policy approved by the Municipal Manager. This is a statement that declares the municipality's commitment to risk management. The risk management policy should be communicated to all incumbent officials and arrangements should be made for communicating the policy to all new recruits.

The risk management policy outlines the municipality's commitment to protecting itself against adverse outcomes, which may impact negatively on service delivery. It will also confirm the municipality's commitment to legal and regulatory compliance.

A municipality’s risk criteria and thresholds along with the municipality’s overall intentions, direction and attitude towards risk should be defined by the risk policy (which is underpinned by the municipality’s risk management framework). The Municipal Manager is accountable for establishing and maintaining this policy.

A municipality’s risk management policy is the key internal governance mechanism to guide compliance to the appropriate level of risk management for all officials of the municipality.

The primary responsibility of the Risk Management official of a municipality, whether this is dedicated position of Chief Risk Officer, or whether it is included in the responsibilities of the Municipal Manager where the municipality is not yet at that maturity level, is to assist the municipality to structure and embed risk management and leverage its benefits to enhance performance.

With reference to the risk governance, this will more specifically include:

a. Working with senior management to develop the vision for risk management and risk management philosophy;

b. Developing, in consultation with management, the municipality's risk management framework incorporating:
i. Risk management strategy;
ii. Risk management policy;
iii. Risk management implementation plan;
iv. Risk identification and assessment methodology;
v. Risk appetite and tolerance; and
vi. Risk classification.

King III highlighted several key principles regarding risk governance, including:

   a. The ultimate responsibility for risk vests in the highest decision-making authority in municipality (Municipal Council) who will task the Municipal Manager to take responsibility for the design and implement a risk management policy and plan, and to ensure that the processes of risk management are implemented according to accepted risk management frameworks and guidelines.

   b. A municipality should set specific limits for the levels of risk the municipality is able to tolerate in pursuit of its objectives. The Council may also set limits regarding the risk appetite, i.e. those risk limits that the municipality desires, or is willing, to take. The limits are both financial and non-financial, and where the risk appetite limits exceed or deviate materially from the risk tolerance limits, this should be disclosed in the annual integrated report.

41. Deliverable

The risk management policy is a brief statement about the municipality's commitment to risk management. The practical implications thereof can be replicated in the risk management plan. It is advisable to publish and circulate the risk management policy to existing and new staff as part of the risk awareness strategy.

The objectives of the risk management policy must be clearly defined such so that is is possible to determine and report on the extent of compliance against the policy. It could typically include the following:

   a. Alignment of risk-taking behaviour with strategic business objectives;
   b. Promote a risk management culture across the municipality and improve risk transparency to the stakeholders;
   c. Maximise stakeholders value and net worth by managing risks that may impact the defined financial and performance drivers;
   d. The way in which conflicts of interest regarding risk management roles are dealt with;
   e. The way in which risk management performance will be measured and reported;
   f. A commitment to review and improve the risk management system periodically
   g. Assist the Municipality in enhancing and protecting those opportunities that represents the greatest service delivery benefits.
42. **Focus areas of a risk management policy**

The risk management policy acts as the primary internal risk governance mechanism, and as such it should provide all the guidance required for the broader municipality to practice sound risk management, therefore enabling the successful drafting of a risk management plan to implement risk management at the operational business level. In practical terms this should guide:

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

43. **Risk categories**

Risks originate from internal sources or from external sources. The table below provides guidance on typical risk categories of a municipality, which would also be reflected in its Risk Universe (see Chapter 4 section 6 for an example of a public sector risk universe).

Tools such as PESTLE and STEEP are typically used to determine the key internal and external drivers of risk, which could be used to determine and draft the risk categories of a municipality.

<table>
<thead>
<tr>
<th>Internal risks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Category</strong></td>
<td><strong>Human resources</strong></td>
</tr>
<tr>
<td>Risks that relate to human resources of municipality. These risks can have an effect on a municipality’s human capital with regard to:</td>
<td></td>
</tr>
<tr>
<td>Integrity &amp; Honesty;</td>
<td></td>
</tr>
<tr>
<td>Recruitment;</td>
<td></td>
</tr>
<tr>
<td>Skills &amp; competence;</td>
<td></td>
</tr>
<tr>
<td>Employee wellness;</td>
<td></td>
</tr>
<tr>
<td>Employee relations;</td>
<td></td>
</tr>
<tr>
<td>Retention; and</td>
<td></td>
</tr>
<tr>
<td>Occupational health &amp; safety.</td>
<td></td>
</tr>
</tbody>
</table>
| Knowledge and information management | Risks relating to a municipality’s management of knowledge and information. The following aspects relate to knowledge and information management:
  - Availability of information;
  - Stability of the information;
  - Reliability and integrity of information data;
  - Relevance of the information;
  - Retention; and
  - Safeguarding of data and information. |
| Litigation | Risks that the municipality might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from:
  - Claims by employees, the public, service providers and other third parties; and
  - Failure by a municipality to exercise certain right that is to its advantage. |
| Loss / theft of assets | Risks that a municipality might suffer losses due to either theft or loss of an asset of the municipality. |
| Material resources (procurement risk) | Risks relating to a municipality’s material resources. Possible aspects to consider include:
  - Availability of material;
  - Costs and means of acquiring / procuring resources; and
  - The wastage of material resources. |
| Information Technology | The risks relating specifically to the municipality’s IT objectives, infrastructure requirement, etc. Possible considerations could include the following when identifying applicable risks:
  - Security concerns;
  - Technology availability (uptime)
  - Applicability of IT infrastructure;
  - Integration / interface of the systems;
  - Effectiveness of technology; and
  - Obsolescence of technology. |
| Third party performance | Risks related to a municipality’s dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with a municipality. Non-performance could include:
  - Outright failure to perform
  - Not rendering the required service in time;
  - Not rendering the correct service; and
  - Inadequate / poor quality of performance. |
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health &amp; Safety</td>
<td>Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within the municipality.</td>
</tr>
</tbody>
</table>
| Disaster recovery and business continuity | Risks related to a municipality's preparedness or absence thereto to disasters that could impact the normal functioning of the municipality e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include:  
  * Disaster management procedures; and  
  * Contingency planning. |
| Compliance \ Regulatory          | Risks related to the compliance requirements that a municipality has to meet. Aspects to consider in this regard are:  
  * Failure to monitor or enforce compliance;  
  * Monitoring and enforcement mechanisms;  
  * Consequences of non-compliance; and  
  * Fines and penalties paid. |
| Fraud and corruption              | These risks relate to illegal or improper acts by employees resulting in a loss of the municipality's assets or resources and irregular expenditure. |
| Financial                         | Risks encompassing the entire scope of general financial management. Potential factors to consider include:  
  * Cash flow adequacy and management thereof;  
  * Liquidity and solvency;  
  * Financial losses;  
  * Fruitless and wasteful expenditure;  
  * Budget allocations;  
  * Financial statement integrity;  
  * Revenue collection; and  
  * Increasing operational expenditure. |
| Cultural                          | Risks relating to a municipality’s overall culture and control environment. The various factors related to municipality culture include:  
  * Communication channels and its effectiveness;  
  * Cultural integration;  
  * Entrenchment of ethics and values;  
  * Goal alignment; and  
  * Management operating style. |
<p>| Reputation                        | Factors that could result in the tarnishing of a municipality’s reputation, public perception and image. |</p>
<table>
<thead>
<tr>
<th>Risk category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic Environment</td>
<td>Risks related to the municipality's economic environment. Factors to consider include: • Credit downgrade; • Inflation; • Foreign exchange fluctuations; and • Interest rates</td>
</tr>
<tr>
<td>Political Environment</td>
<td>Risks emanating from political factors and decisions that have an impact on the municipality's mandate and operations. Possible factors to consider include: • Political unrest; • Local, Provincial and National elections; and • Changes in key office bearers.</td>
</tr>
<tr>
<td>Social environment</td>
<td>Risks related to the municipality's social environment. Possible factors to consider include: • Unemployment; and • Migration of workers.</td>
</tr>
<tr>
<td>Natural environment</td>
<td>Risks relating to the municipality's natural environment and its impact on normal operations. Consider factors such as: • Depletion of natural resources; • Environmental degradation; • Spillage; and • Pollution.</td>
</tr>
<tr>
<td>Technological environment</td>
<td>Risks emanating from the effects of advancements and changes in technology.</td>
</tr>
<tr>
<td>Legislative environment</td>
<td>Risks related to the municipality's legislative environment e.g. changes in legislation, conflicting legislation.</td>
</tr>
</tbody>
</table>

Table 15: Municipal Risk categories
44. How to draft a risk management policy

A risk management policy communicates the Municipality's stance with regard to risk management. The risk management policy is informed by the Municipality's risk profile, appetite for risk, loss tolerance levels, regulatory compliance expectations, safety and health demands, sustainability management, corporate governance requirements etc.

The risk management policy should:

- be drafted in consultation with key stakeholders;
- be reviewed at least annually to reflect the current stance on risk management;
- communicate the municipality’s risk management philosophy in the context of how risk management is expected to support the municipality in achieving its objectives;
- incorporate a statement committing the municipality to implementing and maintaining an effective, efficient and transparent system of risk management;
- define risk and risk management as they apply within the municipality’s particular context;
- spell out the objectives of risk management;
- outline the risk management approach; and
- identify the key role players and their responsibilities, such as:
  - Municipal Council;
  - Municipal Manager;
  - Risk Management Committee;
  - Audit Committee;
  - Management;
  - Other Officials;
  - Internal Audit;
  - External Audit; and
  - Chief Risk Officer.

See example 4 for a typical example of a risk management policy.
Example 4: Risk management policy

Purpose

Outline the purpose of the risk management policy.

Example:

The purpose of the risk management policy is to provide guidance regarding the management of risk to support the achievement of corporate objectives, protect staff and assets and ensure financial sustainability.

Scope

Specify who this policy applies to.

Example:

This policy applies to all municipal activities. It forms part of the governance framework and is applies to all employees, contractors and volunteers.

Risk Governance

Provide an overview of the risk governance structure of the municipality. Indicate who is involved in risk management and what their responsibilities are.

<table>
<thead>
<tr>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Council</td>
</tr>
<tr>
<td>Audit and Risk Committee</td>
</tr>
<tr>
<td>Municipal manager</td>
</tr>
<tr>
<td>Senior Managers</td>
</tr>
<tr>
<td>First line of assurance</td>
</tr>
<tr>
<td>Risk Manager</td>
</tr>
<tr>
<td>Second line of assurance</td>
</tr>
<tr>
<td>Internal audit</td>
</tr>
<tr>
<td>Third line of assurance</td>
</tr>
<tr>
<td>Staff and Contractors</td>
</tr>
</tbody>
</table>
**Risk Management Process**

Outline the steps involved in the risk management process. Make reference to the risk management procedure for practical guidance on the process.

**Example:**

When undertaking a risk management process the following steps must be taken:

I. establish the context,
II. identify the risk,
III. analyse the risk,
IV. evaluate the risk,
V. treat the risk; and
VI. monitor and review the risk.

Refer to the risk management procedure for details on how to perform each step in the process.

**Integration with other systems and processes**

Describe how risk management is integrated and embedded into municipal processes.

**Example:**

Risk management is factored into the strategic and operational planning, performance management, audit and assurance, business continuity management and project management processes of the municipality.

**Risk Categories**

Specify risk categories to be included in the risk register and in risk reporting.

**Example:**

Risk categories may include strategic, financial, environmental, safety, people and reputation.

**Risk Register**
Specify the purpose of the risk register. Include details on the types of risks to be included on the risk register (e.g. operational or strategic), the criterion for adding and removing risks from the register, who will review the risk register and how often it will be reviewed.

**Business Continuity and Disaster Recovery Plan**

Specify the details of the business continuity plan and the disaster recovery plan, and how management should deal with it.

**Fraud Prevention Plan**

Specify the details of the fraud prevention plan and how management should deal with it.

**Risk Reporting**

Outline the risk reporting requirements. The purpose of risk reporting is to create awareness of key risks, improve accountability for the management of risk and the timely completion of risk treatment plans. Details as to who prepares reports, who reviews reports and how often reports are reviewed should be included.

**Example:**

The strategic risk register is prepared by the Chief Risk Officer and reviewed by the Audit Committee on a quarterly basis.

**Risk Management Performance**

Outline how the performance of risk management will be measured. Measuring performance is a key monitoring activity to assess how effective risk management is at supporting corporate objectives.

**Example:**

Risk management performance indicators may include the number of internal audits completed per annum, the number of internal audit findings accepted by management, the timeliness of remediating internal audit findings, the reduction in the number of extreme risks in the risk register.

**Risk Appetite**

Articulate the municipality’s risk appetite through a risk appetite statement. The risk appetite statement influences and guides decision making, clarifies strategic intent and ensures choices align with the capacities and capabilities of the municipality.

**Example:**
There is no standard or universal risk appetite statement. Instead each municipality may choose to determine/select its risk bearing capacity in financial terms, which could then serve as it risk appetite. It could also choose to define its risk appetite statement in qualitative terms.

Inter-governmental and State Significant Risks

State the municipality's approach to identifying and managing inter-governmental and state significant risks.

Review and approval

State how often and who will review the risk management policy. Review of the risk management policy should take into the account progress made against the risk management improvement plan, which is a blueprint for how the risk management policy is implemented across the municipality.

References and related documents

<table>
<thead>
<tr>
<th>Associated policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management Improvement Plan</td>
</tr>
<tr>
<td>Risk Management Procedure</td>
</tr>
<tr>
<td>Risk Register</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>References/statutory references</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Treasury <em>Risk Management Framework</em></td>
</tr>
<tr>
<td>COSO Enterprise risk framework</td>
</tr>
<tr>
<td>ISO 31000</td>
</tr>
</tbody>
</table>
Chapter 9: Information technology

45. Introduction

Information and the technology that supports it represent a valuable asset. Successful institutions recognise the benefits of information technology and use it to drive their stakeholders’ value. These institutions also understand and manage the associated risks, such as increasing regulatory compliance and critical dependence of many business processes on information technology (IT).

The need for assurance about the value of IT, the management of IT-related risks and increased requirements for control over information are now understood as key elements of IT governance. Value, risk and control constitute the core of IT governance. IT governance is the responsibility of the municipal council and the municipal manager, and consists of the leadership, municipal structures and processes that ensure that IT sustains and extends the municipality’s strategies and objectives.

IT governance integrates and embeds good practices to ensure that IT supports the business objectives. IT governance enables the municipality to take full advantage of its information, thereby maximising benefits and capitalising on opportunities. These outcomes require a framework for control over IT that fits with and supports the COSO Internal Control - Integrated Framework, such as the widely accepted control CobIT framework for IT governance and risk management, and similar compliant frameworks.

IT governance includes the following focus areas:

a. **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with municipal operations.

b. **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.

c. **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.

d. **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the municipality.

e. **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.
46. **Boundaries of business, general and application controls**

The municipality’s system of internal controls impacts IT at three levels:

a. At the municipal management level, business objectives are set, policies are established and decisions are made on how to deploy and manage the resources of the municipality to execute the municipality strategy. The overall approach to governance and control is established by Council and communicated throughout the municipality. The IT control environment is directed by this top-level set of objectives and policies.

b. At the business process level, controls are applied to specific business activities. Most business processes are automated and integrated with IT application systems, resulting in many of the controls at this level being automated as well. These controls are known as application controls. However, some controls within the business process remain as manual procedures, such as authorisation for transactions, separation of duties and manual reconciliations. Therefore, controls at the operational process level are a combination of manual controls operated by the business and automated business and application controls. Both are the responsibility of the municipality to define and manage, although the application controls require the IT function to support their design and development.

c. To support the business processes, IT provides IT services, usually as a shared service to many business processes, as many of the development and operational IT processes are provided to the whole municipality, and much of the IT infrastructure is provided as a common service (e.g., networks, databases, operating systems and storage). The controls applied to all IT service activities are known as IT general controls. The reliable operation of these general controls is necessary for reliance to be placed on application controls. For example, poor change management could jeopardise (accidentally or deliberately) the reliability of automated integrity checks.

**IT General controls** are controls embedded in IT processes and services. Examples include:

a. Systems development;
b. Change management;
c. Security; and
d. Computer operations.

**IT Application controls** are embedded in business process applications and are commonly referred to as application controls. Examples include:

a. Completeness;
b. Accuracy;
c. Validity;
d. Authorisation; and
e. Segregation of duties.

Diagram 8 depicts the boundaries between business, general and application controls, i.e. which part of the municipality is responsible for which types of IT related risks and controls.
Diagram 8: Boundaries of business, IT general and IT application controls
Chapter 10: Risk identification and assessment

47. Introduction

Risk assessment is a systematic process to quantify or qualify the level of risk associated with a specific threat or event, to enrich the value of risk information available to the municipality. The main purpose of risk assessment is to help the municipality to prioritise the most important risks as the Municipality is not expected to have the capacity to deal with all risks in an equal manner.

Risk assessment provides an understanding of risks, their causes, consequences and their probabilities. This provides input to decisions about:

- a. whether an activity should be undertaken;
- b. how to maximise opportunities;
- c. whether risks need to be treated;
- d. choosing between options with different risks;
- e. prioritising risk treatment options; and
- f. the most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level.

48. The purpose of a risk assessment

The purpose of risk assessment is to provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options. Some of the principal benefits of performing risk assessment include:

- a. understanding the risk and its potential impact upon objectives;
- b. providing information for decision makers;
- c. understanding of risks, in order to assist in selection of treatment options;
- d. identifying the contributors to risks and weak links in systems and municipality;
- e. comparing of risks in alternative systems, technologies or approaches;
- f. communicating risks and uncertainties;
- g. assisting with establishing priorities;
- h. contributing towards incident prevention through post-incident investigation;
- i. selecting different forms of risk treatment;
- j. meeting regulatory requirements;
- k. providing information that will help evaluate whether the risk should be accepted when compared with pre-defined criteria.
49. The risk assessment process

Risks should be assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence on the particular objective(s) it is likely to affect. Risks should be expressed in the same unit of measure used for the key performance indicator(s) concerned. In simplified terms, there should be high correlation between key performance indicators and key risk indicators.

Risk assessment should be performed through a three stage process:

a. Firstly, the inherent risk should be assessed to establish the level of exposure in the absence of deliberate management actions to influence the risk;
b. Secondly, a residual risk assessment should be performed to determine the actual remaining level of risk after the mitigating effects of management actions to influence the risk; and
c. Thirdly, the residual risk should be benchmarked against the Municipality’s risk appetite to determine the need for further management intervention, if any.

Risk assessment should be strengthened by supplementing management’s perceptions of risks, inter alia, with:

a. review of the reports to the Audit Committee;
b. financial analyses, inclusive of liquidity and solvency analysis;
c. historic data analyses, which might include audit reports and incident reports and actual loss data;
d. interrogation of trends in key performance indicators;
e. benchmarking against municipality of the same nature and size;
f. market and economic sector information;
g. scenario analyses; and
h. forecasting and stress testing.

Risk assessments should be re-performed for the key risks in response to significant environmental and/or municipal changes, but at least once a year, to ascertain the shift in the magnitude of risk and the need for further management action as a result thereof.

The outline below summarises the steps of the risk management process. It normally comprises of five phases, namely:

Diagram 9: Risk management process
### Establish the context
Establishing context is about setting the parameters or boundaries around the risk appetite and risk management activities. It requires consideration of the external factors such as social, cultural, political and economic and the alignment with internal factors such as strategy, resources and capabilities. The risk manager will then need to establish context of the risk management processes which includes amongst other things establishing a risk management policy, processes, methodologies, plans, risk rating criteria, training and reporting processes.

### Identify the risk
Comprises of the processes for identifying, analysing and evaluating risks. Ideally, the municipality will utilise a range of risk identification techniques including brainstorming, work breakdown analysis, and expert facilitation.

### Analyse the risk
Risk analysis considers possible causes, sources, likelihood and consequences to establish the inherent risk. Existing management controls should be identified and effectiveness assessed to determine the level of residual risk.

### Assess the risk
After this analysis, an evaluation of the level of risk is required to make decisions about further risk treatment.

### Treat the risk
Where the level of risk remains intolerable, risk treatment is necessary. Risk owners can treat risks by avoiding the risk, treating the risk sources, modifying likelihood, changing consequences or sharing elements of the risk. The remaining level of risk retained should be within risk appetite.
50. Risk context

Risk analysis requires a thorough understanding of the risk context, including its internal and external environment and the purpose of risk management activity. It also includes assigning roles and responsibilities of various parts of the municipality participating in the risk management process. Understanding the external environment of a municipality involves looking at the impact of the social, cultural, regulatory and political activities when developing risk management criteria. In this way it is possible to prepare for external threats and take advantage of externally generated opportunities.

The internal context highlights a municipality’s culture, its internal stakeholders, municipality structure, and its human resource capabilities. It also looks at a municipality’s strategic goals, and its operational functions and processes involved in achieving its objectives. It further includes:

a. Policies, objectives, and the strategies that are in place to achieve them;
b. Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
c. Inter-dependencies of the various management systems, functions and activities of the municipality;
d. Information systems, information flows and decision-making processes (both formal and informal);
e. Relationships with, and perceptions and values of, internal stakeholders;
f. The municipality’s culture;
g. Standards, guidelines and models adopted by the municipality; and
h. Form and extent of contractual relationships.

This helps a municipality to set a strategic direction for risk management as a key component of the entire municipality’s operations. Establishing the context is not a once off step. It is ongoing as it ensures adaptability of municipal risk management to an ever changing internal and external environment.

51. Risk management context

Establishing the Risk Management Context involves determining the objectives, strategies, scope and parameters of the activities of the municipality. The management of risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk
management. The resources required, responsibilities and authorities, and the records to be kept should also be specified as part of the risk management context.

The risk management context will vary according to the needs of the municipality and can involve:

a. Defining the goals and objectives of the risk management activities;
b. Defining responsibilities for and within the risk management process;
c. Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;
d. Defining the activity, process, function, project, product, service or asset in terms of time and location;
e. Defining the relationships between a particular project, process or activity and other projects, processes or activities of the municipality;
f. Defining the risk assessment methodologies;
g. Defining the way performance and effectiveness is evaluated in the management of risk;
h. Identifying and specifying the decisions that have to be made; and
i. Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

52. Risk criteria

A municipality should define criteria to be used to evaluate the significance of risk. The risk criteria should reflect the municipality’s values, objectives and resources, and key measures of success, i.e. how a municipality will know that it is performing.

Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the municipality subscribes. Risk criteria should be consistent with the municipality's risk management policy, be defined at the beginning of any risk management process and be continually reviewed throughout the process.

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

a. The nature and types of causes and consequences that can occur and how they will be measured (consequence/severity levels in the risk rating methodology);
b. How likelihood will be defined (likelihood levels in the risk rating methodology);
c. The timeframes of the likelihood and/or consequences;
d. How the level of risk is to be determined (risk rating);
e. The views of stakeholders;
f. The level at which risk becomes acceptable or tolerable; and

Whether combinations of multiple risks should be taken into account (interdependency) and, if so, how and which combinations should be considered.
53. Risk Identification

Risk identification is a deliberate and systematic effort to identify and document the Municipality’s key risks. The objective of risk identification is to understand what is at risk within the context of the municipality’s explicit and implicit objectives and to generate a comprehensive inventory of risks based on the threats and events that might prevent, degrade, delay or enhance the achievement of the objectives. This necessitated the development of risk identification guidelines to ensure that municipalities manage risk effectively and efficiently.

54. The risk identification process

Comprehensive identification and recording of risks are critical, because a risk that is not identified at this stage may be excluded from further analysis. In order to manage risks effectively, a municipality has to know what risks they are faced with. The risk identification process should cover all risks, regardless of whether or not such risks are within the direct control of the municipality. The municipality should adopt a rigorous and on-going process of risk identification that also includes mechanisms to identify new and emerging risks timeously.

Risk identification should be inclusive, not overly rely on the inputs of a few senior officials and should also draw as much as possible on unbiased independent sources, including the perspectives of important stakeholders.

55. Risk workshops and interviews

Risk workshops and interviews are useful for identifying, filtering and screening risks but it is important that these judgment based techniques be supplemented by more robust and sophisticated methods where required, including quantitative techniques.

Risk identification should be strengthened by supplementing management’s perceptions of risks, inter alia, with:

- Review of external and internal audit reports;
- Financial analyses;
- Historic data analyses;
- Actual loss data;
- Interrogation of trends in key performance indicators;
Benchmarking against peer group or quasi peer group;
Market and sector information;
Scenario analyses; and
Forecasting and stress testing.

56. Focus points of risk identification

To ensure comprehensiveness of risk identification the municipality should identify risk factors through considering both internal and external factors, through appropriate processes of:

Strategic risk identification

Strategic risk identification to identify risks emanating from the strategic choices made by the municipality, specifically with regard to whether such choices weaken or strengthen the municipality's ability to execute its Constitutional mandate:

- Strategic risk identification should precede the finalization of strategic choices to ensure that potential risk issues are factored into the decision making process for selecting the strategic options;
- Risks inherent to the selected strategic choices should be documented, assessed and managed through the normal functioning of the system of risk management; and
- Strategic risks should be formally reviewed concurrently with changes in strategy, or at least once a year to consider new and emerging risks.

Operational risk identification

Operational risk identification to identify risks concerned with the Municipality’s operations:

- Operational risk identification should seek to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events;
- Operational risk identification should be an embedded continuous process to identify new and emerging risks and consider shifts in known risks through mechanisms such as management and committee meetings, environmental scanning, process reviews and the like; and
- Operational risk identification should be repeated when changes occur, or at least once a year, to identify new and emerging risks.

Project risk identification

Project risk identification to identify risks inherent to particular projects:

- Project risks should be identified for all major projects, covering the whole lifecycle of each project; and
For long term projects, the project risk register should be reviewed on a regular basis, such as quarterly and annually to identify new and emerging risks.

Although some projects may be multi-year projects, it remains important to continuously identify emerging issues that could have an impact on project objectives – either positive or negative. This could include internal risks such as a change in available resources, and external implications such as national policy or legislative changes that may have an impact on the project outcomes.

57. **How to perform risk identification**

It is crucial to have knowledge of the institutional environment before commencing with risk identification process. It is also important to learn from both past experience and experience of others when considering the risks to which a Municipality may be exposed and the best strategy available for responding to those risks.

Risk identification starts with understanding the Municipal objectives, both implicit and explicit. The risk identification process must identify unwanted events, undesirable outcomes, emerging threats, as well as existing and emerging opportunities. By virtue of a municipality’s existence, risks will always prevail, whether the municipality has controls or not.

When identifying risks, it is also important to bear in mind that "risk" also has an opportunity component. This means that there should also be a deliberate attention to identifying potential opportunities that could be exploited to improve municipal performance. In identifying risks, consideration should be given to risks associated with not pursuing an opportunity, e.g. failure to implement an IT system to collect municipal rates.

Risk identification exercise should not get bogged down in conceptual or theoretical detail. It should also not limit itself to a fixed list of risk categories, although such a list may be helpful.

The following are key steps necessary to effectively identify risks from across the municipality:

- Understand what to consider when identifying risks;
- Gather information from different sources to identify risks;
- Apply risk identification tools and techniques;
- Document the risks;
- Document the risk identification process; and
- Assess the effectiveness of the risk identification process.

58. **Understand what to consider when identifying risks**
In order to develop a comprehensive list of risks, a systematic process should be used that
starts with defining objectives and key success factors for their achievement. This can help
provide confidence that the process of risk identification is complete and major issues have not
been missed.

59. Gather information from different sources to identify risks

Good quality information is important in identifying risks. The starting point for risk identification
may be historical information about this or a similar municipality. Discussions with a wide
range of stakeholders about historical, current and evolving issues, data analysis, review of
performance indicators, economic information, loss data, scenario planning and the like can
produce important risk information.

Furthermore, processes used during strategic planning like Strength Weakness Opportunity
and Threat (SWOT) Analysis, Political Economic Social Technological Environment & Legal.
(PESTLE) Analysis and benchmarking will have revealed important risks and opportunities that
should not be ignored, i.e. they should be included in the risk register.

Certain disciplines like IT, Strategic Management, Health and Safety, etc. already have in
place established risk identification methodologies as informed by their professional norms and
standards. The risk identification process should recognize and utilize the outputs of these
techniques in order not to "re-invent the wheel".

60. Apply risk identification tools and techniques

A Municipality should apply a set of risk identification tools and techniques that are suited to its
objectives and capabilities, and to the risk the Municipality faces. Relevant and up-to-date
information is important in identifying risks. This should include suitable background
information where possible. People with appropriate knowledge should be involved in
identifying risks.

Approaches used to identify risks could include the use of checklists, judgments based on
experience and records, flow charts, brainstorming, systems analysis, scenario analysis, and
system engineering techniques.

- The approach used will depend on the nature of the activities under review, types of
  risks, the Municipal context, and the purpose of the risk management exercise.
- Team-based brainstorming for example, where facilitated workshops are used, is a
  preferred approach as it encourages commitment, considers different perspectives and
  incorporates differing experiences.
- Structured techniques such as flow charting, system design review, systems analysis,
  Hazard and Operability (HAZOP) studies and operational modelling should be used
where the potential consequences are catastrophic and the use of such intensive techniques are cost effective.

- Since risk workshops are useful only for filtering and screening of possible risks, it is important that the workshops are supplemented by more sophisticated or structured techniques described above.
- For less clearly defined situations, such as the identification of strategic risks, processes with a more general structure, such as 'what-if' and scenario analysis could be used.
- Where resources available for risk identification and analysis are constrained, the structure and approach may have to be adapted to achieve efficient outcomes within budget limitations. For example, where less time is available, a smaller number of key elements may be considered at a higher level, or a checklist may be used.

61. Document the risks identified

The risks identified during the risk identification are typically documented in a risk register that includes (at this stage):

- Risk description;
- How and why the risk can happen (i.e. causes and consequences); and
- The existing internal controls that may reduce the likelihood or consequences of the risks.

It is essential when identifying a risk to consider the following four elements:

- Description/event - an occurrence or a particular set of circumstances;
- Causes - the factors that may contribute to a risk occurring or increase;
- The likelihood of a risk occurring; and
- Consequences - the outcome(s) or impact(s) of an event.

It is the combination of these elements that make up a risk and this level of detail will enable a Municipality to better understand its risks.

62. Document your risk identification process

In addition to documenting identified risks, it is also necessary to document the risk identification process to help guide future risk identification exercises and to ensure good practices are maintained by drawing on lessons learned through previous exercises. Documentation of this step should include:
• The approach or method used for identifying risks;
• The scope covered by the identification;
• The participants in the risk identification; and
• The information sources consulted.

Experience has shown that management often disregards well controlled risks when documenting the risk profile of the Municipality. It is stressed that a well-controlled risk must still be recorded in the risk profile of the Municipality. The reason for this logic is that the processes for identifying risks should ignore at this point any mitigating factors (these will be considered when the risk is being assessed).

63. The outputs of risk identification

The document in which the risks are recorded is known as the "risk register" and it is the main output of a risk identification exercise.

A risk register is a comprehensive record of all risks across the municipality or project depending on the purpose/context of the register. There is no single blueprint for the format of a risk register and municipalities have a great degree of flexibility regarding how they lay out their documents.

The risk register serves three main purposes

• It is a source of information to report the key risks throughout the municipality, as well as to key stakeholders.
• Management uses the risk register to focus their priority risks.
• It helps the auditors to focus their plans on the municipality's top risks.

Once the risks have been identified, assessed and rated, and existing controls have been assessed, and it is has been established that controls are inadequate, a risk response strategy needs to be determined, i.e. an assessment, for example, of whether the risk is acceptable or whether it needs to be treated.
64. **Risk Analysis**

Risk analysis is a fundamental component of the risk management process. It helps to guide the evaluation of risks by defining the key parameters of the risk and how these may impact on the achievement of municipality's objectives.

One of the key outcomes of the risk assessment process is determining levels of risk exposure for the municipality. In addition, the data and related information collected during the risk assessment process can be used to assist in guiding risk response decisions.

65. **Risk Analysis Methods**

Methods used in analysing risks can be qualitative, semi-quantitative or quantitative. The degree of detail required will depend upon the particular application, the available data, the potential risks and the decision-making needs of the municipality, or if prescribed by legislation.

a. **Qualitative assessment**: defines consequence, likelihood and level of risk by significance levels such as “high”, “medium” and “low”, may combine consequence and likelihood, and evaluates the resultant level of risk against qualitative criteria. In qualitative analysis there should be a clear explanation of all the terms employed and the basis for all criteria should be recorded.

b. **Semi-quantitative methods**: use numerical rating scales for consequence and likelihood descriptions and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship and the formulae used can also vary.

c. **Quantitative analysis**: estimates numerical, practical values for consequences and their probabilities, and produces values of the level of risk in specific quantitative units. Full quantitative analysis may not always be possible due to insufficient data or information and often, due to the nature of the risk, the effort required of quantitative analysis is not warranted.

Even where full quantification has been carried out, it must be remembered that the calculations are estimates and they must not be attributed a level of accuracy and precision that is beyond the accuracy of the data and methods employed.
66. **Risk analysis techniques**

ISO 31010 lists several tools for risk analysis, but the more common ones are summarized below:

a. **Root Cause Analysis**

The analysis of a major loss to prevent its reoccurrence is referred to as Root Cause Analysis (RCA). It attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms. Corrective action may not always be entirely effective and continuous improvement may be required.

RCA is applied in various contexts with the following broad areas of usage:

i. *Safety-based RCA*: for accident investigations and occupational health and safety;
ii. *Failure analysis*: in technological systems related to reliability and maintenance;
iii. *Production-based RCA*: applied in the field of quality control in capital projects like the development of a new city bus service or road building;
iv. *Process-based*: focused on business processes;
v. *System-based*: developed as a combination of the previous areas to deal with complex systems with application in change management, risk management and systems analysis.

b. **Cause-and-effect analysis**

Cause-and-effect analysis identified possible causes of an undesirable event or problem and organises the contributory factors into broad categories so that all possible options can be considered. The information is organised in either a Fishbone (also called Ishikawa) or sometimes a tree diagram, and can be used as follows:

i. Provides a structured pictorial display of a list of causes of a specific effect. The effect may be positive (an objective) or negative (a problem) depending on context.
ii. Used consider all possible scenarios and causes generated by a team of experts and allows consensus to be established as to the most likely causes.
iii. It is most valuable at the beginning of an analysis to broaden thinking about possible causes that can be considered more formally late
iv. It allows for a structured way to identify root causes, and identifies six groups of root causes, namely:

- *Materials*, which includes lack of stock or medicines, lack of funding;
- *Machines*, which includes lack of equipment, or poorly designed application programs;
- *Methods*, which includes a lack of processes, or poorly designed processes;
- *Manpower*, which includes lack of staff or skills, management incompetence or high vacancy rates, poor ethical practices;
- *Measurements*, which include lack of dashboards, real-time monitoring of risks or lack of detection controls; and
• *Mother Nature*, which reflects on external risks or political interference.

c. **Decision tree analysis**

A decision tree represents decision alternatives and outcomes in a sequential manner which takes account of uncertain outcomes. It is similar to an event tree in that it starts from an initiating event or an initial decision and models different pathways and outcomes as a result of events that may occur and different decisions that may be made. It can be used as follows:

i. In managing project risks and to help select the best course of action where there is uncertainty; and

ii. For communicating decisions.

d. **Bow Tie Analysis**

Bow tie analysis is a simple diagrammatic way of describing and analysing the links within a risk from causes to consequences. A Bow Tie is similar to a combination of a fault tree analysing the causes of an event and an event tree analysing the consequences. It can be used as follows:

i. The focus of the bow tie is on the barriers between the causes and the risk, and the risk and consequences.

ii. Bow Ties show a range of possible causes and consequences.

iii. Bow tie analysis is often easier to understand than fault and event trees, and is a useful communication tool.

67. **Risk assessment**

Risk assessment involves interrogating risks at two levels, namely at the inherent risk level and the residual risk level, using the same rating criteria for each assessment.

Inherent risk considers the "worst case" scenario. This involves considering the likelihood and impact of the risk in the absence of any management control interventions. This level of assessment provides a perspective of the consequences of the risk to the municipality in its unmanaged state.

The second tier of assessment concerns establishing the residual risk. Residual risk is the level of risk remaining after the mitigating influence of the existing control interventions is
considered. Normally, management would introduce sufficient control to reduce the risk to within a pre-determined level, as informed by the optimal risk level. The residual risk is a critical indicator of whether the existing controls are effective in reducing the risk to an acceptable level.

When risks are assessed for the fragmented risk maturity status, the risks are assessed on a simplistic basis, as either high medium or low. When risk management has an integrated or risk intelligent status, risks are assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence (Risk = Likelihood x Impact).

When assessing risk for risk intelligent municipalities, additional risk criteria could be applied, such as the level of volatility of the risk (i.e. the rate at which the risk could change if not addressed and responded to). This will further facilitate decision-making regarding the urgency of addressing particular risks, i.e. including or excluding certain risks from a risk response strategy, depending on whether it will deteriorate or diminish over time.

The magnitude of the consequences of an event, should it occur, and the likelihood of the event and its associated consequences, should be assessed in the context of the effectiveness of the existing strategies and controls.

Consequences and likelihood may be estimated using statistical assessment and calculations. Where no reliable or relevant past data is available, subjective estimates may be made which reflect an individual's or Municipality's degree of belief that a particular event or outcome will occur.

When rating the impact it is important to consider factors such as:

a. The value of transactions that pass through the process;
b. The importance of the activity in terms of the entity achieving its objective;
c. The impact this may have on other processes within the entity;
d. The geographical dispersion of operations;
e. Ethical climate and pressure on management to meet objectives;
f. Financial and economic conditions - frequency of losses;
g. Competency, adequacy and integrity of staff;
h. Management information - key measurable indicators; and
i. Degree of information being processed on computerised information systems.

Impact ratings can be defined as:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Loss of ability to sustain ongoing operations. A situation that would cause a standalone business to cease operation.</td>
</tr>
<tr>
<td>Major</td>
<td>Significant impact on achievement of strategic objectives and targets relating to the IDP of the municipality.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Disruption of normal operations with a limited effect on the</td>
</tr>
</tbody>
</table>

137
achievement of strategic objectives or targets relating to the IDP.

<table>
<thead>
<tr>
<th>Minor</th>
<th>No material impact on achievement of the municipality’s strategy or objectives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
<td>Negligible impact.</td>
</tr>
</tbody>
</table>

Table 16: Inherent risk ratings

When rating the likelihood it is important to consider factors such as:

- Broad or vague legislative authority or regulations, missions, goals or objectives;
- High degree of complexity;
- Administration of contracts or grants;
- Liquidity of assets;
- Major restructuring of the municipality;
- Relationship with suppliers and customers;
- Life expectancy of the internal control area;
- Appropriateness of centralisation;
- Classified or sensitive material;
- Potential for conflict of interest; and
- Management responsiveness.

The ratings can be defined as:

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost certain</td>
<td>The risk is almost certain to occur more than once within the next 12 months. (Probability = 100% p.a.)</td>
</tr>
<tr>
<td>Likely</td>
<td>The risk is almost certain to occur once within the next 12 months. (Probability = 50 – 100% p.a.)</td>
</tr>
<tr>
<td>Moderate</td>
<td>The risk could occur at least once in the next 2 – 10 years. (Probability = 10 – 50% p.a.)</td>
</tr>
<tr>
<td>Unlikely</td>
<td>The risk could occur at least once in the next 10 - 100 years.</td>
</tr>
<tr>
<td>Rare</td>
<td>The risk will probably not occur, i.e. less than once in 100 years. (Probability = 0 – 1% p.a.)</td>
</tr>
</tbody>
</table>

Table 17: Likelihood ratings

The most relevant sources of information and techniques should be used when analysing consequences and likelihood. Sources of information should include:
a. Past records, both financial and operational;  
b. Audit reports from both internal and external auditors;  
c. Current legislation;  
d. Practice and relevant experience;  
e. Relevant published literature;  
f. Market research;  
g. The results of public consultation;  
h. Experiments and prototypes;  
i. Economic, engineering or other models; and  
j. Specialist and expert judgments.

Techniques that can be utilised will include:

a. Structured interviews with experts in the area of interest;  
b. Use of multi-disciplinary groups of experts;  
c. Individual evaluations using questionnaires; and  
d. Use of models and simulations.

Risk assessment should be performed in accordance with approved rating criteria for both likelihood and impact.

68. **Determine the inherent risk rating**

Once you have rated the likelihood and impact, combine the two to determine the overall risk rating.

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Almost certain</th>
<th>Likely</th>
<th>Moderate</th>
<th>Unlikely</th>
<th>Rare</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Insignificant</td>
<td>Minor</td>
<td>Moderate</td>
<td>Major</td>
<td>Catastrophic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Almost certain</th>
<th>Likely</th>
<th>Moderate</th>
<th>Unlikely</th>
<th>Rare</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likelihood</td>
<td>Insignificant</td>
<td>Minor</td>
<td>Moderate</td>
<td>Major</td>
<td>Catastrophic</td>
</tr>
</tbody>
</table>

Almost certain: 5 10 15 20 25
Likely: 4 8 12 16 20
Moderate: 3 6 9 12 15
Unlikely: 2 4 6 8 10
Rare: 1 2 3 4 5
RISK RATING:

The colour coding will then lead to risk rating, which is reflected below:

<table>
<thead>
<tr>
<th>Extreme</th>
<th>High</th>
<th>Moderate</th>
<th>Low</th>
</tr>
</thead>
</table>

Table 18: Heatmap – risk rating

Based on the risk assessment, risks are classified by level to determine the appropriate level of response to those risks. Specific responses are defined at the "Risk Response" phase.

69. Identify and evaluate existing control effectiveness

Controls may reduce the likelihood of occurrence of a potential risk, the impact of such a risk, or both. Management then needs to assess the control effectiveness based on their understanding of the control environment currently in place. Residual risk will therefore inform management of the actual level of control effectiveness.

Controls should be considered on the basis of:

a. Design effectiveness - is the control "fit for purpose" in theory i.e. is the control designed appropriately for the function for which it is intended; and

b. Operational effectiveness - does the control work as practically intended. It is useful to involve staff with an understanding of the controls when rating them. Internal audit, business analysts and operational/financial management can all provide input into control identification and assessment.

A well-designed and implemented control can often mitigate or reduce more than one risk or type of risk. Once effectiveness has been assessed, the residual risk rating can be calculated. Controls then need to be evaluated. The first step in the process of risk control evaluation is to determine the adequacy of an individual control. This adequacy can be determined by asking questions around the control’s design intent and purpose, its communication, whether performance parameters have been defined and whether the control requires continual maintenance.

The second step is to determine the effectiveness of the control, i.e. how well is it used, is the control available when required, is it used as intended, has it been checked/validated?

For each control identified the risk control effectiveness value of the control must be established and rated. This can be done using the generic table below:
<table>
<thead>
<tr>
<th>Risk Control Effectiveness</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully effective</td>
<td>Controls are well designed for the risk. Review and monitor existing controls.</td>
</tr>
<tr>
<td>Partially effective</td>
<td>Most controls are designed adequately and operate effectively. Address control weaknesses or improve operational efficiency.</td>
</tr>
<tr>
<td>Ineffective</td>
<td>A number of controls are not being used as intended, or not designed to treat the root causes of the risk.</td>
</tr>
<tr>
<td>Totally ineffective</td>
<td>Significant weaknesses in control design, with many gaps. Redesign controls with focus on detection controls.</td>
</tr>
<tr>
<td>None</td>
<td>Inadequate design of controls/no controls in place to mitigate risk.</td>
</tr>
</tbody>
</table>

Table 19: Effectiveness ratings

70. Reference to the maturity index

The risk maturity index provides some clarity on the risk assessment process for municipalities with different maturities, as seen in the table below:

<table>
<thead>
<tr>
<th>Risk assessment</th>
<th>Fragmented</th>
<th>Integrated</th>
<th>Risk intelligent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement</td>
<td>Risks are measured in green, yellow and red.</td>
<td>Risks are measured on a colour scale, and ranked with a consistent metric like likelihood and impact.</td>
<td>Quantitative probabilities and impacts are estimated, using ranges for uncertainty. Volatility of risks and the risk environment is taken into consideration in prioritizing risk response strategies.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Risks are aggregated and only measured on the worst case scenario, on an ad hoc basis.</td>
<td>Risks are aggregated for key performance objectives, business processes and/or risk universe categories.</td>
<td>Quantified probabilities and impacts allows for easy aggregation of risks across different dimensions and at any level of confidence using statistics.</td>
</tr>
</tbody>
</table>
One view of aggregated risk table is applied for Combined Assurance purposes.

**Table 20: Risk assessment per risk maturity index**

The risk assessment templates are therefore adjusted accordingly.

### 71. Assessing of risk – fragmented risk maturity

The risk assessment in a fragmented status allows for risk management on a simplistic basis, where risks are assessed and aligned with control processes. Risk management might even be performed by internal audit units. Effectiveness of control processes are evaluated by internal and external auditors, and the criteria for assessing risk and control is very basic (high, medium and low). There is no ability to calculate the risk appetite, or identify root causes for system failures. There is a very low correlation between key performance indicators and risk indicators. An example of such a risk register will have the following layout:

<table>
<thead>
<tr>
<th>Elements of operational risk register</th>
<th>Operational risk 1</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational objective</td>
<td>Financially sustainable municipality, well maintained assets</td>
<td>Obtained from the IDP</td>
</tr>
<tr>
<td>Risk description</td>
<td>Irregular expenditure</td>
<td></td>
</tr>
<tr>
<td>Risk category</td>
<td>Financial</td>
<td>Financial, operational or compliance - risk categories under the risk identification module</td>
</tr>
<tr>
<td>Inherent risk rating</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Risk response</td>
<td>Mitigation</td>
<td></td>
</tr>
<tr>
<td>Control processes</td>
<td>Bid evaluation and adjudication processes.</td>
<td>Identify current processes in place</td>
</tr>
<tr>
<td>Control effectiveness</td>
<td>Ineffective</td>
<td>Partially effective</td>
</tr>
<tr>
<td>Residual risk</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Action plan</td>
<td>Implement accountability controls Allocate budget towards establishing risk management/ internal audit unit.</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Responsible official</td>
<td>Municipal Manager</td>
<td></td>
</tr>
<tr>
<td>Due date</td>
<td>June 2017</td>
<td></td>
</tr>
</tbody>
</table>

Table 21: Operational risk register – fragmented status
### 72. Assessing of likelihood and consequence – integrated risk management

The risk assessment in integrated risk management allows for the identification of likelihood and impact of different risks, and the ability to integrate risks between different functions or responsibilities. Risk appetite is calculated, and residual risk is measured against the risk appetite. The risk exposure is reported to the 4th and 5th line of assurance as a matter of routine. An example of such a risk register will have the following layout:

<table>
<thead>
<tr>
<th>Elements of operational risk register</th>
<th>Operational risk</th>
<th>Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operational objective</strong></td>
<td>Financially sustainable municipality</td>
<td>Obtained from the strategic plan</td>
</tr>
<tr>
<td><strong>Risk description</strong></td>
<td>Irregular expenditure</td>
<td></td>
</tr>
<tr>
<td><strong>Risk category</strong></td>
<td>Financial</td>
<td>Financial, operational or compliance, etc</td>
</tr>
<tr>
<td><strong>Root causes – internal</strong></td>
<td>Over-riding of financial controls No second line of assurance</td>
<td>Use the fishbone diagram to determine the potential root causes for the risk</td>
</tr>
<tr>
<td><strong>Root causes – external</strong></td>
<td>Political interference</td>
<td>Use the fishbone diagram to determine the potential root causes for the risk</td>
</tr>
<tr>
<td><strong>Consequence</strong></td>
<td>Cash flow pressure Inability to borrow</td>
<td>Brainstorm the consequences should the risk materialise</td>
</tr>
<tr>
<td><strong>Likelihood</strong></td>
<td>5</td>
<td>Rate the likelihood of risk materialising on a level of 1 - 5</td>
</tr>
<tr>
<td><strong>Impact</strong></td>
<td>4</td>
<td>Rate the impact if risk materialises on a level of 1 - 5</td>
</tr>
<tr>
<td><strong>Inherent risk rating</strong></td>
<td>20</td>
<td>Multiply likelihood and impact and rate risk according to the assessment scale</td>
</tr>
<tr>
<td><strong>Risk response</strong></td>
<td>Mitigation</td>
<td>Identify risk response – mitigate, avoid, accept or transfer</td>
</tr>
<tr>
<td><strong>Control processes</strong></td>
<td>Bid evaluation/ adjudication processes.</td>
<td>Identify current processes in place</td>
</tr>
<tr>
<td><strong>Control effectiveness</strong></td>
<td>Effective</td>
<td>Rate the effectiveness of the risk</td>
</tr>
<tr>
<td><strong>Residual risk</strong></td>
<td>9</td>
<td>Calculate the remaining risk</td>
</tr>
<tr>
<td><strong>Risk appetite</strong></td>
<td>Zero tolerance for irregular expenditure</td>
<td>Measure the residual risk against the risk appetite</td>
</tr>
<tr>
<td><strong>Action plan</strong></td>
<td>Implement accountability controls Allocate budget towards establishing risk management</td>
<td></td>
</tr>
</tbody>
</table>
### Assessing of likelihood and consequence – risk intelligent management

The risk assessment in a risk intelligent environment allows for the identification of likelihood and impact of different risks, and the ability to integrate risks between different functions or responsibilities. Risk appetite is calculated, and residual risk is measured against the risk appetite. The future risk exposure is measured and reported to the 4\textsuperscript{th} and 5\textsuperscript{th} line of assurance as a matter of routine. In addition the second line of assurance monitors risk exposure on an ongoing preventative basis and inform management timely when a risk might materialise. An example of such a risk register will have the following layout:

<table>
<thead>
<tr>
<th>Elements of operational risk register</th>
<th>Operational risk 1</th>
<th>Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational objective</td>
<td>Financially sustainable municipality</td>
<td>Obtained from the strategic plan</td>
</tr>
<tr>
<td>Key performance indicator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk description</td>
<td>Irregular expenditure</td>
<td></td>
</tr>
<tr>
<td>Risk category</td>
<td>Financial</td>
<td>Financial, operational or compliance, etc</td>
</tr>
<tr>
<td>Root causes – internal</td>
<td>Over-riding of financial controls</td>
<td>Use the fishbone diagram to determine the potential root causes for the risk</td>
</tr>
<tr>
<td>Root causes – external</td>
<td>Political interference</td>
<td>Use the fishbone diagram to determine the potential root causes for the risk</td>
</tr>
<tr>
<td>Consequence</td>
<td>Cash flow pressure</td>
<td>Brainstorm the consequences should the risk materialise</td>
</tr>
<tr>
<td></td>
<td>Inability to borrow</td>
<td></td>
</tr>
<tr>
<td>Likelihood</td>
<td>5</td>
<td>Rate the likelihood of risk materialising on a level of 1 - 5</td>
</tr>
<tr>
<td>Impact</td>
<td>4</td>
<td>Rate the impact if risk materialises on a level of 1 - 5</td>
</tr>
<tr>
<td>Inherent risk rating</td>
<td>20</td>
<td>Multiply likelihood and impact and rate risk according to the assessment scale</td>
</tr>
<tr>
<td>Risk response</td>
<td>Mitigation</td>
<td>Identify risk response – mitigate, avoid, accept or transfer</td>
</tr>
</tbody>
</table>

#### Table 22: Operational risk register – integrated status
<table>
<thead>
<tr>
<th>Control processes implemented by management</th>
<th>Bid evaluation/ adjudication processes.</th>
<th>Identify current processes in place</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ongoing monitoring by risk management</td>
<td>Residual risk &gt; risk appetite, automated aggregation and reporting to management, audit committee and internal audit</td>
<td>Ongoing monitoring by risk management</td>
</tr>
<tr>
<td>Control effectiveness</td>
<td>Effective</td>
<td>Rate the effectiveness of the risk. Combined assurance, inclusive of independent assurance by internal audit</td>
</tr>
<tr>
<td>Residual risk</td>
<td>9</td>
<td>Calculate the remaining risk</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>Zero tolerance for irregular expenditure</td>
<td>Measure the residual risk against the risk appetite</td>
</tr>
<tr>
<td>Residual risk &gt; risk appetite</td>
<td></td>
<td>Calculating the risk exposure</td>
</tr>
<tr>
<td>Continuous monitoring by management</td>
<td>Reported as a key risk indicator, measured against the key performance indicator above</td>
<td>Preventative reporting – risk is reported to management before it actually materialise</td>
</tr>
<tr>
<td>Ongoing monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action plan</td>
<td>Implement accountability controls Allocate budget towards establishing risk management</td>
<td></td>
</tr>
<tr>
<td>Responsible official</td>
<td>Municipal Manager</td>
<td></td>
</tr>
<tr>
<td>Due date</td>
<td>June 2017</td>
<td></td>
</tr>
</tbody>
</table>

Table 23: Operational risk register – risk intelligent status
74. Document risk assessment process

Documentation of the risk assessment process provides a record of how risks were analysed in previous periods, thereby informing future risk assessment exercises and providing consistency in how risks are identified, assessed and how decisions are made regarding how risks are responded to. A key outcome of documenting the risk assessment process is enabling accurate tracking of risks over time using historical reference data.

Documentation should include:

- Key assumptions and limitations;
- Sources of information used;
- Explanation of the assessment method, and the definitions of the terms used to specify the likelihood and consequences of each risk;
- Existing controls and their effectiveness;
- Description and severity of consequences;
- The likelihood of these specific occurrences; and
- Resulting level of risk.

Detailed documentation may not be required for very low risks; however a record should be kept of the rationale for initial screening of very low risks, for example, in a volatile environment where risks of low severity may change due to changing circumstances.

75. Risk assessment considerations

There are a number of other issues that must be considered in the context of risk assessment, which are noted below:

a. The risk assessment tables need to be consistently applied for all key risks in the municipality.
b. Certain disciplines, for example, IT and Health and Safety, may utilise assessment methodologies that are informed by their professional norms and standards. In such circumstances, it would be prudent for the sake of the operational efficiency of these disciplines to allow them to use their preferred methodology. However, in order to maintain consistency at the municipal level the same risks should be re-assessed in terms of the municipality-wide risk assessment methods.
c. The results of risk assessment could be represented in 'heat maps'. These are a simple graphical representation of each risk according to the two scales, namely likelihood and impact.
d. Assessment of likelihood more often than not imposes a challenge to management. Guidance in this respect can be obtained from the historical experience of the municipality, as well as the experience of a similar municipality.
e. The assessments must be considered together with the municipality's risk appetite to determine whether the risk is acceptable or not. This in turn will inform whether additional interventions will be required.
76. Outputs

The output of risk assessment is a more sophisticated risk register which is enriched by the addition of ratings for each risk. This allows management to separate the more important risks from the less important ones and direct management attention accordingly.

77. Risk evaluation

The decision-making criteria should have been specified at the beginning of the risk management process and there may be other specific criteria mandated by legislation. Where risks are accepted ‘as is’ it is important to note any factors that may escalate them upwards, and hence require a response (consideration of the volatility of the risk and the risk environment). The decision about whether and how to treat the risk may depend on the costs and benefits of taking the risk and the costs and benefits of implementing improved controls. Following evaluation, risks can be divided into five bands as can be seen in the table below:

<table>
<thead>
<tr>
<th>Risk index</th>
<th>Risk magnitude</th>
<th>Risk acceptability</th>
<th>Actions proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 – 25</td>
<td></td>
<td>Unacceptable</td>
<td>Take action to reduce risk with highest priority</td>
</tr>
<tr>
<td>15 – 19</td>
<td></td>
<td></td>
<td>Take action to reduce risk – inform management</td>
</tr>
<tr>
<td>10 – 14</td>
<td></td>
<td>Acceptable</td>
<td>Limited or no risk reduction, control and monitor, report to line manager.</td>
</tr>
<tr>
<td>5 – 9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 – 4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 24: Risk index
78. **Treat the risk - risk response**

A key outcome of the risk identification and assessment process is a detailed list of all key risks including those that require treatment as determined by the overall level of the risk against the municipality's risk tolerance levels. However, not all risks will require treatment as some may be accepted by the municipality and only require occasional monitoring throughout the period.

Although all key risks identified should be responded to, not all these risks will require treatment. The risks that fall outside of the municipality's risk tolerance levels are those which pose a significant potential impact on the ability of the municipality to achieve set objectives and therefore require treatment.

The purpose of responding to and treating risks is to minimize or eliminate the potential impact the risk may pose to the achievement of set objectives.

Risk response is concerned with developing strategies to reduce or eliminate the threats and events that create risks. Risk response should also make provision for the exploitation of opportunities to improve the performance of the municipality. Responding to risk involves identifying and evaluating the range of possible options to mitigate risks and implementing the chosen option. Management should develop response strategies for all material risks, whether or not the management thereof is within the direct control of the municipality, prioritising the risks exceeding or nearing the risk appetite level.

Where the management of the risk is within the control of the municipality, the response strategies should consider:

a. Avoiding the risk by, for example, choosing a different strategy or terminating the activity that produces the risk;
b. Treating the risk by, for example, implementing or improving the internal control system;
c. Transferring the risk to another party more competent to manage it by, for example, contracting out services, establishing strategic partnerships or buying insurance;
d. Accepting the risk where cost and strategy considerations rule out alternative strategies; and
e. Exploiting the risk factors by implementing strategies to take advantage of the opportunities presented by such risk factors.
In instances where the management of risk is not within the control of the municipality, the response strategies should consider measures such as forward planning and lobbying. Response strategies should be documented and the responsibilities and timelines attached thereto should be communicated to the relevant persons.

79. Developing a risk response strategy

Risk response plans identify responsibilities, schedules, the expected outcome of responses, budgets, performance measures and the review process to be set in place.

The risk response plan usually provides detail on:

a. Actions to be taken and the risks they address;
   b. Who has responsibility for implementing the plan;
   c. What resources are to be utilized;
   d. The budget allocation;
   e. The timetable for implementation; and
   f. Details of the mechanism and frequency of review of the status of the response plan.

80. How to respond to risks?

Responding to risks involves the following key steps, each of which is covered in detail in this section:

a. Identify risk response options;
   b. Select risk response options;
   c. Assign risk ownership;
   d. Prepare risk response plans; and
   e. Identify risk response options.

Identify risk response options

Risk response design should be based on a comprehensive understanding of how risks arise. This includes understanding not only the immediate causes of an event but also the underlying factors that influence whether the proposed response will be effective.

Risk response options are not necessarily mutually exclusive or appropriate in all circumstances. They should include the following:

a. Avoiding risk – not engaging in the activity that creates risk exposure;
   b. Mitigating risk – applying procedures that reduce the risk;
   c. Transferring risks – transferring the risk exposure to other parties who may be better equipped or positioned to deal with it;
d. Exploiting risk – exploiting risks that represents an otherwise potential missed opportunity;
e. Accepting risk – accepting a risk with a low level of exposure;
f. Terminating risk – stopping the activity that gives rise to a risk higher than the acceptable level; and
g. Integrating some risks – applying some or all of the risk response to address a risk.

Select options for response

Once risks have been assessed and a level of risk rating has been assigned, an option for response is selected. Consideration should be given to the cost of the response option as compared to the likely risk reduction that will result.

For example, if the only available response option would cost in excess of R10m to implement and the cost impact of the risk is only R5m, it may not be advisable. If the risk volatility, however, is such that it may rapidly increase to exceed R10M, then this may become a viable decision.

In order to understand the costs and benefits associated with each risk response option, it is necessary to conduct a cost-benefit analysis.

Basic cost benefit analysis includes:

- Defining or breaking down the risk into its elements by drawing up a flowchart or list of inputs, outputs, activities and events;
- Calculating, researching or estimating the cost and benefit associated with each element. (Include, if possible, direct, indirect, financial and social costs and benefits); and
- Comparing the sum of the costs with the sum of the benefits.

Assign risk ownership

The Municipal Manager allocates responsibility for risk to an operational or functional area line manager.

Risk owners nominated by the Municipal Manager should assume responsibility for developing effective risk response plans. The risk owner (the person accountable for managing a particular risk) should be a manager with sufficient technical knowledge about the risk and/or risk area for which a response is required.

The risk owner will often delegate responsibility (but not accountability) to his/her direct reports or consultants for detailed plan development and implementation. Once the options have been brainstormed and assessed, a risk treatment plan will be developed. This can be a stand-alone plan, or additional columns on the risk register.

The process for developing the treatment plan is as follows:
a. Include the risk description and its risk rating in terms of consequence, likelihood and the overall rating.
b. List the treatment actions that were decided on following the risk treatment options discussion
c. Allocate a risk treatment owner who will take responsibility for the overall risk treatment.
d. Specific actions or tasks need to be determined to ensure the development of the Treatment Actions, i.e. the detailed steps.
e. Owners for the detailed actions or tasks need to be appointed
f. Resources that are required for achieving the tasks need to be determined, including financial, human and technical resources
g. The reporting requirements of progress with the completion of the tasks and actions need to be specified
h. Progress comments need to be made as part of the monitoring of the treatment action plan.

An example of a template is shown below:

<table>
<thead>
<tr>
<th>Risk description:</th>
<th>Risk rating:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Treatment action</td>
<td>Treatment owner</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Template 3: Treatment of risk**

**Prepare response plans**

Once response options for individual risks have been selected, they should be consolidated into risk action plans and/or strategies.

As one risk response may impact on multiple risks, response actions for different risks need to be combined and compared so as to identify and resolve conflicts between plans and to reduce duplication of effort.

Response plans should:

- Identify responsibilities, schedules, the expected outcome of responses, budgets, performance measures and the review process to be set in place include mechanisms for assessing and monitoring response effectiveness, within the context of individual responsibilities;
• Determine processes for monitoring response plan progress against critical implementation milestones aligned with the municipality’s objectives. This information should all arise from the response design process; and
• Document how the chosen options will be implemented practically.

The successful implementation of the risk response plan requires an effective management system that specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against specified criteria. Communication is a very important part of response plan implementation.

81. Opportunities versus threats

Measuring both the downsides and upsides of risk-taking provides a context that can be used to determine the type and amount of resources needed to support any project. Favourable outcomes, as projected by strategic planners and executive management, require a metric that is meaningful to the municipality. For example, the risk should be measured in terms of its impact on service delivery.

A benefit of measuring risks as a group is that analysing the range of possible outcomes against what was actually achieved may also provide executive management with insights into individual operational performance capabilities.

To be sure, the benefits of identifying and assessing both risks and opportunities at the same time might seem obvious, yet it is rarely practiced. One reason is that the two most widely used tools currently employed in Enterprise Risk management (ERM) risk assessment are the risk register and risk heat map. The focus of both of these is only the perceived threats to a municipality - they provide no consideration of the positive value that could be created by taking risks.

Risk registers and risk maps have value under certain circumstances. Based on our research and analysis, we conclude that:

• If the municipal goal is to respond only to known and identified threats, and the ERM process is viewed as an extension of audit and compliance, risk registers and risk heat maps can be useful.
• If the municipal goal is to respond to known threats and opportunities and gain risk intelligence about emerging perils on the horizon, traditional risk registers and risk heat maps fall short.
• If the municipal goal is to grow service delivery and create value for stakeholders, traditional risk registers and risk heat maps are useless.
• A new tool is required to measure both risks and opportunities. One example of such a tool is the Value Map – displayed below. Here both the threats and the opportunities are displayed.
A Sample Value Map

A Value Map is a graphical illustration of both threats and opportunities. Because threats and opportunities are two sides of the same coin, a value map also has two sides, as illustrated above. Threats (negative outcomes) are plotted on the left side of the map, while opportunities (positive outcomes) are located on the right side. Those outcome values may be measures of successful service delivery or a project's net present value, for example.

The vertical axis shows the relative likelihood of an event happening. Rather than plotting a single point on a risk map, the value map illustrates the range of the magnitude of each situation.

The net value of threat(s) versus opportunity(ies) could then be determined, for example, for pursuing a particular municipal strategy.
Chapter 11: Risk Appetite and Risk Tolerance

82. Introduction

Enterprise risk management enables management to identify, assess, and manage risks in the face of uncertainty, and is integral to value creation and preservation, which should lie at the core of a municipality’s strategy. All entities face uncertainty, and the challenge for management is to determine how much uncertainty it is prepared to accept as it strives to grow stakeholder value. This level of uncertainty a municipality is prepared to accept, is termed it risk appetite. There is a distinct relationship between an entity’s risk appetite and its strategy. A municipality must consider its risk appetite at the same time it decides which goals or operational tactics to pursue. Usually any of a number of different strategies can be designed to achieve desired growth and return goals, each having different risks.

Risk intelligent municipalities will apply and align both principles of risk appetite (strategic) and tolerance (operational), based on the municipality’s risk bearing capacity.

Municipalities express risk appetite as the level of risk they will accept in providing value to their stakeholders. It is not always efficient or possible to manage risks to zero residual risk or a very low residual risk threshold because of the time, cost and effort that will be required, and which could result in the cost-benefit dynamics to become skewed. On the other hand it is also poor management practice to accept risks which create unnecessary exposure for the municipality.

If a municipality is making decisions regarding their credit control policy and the implementation of a cut and collect process, the risk appetite might be a collection rate of 85% and a current ratio of 1,5:1. This means that failing to collect 15% of outstanding debtors will still allow a municipality to pay its short term creditors. Risk tolerance however, determines that if a municipality only collects 78% of their debtors, the current ratios will deteriorate to 0,9:1, which is creating a material uncertainty to operate as a going concern.

The COSO ERM framework sets out five principles related to risk appetite:

a. It is a guidepost in strategy setting;
b. It influences resource allocation;
c. It aligns the municipality with people, processes, and infrastructure;
d. It reflects the entity’s risk management philosophy and influences the culture and operating style; and
e. It is considered in strategy setting so that strategy aligns with risk appetite.

When developing the risk appetite for a municipality, there are a number of considerations that come into play, including:

a. The existing risk profile, as an indication of the risks it currently addresses;
b. The municipality’s capacity to take on extra risk in seeking its objectives;
c. The municipality’s attitude towards growth, risk and return; and
d. The acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives.

Given the aforementioned dynamics it is important for the municipality to make an informed decision on the amount of risk the municipality is capable of bearing as part of normal management practice. This level of acceptable risk is known as a “tolerated risk” or “tolerance level” and establishes the benchmark for the municipality's risk tolerance. This differs from risk appetite which is the amount of residual risk that a municipality is willing accept. More often than not, risk appetite in a municipality is set as the total impact of risk a municipality is willing to accept regardless of whether it has the necessary capacity to recover from such impact. It would be more prudent and risk intelligent for a municipality to define its risk appetite to remain within its risk bearing capacity. Risk appetite differs from municipality to municipality and can equally differ in terms of various categories of risk a municipality may face at a point in time.

The aim of defining risk tolerance is to get people to think effectively about risk when they make important decisions. Performance management systems encourage officials to think about targets and rewards for meeting them. However the systems should equally tell officials about what management wants and what it does not want. In essence, effective risk taking that is aligned to overall municipal strategy should be a core skill and competency, especially in a risk intelligent municipality.

Tolerance levels may vary by context and are influenced by the following:

- Ability and willingness of the Municipal Manager to take and manage risks;
- Size and type of municipality;
- Skills and experience of officials;
- Maturity and sophistication of risk management processes and control environments;
- The current level of a municipality's performance;
- The liquidity of a municipality and its ability to pay short term liabilities and operational expenditure; and
- The solvency of the municipality and its ability to withstand significant impact on its net asset value.

83. Approach

A municipality’s risk appetite should be reviewed annually to align it to new circumstances. The risk appetite should also be visited during the six-monthly adjustment budget process. Specific attention should be given to determine whether revenue collection estimates are still achievable, and to what extent under collection of revenue will influence liquidity and its effect on the risk appetite.

The risk tolerance levels should also be reviewed annually together with the municipality’s targets and the budget to determine the municipality’s risk bearing capacity. In addition it is important for management to be explicit about the bare minimum levels of performance. Failing to deliver on the bare minimum service requirements will affect the consumer’s willingness to
pay for services, and consequently might lead to non-payment and increased liquidity risk. Legal risk becomes more relevant in these cases and contingent liabilities normally increase as consumers and suppliers take legal action against the municipality.

It is advisable to determine and communicate the level of unexpected losses that the municipality is willing to accept in the event the risk materializes. These levels should be documented and communicated to all key stakeholders involved in the management of the risk. Zero tolerance risk exposures such as fraud and corruption, regulatory compliance unauthorised and irregular expenditure and health safety should be determined and communicated to all officials.

As management decisions are informed by targets being pursued, there should be a mechanism in place, which enables tracking of numbers involved to ensure that tolerance guidelines are complied with or applied as specified. This may require management to determine key risk drivers and to monitor performance in relation to actual risk event occurrences. Setting risk tolerance will assist management to monitor events and their impact against the stated risk appetite.

There is no "one-size fits all" approach to establishing the right risk tolerance levels. Practices will differ amongst municipality based on the maturity of the risk management practice, available data, management expertise, sector specific dynamics and other pertinent factors. Thus it is advisable to rather follow certain guiding principles rather than "hard and fast" rules.

A municipality’s risk appetite should be articulated and communicated so that staff understand that they need to pursue objectives within acceptable limits, as well as the extent to which these can be pursued, i.e. understand that there are limits involved, and how to apply to make decisions regarding the pursuit of their objectives and still remain within the municipal risk appetite.

A risk appetite statement effectively sets the tone for risk management. The municipality is more likely to meet its strategic goals when its appetite for risk is linked to operational, compliance and reporting objectives. A risk appetite statement is useful only if it is clear and can be communicated, interpreted and implemented across the municipality. It therefore should:

a. Directly link to the municipality’s objectives;
b. Be stated precisely enough so that it can be communicated throughout the municipality, can be monitored, and can be adjusted over time;
c. Help with setting acceptable tolerances for risk, thereby identifying the parameters of acceptable risk;
d. Facilitate alignment of people, processes, and infrastructure in pursuing municipal objectives within acceptable ranges of risk;
e. Facilitate monitoring of the competitive environment and considers shareholders’ views in identifying the need to reassess or more fully communicate the risk appetite
f. Recognise that risk is temporal, volatile and relates to the time frame of the objectives being pursued;
g. Recognise that the municipality has a portfolio of projects and objectives, as well as a portfolio of risks to manage, implying that risk appetite has meaning at the individual objective level and at the portfolio level.

Risk tolerance relates to risk appetite but differs in one fundamental way: risk tolerance represents the application of risk appetite to specific objectives. Risk tolerance can be defined as the acceptable levels of variation relative to the achievement of objectives.

While risk appetite is broad, risk tolerance is tactical and operational. Because risk tolerance is defined within the context of objectives and risk appetite, it should be communicated using the metrics in place to measure performance. Risk tolerance is best measured in the same units as the related objectives, and associated performance criteria. In that way, risk tolerance sets the boundaries of acceptable performance variability.

The typical steps involved in establishing and implementing risk tolerance are:

- Complete an analysis of the municipality's ability to physically and financially recover from a significant event (e.g. risk such as human influenza pandemic, inability to supply, credit crunch, etc.).
- The above analysis will highlight the need and importance of contingency plans, financial, physical and human resources and the importance of controls. From the analysis, determine the tolerance the municipality can bear or accept.
- Management determines the level of tolerance which should then be endorsed by the Municipal Manager.
- The risk tolerance levels set by the municipality will be reflected in the risk rating scales used to assess the risks:
  - An upper band where adverse risks are intolerable, whatever benefits the activity may bring, and risk reduction measures are essential whatever their cost.
  - A middle band (or 'grey' area) where costs and benefits are taken into account and opportunities balanced against potential adverse consequences.
  - A lower band where positive or negative risks are negligible, or the costs associated with implementing treatment actions outweigh the costs of the impact of the risk should it occur.

These levels of risk tolerance will help determine the type and extent of actions required to treat risks, and the level of management attention required in managing and monitoring the risks.

Risk tolerance levels can be practically defined through colour coding of a risk likelihood/consequence matrix. The principle applied in this instance is that if a risk is placed on the high risk colour coding (red) then additional controls have to be implemented to address the risk or rather the risk treatment plan has to be revised. On the contrary if the risk is placed on low risk colour coding (green) there is no need to effect any changes to how the risk is treated. Threshold limits may be set for individual risks or per risk category. This however does not affect the role of the third line of assurance in providing assurance on the effectiveness of controls.
84. Calculating risk appetite

Risk appetite statements often start out broad and become more precise as they cascade into functions and operations across the municipality. Some municipalities find that broad qualitative statements crafted around terms such as “low”, “medium” and “high” appetite meet their requirements. Others are more precise, making more quantitative statements like “we are not comfortable with a current ratio of smaller than 2:1 as it will prevent us achieving our service delivery objectives”.

Quantitative approaches could be built on more sophisticated metrics like economic value at risk and/or financial strength at risk. Common methods for expressing risk appetite include:

a. Setting a boundary on a probability and impact grid;
b. Economic capital measures/balance sheet-based expressions;
c. Changes in credit ratings (headroom before a potential downgrade);
d. Profit and loss measures (e.g. tolerable level of annual loss);
e. Value based measures (based on probability of ruin or default);
f. Limits/targets or thresholds for key indicators (e.g. +/- 5% variation in profit or 1 - 2.5% variation in revenue);
g. Qualitative statements (e.g. zero tolerance for regulatory breaches or loss of life)

The table below indicates some of the metrics that can be used for different risk types:

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Metric</th>
<th>Risk tolerance range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>Going concern issues</td>
<td>Zero tolerance</td>
</tr>
<tr>
<td></td>
<td>Minimum service delivery levels</td>
<td>80-90%</td>
</tr>
<tr>
<td></td>
<td>Own revenue growth</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>Indigent growth</td>
<td>0</td>
</tr>
<tr>
<td>Financial, credit and liquidity risk</td>
<td>Current ratio</td>
<td>1.5 to 2 : 1</td>
</tr>
<tr>
<td></td>
<td>Debt impairment</td>
<td>&lt; 10%</td>
</tr>
<tr>
<td></td>
<td>Debtors collection days</td>
<td>75 days</td>
</tr>
<tr>
<td></td>
<td>Creditor payment days</td>
<td>60 days</td>
</tr>
<tr>
<td></td>
<td>Reliance on government grants</td>
<td>&lt;20%</td>
</tr>
<tr>
<td>Operational risk</td>
<td>Vacancy rate</td>
<td>&lt; 10%</td>
</tr>
<tr>
<td></td>
<td>% High risk control issues</td>
<td>&lt;10%</td>
</tr>
<tr>
<td></td>
<td>% Ineffective controls – assessed by both internal/external audit</td>
<td>&lt;5%</td>
</tr>
<tr>
<td></td>
<td>% cyber incidents with high impact</td>
<td>0</td>
</tr>
<tr>
<td>Compliance risk</td>
<td>Unauthorised expenditure</td>
<td>&lt; 5%</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>Fruitless and wasteful expenditure</td>
<td>&lt; 5%</td>
</tr>
<tr>
<td></td>
<td>Irregular expenditure</td>
<td>&lt; 5%</td>
</tr>
<tr>
<td>High impact non-compliance issues</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Assurance on effectiveness</td>
<td></td>
<td>90%</td>
</tr>
<tr>
<td>Reputational risk</td>
<td>Retention of key managers</td>
<td>&gt;80%</td>
</tr>
<tr>
<td></td>
<td>Customer satisfaction – delivery protests</td>
<td>&gt;85%</td>
</tr>
<tr>
<td></td>
<td>Legal, regulatory and ethical events</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 25: Risk tolerance

Which type of statement is best for a particular entity is a management decision. As a municipality become more experienced in risk management, they can start moving away from broad low, medium and high statements, to statements that are more precise.

85. Risk tolerance statements

Some tolerances are easy to express in qualitative terms. For example, a municipality may have a low risk appetite for non-compliance with laws and regulations and may communicate a similarly low tolerance for violations — for example, a zero tolerance for some types of violations and slightly higher tolerances for other types of violations. Or tolerance may be stated in quantitative terms. A municipality could state that it relies on the reliability and disaster recovery of their computer systems so that the probability of computer failure is less than 0.01%.

Other examples include:

a. A municipality targets water leakage maintenance at 98% within 2 hours, with acceptable variation in the range of 97%-100% of the time;
b. It targets minimum competency accreditation at 90%, with acceptable performance of at least 75%;
c. It expects staff to respond to all customer complaints within 24 hours, but accepts that up to 25% of complaints may receive a response within 24-36 hours.

Potential risk events that could cause these performance levels not be achieved, would need to be managed responded to, to bring the potential impact within acceptable tolerance levels.
86. **Graphical depiction of risk appetite**

The following is an example of a “Risk Heat Map” indicating Risk Appetite and Risk Tolerance levels.

![Risk Heat Map Diagram](image)

**Diagram 11: Graphical depiction of risk appetite and risk tolerance**

The table below depicts how a municipality may define risk appetite for various categories of risk. This is illustrated in the examples of a risk matrix or heat map (see Diagram 11, and Report 2).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>13 - 25</td>
<td>High</td>
<td>Risk exceeds the risk acceptance level and requires urgent and immediate management attention to bring it within the acceptable level. Controls require substantial redesign, or a</td>
</tr>
</tbody>
</table>
greater emphasis on proper implementation

<table>
<thead>
<tr>
<th>9 - 12</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk exceeds the tolerance level, but within the acceptable level and requires proactive management to bring it within tolerable level. Controls require some redesign or more emphasis on proper implementation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1 - 8</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks that are below the tolerance level and do not require active management, but require active monitoring. Controls are adequately designed and may require close monitoring to maintain the risk within a tolerable level</td>
<td></td>
</tr>
</tbody>
</table>

Table 26: Risk rating parameters

General guiding principles for development of risk tolerance:

a. Risk tolerance should be expressed in the same indicators as its related objectives;
b. In setting the risk tolerance management should consider the relative importance of the related objective;
c. Tolerance levels should not be out of line with the materiality framework of the Municipality;
d. Without exception, all tolerance levels should be supported by rigorous analysis and expert management judgement;
e. Tolerances may be established for individual material risks, as well as aggregate tolerance for particular categories of risk;
f. Tolerances may also be established per individual business activity;
g. Risk tolerance levels should be revised as more reliable information becomes available;
h. Setting risk tolerance should be a collective senior management responsibility; and
i. Risk appetite is developed at the Municipal level by senior management and proposed to the Municipal Manager for approval. Once approved, it is communicated to all within the Municipality, including staff and key stakeholders.

87. Communication of risk appetite

Three approaches for communicating risk appetite include:

a. Expressing overall risk appetite using broad statements;
b. Expressing risk appetite for each major class of municipality objectives; and

c. Expressing risk appetite for different categories of risk. Some municipalities use broad, generic risk categories, such as economic, environmental, political, staff, or technology, in their risk appetite statements. Others use more tailored risk categories that apply to their field.
88. **Risk targets**

Risk tolerances may be accompanied by a risk target. A risk target is a desired level of risk that the municipality believes is optimal to meet its objectives. This often can be some level within the risk tolerance boundaries, possibly depicted along a risk/reward curve. Implicit in the risk tolerance and risk target concepts are reviews to determine the suitability, adequacy and effectiveness in operating within the boundaries at the desired target levels.

Monitoring changes from the expected outcomes is vital for risk tolerance statements to be meaningful. Unexpected or unacceptable deviations should trigger further analysis and action, including escalation to senior management.

As with appetite, a municipality’s risk tolerance generally is driven by its objectives and stakeholder expectations, ranging from value protection (generally lower tolerance levels) to value creation (generally higher tolerance levels). Tolerances are also highly dependent on how well capitalized or financed the municipality is.

The output is a clearly defined tolerable level of risk established through a rigorous process of analysis and expert management judgement. Depending on the nature of risk, the tolerance may be expressed either in qualitative or quantitative terms.

In some instances, risks as assessed would exceed the tolerance level, but cannot be avoided (e.g. matter of national priority). In this case, these risks will have to be approved by Municipal Manager and regularly monitored.

The advantage of working within clearly defined risk tolerance levels assists with avoiding the danger of over controlling risks.
Chapter 12: Communication and Reporting

89. Introduction

Risk management reporting is the regular provision of appropriate risk and risk management information to stakeholders and decision-makers within a municipality in order to support understanding of risk management issues and to assist all officials in performing their duties within the municipality.

Relevant information, properly and timeously communicated to and amongst relevant stakeholders, is essential in order to equip such stakeholders with the means to identify, assess and respond to risks, enabling decision-making at all levels.

Reporting on risk management performance will also provide the necessary confidence that the municipality is managing its risks to a satisfactory level.

Stakeholders need to be informed of the level of performance of risk management through reporting on the extent to which:

a. the risk exposure of the municipality is improving over time;
b. the municipality is meeting its risk management compliance requirements;
c. the right balance of risk taking and risk mitigation is achieved;
d. the municipality is operating within its risk bearing capacity; and
e. the risk management of the municipality is adding value by impacting positively on service delivery.

90. Implementing an efficient and effective risk management reporting system

It is important that risk reporting demonstrates that the municipality is managing its key risks and applying the most appropriate level of risk management maturity relevant to its exposure to threats, as well as its capacity, skills and budget for risk management.

This requires a municipality to determine and communicate risk reporting arrangements to all stakeholders. A clearly defined risk reporting structure is essential to facilitate effective communication among stakeholders in the risk management process. Used effectively, risk reporting pinpoints key areas of concern of the municipality which would require further attention.

An example would be a report highlighting where controls are:

- *Inadequate*, which in essence indicate a lack of or poorly designed controls;
- *Ineffective*, which indicates that staff and management is not applying the controls that have been designed; and
• *Excessive* and where they may be reduced to enable deviation of resources to areas where controls may be less adequate. Excessive controls are costly and add to the red-tape that prevent effective and efficient service delivery.

Common language, consistent form of reporting and collaboration among stakeholders are critical to ensuring that risk reports are effectively utilised to drive municipal performance. It is also crucial that risk reporting is not only a bottom up approach. While risk reporting is meant to aid managers to make risk-based decisions, it is equally important for such information and decisions to be communicated to operational staff.

Effective information and communication is intended to support enhanced decision making and accountability through:

a. Relevant, timely, accurate and complete information; and
b. Communicating responsibilities and actions.

When deciding on information and communication protocols, the following should be considered:

i. Understanding clearly the needs and requirements of each stakeholder group. This would include agreeing with them the manner, content and form in which the information should be communicated and the frequency of reporting;

ii. To what extent existing reporting channels can be utilised to transmit the required information rather than creating new channels.

Various internal and external data and information sources could be used to source information for reporting. Furthermore, this information could be in quantitative and qualitative form. The challenge for management is to process and refine large volumes of data into relevant and actionable information, and to keep historical records of analysis, trends and decisions. This challenge can be overcome by implementing an information system to source, capture, and process, analyse and report relevant information.

91. **Information systems for risk reporting**

The use of an on-line information system facilitates the real-time ongoing analysis, monitoring and reporting of risks, enabling more effective decision-making to achieve optimal effectiveness and efficiency in the management of risk.

The use of the risk management software will enable management to obtain "real time" information for decision making. This will also enhance monitoring activities. Technology may provide the necessary audit trail that could be used by risk owners and assurance providers to determine whether controls are working effectively, including whether target dates for action plans are being fully complied with.

An on-line information system would also provide the following further benefits:
a. **Infrastructure**: Enhance the infrastructure for reporting key information, particularly that used by the Municipal Council and senior management to identify, monitor and manage risks.

b. **Decision-making**: Improve the decision-making processes throughout the municipality by improvement in the flow of risk information.

c. **Legal entity & global**: Enhance the management of information across legal entities, while facilitating a comprehensive assessment of risk exposures at the consolidated level.

d. **Reduce losses**: Reduce the likelihood and consequence/severity of losses resulting from risk management weaknesses (including under-capacitated risk management functions and/or low levels of maturity).

e. **Timeliness**: Improve the speed at which information is available and decisions can be made.

f. **Strategic planning**: Improve the municipality’s quality of strategic planning and the ability to manage the risk associated with new products and services due to the analytical capacity of on-line information systems.

Although technology may provide value to risk reporting, it is important that processes around risk reporting are properly designed before implementation of technology is considered.

Whether or not automated or manual processes are used it is advisable to have customised reports as an early warning system. A risk dashboard can be used to expedite the flow of critical information to enhance decision-making. Supplementary information can be included in more detailed reports such as progress with risk management implementation, incident reports, and emerging risk reports.

The quality of risk reporting is dependent on a fully functioning risk management system. Incomplete or unreliable risk identification, assessment, prioritisation and treatment outputs will reflect in poor reporting outputs.

There is no single risk report that meets the needs of all stakeholders. Reports should be developed and customised to reflect the needs and preferences of the target audience and its purpose. Input from stakeholders must be obtained before implementing a risk reporting solution, as this should be part of existing reports and reporting frameworks.

Customised risk reports need to be sent to different stakeholder groups to meet their needs throughout the year. Avoid providing too much or too little information in risk reports. Senior Management and the Municipal Council will typically prefer a summary of risks and risk trends, focusing on high risk and strategic issues across the municipality, while those involved in managing specific risks will require detailed information covering their areas of responsibility.

Some of the considerations for implementing effective risk reporting are outlined below:

| Inter-linkage of information | Information needs to flow between risk data aggregation and risk reporting and across the municipality. This is achieved through strong risk data aggregation capabilities, and sound infrastructure and governance. |

166
Risk data aggregation and risk reporting practices cannot exist in isolation.

Simultaneous adoption

All risk data aggregation and risk reporting principles should be met simultaneously. If trade-offs or exceptions are to be made, it must be ensured that these do not materially impact risk management decisions.

Materiality

Materiality related to the level of importance of risk information.

In applying materiality, considerations that must be taken into account go beyond the number or size of the exposures and the type of risks involved. The potential future impact of the information excluded from the decision-making process must be taken into account and the omissions of information must be explained and verifiable.

Forward-looking and early warnings

Forward-looking reporting capabilities need to be developed to provide early warnings of any potential risks that may exceed the risk tolerance/appetite.

These risk reporting capabilities should also allow for effective stress testing providing forward-looking risk assessments to anticipate problems.

Incomplete data

Expert judgment may be required where data is incomplete data or results need to be interpreted.

Reliance on expert judgment in place of complete and accurate data should occur only on an exception basis, and should not have an impact on compliance with the principles. When expert judgment is applied the process must be clearly documented and transparent so as to allow for independent review.

Table 27: Considerations for implementing effective risk reporting Risk index

92. Types of risk management reports

In integrated and risk intelligent municipalities, risk and risk management performance reporting should include the following broad categories of reporting:
a. **Risk profile reporting** to reflect risk profile improvement, indicating the extent to which the municipality is:
   - Achieving the right balance between risk taking and risk mitigation;
   - Reducing its risk exposure, to ensure that the municipality is operating within its risk bearing capacity.

b. **Risk management maturity reporting** to reflect risk management process improvement, indicating whether the municipality is:
   - Making progress in moving towards a greater level of maturity;
   - Achieving cost benefit of its risk management processes by embedding risk management as much as possible into all operational and decision-making processes
   - Adding value through the achievement of its service delivery objectives.

c. **Risk management compliance reporting**, indicating:
   - The extent to which the municipality complies with the prescribed risk management processes as per the risk management policy;
   - The extent to which the municipality remains within its risk tolerance levels;
   - Improvement of the municipality’s compliance to predetermined levels of performance.
The following summary illustrates the typical reports that might be used and the content, frequency, source information and impact of the reports:

<table>
<thead>
<tr>
<th>Report name</th>
<th>Content</th>
<th>Frequency</th>
<th>Source</th>
<th>Desired impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual Council Report</td>
<td>Assurance that the municipality has risk management processes in place.</td>
<td>Annually</td>
<td>Combined assurance report, Risk Management Maturity Assessment, Business continuity assessment, Disaster recovery assessment</td>
<td>Assure that processes are effective in controlling risks to satisfactory level. Include information for external stakeholders about key risks within the municipality and approaches to addressing these risks. Assurance on progress on risk management maturity.</td>
</tr>
<tr>
<td></td>
<td>Progress and status of Risk Management Maturity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business continuity and disaster recovery reports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Overview of risk management implementation progress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Committee Report</td>
<td>Risk Management Implementation</td>
<td>Quarterly</td>
<td>Plans</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------</td>
<td>-----------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>New and emerging risks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assurance on management of</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>existing risks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk Management compliance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exco Report</td>
<td>Overview of risk management</td>
<td>Quarterly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>implementation progress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Significant changes in the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>risk profile (including</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>“emerging” risks) since the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>last report and the reasons</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>for the changes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consolidated risk profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>showing the key risks and risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>control</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Verifying progress of risk management.**
- **Provision of assurance that risks have been identified, are being managed, controls are in place to manage the risks and the effectiveness of the controls is understood.**
- **Provision of assurance on improvement of the municipality’s compliance to predetermined levels of performance.**
- **Provision of assurance on coordinated responsibility for assurance on risks and controls.**

- **Ultimate Audit Committee and Council Assurance of risk management.**
- **Awareness, engagement and buy in of risk management.**
| Business process Report | New and emerging risks.  
Update on the management of existing risks  
Progress with treatment plans  
Results from monitoring activities  
Risk management implementation and performance in Business Unit | Monthly | Risk management implementation plan for business unit(s)  
Awareness of new risks and update on existing risks.  
Demonstration of progress with actions and improvement in management of risks.  
Demonstration of improvements in control effectiveness.  
Understanding and awareness of risk management implementation and performance. |
|---|---|---|---|
| Risk Management Report | Risk management implementation and implementation plans for the following six months  
Progress with the risk management plan over the previous six months | 6 monthly | Consolidated risk management implementation plans  
Monitoring and chasing progress of risk management and assurance of processes already complete and in place. Understanding and demonstrating improvement in risk management implementation. |
| Risk Register Reports | New risks identified and existing risks remaining  
Detail on the risk assessment methodology  
In the case of reviewed risk registers:  
Changes to ratings and other information  
Progress with treatment plans  
Results from monitoring activities | Monthly / Quarterly | Strategic risk register  
Operational risk registers  
Consolidated risk reports | Awareness of new risks and update on existing risks.  
Demonstration of progress with actions and improvement in management of risks.  
Demonstration of improvements in control effectiveness. |
|---|---|---|---|---|
| Risk Champion Report | Existing risks  
New and emerging risks  
Update on the management of existing risks  
Effectiveness of Controls  
Progress with treatment plans  
Risk management implementation and performance | Monthly | Risk management implementation plan  
Operational risk register | Awareness of new risks and update on existing risks.  
Demonstration of progress with actions and improvement in management of risks.  
Demonstration of improvements in control effectiveness.  
Communicate progress with risk management implementation and performance |
<table>
<thead>
<tr>
<th>Risk and Control Owner Reports</th>
<th>Update on the management of existing risks</th>
<th>Monthly</th>
<th>Operational risk register</th>
<th>Demonstration of progress with actions and improvement in management of risks. Demonstration of improvements in control effectiveness.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Effectiveness of Controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Progress with treatment plans</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top Risks/Strategic Risks</td>
<td>Prioritised list of the top 10 to 20 risks based on consequence and likelihood scores</td>
<td>Quarterly / annually</td>
<td>Consolidated risk registers Combined assurance table</td>
<td>Includes details about the risk, controls and their effectiveness and additional treatments.</td>
</tr>
</tbody>
</table>

**Table 28: Types of reports to be generated**
93. **Risk report formats**

There are several report formats that can be used to report risks to the various stakeholders. Some examples are included below:

**Summary of risks with both inherent and residual rating**

The risk register is summarised to provide the first, fourth and fifth line of assurance with a picture of inherent and residual risk. Take note that effectiveness of control would cause a significant change in the rating from inherent to residual.

<table>
<thead>
<tr>
<th>Ref</th>
<th>Focus area</th>
<th>Risk Name</th>
<th>Inherent Rating</th>
<th>Residual Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Financial Viability</td>
<td>Ineffective financial management</td>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>Service Delivery and Infrastructure Development</td>
<td>Inadequate financial management</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>Good Governance and public participation</td>
<td>Poor management</td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>Institutional Transformation and Development</td>
<td>Inadequate /ineffective institutional structure</td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>Local Economic Development</td>
<td>Poor municipal economic activity</td>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>Information, Communication and Technology</td>
<td>Poor and ineffective information system</td>
<td>16</td>
<td>13</td>
</tr>
</tbody>
</table>

**Report 1: Inherent vs residual rating**

**Heatmaps**

Heat maps are commonly used to report on the top risks faced by the municipality, graphically illustrated and showing the relative severity of risks in relation to each other. It indicates all the risks on one page, whilst rating their relative importance.

**Report 2: Risk matrix**
Individual risk analysis

A simplistic report that reflects one risk, which can normally be used to inform the risk owner about risks and controls.

Report 3: Individual risk summary

Pie charts

Pie charts are very useful when risks are categorised according to risk categories or a operational objectives.

Some examples include:
Report 4: Pie charts

Dashboards

A dashboard report is useful to show all Strategic or Operational Risks on one single dashboard, with supporting information available to readers on request. Options for the dashboard can include, amongst others:

- The Risk Matrix with the count of risks
- A pie chart of controls by their effectiveness
- Risks by category
- Risks by strategic objectives

Examples of dashboards are displayed on the next page.
Consolidated risk management performance dashboards

Consolidated 1-pager dashboards are effective reporting mechanisms for high-level risk management performance presentations to the Municipal Council, the Audit and Risk Committees, and Exco in integrated and risk intelligent municipalities.

Such dashboards could include the three broad types of reporting as per section 5 of this chapter, namely:
a. **Risk profile reporting** to reflect risk profile improvement, indicating the extent to which the municipality is:
   - Achieving the right balance between risk taking and risk mitigation
   - Reducing its risk exposure, to ensure that the municipality is operating within its risk bearing capacity

b. **Risk management maturity reporting** to reflect risk management process improvement, indicating whether the municipality is:
   - Making progress in moving towards a greater level of maturity
   - Achieving cost benefit of its risk management processes by embedding risk management as much as possible into all operational and decision-making processes
   - Adding value through the achievement of its service delivery objectives

c. **Risk management compliance reporting**, indicating:
   - The extent to which the municipality complies with the prescribed risk management processes as per the risk management policy
   - The extent to which the municipality remains within its risk tolerance levels
   - Improvement of the municipality’s compliance to predetermined levels of performance

An example of a consolidated risk profile report is shown in Example 5 below.
Example 5: Risk Profile Report

1. Comparison between previous and current risk profile

1.1 Inherent and Residual Risks

<table>
<thead>
<tr>
<th>Inherent Risks: Comparison between previous and current risk profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Rated Risks</td>
</tr>
<tr>
<td>Medium Rated Risks</td>
</tr>
<tr>
<td>Low Rated Risks</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Residual Risks: Comparison between previous and current risk profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Rated Risks</td>
</tr>
<tr>
<td>Medium Rated Risks</td>
</tr>
<tr>
<td>Low Rated Risks</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>
### Implementation status (Inherent risks)

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Implemented</th>
<th>Implementation in progress (20%)</th>
<th>Implementation in progress (50%)</th>
<th>Implementation in progress (80%)</th>
<th>Not yet started</th>
<th>Not indicated</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous</td>
<td>52</td>
<td>18</td>
<td>12</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>88</td>
</tr>
<tr>
<td>Current</td>
<td>52</td>
<td>18</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>80</td>
</tr>
</tbody>
</table>

**Implementation status:**

*Comparison between previous and current status*

- **Implemented:**
  - Previous: 52
  - Current: 52

- **Implementation in progress (20%):**
  - Previous: 18
  - Current: 18

- **Implementation in progress (50%):**
  - Previous: 4
  - Current: 0

- **Implementation in progress (80%):**
  - Previous: 3
  - Current: 1

- **Not yet started:**
  - Previous: 3
  - Current: 0

- **Not indicated:**
  - Previous: 0
  - Current: 0

**Total:**

- Previous: 88
- Current: 80
# Changes in risk profile

## 2.1 Number of risks

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous number of risks</td>
<td>88</td>
</tr>
<tr>
<td>Additional risks</td>
<td>0</td>
</tr>
<tr>
<td>Deleted risks</td>
<td>8</td>
</tr>
<tr>
<td>Current number of risks</td>
<td>80</td>
</tr>
</tbody>
</table>

## 2.2 Changes according to monitoring fields

<table>
<thead>
<tr>
<th>Monitoring categories</th>
<th>Number of Risks</th>
<th>% of Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>No change</td>
<td>70</td>
<td>88%</td>
</tr>
<tr>
<td>Changes to linkage with IDP and SDBIP</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Changes to detailed risk</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Changes to risk owner</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Changes to risk assessment</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Changes to risk strategy and treatment</td>
<td>10</td>
<td>13%</td>
</tr>
<tr>
<td>Changes to implementation status and perceived control effectiveness</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Changes to desired control effectiveness</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>80</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IDP Objective</th>
<th>Number of Risks</th>
<th>% of Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>KPA 1: Basic Service delivery and Infrastructure Development</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>KPA 2: Municipal Transformation and Municipal Development</td>
<td>7</td>
<td>13%</td>
</tr>
<tr>
<td>KPA 3: Local Economic Development</td>
<td>12</td>
<td>21%</td>
</tr>
<tr>
<td>KPA 4: Municipal Financial Viability and Management</td>
<td>27</td>
<td>48%</td>
</tr>
<tr>
<td>KPA 5: Good Governance and Public Participation</td>
<td>10</td>
<td>18%</td>
</tr>
<tr>
<td>Total</td>
<td>56</td>
<td>100%</td>
</tr>
</tbody>
</table>
3. Current Risk Profile

3.1 Inherent and Residual Risks

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Inherent Risks</th>
<th>Residual Risks</th>
<th>Inherent Risks %</th>
<th>Residual Risks %</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Rated Risks</td>
<td>6</td>
<td>3</td>
<td>21%</td>
<td>43%</td>
</tr>
<tr>
<td>Medium Rated Risks</td>
<td>1</td>
<td>2</td>
<td>3%</td>
<td>29%</td>
</tr>
<tr>
<td>Low Rated Risks</td>
<td>22</td>
<td>2</td>
<td>76%</td>
<td>29%</td>
</tr>
<tr>
<td>Total</td>
<td>29</td>
<td>7</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
3.3 Risk Categories

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Number of Risks</th>
<th>% of Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental(External)</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Internal Control</td>
<td>1</td>
<td>14%</td>
</tr>
<tr>
<td>Strategic</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Operational</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Information Communication &amp; Technology</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Financial</td>
<td>1</td>
<td>14%</td>
</tr>
<tr>
<td>Integrity</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>1</td>
<td>14%</td>
</tr>
<tr>
<td>Service Delivery</td>
<td>4</td>
<td>57%</td>
</tr>
<tr>
<td>Total</td>
<td>7</td>
<td>100%</td>
</tr>
</tbody>
</table>

![Risk Categories Chart]

- Service Delivery: 57%
- Infrastructure: 14%
- Financial: 14%
- Information Communication & Technology: 0%
- Operational: 0%
- Strategic: 0%
- Integrity: 0%
- Internal Control: 14%
- Environmental(External): 0%
### 3.4 Risk Response Strategies

<table>
<thead>
<tr>
<th>Risk Strategies</th>
<th>Number of Risks</th>
<th>% of Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avoiding</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Accepting</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Reducing</td>
<td>7</td>
<td>100%</td>
</tr>
<tr>
<td>Sharing</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Not indicated</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>7</td>
<td>100%</td>
</tr>
</tbody>
</table>

### 3.5 Control Types

<table>
<thead>
<tr>
<th>Control Types</th>
<th>Number of Risks</th>
<th>% of Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventative</td>
<td>2</td>
<td>29%</td>
</tr>
<tr>
<td>Detective</td>
<td>1</td>
<td>14%</td>
</tr>
<tr>
<td>Corrective</td>
<td>4</td>
<td>57%</td>
</tr>
</tbody>
</table>
### Implementation status (Inherent risks)

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Implemented</th>
<th>Implementation in progress (20%)</th>
<th>Implementation in progress (50%)</th>
<th>Implementation in progress (80%)</th>
<th>Not yet started</th>
<th>Not indicated</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Rated Risks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Medium Rated Risks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Low Rated Risks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total %</strong></td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
<td>0%</td>
<td>100%</td>
</tr>
</tbody>
</table>
## Risk action plan example

<table>
<thead>
<tr>
<th>RISK IDENTIFICATION</th>
<th>RISK TREATMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>Action</td>
</tr>
</tbody>
</table>
| Failure to meet compliance obligations | AVOID | Implement formal compliance monitoring process:  
1. Identification of compliance requirements  
2. Identification of system or tool to manage compliance requirements  
3. Monthly review of compliance requirements to ensure there have been no material compliance breaches. | Practitioner | 30-Sep-12 |
| Loss of Practitioner | REDUCE | Implement succession plan:  
1. Put in place power of attorney arrangements  
2. Document key processes  
3. Put in place a key client management system to ensure adequate documentation is maintained for key clients  
4. Adequately train a secondary level of management and/or identify a potential candidate for partner. | Practitioner | 31-Oct-12 |
| Failure to collect receivables in a timely manner | REDUCE | Implement receivables tracking and debtor follow-up process:  
1. Identify requirements to track receivables, consider such things as payment terms and conditions  
2. Develop process to track aged debtors/receivables and supporting requirements including system reports  
3. Consider monitoring requirements including frequency. | Office Manager | 15-Sep-12 |
3.7 Perceived Control Effectiveness

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Very good</th>
<th>Good</th>
<th>Satisfactory</th>
<th>Weak</th>
<th>Unsatisfactory</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Rated Risks</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>Medium Rated Risks</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Low Rated Risks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>Total %</td>
<td>0%</td>
<td>43%</td>
<td>14%</td>
<td>43%</td>
<td>0%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Control Types
- Preventive: 29%
- Corrective: 57%
- Detective: 14%

Perceived Control Effectiveness
- High Rated Risks
- Medium Rated Risks
- Low Rated Risks

- Very good
- Good
- Satisfactory
- Weak
- Unsatisfactory

- Weak 43%
- Satisfactory 14%
- Good 43%
### Materialisation and escalation of risks

**Risks that materialised:**

<table>
<thead>
<tr>
<th>Number of risks that materialised</th>
<th>Number of Risks</th>
<th>% of Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>26</td>
<td>100%</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Total number of risks</strong></td>
<td><strong>26</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

**Risks that should be escalated:**

<table>
<thead>
<tr>
<th>Number of risk that should be escalated</th>
<th>Number of Risks</th>
<th>% of Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>78</td>
<td>78</td>
<td>99%</td>
</tr>
<tr>
<td><strong>Total number of risks</strong></td>
<td><strong>79</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
94. Incident reporting system

Incident reporting is another means of risk monitoring and reviewing the effectiveness of controls. The principle of real-time incident reporting for key processes is growing in prominence globally. Certain disciplines such as Safety, Health, Environmental and Quality may already have in place incident reporting systems. Such reporting systems should be integrated into the broader risk management incident reporting systems in order to avoid duplication of effort.

Incident reporting however relies on an effective system of automated monitoring and reporting of risks. Quantification of the number of the incidents can be a very reliable source of information to continuously evaluate changes in likelihood. One format of an incident report can be seen below.

<table>
<thead>
<tr>
<th>Incidents for the last two years</th>
<th>Number of incidents</th>
<th>Value</th>
<th>Control deficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Has the institution been defrauded in the last two years - if yes provide the value regarding the following categories: internal parties, outside parties, financial misstatement?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Has the institution incurred material damage to property, stock, machinery, etc. in the last two years? If so please indicate the value and number.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Has there been any loss of life due to injury at work.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. How many incidents of injury on duty have been reported in the last two years? Please give a brief description of the type of incidents etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Have there been any accidents on duty? Please give a brief description of the type of accidents etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. How many fires have occurred in the last two years and indicate value of damage?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Has the institution paid any fines/penalties, e.g. contravention of legislation, environment issues, tax penalties, etc.? Give a brief description of the fines/penalties.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Has the institution had to settle any lawsuits? Give brief details.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incidents for the last two years</td>
<td>Number of incidents</td>
<td>Value</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>-------</td>
</tr>
<tr>
<td>9</td>
<td>Have there been any incidents of rioting/flooding, etc. that have impacted the institution's operations?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Has the institution lost major assets due to theft? What is the value of such losses?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Has there been any reports of pollution as result of the institution’s activities? If so, give brief details.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Has there been any business interruption which has impacted on the institution’s operations? If so, give brief details.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Has there been any theft of vehicles or damages to vehicles in last two years? If so, give brief details.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Have there been any incidents of bad publicity for the last two years? If so, give brief details.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Any other relevant information?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 29: Incident report**

### 95. Emerging risk warning system

Effective risk management will incorporate a process of identifying emerging trends, which could pose threats and risks. The frequency with which emerging risks are deliberately interrogated will be influenced by the rate of change and dynamism the Municipality is confronted with. The following nine points will assist municipalities to enhance the capacity to deal with uncertainty and emerging risks:

a. Creating transparency (sharing all assessments and management efforts with stakeholders and the public, except for confidential information);

b. Ascertaining accountability on all levels – risk identification, assessment, evaluation and management;

c. Fostering inclusion - bringing together actors such as governments (all branches and agencies), private sector (corporations and associations), civil society (NGOs, media, social organisations) and experts;

d. Striving for integration among and between different impacts (physical, economic, environmental, social, psychological); departments (health, environment, treasury,
labour, etc.); and public and private entities (on a continuum between 100% public and 100% private);
e. Providing convincing methods for monitoring and evaluating management options and their consequences (evaluation according to effectiveness, efficiency, fairness and sustainability);
f. Prioritising risks as there are always more emerging threats than one can deal with. Criteria are needed to distinguish the serious threats from the background noise;
g. Determining the right timing – monitoring signals about emerging threats and changing contexts for technological applications - based on these signals appropriate interventions need to be deployed on time;
h. Ensuring flexibility and adaptability over time (identifying appropriate intervention points, assuring learning and monitoring, embracing the philosophy of adaptive management); and
i. Communication – the necessity to communicate about the need to address emerging risks, the tools and processes used for that purpose, and the data and information collected.

Emerging risks are previously unrecognised risks that may be an imminent threat. Such risks may emanate through changes in the regulatory environment, external events, internal changes or social trends. In King III these risks are identified as risks with a low likelihood, but potentially high impact. The moment the likelihood changes, it changes the urgency of the risk mitigation processes. In general municipality tend to neglect these risks as they do not require immediate attention. These risks are equally important, and examples include disaster recovery and business continuity.

The template below provides a basis to report on merging risk.

<table>
<thead>
<tr>
<th>Event</th>
<th>Emerging risk</th>
<th>Identifying manager</th>
<th>Department / Section</th>
<th>Way forward</th>
</tr>
</thead>
<tbody>
<tr>
<td>A description of the event needs to be recorded in this column.</td>
<td>A description of the risk needs to be recorded in this column. It is important to ensure that the description of the risk is accurately recorded.</td>
<td></td>
<td></td>
<td>The risk response to manage the identified emerging risk needs to be recorded in this column.</td>
</tr>
</tbody>
</table>

Table 30: Emerging risks

96. Principles for effective risk data aggregation and risk reporting

The following 11 principles apply to data aggregation and risk reporting:
Principle 1: Risk data aggregation capabilities and risk reporting practices should be subject to strong governance consistent with other principles and guidance

a. The Municipal Council and senior management should promote the identification, assessment and management of data quality risks as part of its overall risk management framework.

b. This must include agreed service level standards for both outsourced and in-house risk data-related processes and policies on data confidentiality, integrity and availability.

c. The Municipal Council and senior management should review and approve the risk data aggregation and risk reporting and ensure that adequate resources are deployed.

d. Risk data aggregation capabilities and risk reporting practices should be:
   i. Fully documented and subject to high standards of validation to review appropriateness and effectiveness and the quality of the governance surrounding the processes.
   ii. Considered as part of any new initiatives, projects, acquisitions or product development, as well as broader process and IT change initiatives.

Principle 2: Data architecture and IT infrastructure

a. Data architecture and IT infrastructure must be designed, built and maintained to fully support risk data aggregation capabilities and risk reporting practices not only in normal times but also during times of stress or crisis. These must be included in business continuity planning processes and be subject to an impact analysis.

b. Integrated data taxonomies and architecture must be established across the municipality, including information on characteristics of the data (metadata) and naming conventions for data.

c. Roles and responsibilities should be established as they relate to the ownership and quality of risk data and information for both the business and IT functions. The owners (business and IT functions), in partnership with risk managers, should ensure there are adequate controls throughout the lifecycle of the data and for all aspects of the technology infrastructure.

Principle 3: Accuracy and Integrity

a. Accurate and reliable risk data must be generated to meet normal and stress/crisis reporting accuracy requirements. Data should be aggregated on a largely automated basis so as to minimise the probability of errors.

b. Risk data must be aggregated in a way that is accurate and reliable.

c. A “dictionary” must be in place of the concepts used, such that data is defined consistently across a municipality.

d. There should be an appropriate balance between automated and manual systems. Where professional judgments are required, human intervention may be appropriate.

e. Metrics must be developed to monitor the accuracy of data and for appropriate escalation channels and action plans to be in place to rectify poor data quality.
Principle 4: Completeness

a. All material risk data across the municipality must be captured and aggregated and be available by business line, legal entity, asset type, industry and other groupings that permit identifying and reporting risk exposures, concentrations and emerging risks.

b. The data aggregation capabilities should include all material risk exposures, including those that are off-balance sheet.

c. Risk data aggregation capabilities should be the same regardless of the choice of risk aggregation systems implemented and specific approaches used to aggregate exposures for any given risk measure must be specified to allow the Municipal Council and senior management to assess the results properly.

d. Metrics are required to measure the completeness of the risk data and if it is not entirely complete, the impact should not be critical to the management of risks.

Principle 5: Timeliness

a. Aggregate and up to date risk data must be generated in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptability. The timing will also depend upon the nature and potential volatility of the risk and its criticality to the overall risk profile. Timeliness must meet requirements for normal and stress/crisis risk management reporting.

b. Different types of data will be required at different speeds, depending on the type of risk, and that certain risk data may be needed faster in a crisis situation. Risk systems need to be capable of producing aggregated risk data rapidly during times of crisis for all critical risks.

Principle 6: Adaptability

a. Aggregate risk data should be generated to meet a broad range of on-demand, ad hoc risk management reporting requests, including requests during crisis situations, requests due to changing internal needs and requests to meet supervisory queries.

b. Adaptability will enable municipality to conduct better risk management, including forecasting information, as well as to support stress testing and scenario analyses.

c. Adaptability includes:
   i. Data aggregation processes that are flexible and enable risk data to be aggregated for assessment and quick decision-making
   ii. Capabilities for data customisation of dashboards to users’ needs
   iii. Capabilities to incorporate new developments and/or external factors that influence the municipality’s risk profile or measurement requirements

d. To manage risk effectively, the right information needs to be presented to the right people at the right time. Risk reports based on risk data should be accurate, clear and complete, contain the correct content and be presented to the appropriate decision-makers in a time that allows for an appropriate response.
Principle 7: Accuracy

a. Reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated.

b. Reports should be accurate and precise to ensure the Municipal Council and senior management have the confidence to make critical decisions.

c. The following must be in place to ensure accuracy:
   i. Defined requirements and processes to reconcile reports to risk data;
   ii. Automated and manual edit and reasonableness checks, validation rules for quantitative information and explanations of the mathematical conventions used;
   iii. Integrated procedures for identifying, reporting and explaining data errors or weaknesses in data integrity via exceptions reports.

d. The Municipal Council and senior management should establish accuracy and precision requirements for both regular and crisis reporting, including critical position and exposure information. These requirements should reflect the criticality of decisions that will be based on this information.

e. Accuracy requirements should align to accounting materiality.

Principle 8: Comprehensiveness

a. Risk management reports should cover all material risk areas within the municipality and be consistent with the size and complexity of the municipality’s operations and risk profile, as well as the requirements of the recipients.

b. Risk management reports should include exposure and position information for all significant risk areas (e.g. credit risk, liquidity and solvency risk, operational risk) and all significant components of those risk areas and other risk-related measures.

c. Reports should identify emerging risks and provide information in the context of risk appetite/tolerance and proposed recommendations for action.

d. Reports should include the current status of measures agreed by the Municipal Council or senior management to reduce risk or deal with specific risk situations as well as monitoring emerging trends.

e. Risk management reports must be complete and supervisors will need to be satisfied with the coverage, analysis and interpretation, scalability and comparability across the municipality.

Principle 9: Clarity

a. Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand yet comprehensive enough to facilitate informed decision-making. Reports should include an appropriate balance between risk data, analysis and interpretation, and qualitative explanations.

b. Risk reports should contribute to sound risk management and decision making and ensure that information is meaningful and tailored to the needs of the recipients.

c. There must be a balance between qualitative and quantitative information which will vary at different levels within the municipality and will also depend on the level of aggregation that is applied to the reports.
d. The Municipal Council should ensure that it is asking for and receiving relevant information that will allow it to fulfil its governance mandate and ensure it is operating within its risk-bearing capacity.

e. Feedback must be provided to senior management when the risk reports do not meet requirements and do not provide the right level and type of information.

f. Senior management should ensure that it is receiving relevant information that will allow it to fulfil its management mandate and the risks to which it is exposed.

g. Reports should balance detailed data, qualitative discussion, explanation and recommended conclusions. Interpretation and explanations of the data, including observed trends, should be clear.

Principle 10: Frequency

a. The Municipal Council and senior management should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed at which the risk can change, as well as the importance of reports in contributing to sound risk management and decision making.

b. The frequency of reports should be increased during times of crisis.

c. The frequency of risk reports will vary according to the type of risk, purpose and recipients. The ability to produce accurate reports needs to be tested to see if they are effective within established timeframes, particularly in a crisis.

Principle 11: Distribution

a. Risk management reports should be distributed to the relevant parties and includes meaningful information tailored to the needs of the recipients, while ensuring confidentiality is maintained.

b. There are differing information needs of the Municipal Council, senior management, and the other levels of the municipality

c. Procedures should be in place to allow for rapid collection and analysis of risk data and dissemination of reports to provide for timely presentation to all appropriate recipients.
Chapter 13: Disaster recovery and business continuity

97. Business Continuity

Business Continuity (BC) is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. As municipalities face continuous service delivery protests and liquidity problems, and with all the cyber attacks on information systems, assessment of the business continuity and disaster recovery ability should be performed.

The following assessment templates for disaster recovery and back-up and recovery are added as examples of such an assessment:

<table>
<thead>
<tr>
<th>Risk classification</th>
<th>1 LOA</th>
<th>2 LOA</th>
<th>3 LOA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes/ no</td>
<td>Yes/ no</td>
<td>Yes/ no</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disaster recovery</th>
<th>1</th>
<th>During the course of a disaster or significant disruption, does your municipality have written plans for business continuity and IT disaster recovery?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>If you answered “Yes” to question (1) do the established plans cover critical business functions with recovery priorities?</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Have you performed a business impact analysis including Recovery Time Objective and Recovery Point Objective?</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Does your Business Impact Analysis calculate and classify the financial risk of disturbances to all vital functions?</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Have you taken actions to mitigate known risks and single points of failure (e.g. power loss, physical access, etc.)?</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Do you have a dedicated team of professionals focused on business continuity and/or IT disaster recovery?</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>If you answered “No” to question (6), is there an established external business continuity and disaster recovery service provider to handle your planning needs?</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Is senior management fully committed to disaster recovery and business continuity?</td>
</tr>
<tr>
<td></td>
<td>Question</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>9</td>
<td>Are your disaster recovery costs, options, and disaster declaration procedures understandable?</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Do you have a sufficient budget to support your disaster recovery program?</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Is your business continuity plan updated regularly to keep it current with hardware, software, business and staffing changes?</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Is there an organized training and awareness program for your employees?</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Does your disaster recovery center have an operation center?</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Is there remote accessibility to your disaster recovery center?</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Do you practice spontaneous tests to recover from a Disaster Recovery Site and resume the day from that location?</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Have you tested your plan using a worst-case scenario?</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>In the case of a disaster are you prepared to address liabilities and responsibilities?</td>
<td></td>
</tr>
</tbody>
</table>

Table 31: Disaster recovery assessment

<table>
<thead>
<tr>
<th>Risk classification</th>
<th>1 LOA</th>
<th>2 LOA</th>
<th>3 LOA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes/no</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Back-up and Recovery

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Do you have a recovery strategy?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Do you have a backup strategy?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Do you have written backup and archive procedures?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4</td>
<td>Do you have industry-standard back-up solutions? (media, tape drives, library, software etc.)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>To ensure sufficient permanent access do you have a migration policy to &quot;refresh&quot; tape technology and data formats every three to five years to?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Do you periodically test your back-up media?</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Can you access to your past data with your back-up strategy?</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Are backups fully automated for unattended operation (autoloaders, etc.)?</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>If your backups are manual, do you follow a sound process and written procedures?</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>If your backups are not manual, do you have online backup?</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Does your current backup and recovery methodology fulfill management’s business uptime needs?</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Do you regularly send your backup copy to a safe, off-site archive?</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Do you have retention period on backup data for legal obligations?</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Is media properly taken care of when shipped, handled, stored, and used?</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Is your archive system designed to facilitate data format standards and an archive tape tracking method?</td>
<td></td>
</tr>
</tbody>
</table>

Table 32: Back-up and recovery assessment