RISK MANAGEMENT FRAMEWORK

PIXLEY KA SEME DISTRICT MUNICIPALITY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Risk management is a central part of any organization's strategic management. It is the process whereby an organization both methodically and intuitively addresses the risk attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of activities.

Risk management is recognized as an integral part of sound organizational management and is being promoted in internationally and in South Africa as good business practice applicable to the public and private sectors.

LEGAL MANDATE

Since 2003 this practice has been further supported by the Municipal Finance Management Act which stipulates in Section 62(1) (c) that:

The accounting officer…has and maintains effective, efficient and transparent systems:

i) of financial and risk management and internal control;

The extension of the general responsibilities, in terms of Section 62 of the MFMA, to all managers is a cornerstone in the institutionalization of risk management in the public service. It establishes responsibility for risk management at all levels of management, extending it beyond the roles of the Accounting Officer the internal audit units or the Audit Committee in this regard.

The roles and responsibilities for the implementation of a Risk Management strategy is contained in the treasury regulations published in terms of the PFMA. Section 3.2 of the regulations revolves around risk management and can be summarized as follows:

> *The accounting officer must ensure that a risk assessment is conducted regularly to identify emerging risks for the institution.*
>
> *The risk management strategy, which must include a fraud prevention plan, must be used to direct internal audit effort and priority and to determine the skills required of managers and staff to improve controls and to manage these risks.*
>
> *The risk management strategy must be clearly communicated to all officials to ensure that it is incorporated into the language and culture of the institutions, and embedded in the behavior and mindset of its people.*

The King report on Corporate Governance also reflects on risk management as an integral part of strategic and operational activities.

Guidelines

These guidelines were based on South African experience in implementing risk management and research on international best practice in the public service. The importance of own experience and lessons learnt contributed immensely to the value of these guidelines for the South African public service.

Officials will only be able to integrate risk management practices into their daily work if adequate training on risk management is provided to them. The development of risk management guidelines is an essential step in ensuring that officials are aware of their responsibilities and understand their obligations. It will also lead to greater awareness of their responsibility to report on and manage risk.

Specific mention should also be made of the use of the following guidelines as research material in developing this guideline.

- The guidelines for management of risk in the Australian and New Zealand public sector (AS/NZS 43/1999)
- The Canadian Risk Management Framework was used as research material in compiling these guidelines.

- The draft COSO (The Committee of Sponsoring Organizations of the Treadway Commission) Enterprise Risk Management Framework.

Risk Management

The Institute of Internal Auditors defines risk as "…the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences and likelihood."

Risk management is defined as:

" *a continuous, proactive and systematic process, effected by a department's executive authority, accounting officer, management and other personnel, applied in strategic planning and across the department, designed to identify potential events that may affect the department, and manage risks to be within its risk tolerance, to provide reasonable assurance regarding the achievement of department objectives."*

Risk management is more than an exercise in risk avoidance. It is as much about identifying and utilizing opportunities as avoiding or mitigating losses.

Benefits of Risk Management

The following benefits flow from an effective risk management process:

Risk management is pro active and anticipatory, enabling a Municipality to achieve its objectives with greater certainty.

A robust risk management process aims at increased awareness, transparent evaluation, and sound mitigation of risks facing a Municipality.

As a management tool, an integrated risk management framework assists in achieving objectives more efficiently. Risk Analysis as a management tool also promotes effective and efficient resource utilization.

Risk Management;

Is a tool that is forward looking, anticipating any potential impediment/risks to physical and human assets in reaching the organizational objectives of the Municipality
.
Focuses management on understanding the nature of the risks and ensure that management takes steps to mitigate the potential negative consequences.

Can improve the rendering of services by ascertaining what can go wrong in the context of the objectives of the Municipality.

Allows management to evaluate, prioritize and address the critical risks and channel resources to these risks, ultimately improving the utilization of resources, addressing the most important risks.

It leads to the evaluation of the effectiveness of control measures and the design of control measures, to adequately address the risks with due consideration of the cost of control measures.

Risk Management assists management to take the right decisions in an uncertain environment. Focusing of risk analysis and responses improves the quality of strategic plans. It generates plans, which are comprehensive and analytical.

It is a powerful tool to deal with uncertainties in the environment and to establish pre-emptive strategies to enhance service delivery.

Risk Management is a preventative anti-corruption technique and can assist with ascertaining what the fraud propensity of the Municipality or section is; raising the awareness of corruption in doing so and contribute to preventing corruption e.g. risk management analyze the risks/fraud opportunities in procurement and payment systems as a means of preventing fraud and corruption.

Part of any fraud risk analysis relates to a management style and the organizational culture or ethics prevailing in an organization. Examples of cultural/ethical risk factors are autocratic management styles, poor commitment to control, and absence of a code of ethics and non-compliance with principles of good governance.

A major component of risk management is the establishment of a fraud prevention plan. Managing the risk of fraud and corruption entails the development, implementation, and maintenance of cost effective internal controls.

It improves accountability and links professional ethical behavior with service excellence. It raises awareness of the risks inherent to the activities that are being managed and for which managers are held accountable and fosters and enhances a culture of accountability and empowered decision-making instead of a culture of no tolerance for mistakes. By prioritizing fraud risks, individuals in positions where the opportunity for fraud and corruption is high can be better assisted in managing those risks.

It also allows a Municipality to align its auditing plan with the risk profile of the Municipality. It ensures a focused audit plan, contributes to the monitoring of changes in the risk profile of the organization and leads to the measurement of the effectiveness of control measures. It also ensures that limited internal audit capacity is more effectively focused and used. This important preventive measure can be instituted to limit the opportunities for corruption.

Risk management enhances asset management. Risk management does not focus on physical assets alone. It also focuses on soft assets like human resources, information and knowledge as well as organizational reputation.

Risk management enhances the capability of a Municipality or entity to identify potential risks, assess these risks, and manage them, thereby reducing the occurrence of surprises and related costs.

Structured approach to Risk Management

The process of managing risk as described in these guidelines is a structured approach that enables Municipalities to incorporate risk management into the broader management frameworks.

The guidelines follow an eight-step approach that includes the following:

- Control environment;
- Objective setting;
- Risk identification;
- Risk assessment;
- Risk management strategy;
- Control activities;
- Information and communication; and
- Monitoring.

This Risk Management Framework (RMF) provides a generic guide for the implementation of risk management strategies in the public service, and suggests that risk management is a formal step-by-step process that can be applied at all levels of a Municipality. These principles need to be implemented within the context of each Municipality who should implement this framework in the development of their own risk management strategies.

Risk management is a process, not an event and requires organisations to pay closer attention to the developments both in the external and control environments. Top management's strategic direction and commitment are also regarded as very important if risk management processes are to be successful and effective.

Here management is expected to lead the process and ensure that everybody within the organisation understands the benefits risk management has for the Municipality. This represents the challenge to management to set the tone or to establish a supportive internal environment. Involvement of all personnel and all levels of management ensures that risk management activities are applied consistently across all levels within the organisation. Again, the philosophy that everybody is a risk manager ensures that everybody is involved in risk management process.

Risk management is not undertaken in isolation, it has to be integrated with other management processes like internal audit that are happening in the organisations. This involves, but is not limited to, strategic planning processes, performance management systems, human resource management systems, guidelines, systems, and other internal control activities. The main activities involved here include defining the context within which the risk management activities will be undertaken as well as the scope or coverage of risk management activities.

The whole system is facilitated by effective communication between all levels. Without it, employees are less likely to know and understand the purpose and importance of their activities in the whole risk management process and in contributing to the overall objectives of the organisation. A clear definition and communication of the concept of risk is pivotal to the success of risk management programmes. Defining guidelines, methods, frequency of reporting, clear lines of reporting and accountability make a significant contribution to a well-informed and motivated organisational team.

Summary

Risk management has been clearly identified as a deficient process in the various projects in local government. It should be at the forefront of each Municipality's improvement agenda.

1. Introduction

The risk management framework (RMF) strengthens the risk management practices in the Public Service. The need for more affordable and effective government combined with trends towards revitalizing human resources capacity and redesigning service delivery are dramatically affecting the structure and culture of public organizations. The faster pace and need for innovation, combined with significant risk-based events from computer failures to natural disasters has focused attention on risk management as an essential in sound decision-making and accountability.

Recognizing the need for definitive guidance on risk management, National Treasury, in conjunction with the Public Service Commission, developed a conceptually sound framework based on integrated principles, common terminology and practical implementation guidance to support departments' efforts to develop or benchmark their risk management processes. The framework respects core public service values such as honesty, integrity and probity at all levels, and contributes to improved results by managing risk proactively.

This RMF sets out key elements of risk management, including the definition, components and underlying principles of risk management, as well as its benefits and limitations and roles and responsibilities of various parties.

The purpose of the RMF is to:

- Advance the development and implementation of modern management practices and to support innovation throughout the Public Service;

- Contribute to building a risk-smart workforce and environment that allows for innovation and responsible risk-taking while ensuring legitimate precautions are taken to protect the public interest, maintain public trust, and ensure due diligence;

- Provide a comprehensive approach to better integrate risk management into strategic decision-making; and

- Provide guidance for accounting officers, executive authorities, managers and staff when overseeing or implementing the development of processes, systems and techniques for managing risk, which are appropriate to the context of the department or public entity.

It is anticipated that the implementation of the RMF will:

Support the government's governance responsibilities by ensuring that significant risk areas associated with policies, plans, programs and operations are identified and assessed, and that appropriate measures are in place to address unfavorable impacts;

Improve results through more informed decision-making, by ensuring that values, competencies, tools and the supportive environment form the foundation for innovation and responsible risk-taking, and by encouraging learning from experience;

Strengthen accountability by demonstrating that levels of risk associated with policies, plans, programs and operations are explicitly understood and that investment in risk management measures and stakeholder interests are optimally balanced; and

Enhance stewardship and transparency by strengthening public service capacity to safeguard human resources, property and interests.

The RMF has been developed in the knowledge that some Municipalities have already produced their own guidelines for internal use. It is not the intention to supersede such guidelines, but rather to supplement and/or provide a minimum benchmark that can be used for comparison purposes.

Legal mandate

The Municipal Finance Management Act, 2003 supplemented by the relevant Treasury Regulations, has legislated some key governance best practices which have also been included in the revised King Report on Corporate Governance.

Section 62 (1) (c) of the MFMA requires that:

"*The Municipality…has and maintains:*

- *i) Effective, efficient and transparent systems of financial and risk management and internal control; and*
- *ii) A system of internal audit operating in accordance with any prescribed norms and standards…"*

The extension of the general responsibilities, in terms of Section 62 of the MFMA, to all managers is a cornerstone in the institutionalization of risk management in the public service. It establishes responsibility for risk management at all levels of management, and does not limit it to the accounting officer or internal audit units.

The roles and responsibilities for the implementation of a Risk Management strategy is contained in the Treasury Regulations published in terms of the PFMA. Section 3.2 of the regulations revolves around risk management and can be summarized as follows:

The accounting officer must ensure that a risk assessment is conducted regularly to identify emerging risks for the institution.

The risk management strategy, which must include a fraud prevention plan, must be used to direct internal audit effort and priority and to determine the skills required of managers and staff to improve controls and to manage these risks.

The risk management strategy must be clearly communicated to all officials to ensure that it is incorporated into the language and culture of the institutions and embedded in the behavior and mindset of its people.

The King report on Corporate Governance also reflects on risk management as an integral part of strategic and operational activities.

2. Relevance of Risk Management

The underlying premise of risk management is that every governmental body exists to provide value for its stakeholders. Such value is based on the quality of service delivery to the citizens.

All Municipalities face uncertainty, and the challenge for management is to determine how much **uncertainty** the Municipality is prepared to accept as it strives to grow stakeholder value.

Uncertainty presents both risk and opportunity, with the potential to erode or enhance **value**. The framework provides a basis for management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance its capacity to build value.

Uncertainty

Municipalities operate in environments where factors such as globalization, technology, regulation, restructuring, changing markets, and political influence create uncertainty.

Uncertainty emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes.

Value

Value is created, preserved or eroded by management decisions ranging from strategic planning to daily operation of the Municipality. Inherent in decisions is recognition of risk and opportunity, requiring that management consider information about the internal and external environment deploys precious resources and appropriately adjusts Municipal activities to changing circumstances.

Municipalities realize value when stakeholders derive recognizable benefits that they in turn value. For Municipalities, value is realized when constituents recognize receipt of valued services at an acceptable cost. Risk management facilitates management's ability to both create sustainable value and communicate the value created to stakeholders.

While each Municipality will find its own way to integrate risk management into existing decision-making structures, the following are factors to be considered:

- Aligning risk management with objectives at all levels of the Municipality;
- Introducing risk management components into existing strategic planning and operational practices;
- Communicating Municipal directions on an acceptable level of risk;
- Including risk management as part of employees' performance appraisals; and
- Continuously improving control and accountability systems and processes to take into account risk management and its results.

3. Benefits of Risk Management

Municipalities do not operate in a risk-free environment, and the risk management process does not create such an environment. Effective risk management assists Municipalities to achieve its

performance and service delivery targets, and to reduce the potential loss of resources. This results in effective responsibility and accountability structures, the improvement of the format used to report performance, and with the compliance with laws and regulations, thus avoiding damage to its reputation and other consequences.

Key benefits include:

- Effective and efficient service delivery ;
- A rigorous basis for strategic management through consideration of key elements of risk;
- Enhanced risk management strategy decisions through quantification of risk tolerances;
- Identification and management of risks affecting different department and/or different processes;
- Identification and implementation of cost effective, integrated responses to multiple risks;
- Minimizing operational surprises, costly and time-consuming litigation and unexpected losses;
- Rationalization of capital and financial resources;
- Continuity of service delivery;
- Greater transparency in decision making and ongoing management processes; and
- Enhanced accountability and corporate governance processes.

Key risks associated with ineffective risk management

The following key risks can be associated with ineffective risk management processes:

Breakdowns in internal controls could prevent the Municipality from achieving its objectives;

Risk management fails to be incorporated in the culture and will remain an, 'add on,' with minimal impact;

Reactive responses to potential risks, rather than proactive;

Municipality may have inadequate plans to deal with adverse events which could have a significant impact on its operations;

Inappropriate controls may be used which adversely affect the responsiveness and flexibility of the organization;

Changing/new risks are not adequately considered and managed; and

Internal control practices become outdated with limited account taken of best practice developments.

Definition of Risk Management

Risk management is not new to the public sector. It is an integral component of good management and decision-making at all levels. Risk management is about making decisions that contribute to the achievement of an organization's objectives. It assist with decisions such as the reconciliation of costs with benefits and expectations in investing limited public resources, the governance and control structures needed to support due diligence, responsible risk taking, innovations and accountability.

Risk management is defined as follows:

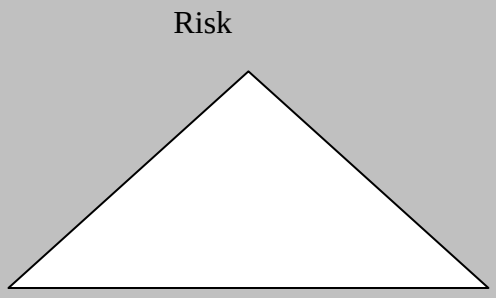
Risk management is a continuous, proactive and systematic process, affected by a Municipality's executive authority, accounting officer, management and other personnel, applied in strategic planning and across the Municipality, designed to identify potential events that may affect the Municipality, and manage risks to be within its risk tolerance, to provide reasonable assurance regarding the achievement of Municipal objectives.

This definition is purposefully broad for several reasons. It captures key concepts fundamental to how Municipalities should manage risk, providing a basis for application across different types of Municipalities, industries and sectors. It focuses directly on achievement of Municipal objectives and provides a basis for defining risk management effectiveness.

The fundamental concepts outlined in the definition above are discussed in the following paragraphs.

A continuous, proactive and systematic process	Risk management is not one event, but a series of continuous actions that permeate a Municipality's activities. These actions are pervasive and inherent in the way management runs the Municipality. Risk assessment requires incremental effort to develop needed models and make necessary analysis and calculations. However, these and other risk management mechanisms are intertwined with a Municipality's operating activities. Risk management is most effective when these mechanisms are built into the Municipality's control processes and infrastructure. Simultaneously the risk response plan should be aligned with the fraud prevention plan. Risk normally reflects an opportunity for fraud theft and corruption, and the fraud prevention plan focuses the attention to preventing irregular activities.
Effected by human resources	The executive authority, management and other personnel effect risk management. Although the executive authority primarily provides oversight, they also provide direction and approve strategy and policies. Management of a Municipality accomplishes risk management as they establish the Municipality's mission/vision, strategy and objectives and put risk management mechanisms in place. Each individual brings to the workplace a unique background and technical ability, and has different needs and priorities. Each person has a unique point of reference which influences how they identify, assess and respond to risk. Risk management provides the mechanisms needed to help individuals understand risk in the context of the Municipality's objectives.

	Individuals must know their responsibilities and limits of authority. Accordingly, a clear and close linkage needs to exist between responsibilities and the way in which they are carried out, as well as with the Municipality's strategy and objectives.
Applied in setting strategy	Risk management is applied in setting strategy as the Municipality sets out its mission or vision and establishes strategic objectives, which are the high-level goals that align with and support its vision or mission. The strategy for achieving its strategic objectives should consider risks relative to alternative strategies
Applied across the department	To successfully apply risk management, a Municipality must consider its entire scope of activities. Risk management considers activities at all levels of the Municipality and applies to special projects and new initiatives that might not yet have a designated place in the Municipality's hierarchy. Risk management requires a Municipality to take a *portfolio view* of risk. This might involve each manager responsible for a Municipal unit, function, process or other activity developing an assessment of risk for the unit. The assessment may be quantitative or qualitative. With a composite view at each succeeding level of the Municipality, senior management is positioned to make a determination whether the Municipality's overall risk profile is commensurate with its risk tolerance.
Risk tolerance	Risk tolerance is the amount of risk a Municipality is willing to accept in pursuit of value. Municipalities often consider risk tolerance qualitatively, with such categories as high, moderate or low, or they may take a quantitative approach, reflecting and balancing goals for growth, stakeholder value and risk. Risk tolerance is directly related to a Municipality's strategy. Different strategies will expose the Municipality to different risks. When applied in the strategic planning process, risk management assists management in selecting a strategy consistent with the Municipality's risk tolerance. Risk tolerance guides resource allocation by aligning the Municipality, human resources and processes when designing the infrastructure necessary to effectively respond to and monitor risks. (Refer to examples under, "control environment")
Provides reasonable assurance	Well-designed and operated risk management tools can provide management and the executive authority with reasonable assurance regarding achievement of a Municipality's objectives

	that: • They understand the extent to which the Municipality's strategic and operational objectives are being achieved; • The Municipality's reporting is reliable; • Assets are adequately safeguarded; and • Applicable laws and regulations are being complied with. Reasonable assurance reflects the notion that uncertainty and risk relate to the future, which no one can predict with certainty
Achievement of objectives	Effective risk management can be expected to provide reasonable assurance of achieving the organizations strategic and operational objectives as well as those relating to the reliability of reporting, and compliance with laws and regulations. Achievement of these objectives is not always within the Municipality's control and depends on how well the Municipality's related activities are performed. For these objectives, risk management can only provide reasonable assurance that management, and the executive authority in its oversight role, are made aware, in a timely manner, of the extent to which the Municipality is moving toward achievement of these objectives.  These three aspects are interrelated and indivisible. The achievement of objectives requires of government managers to take action and perform certain tasks and using assets (human, financial and other assets) in the process. To identify the risks for the organization, the objectives should be identified first and should be clear. Controls are developed, implemented, and maintained over numerous activities/processes within the workplace. Controls are specifically implemented to control risks. Controls are always risk-driven. The risk determines the level of control required. Risk in turn, is driven by the objectives that have to be met. The important aspect to keep in mind is that the costs to control (minimising) a risk should not exceed the benefits to the organization and controls can never eliminate risk.

4. Risk management components

The process of managing risk is a structured approach for incorporating risk management into the daily, broader management process. Risk management is more than an exercise of risk avoidance. It is as much about identifying opportunities as avoiding or mitigating losses.

Risk management is an ongoing process at every level, and consists of eight interrelated components, namely:

the control environment;

objective setting;

risk identification;

risk assessment;

risk management strategy;

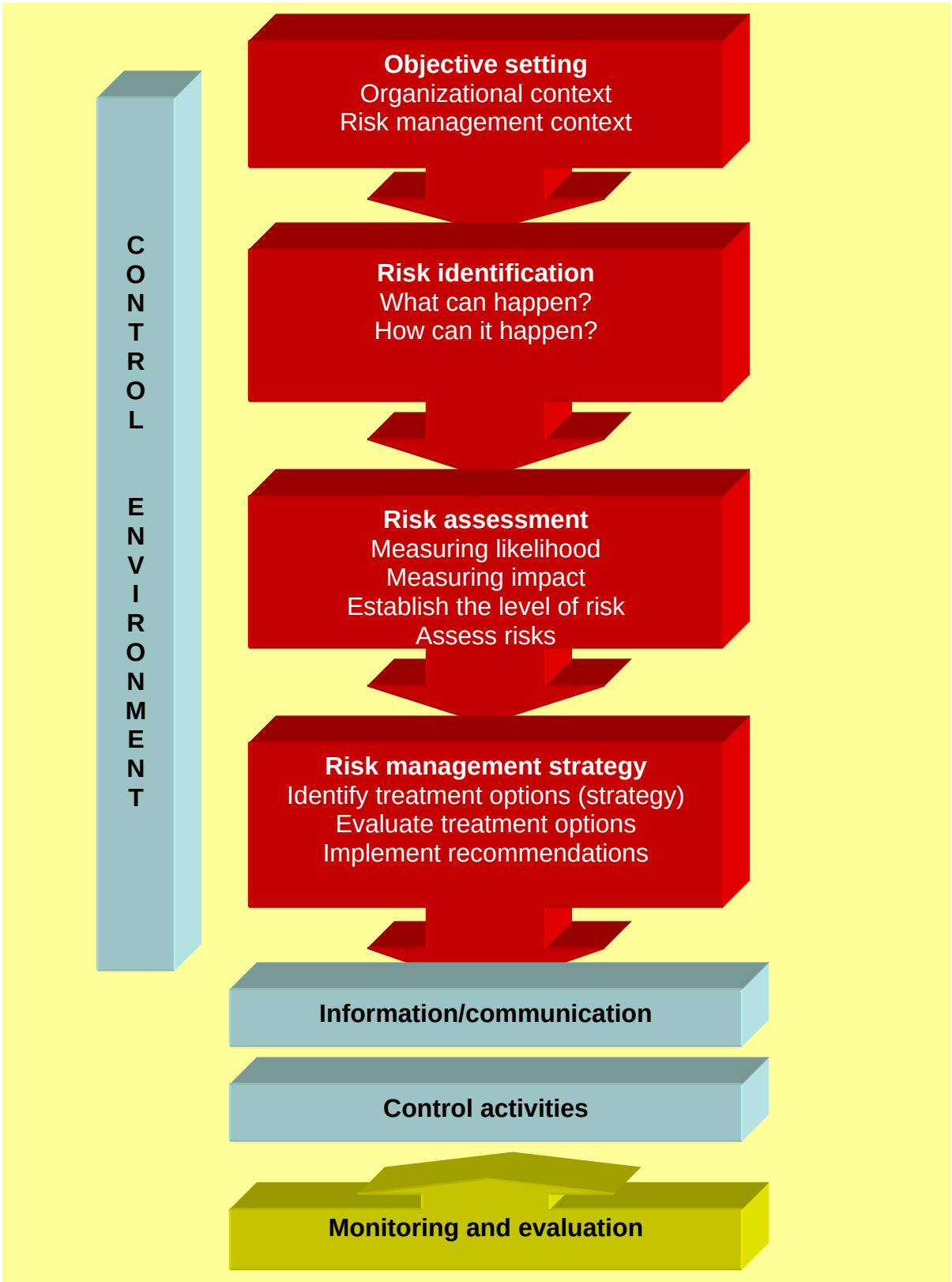
information and communication;

control activities; and

monitoring.

The following table indicates the different relationships between the components:

Eight components of risk management



The components are described as follows:

Component 1: Control environment

The Municipality's control environment is the foundation of risk management, providing discipline and structure. The control environment influences how strategy and objectives are established, municipal activities are structured, and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems, and monitoring activities.

The control environment comprises many elements, including a Municipality's ethical values, competence and development of personnel, management's operating style and how it assigns authority and responsibility.

The executive authority is a critical part of the control environment and significantly influences other control environment elements. As part of the control environment, management establishes a risk management philosophy, establishes the Municipality's risk tolerance levels, inculcates a risk culture and integrates risk management with related initiatives.

The control environment consists of ten different layers that should all be present and functioning. The ten layers are discussed below:

a. Risk management philosophy

A risk management philosophy facilitates the employees' ability to recognize and effectively manage risk. The philosophy – the department's beliefs about risk and how it chooses to conduct its activities and deal with risk – reflects the value the department seeks from risk management and influences how risk management will be applied.

Management should communicate its risk management philosophy to employees through policy statements and other communications.

b. Risk tolerance

Risk tolerance is the degree of risk that a Municipality is willing to accept in pursuit of its goals. The tolerance is established by management and reviewed by the executive authority. Risk management helps management to select a strategy consistent with its risk tolerance. Management looks to align the department, human resources, processes and infrastructure to facilitate successful strategy implementation and enable the department to stay within its risk tolerance levels.

Examples of risk tolerances include:

A Municipality's targets on-time delivery at 98%, with acceptable level of variation in the range of 97%–100% of the time;

Targeting training with a pass rate of 90%, with acceptable performance variation being a pass rate of at least 75%; and

Expecting staff to respond to all customer complaints within 24 hours, but accepting that up to 25% of these complaints may receive a response within 24 –36 hours.

c. Risk culture

Risk culture is the set of shared attitudes, values and practices that characterize how a Municipality considers risk in its day-to-day activities. For those Municipalities that do not explicitly define their risk philosophy, the risk culture may form haphazardly, resulting in significantly different risk cultures within a Municipality or even within a particular Municipal unit or function. Management should strive towards establishing a risk management culture that explicitly considers risk in its day-to-day activities.

d. Executive authority

The executive authority[1] is a critical part of the control environment and significantly influences other control environment elements. Their independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and appropriateness of its actions all play a role. Other factors include the degree to which difficult questions are raised and pursued with management regarding strategy, plans and performance, and interaction that the audit committee has with internal and external auditors.

e. Integrity and values

Strategy and objectives and the way they are implemented and achieved are based on preferences, value judgments and management styles. Management's integrity and commitment to ethical values influence these preferences and value judgments, which are translated into standards of behavior.

[1] Refer definition of Executive Authority under 11 – Roles and Responsibilities

Management integrity is a prerequisite for ethical behavior in all aspects of a Municipality's activities. The effectiveness of risk management cannot rise above the integrity and ethical values of those who create administer and monitor activities.

Formal codes of corporate conduct are important to the foundation of an effective ethics program. Codes address a variety of behavioral issues, such as integrity and ethics, conflicts of interest, illegal or otherwise improper payments, and anti-competitive arrangements. Upward communications channels where employees feel comfortable bringing relevant information is also important. Compliance with ethical standards, whether or not embodied in a written code of conduct, is best ensured by top management's actions and examples.

Of particular importance are resulting penalties to employees who violate such codes. Mechanisms should exist to encourage employee reporting of suspected fraud, corruption and theft, and disciplinary actions against employees who fail to report violations.

f. Commitment to competence

Competence reflects the knowledge and skills needed to perform assigned tasks. Management should decide how well these tasks need to be accomplished weighing the Municipality's strategy and objectives against plans for strategy implementation and achievement of the objectives. A trade-off often exists between competence and cost.

The competency levels for particular jobs should be specified and translated into requisite knowledge and skills. The necessary knowledge and skills in turn may depend on individuals' training and experience.

Factors considered in developing knowledge and skill levels include the nature and degree of judgment to be applied to a specific job. Often a trade-off can be made between the extent of supervision and the requisite competence level of the individual.

g. Philosophy and operating style

Management's philosophy and operating style affect the way the Municipality is managed, including the kinds of risks accepted. A Municipality that has been successful accepting significant risks may have a different outlook on risk management than one that has faced harsh economic or regulatory consequences as a result of venturing into dangerous territory. An informally managed Municipality may control operations largely by face-to-face contact with key managers. A more formally managed one may rely more on written policies, standards of behavior, performance indicators and exception reports. Other elements of management's philosophy and operating style include conscientiousness and conservatism with which

accounting estimates are developed and attitudes toward financial reporting, information technology, business processes and personnel.

The attitude and daily operating style of top management affect the extent to which actions are aligned with risk philosophy and tolerance. An effective environment does not require that risks be avoided; rather it reinforces the need to be knowledgeable about the risks associated with strategic choices and the department's operating environment, both internal and external.

h. Organizational structure

A Municipality's organizational structure provides the framework to plan, execute, control and monitor its activities. A relevant organizational structure includes defining key areas of authority and responsibility and establishing appropriate lines of reporting. A Municipality develops an organizational structure suited to its needs. Some are centralized, others decentralized. Some have direct reporting relationships; others are more of a matrix organization.

The appropriateness of a Municipality's organizational structure depends, in part, on its size and the nature of its activities. A highly structured organization with formal reporting lines and responsibilities may be appropriate for a large Municipality that has numerous operating divisions. However, such a structure could impede the necessary flow of information in a small Municipality. Whatever the structure, a Municipality should be organized to enable effective risk management, and to carry out its activities so as to achieve its objectives.

i. Authority and responsibility

Assignment of authority and responsibility involves the degree to which individuals and teams are authorized and encouraged to use initiative to address issues and solve problems. It also includes the establishment of reporting relationships and authorization protocols, and it pertains to policies that describe appropriate Municipal practices, knowledge and experience of key personnel, and resources provided for carrying out duties.

Alignment of authority and accountability often is designed to encourage individual initiatives, within limits. Delegation of authority, or "empowerment," means surrendering central control of certain decisions to lower echelons – to the individuals whom are closest to everyday business transactions.

A critical challenge is to delegate only to the extent required to achieve objectives. This means ensuring that risk acceptance is based on sound practices for risk identification and assessment, including a comparison between the risks and any potential losses versus gains in arriving at good service delivery decisions.

Another challenge is ensuring that all personnel understand the Municipality's objectives and how their actions interrelate and contribute to achievement of the objectives.

The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. This holds true all the way to the accounting officer, who, with executive authority oversight, has ultimate responsibility for all activities within a Municipality.

j. HR policies and procedures

Human resource policies and practices pertaining to hiring, orientation, training, evaluating, counseling, promoting, compensating and taking remedial actions send a message to employees regarding expected levels of integrity, ethical behavior and competence. For example, standards for hiring the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior, demonstrate a department's commitment to competent and trustworthy staff.

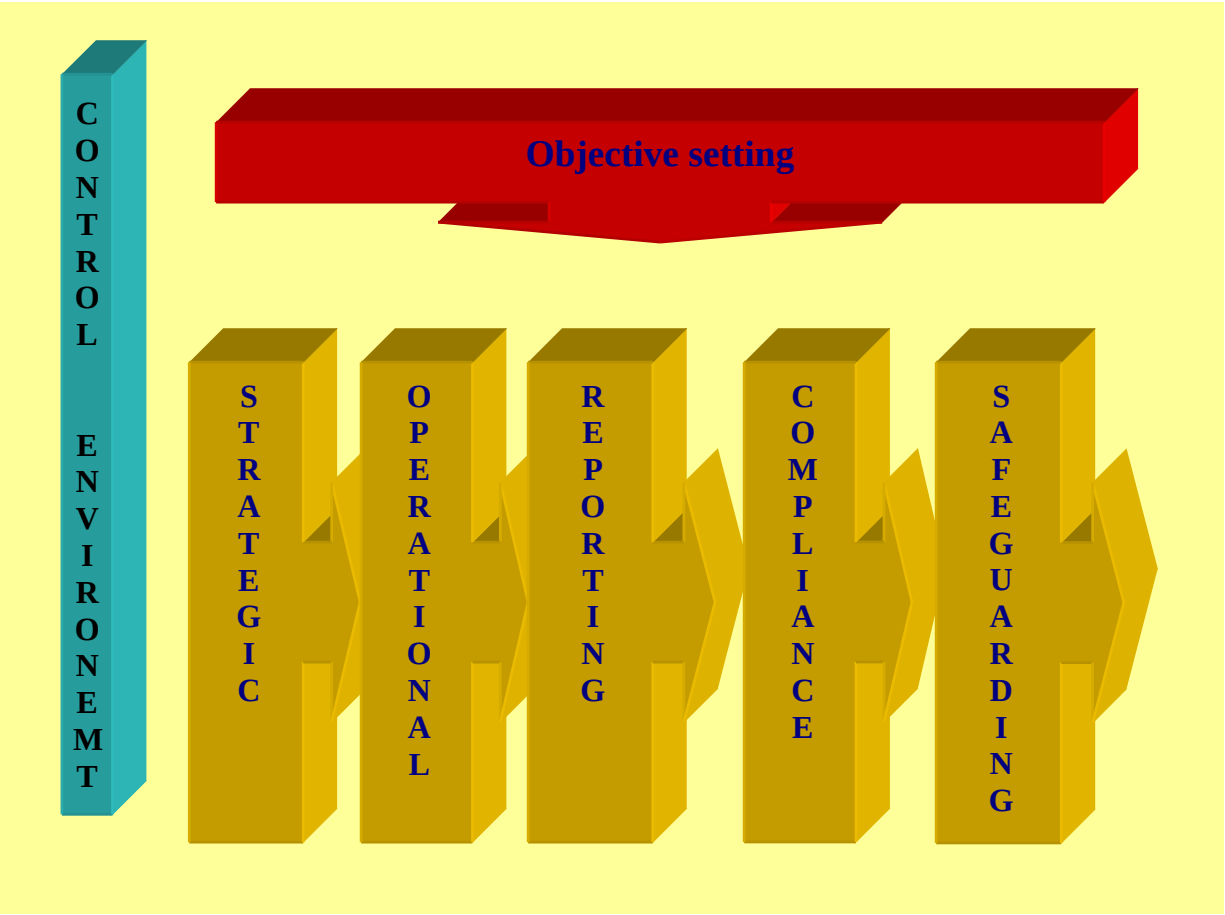
Transfers and promotions driven by periodic performance appraisals demonstrate the Municipality's commitment to the advancement of qualified employees.

Competitive compensation programs that include bonus incentives serve to motivate and reinforce outstanding performance. Similarly disciplinary actions send a message that violations of expected behavior would not be tolerated.

It is essential that employees be equipped to tackle new challenges as issues and risks throughout the department change and become more complex – driven in part by rapidly changing technologies and increasing political influence.

Component 2: Objective Setting

Objectives must exist before management can identify events potentially affecting their achievement. Risk management ensures that management has a process in place to both set objectives and aligns the objectives with the department's mission/vision and is consistent with the department's risk tolerance. The setting of these objectives is usually completed during the, "Strategic planning and Budgetary process."



Municipal objectives can be viewed in the context of five categories:

Strategic – relating to high-level goals, aligned with and supporting the Municipality's mission/vision;

Operations – relating to effectiveness and efficiency of the Municipality's operations, including performance and service delivery goals. They vary based on management's choices about structure and performance;

Reporting – relating to the effectiveness of the Municipality's reporting. They include internal and external reporting and may involve financial or non-financial information;

Compliance – relating to the Municipality's compliance with applicable laws and regulations;

Safeguarding of assets – relating to prevention of loss of a Municipality's assets or resources, whether through theft, waste or inefficiency. This applies to the prevention or timely detection of unauthorized acquisition, use, or disposition of the Municipality's assets.

This categorization of Municipal objectives allows management and the executive authority to focus on separate aspects of risk management, although overlapping of the objectives when processes are managed is almost always applicable.

Component 3: Risk identification

During the phase of risk identification, management considers external and internal, as well as financial and non financial factors that influence a Municipality's policy and management agenda. Identifying major trends and their variation over time is particularly relevant in providing early warnings.

Some external factors to be considered for potential risks include:

- Political: the influence of international governments and other governing bodies;
- Economic: international, national markets and globalizations;
- Social: major demographic and social trends, level of citizen engagement; and
- Technological.

Internal factors reflect management's choices and include such matters as:

- The overall management framework;
- Governance and accountability frameworks;
- Level of transparency required;
- Values and ethics;
- Infrastructure;
- Policies, procedures and processes;
- Human resource capacity; and
- Technology.

A Municipality's risk identification methodology may comprise a combination of techniques together with supporting tools. Risk identification techniques look to both the past and the future. Techniques that focus on past events and trends consider such matters as payment default histories, overspending patterns, fraud and corruption and historic poor service delivery.

Techniques that focus on future exposures consider such matters as shifting demographics, new laws and regulations and the impact of HIV on the resident population.

It may be useful to group potential events into categories. By aggregating events horizontally across a Municipality and vertically within operating units, management develops an understanding of the interrelationships between events, gaining enhanced information as a basis for risk assessment.

Events potentially either have a negative impact, a positive impact or both. Events that have a potentially negative impact represent risks, which require management's assessment and response. Accordingly, risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives.

Events with a potentially positive impact represent opportunities or offset the negative impact of risks. Those representing opportunities are channeled back to management's strategy or objective-setting processes, so that actions can be formulated to seize the opportunities, whereas events potentially offsetting the negative impact of risks are considered in management's risk assessment and response.

Possible Methods of Identifying Risks

- interview/focus group discussion;
- audits or physical inspections;
- brainstorming;
- survey, questionnaire, Delphi technique;
- examination of local and/or overseas experience;
- networking with peers, industry groups and professional associations;
- judgmental – speculative, conjectural, intuitive;
- history, failure analysis;
- examination of personal experience or past department or public entity experience;
- incident, accident and injury investigation;
- databank of risk events which have occurred;
- scenario analysis;
- decision trees;
- strengths, weaknesses, opportunities, threats (SWOT) analysis;
- flow charting, system design review, systems;
- analysis, systems engineering techniques e.g. Hazard and Operability (HAZOP) studies;
- work breakdown structure analysis; and
- operational modeling.

Possible Sources of Risk

(a) new activities and services;
(b) disposal or cessation of current activities;
(c) outsourcing to external service providers;
(d) commercial/legal changes;
(e) changes in the economic conditions;
(f) socio-political changes, like elections;
(g) national and international events;
(h) personnel/human behaviour;
(i) behaviour of contractors/private suppliers;
(j) financial/market conditions;
(k) management activities and controls;
(l) misinformation;
(m) technology/technical changes, i.e. new hardware and software implementations;
(n) operational (the activity itself) changes;
(o) department interruption;
(p) occupational health and safety;
(q) property/assets;
(r) security (including theft/fraud/impersonation);
(s) natural events;
(t) public/professional/product liability

Possible Areas of Risk Impact

A risk assessment should concentrate on all significant possible areas of impact relevant to the organization or activity, and may include:

- assets and resources, including human, physical, financial, technical and information;
- cost, both direct (including budget impacts) and indirect;
- human resources;
- community groups;
- Minister/Government;
- performance of activities (i.e. how well activity performed);
- timeliness of activities, including start-time, downstream or follow-up impacts;
- organizational behaviour;
- changes in departments' roles;
- environment; and
- Intangibles.

Key questions that can be used to identify and control risks

- What, when, where, why and how risks are likely to occur, and who might be involved?
- What is the source of each risk?
- What are the consequences of each risk?
- What controls presently exist to mitigate each risk?
- To what extent are controls effective?
- What alternative, appropriate controls are available?
- What are the department obligations – external and internal?
- What is the need for research into specific risks?
- What is the scope of this research, and what resources are required?
- What is the reliability of the information?
- Is there scope for bench-marking with peer organizations?

Component 4: Risk Assessment

Risk assessment allows a Municipality to consider how potential events might affect the achievement of objectives. Management assesses events by analyzing the likelihood and its impact

The risk assessment process includes 4 steps:

Step 1: Quantifying the parameters (scoring system) of impact and likelihood before the actual assessment (see the example below);

Example: Impact on cost		
Score	**Impact**	**Consequence**
5	Catastrophic	Leads to termination of the project
4	Critical	cost increase > 20%
3	Major	cost increase > 10%
2	Significant	cost increase < 10%
1	Negligible	Minimal or no impact on cost

Example: Certainty of occurrence		
Score	**Likelihood**	**Occurrence**
5	Maximum	Certain to occur, almost every time
4	High	Will occur frequently, 1 out of 10 times
3	Medium	Will occur sometimes, 1 out of 100 times
2	Low	Will seldom occur, 1 out of 1000 times
1	Minimum	Will almost never occur, 1 out of 10 000 times

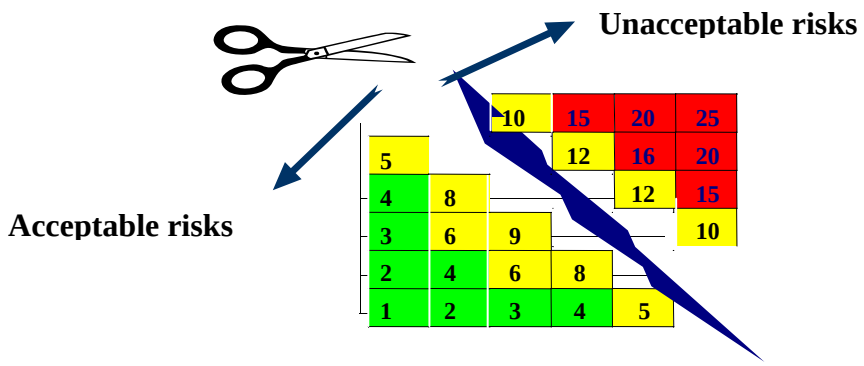
Step 2: Applying the parameters to the risk matrix to indicate what areas of the risk matrix would be regarded as high, medium or low risk (see the example below);

Risk index = impact x likelihood

I	5	5	10	15	20	25
M	4	4	8	12	16	20
P	3	3	6	9	12	15
A	2	2	4	6	8	10
C	1	1	2	3	4	5
T		1	2	3	4	5
LIKELIHOOD						

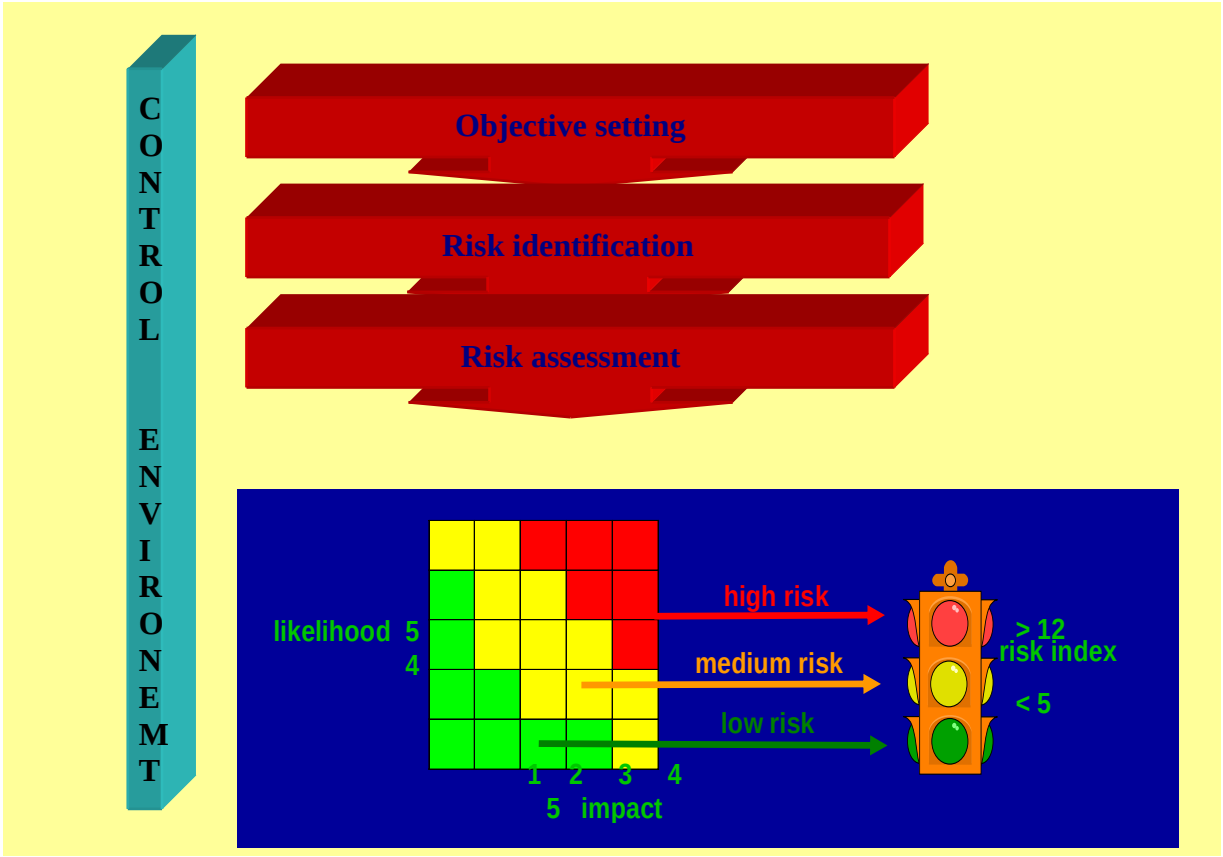
Risk index	Risk Magnitude
20 - 25	Maximum
15 - 19	High risk
10 - 14	Medium risk
5 - 9	Low risk
1 - 4	Minimum risk

Step 3: Determining the risk acceptance criteria by identifying what risks will not be tolerated (see the example below);



Step 4: Determine risk acceptability and what action will be proposed to reduce the risk (see the example below).

Risk index	Risk magnitude	Risk acceptability	Proposed actions
20 – 25	Maximum risk	Unacceptable	Take action to reduce risk with highest priority, accounting officer and executive authority attention.
15 – 19	High risk	Unacceptable	
10 – 14	Medium risk	Unacceptable	Take action to reduce risk, inform senior management.
5 – 9	Low risk	Acceptable	No risk reduction - control, monitor, inform management.
1 - 4	Minimum risk	Acceptable	No risk reduction - control, monitor, inform management.



Likelihood represents the possibility that a given event will occur, while impact represents its effect should it occur. Estimates of risk likelihood and impact often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates. Internally generated data based on a department's own experience may reflect less subjective personal bias and provide better results than data from external sources. However, even where internally generated data are a primary input, external data can be useful as a checkpoint or to enhance the analysis. Users must be cautious when using past events to make predictions about the future, as factors influencing events may change over time.

A Municipality's risk assessment methodology normally comprises a combination of qualitative and quantitative techniques. Management often uses qualitative assessment techniques where risks do not lend themselves to quantification or when sufficient credible data required for quantitative assessments either are not practicably available or obtaining or analyzing data are not cost-effective. Quantitative techniques typically bring more precision and are used in more complex and sophisticated activities to supplement qualitative techniques. The quantification of likelihood and impact is normally displayed in a heat map, by performing the four steps explained as part of the control environment.

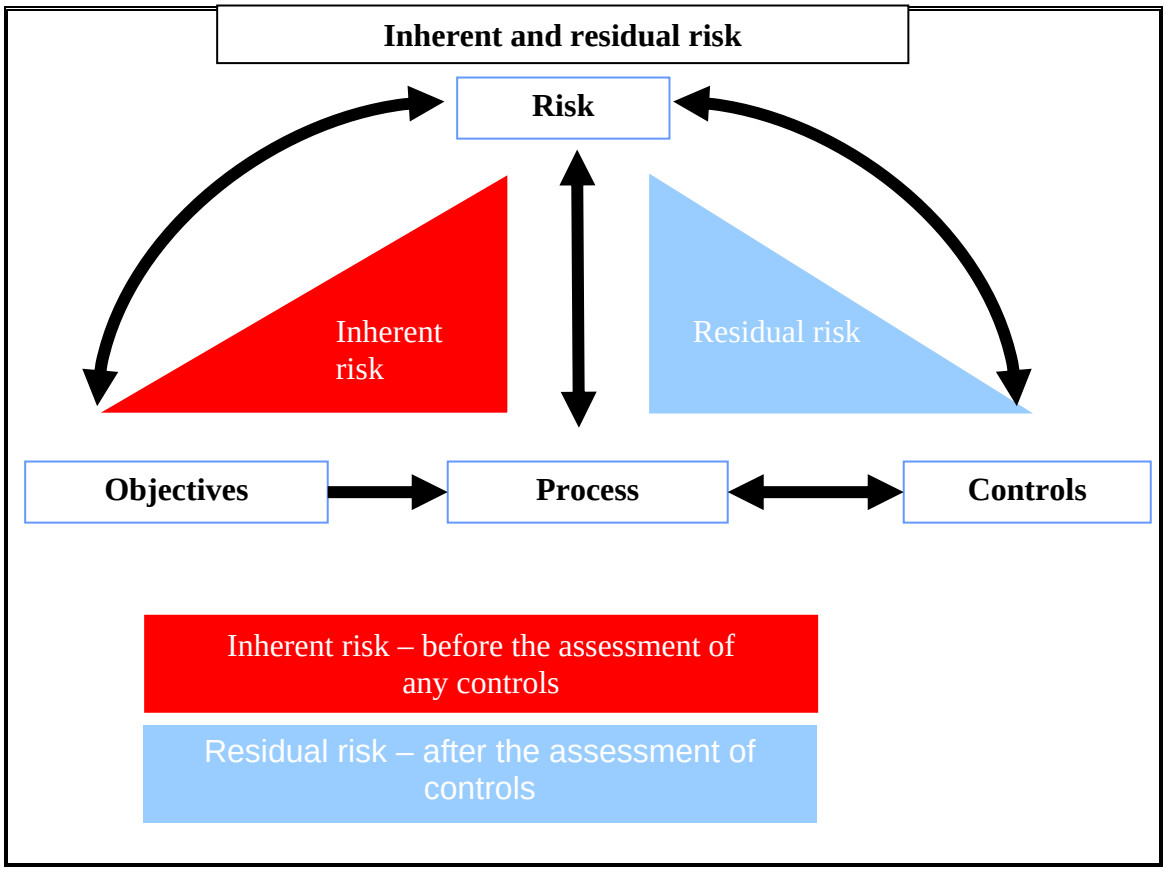
Management often uses performance measures in determining the extent to which objectives are being achieved. It may be useful to use the same unit of measure when considering the potential impact of a risk to the achievement of a specified objective.

Management may assess how events correlate, where sequences of events combine and interact to create significantly different probabilities or impacts. While the impact of a single event might be slight, a sequence of events might have more significant impact.

Where potential events are not directly related, management should assess them individually. Where risks are likely to occur within multiple Municipal units, management may assess and group identified events into common categories. There is usually a range of possible results associated with a potential event, and management considers them as a basis for developing a risk management strategy. Through risk assessment, management considers the positive and negative consequences of potential events, individually or by category, across the Municipality.

Risk assessment is applied first to inherent risk – the risk to the department in the absence of any action management might take to alter either the risk's likelihood or impact. Once risk management strategies have been developed, management then uses risk assessment techniques in determining residual risk – the risk remaining after management's action to alter the risk's likelihood or impact.

The following diagram differentiate between inherent and residual risk:

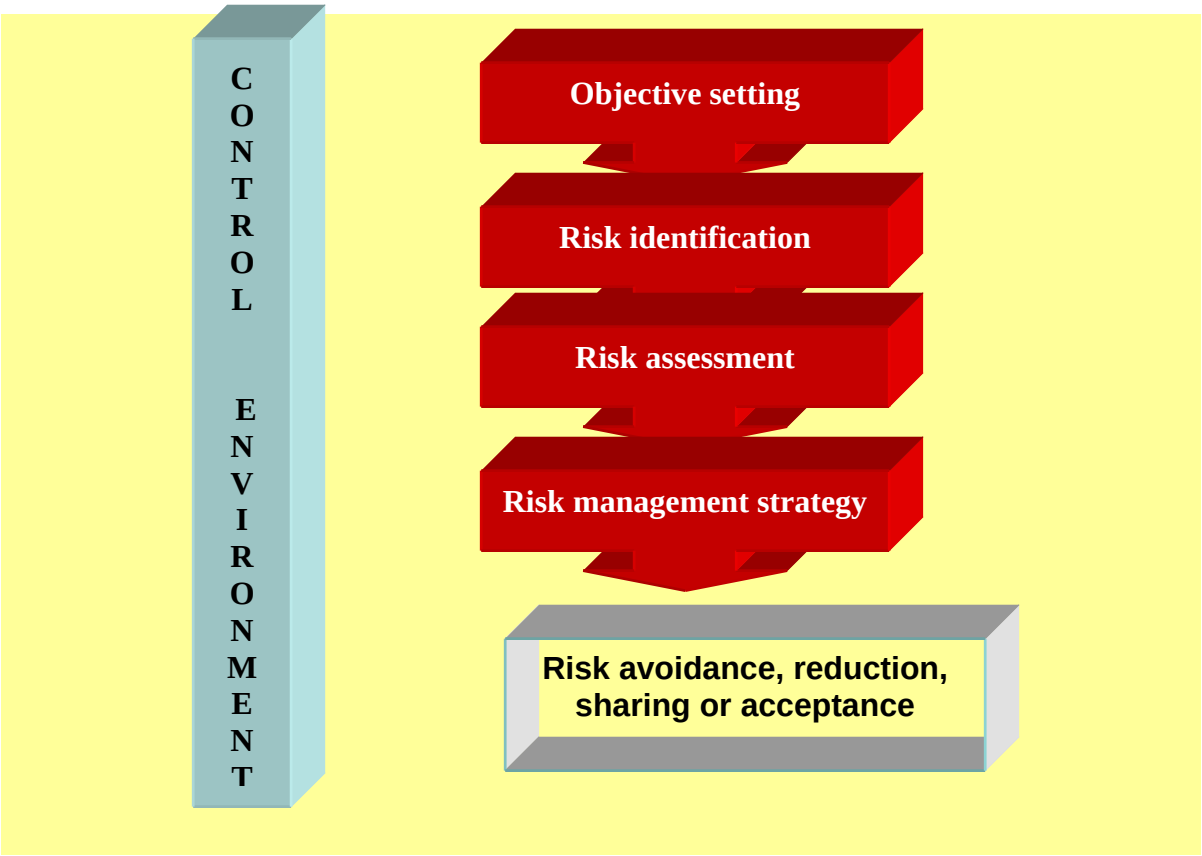

Inherent and residual risk
Risk
Inherent risk
Residual risk
Objectives
Process
Controls
Inherent risk – before the assessment of any controls
Residual risk – after the assessment of controls

Component 5: Risk management strategy

Management identifies risk management strategy options, which should include a fraud prevention plan, and consider their effect on event likelihood and impact, in relation to risk tolerances, costs versus benefits, and thereafter designs and implements response options.

The consideration of risk management strategies and selecting and implementing a risk management strategy is integral to risk management and requires that management select a response that is expected to bring risk likelihood and impact within the department's risk tolerance level.

Risk management strategies fall within the categories of risk avoidance, reduction, sharing and acceptance. Avoidance responses take action to remove the activities that give rise to the risks. Reduction responses reduce the risk likelihood, impact, or both. Sharing responses reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Acceptance responses take no action to affect likelihood or impact because it is such a minimal risk, or the cost to implement the risk is too high relative to the cost of the risk.



As part of risk management, for each significant risk a Municipality considers potential responses from a range of response categories. This gives sufficient depth to response selection and also challenges the “status quo.” Having selected a risk management strategy with appropriate responses, management reassesses the remaining residual risk. Management considers risk from a Municipal-wide, or portfolio**,** perspective, and may take an approach in which the manager responsible for each department, function or department unit develops a composite assessment of risks and risk management strategies for that unit. This view reflects the risk profile of the unit relative to its objectives and risk tolerances. With a view of risk for individual units, the most senior manager of the Municipality is positioned to take a portfolio view, to determine whether the department’s risk profile is commensurate with its overall risk tolerance relative to its objectives.

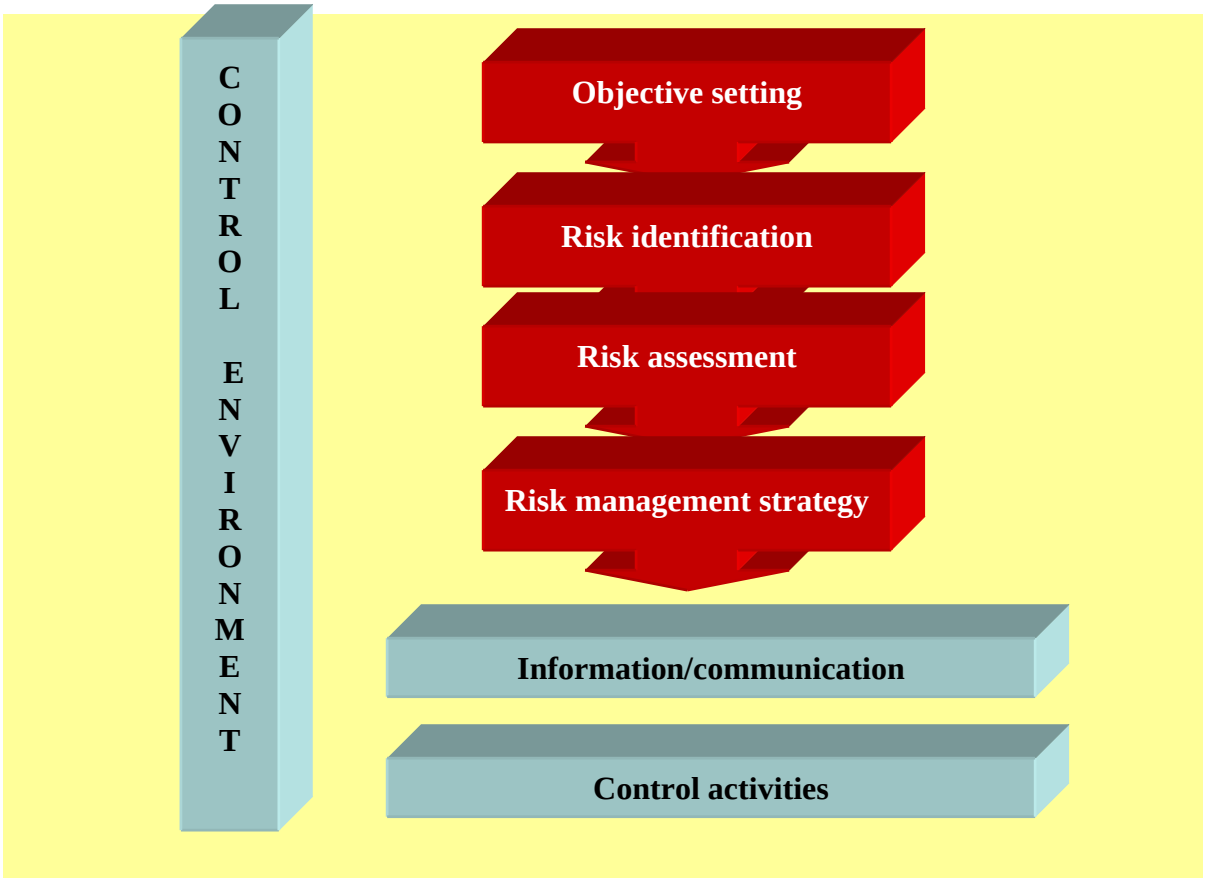
Management should recognize that some level of residual risk will always exist, not only because resources are limited, but also because of inherent future uncertainty and limitations inherent in all activities.

Component 6: Information and Communication

Pertinent information – both from internal and external sources, financial or non-financial – must be identified, captured and communicated in a form and timeframe that enable personnel to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the Municipality, as well as the exchange of relevant information with external parties, such as customers, suppliers, regulators and shareholders.

Information is needed at all levels of a Municipality to identify, assess and respond to risks, and to otherwise run the Municipality and achieve its objectives. An array of information is used, relevant to one or more objectives categories. Information comes from many sources – internal and external, and in quantitative and qualitative forms – and allows risk management responses to changing conditions in real time.

The challenge for management is to process and refine large volumes of data into relevant and actionable information. This challenge is met by establishing an information systems infrastructure to source, capture, and process, analyze and report relevant information. These information systems – usually computerized but also involving manual inputs or interfaces – often are viewed in the context of processing internally generated data relating to transactions.



Information systems have long been designed and used to support Municipal strategy. This role becomes critical as Municipalities need change and technology creates new opportunities for strategic advantage. To support effective risk management, a Municipality captures and uses historical and current data. Historical data allow the Municipality to track actual performance against targets, plans and expectations. It provides insights into how the Municipality performed under varying conditions, allowing management to identify correlations and trends and to forecast future performance. Historical data also can provide early warnings of potential events that warrant management attention.

Present or current state data allow a Municipality to assess its risks at a specific point in time and remain within established risk tolerances. Current state data allow management to take a real-time view of existing risks inherent in a process, function or unit and to identify variations from expectations. This provides a view of the Municipality's risk profile, enabling management to alter activities as necessary to fit in with the acceptable level of risk

Information is a basis for communication, which must meet the expectations of groups and individuals, enabling them to effectively carry out their responsibilities. Among the most critical communications channels is that between top management and the executive authority.

Management must keep the executive authority up-to-date on performance, developments, risks and the functioning of risk management, and other relevant events and issues. The more effective the communication, the more successful the executive authority will be in carrying out its oversight responsibilities, in acting as a sounding executive authority on critical issues and in providing advice, counsel and direction. By the same token, the executive authority should communicate to management what information it needs and provide feedback and direction.

Management provides specific and directed communication addressing behavioral expectations and the responsibilities of personnel. This includes a clear statement of the Municipality's risk management philosophy and approach and delegation of authority.

Communication about processes and procedures should align with, and underpin, the desired risk culture. In addition, communication should be appropriately "framed" – the presentation of information can significantly affect how it is interpreted and how the associated risks or opportunities are viewed.

Communication should raise awareness about the importance and relevance of effective risk management, communicate the Municipality's risk tolerance levels, implement and support a common risk language, and advise personnel of their roles and responsibilities in effecting and supporting the process of risk management. Communications channels also should ensure personnel can communicate risk-based information across Municipal units, processes or functional silos. In most cases, normal reporting lines in a department are the appropriate channels of communication. In some circumstances, however, separate lines of communication are needed to serve as a fail-safe mechanism in case normal channels are inoperative. Whatever channels of communication are used, it is imperative that personnel understand that there will be no reprisals for reporting relevant information.

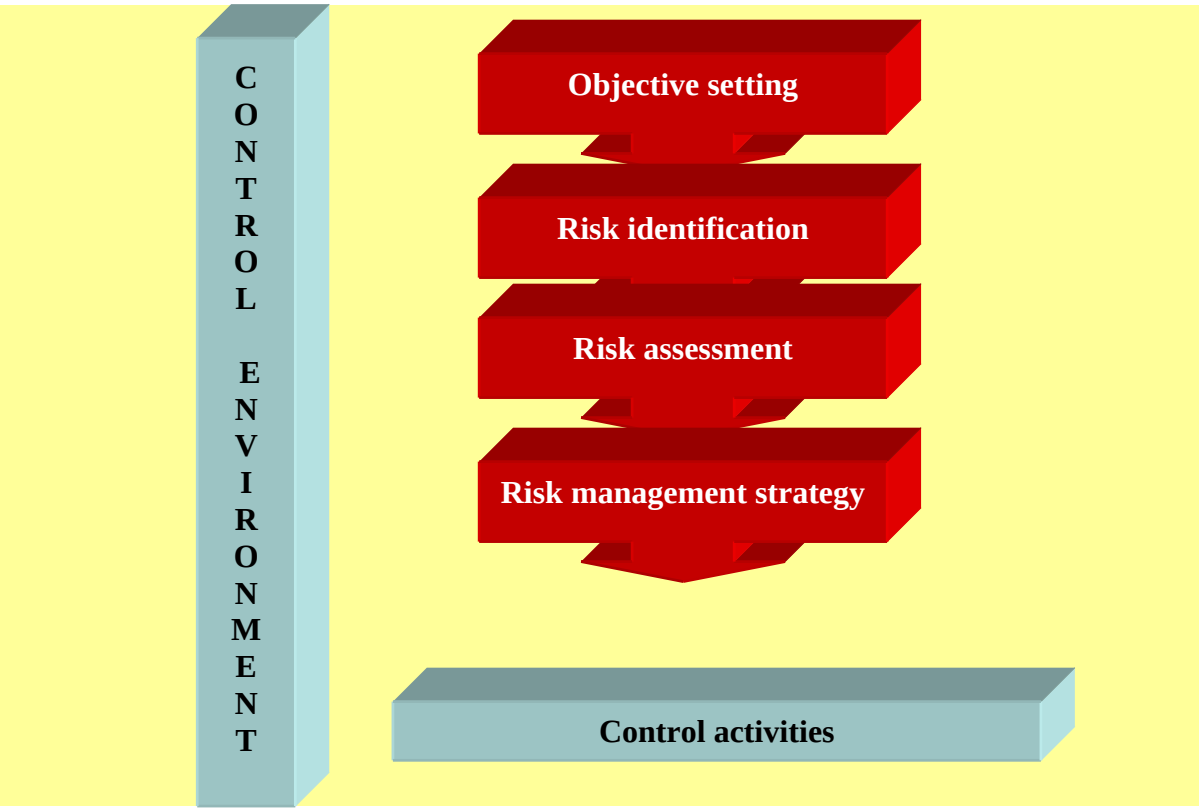
External communications channels can provide highly significant input on the design or quality of products or services. Management considers how its risk tolerance aligns with those of its

customers, suppliers and partners, ensuring that it does not inadvertently take on too much risk through its department interactions.

Component 7: Control Activities

Risk responses serve to focus attention on control activities needed to help ensure that the risk responses are carried out properly and in a timely manner. Control activities are part of the process by which a department strives to achieve its business objectives.

Control activities are the policies and procedures that help ensure risk management strategies are properly executed. They occur throughout the Municipality, at all levels and in all functions.



They usually involve two elements: a policy establishing what should be done and procedures to affect the policy.

Internal Control

Internal control is an integral part of risk management. This RMF encompasses internal control, forming a more robust conceptualization and tool for management.

Control procedures relate to the actual policies and procedures in addition to the control environment that management has established to achieve the department's objectives. Policies and procedures help create boundaries and parameters to authority and responsibility, and also provide some scope of organisational precedent for action.

Control procedures

Specific control procedures include:

Reporting, reviewing and approving reconciliations;

Checking the arithmetical accuracy of records;

Controlling applications and environment of computer information systems;

Maintaining and reviewing control accounts and trial balances;

Approving and controlling documents;

Comparing internal data with external sources of information;

Comparing the results of cash, security and inventory counts with accounting records;

Comparing and analyzing the financial results with budgeted amounts;

Limiting the direct physical access to records.

Context of control

The following concepts are important in understanding the nature and context of control:

- Controls should be capable of responding immediately to evolving risks to the core business of the Municipality arising from factors within the Municipality and to changes in the environment;

- The cost of controls must be balanced against the benefits, including the risks it is designed to manage;

- The system of control must include procedures for reporting immediately to appropriate levels of management any significant findings of weaknesses that are identified together with details of corrective action taken;

- Control can help minimize the occurrence of errors and breakdowns, but cannot provide absolute assurance that they will not occur; and

- The system of internal control should be embedded in the operations of the department and form part of its culture.

Broad internal control focus areas

Internal controls established in a Municipality should focus on the following areas:

Adequate segregation of duties

Key duties and responsibilities in authorizing, processing, recording, and reviewing transactions and events should be separated among individuals;

Custody and accountability for resources

Access to resources and records are to be limited to authorized individuals who are accountable for their custody or use;

Prompt and proper recording and classification of transactions

To ensure that information maintains its relevance and value to management in controlling operations and decision-making and to ensure that timely and reliable information is available to management;

Authorization and execution of transactions

Requires that employees execute their assigned duties in accordance with directives and within the limitations established by management or legislation;

Documentation

I

Internal control structures, i.e. policies and procedures, and all transactions and significant events are to be clearly documented;

Management supervision and review

Competent supervision is to be provided, including assignment, review and approval of an employee's work.

Employees should be provided with the necessary guidance and training to help ensure that errors, wasteful, and wrongful acts are minimized and that specific management directives are understood and achieved.

I In addition, computer controls should be geared towards the following areas:

Access controls

Controls should be designed to prevent:

Unauthorized changes to programs which process data;

Access to files which store accounting and financial information and application programs;

Access to computer operating systems and system software programs;

User-id and passwords should be used to limit access to programs, data files and software applications;

Firewalls should be installed to prevent data corruption from unauthorized external access.

Controls should be designed to manage the operation of the system and to ensure that programmed procedures are applied correctly and consistently during the processing of data.

Computer controls such as scheduling of processing time, execution of programs by competent personnel, monitoring and review of the function of hardware, division and rotation of duties and maintenance of system and manual logs with regular follow-up management should be available.

System Software Programs

Controls should be designed for programs, which do not process data to ensure that they are installed or developed and maintained in an authorized and effective manner, and that access to system software is limited.

This could be achieved through security over system software, database systems, networks and processing by users on personal computers. There should be support structures, error correction methods and adequate documentation for the systems.

Controls should be designed to ensure the continuity of processing, by preventing system interruption or limiting this to a minimum.

Controls that should be in place include physical protection against the elements such as fire, water and power. There should be emergency plan and disaster recovery procedures, provision of alternative processing facilities, backups of data files, maintenance of hardware, adequate insurance, cable protection, uninterruptible power supply, prevention of viruses and personnel controls affecting security and continuity.

Information systems controls

With widespread reliance on information systems, controls are needed over significant systems.

Two broad groupings of information systems control activities can be used.

The first is general controls, which apply to many if not all application systems and help ensure their continued, proper operation.

The second is application controls, which include computerized steps within application software to control the technology application. Combined with other manual process controls where necessary, these controls ensure completeness, accuracy and validity of information.

General controls include controls over information technology management, which will address the information technology oversight process, monitoring and reporting information technology activities, and Municipal improvement initiatives.

Other controls include information technology infrastructure, security management and software acquisition, development and maintenance. These controls apply to all systems from mainframe to client/server to desktop computing environments.

Application controls are designed to ensure completeness, accuracy, authorization and validity of data capture and transaction processing. Individual applications may rely on effective operation of controls over information systems to ensure that interface data are generated when needed, supporting applications are available and interface errors are detected and corrected timeously.

Because each Municipality has its own set of objectives and implementation approaches, there will be differences in objectives, structure and related control activities. Even if two Municipalities had identical objectives and structures, their control activities would likely be different, as different people who use individual judgments in effecting internal control manage them. Moreover, controls reflect the environment and industry in which a Municipality operates, as well as the complexity of its departments, its history and its culture.

Component 8: Monitoring

Risk management should be regularly monitored – a process that assesses both the presence and functioning of its components and the quality of their performance over time. Monitoring can be done in two ways: through ongoing activities or separate evaluations. This will ensure that risk management continues to be applied at all levels and across the Municipality.

Ongoing monitoring is built into the normal, recurring operating activities of a Municipality, is performed on a real-time basis and reacts dynamically to changing conditions and is ingrained in the Municipality. As a result, it is more effective than separate evaluations. Since separate evaluations take place after the fact, problems often will be identified more quickly by ongoing monitoring routines. Many Municipalities with sound ongoing monitoring activities nonetheless conduct separate evaluations of risk management.

The frequency of separate evaluations is a matter of management's judgment. In making that determination, consideration is given to the nature and degree of changes, from both internal and external events, and their associated risks, the competence and experience of the personnel implementing risk management strategies and related controls and the results of the ongoing monitoring. Usually, some combination of ongoing monitoring and separate evaluations will ensure that risk management maintains its effectiveness over time.

The extent of documentation of a Municipality’s risk management varies with the Municipality's size, complexity and similar factors. The fact that elements of risk management are not documented does not mean that they are not effective or that they cannot be evaluated. However, an appropriate level of documentation usually makes monitoring more effective and efficient. Where management intends to make a statement to external parties regarding risk management effectiveness, it should consider developing and retaining documentation to support the statement.

All risk management deficiencies that affect a Municipality’s ability to develop and implement its strategy and to achieve its established objectives should be reported to those positioned to take necessary action. The nature of matters to be communicated will vary depending on individuals' authority to deal with circumstances that arise and on the oversight activities of superiors. The term “deficiency” refers to a condition within the risk management process worthy of attention. A deficiency, therefore, may represent a perceived, potential or real shortcoming, or an opportunity to strengthen the process to increase the likelihood that the Municipality’s objectives will be achieved. Information generated in the course of operating activities usually is reported through normal channels. Alternative communications channels also should exist for reporting sensitive information such as illegal or improper acts, fraud, corruption and theft.

Providing relevant information on risk management deficiencies to the right party is critical. Protocols should be established to identify what information is needed at a particular level for effective decision making. Such protocols reflect the general rule that a manager should receive information that affects actions or behavior of personnel under his or her responsibility, as well as information needed to achieve specific objectives.

5. Limitations of Risk Management

Effective risk management helps management achieve objectives. But Municipal risk management, no matter how well designed and operated, does not ensure a Municipality's success. The achievement of objectives is affected by limitations inherent in all management processes. Shifts in government policy, programs or economic conditions can be beyond management's control. Decision-making is based on judgments and can be faulty, resulting in breakdowns because of such human failures as simple error or mistake. Municipal risk management cannot change an inherently poor manager into a good one. Additionally, controls can be circumvented by the collusion of two or more employees, and management has the ability to override the risk management process, including risk management strategies and controls.

The design of risk management must reflect the reality of resource constraints, and the risk management benefits must be considered relative to their costs. Thus, while risk management can help management achieve its objectives, it is not a panacea.

6. Roles and Responsibilities

Everyone in a Municipality has responsibility for risk management.

Executive authority –

- *The duly elected Council as representatives of the Community.*

Management is accountable to the executive authority, which provides governance, guidance and oversight. By selecting management, the executive authority has a major role in defining what it expects in integrity and ethical values and can confirm its expectations through oversight activities. Similarly, by reserving authority in certain key decisions, the executive authority plays a role in setting strategy, formulating high-level objectives and broad-based resource allocation. The executive authority provides oversight with regard to risk management by:

- Knowing the extent to which management has established effective risk management in the Municipality;
- Being aware of and concurring with the Municipality's risk tolerance;
- Reviewing the Municipality's portfolio view of risks and considering it against the Municipality's risk tolerance; and
- Being aware of the most significant risks and whether management is responding appropriately.

The executive authority is part of the control environment step and must have the requisite composition and focus for risk management to be effective.

Management – The accounting officer is ultimately responsible for and should assume "ownership" of risk management. More than any other individual, the accounting officer sets the "tone at the top" that affects integrity and ethics and other factors of the control environment. In any Municipality, the accounting officer fulfills this duty by providing leadership and direction to senior managers and reviewing the way they manage the Municipality. Senior managers, in turn, assign responsibility for establishment of more specific risk management policies and procedures to personnel responsible for individual units' functions.

In a smaller Municipality, the influence of the accounting officer, often an owner-manager, is usually more direct. In any event, in a cascading responsibility, a manager is effectively an accounting officer of his or her sphere of responsibility. Also significant are leaders of staff functions such as compliance, finance, human resources and information technology, whose monitoring and control activities cut across, as well as up and down, the operating and other units of a Municipality.

Risk Officer – A risk officer works with other managers in establishing and maintaining effective risk management in their areas of responsibility. The risk officer also may have responsibility for monitoring progress and for assisting other managers in reporting relevant risk information up, down and across the department, and may be a member of an internal risk management committee.

Internal Auditors – Internal auditors play an important role in the monitoring of risk management and the quality of performance as part of their regular duties or upon special request of senior

management, which is approved by the audit committee. They may assist both management and the executive authority or audit committee by monitoring, examining, evaluating, reporting on and recommending improvements to the adequacy and effectiveness of management's risk management processes. Such request should however be routed through the audit committee to ensure that such involvement does not effect the completion of the approved audit plan.

Other Personnel – Risk management is, to some degree, the responsibility of everyone in a Municipality and therefore should be an explicit or implicit part of everyone's job description. Virtually all personnel produce information used in risk management or take other actions needed to manage risks. Employees are responsible for communicating risks such as problems in operations, non-compliance with the code of conduct, other policy violations or illegal actions.

A number of external parties often contribute to achievement of a department's objectives. External auditors bring an independent and objective view, contributing directly through the financial statement audit and internal control examinations, and indirectly by providing additional information useful to management and the executive authority in carrying out their responsibilities. Others providing information to the department useful in effecting risk management are regulators, customers, financial analysts and the news media.

External parties, however, are not responsible for the department's risk management.

APPROVED ON THIS _____ DAY OF _____ 2007

MR Z SAUL
MUNICIPAL MANAGER

MS H G JENKINS
EXECUTIVE MAYOR

CHAIR PERSON
AUDIT COMMITTEE

Annexure A: Glossary of selected technical terms

Brainstorming: the unstructured and dynamic generation of ideas by a group of human resources where anything and everything is acceptable. It is particularly useful in generating a list of possible project risks.

Budget: a plan showing the amounts of money allocated to various projects, programmes or activities decided on during the planning stage.

Compound Risk: a risk that comprises a number of inter-related risks.

Contingency: sums of money or amounts of time that are set aside as contingency as determined by risk analysis results, which may be used in the event of risks occurring.

Delphi technique: a group of individuals independently and anonymously estimate the outcome of an uncertain event. The collective results are reported back to the group and the individuals then revise their estimates. This process continues until the collective estimates stabilise.

Event: An incident, outcome, issue or result that occurs in a certain place during a particular interval of time.

Impact: an assessment of the adverse effect of the risk occurring. Commonly used in risk analysis as one part of the assessment of a risk the other being Likelihood.

Likelihood: Likelihood is an assessment of the probability of a risk occurring. Used in Risk Analysis as one part of the assessment of a risk, the other being Impact.

Modelling tools: Scenario analysis and forecasting models to indicate the range of possibilities and to build scenarios into contingency plans.

***Probability*:** usually used in the context of risk as a measure of the likelihood of a risk occurring.

***Qualitative Risk Analysis*:** a generic term for subjective methods of assessing risks e.g. identification of likelihood and impact.

***Quantitative Risk Analysis*:** a generic term for mathematical techniques for analysis and assessing risk e.g. PERT and Monte Carlo Analyses.

***Risk*:** the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences and likelihood.

***Risk Analysis*:** the process of ascertaining the probability and impact of uncertain events using one or more of the techniques available.

Risk Tolerance: the tendency of the organisation to undertake risky projects as reflected in management philosophy and policies.

***Risk Avoidance*:** the process of planning activities to avoid risks, which have been identified by using an alternative method of service delivery.

***Risk factors*:** observable and measurable indications of the presence of risk.

Risk Identification: the process of identifying risks together with their likelihood and impact. The most important feature of identification is a risk statement.

Risk Management: the overall process of managing risk including risk identification, risk analysis, risk reduction, risk transfer, risk avoidance, and contingency planning.

Risk Management Plan: a document that contains all the information about the risks, processes, resources, and techniques that are available and to be utilised in conducting risk management activities.

Risk Matrix (heat map): a matrix containing the identified risks as rows and columns for Impact and Likelihood. Each cell in the matrix contains a classification from the risk ranking process.

Risk Prioritising: the ordering of Risks according to their risk value and then deciding which need to be considered for risk reduction, risk transfer, risk avoidance, contingency allowance, active monitoring, etc.

Risk Ranking: the allocation of a classification to the impact or likelihood of a risk. This may be in the form of High, Medium, Low, or a numeric classification on a scale or index of, say, 1 to 5.

Risk Reduction: action taken to reduce the likelihood or impact of a risk occurring.

Risk tolerance levels: the level of risk exposure that management is prepared to tolerate.

Risk Transfer: where a contractual arrangement exists between two parties for delivery and acceptance of a product the liability for the costs of a risk may be transferred from one party to the other. A good example of risk transfer exists in Private Public Partnerships (PPP's). Note that insurance is also some form of risk transfer.

Risk Value: the number obtained when numeric impact and likelihood values are multiplied.

***Secondary Risk*:** a risk that comes about because of avoiding or reducing another risk.

Annexure B: Best Practices

A. Integrating risk management into other management practices

This section reports on the best practices for integrating risk management into management practices.

1. Promoting an organizational philosophy and culture that says everybody is a risk manager

By far, the predominant practice for integrating risk management is to build an organizational culture in which everybody is a risk manager. Some organizations indicate that this is more important than developing and issuing extensive policies and procedures. Management of risk is embedded in the management philosophy. Employees that take responsibility for their actions and outcomes become risk managers. Ideally, the employees intuitively understand the organization's goals and work towards them. Examples of this practice are:

The installing of restroom mirrors that remind employees that; "you are looking at your safety manager".

Installing a "sense of excellence" in the culture which encourages people to seek solutions and talk honestly about where they need help.

Involving all staff in risk management activities through committees and holding meetings at different work sites.

Sometimes, the culture has to be developed. Examples of practices to achieve this include:

Setting up a risk management department as a centre of excellence to spread risk management procedures and practices across the organization. The aim is to encourage people to be their own risk managers with the risk management department acting in a support capacity.

Recruiting on attitude instead of experience, in order to provide outstanding customer service. This helps manage customer risk.

Introducing penalties. One government introduced a "corporate killing" offense designed to punish directors when they fail to correct unsafe practices that result in death.

Setting up recognition and reward initiatives that encourage employees to manage risks and take advantage of opportunities.

Implementing remuneration packages that discourage excessive risk taking.

Evaluating employees' performance in managing risks, through the performance appraisal process.

Defining risk management as part of the requirement for all management positions.

Re-inforcing ethics and values by issuing a written code of ethics or communicating them through training, meetings or workshops.

The reported benefit of a risk management culture is that organizations can change more rapidly and can manage risks more effectively.

2. Senior management and/or governing bodies champion risk management and define and communicate acceptable levels of risk

The responsibility for driving risk management is placed high in the organization. This is also a tool for embedding risk management in the culture. The support of senior management (and/or the governing bodies) is essential. As a start, senior management must be aware of and understand risk management. There is a wide variety of ways in which the senior leaders are involved in risk management. However, underlying these ways is the role of senior management to send the message internally and externally about the importance of managing risk.

Also, it is important that other managers, stakeholders, and employees see their authority or senior management, defines, develops and approves a Risk Policy.

3. Establishing open communication channels

The practices reported demonstrate that open communication is necessary for risk management to succeed. For example, teams rely on communication to address risks and achieve objectives. Also, many report that open communication is a way to easily integrate risk management into existing processes. If communication is not there, risk management cannot be "everybody's business".

Managers require direct communication channels up, down and across their business units to help identify risks and take appropriate actions. New looser-information based structures are replacing traditional organization structures with defined reporting relationships. Information must be shared.

Examples of open and good communication are:

Using the intranet to communicate the organization's efforts and involve all employees in managing risk. It is also used to communicate objectives;

Appointing managers whose only task is to communicate risks to employees;

Holding quarterly meetings of a risk management committee to review and discuss the organization's exposure and protection measures;

Using the risk management function to communicate objectives;

Promoting awareness of risk management issues through monthly, quarterly and annual reports. The reports focus on areas that require help from the risk management group;

Making presentations to senior management and/or the governing body on the risk management process;

Encouraging people to discuss mistakes.

4. Using teams and committees

Informal and formal teams are a mechanism that many organizations report they are using to manage risks.

Teaming brings to light the dynamics between disciplines, brings together various risk attitudes, and brings fresh thinking to issues, opportunities, strategies and solutions. It is perceived as a way to focus diverse disciplines on common objectives, one of which is minimizing risk. Teams provide balance. Also, teams pollinate a concern for risk management throughout the organization, rather than being the concern of a function or discipline. While the practice of teaming is recognized as a "best practice", there is no common practice concerning the composition of the team.

The composition of formal risk management teams included:

- Line management, treasury, audit, compliance, public relations, human resources and risk management professionals;
- Specific risk management teams for each of contract management control, health and safety, insurance, transport and treasury management;
- Multi-disciplinary teams for projects and product development;
- Seeding management teams with individuals with varying risk attitudes;
- A cross-functional risk management committee with representation from operating units and treasury/finance, human resources and risk management;
- A risk management strategy steering group where all major functions are represented;
- A risk management committee composed of division heads.

In other cases, various disciplines are encouraged to work together, such as:

The audit group, the Chief Financial Officer, senior management, and treasury;

A workers' compensation claims department, medical department, corporate ethics department, security, human resources and legal department jointly taking on risk management responsibilities;

A claims coordinator working closely with the human resources department;

A team of loss control specialists and claim handlers available during construction projects;

A project team of corporate audit, finance and control, and a chartered accountant which supports managers' self-assessment of risk.

Teams provide a wider perspective and look at various angles of risks and consequences. To operate, teams require open communication.

5. Using a simple, common business risk language

In order to integrate risk management into other management processes, the terminology should be easily understandable by managers. The approaches should also be simple to understand and use. By developing a common business risk language, managers can talk with individuals from the, “boardroom to the boiler room” in terms that everybody understands.

This is important also in cases where everybody is expected to manage risks. The risk management approaches and processes must be simple to be accepted by management.

Organizations have reported that complex, intellectual tools have proven to be unsuccessful. Others caution that the approaches must also be flexible to be meaningful across business units. Though the process must be simple and useful across units, the process should not be oversimplified. The designers of the process must balance simplicity with usefulness.

6. Setting up a risk management function

Many organizations have set up a responsibility centre for risk management. Some units are headed by a Chief Risk Officer (CRO) who defines consistent approaches to managing risk. As the organizational risk champion, the CRO is responsible for providing leadership and establishing and maintaining risk awareness across the organization. The CRO might also set up risk control objectives, a risk framework, and design ways to measure risk. These senior risk managers must have strong persuasion skills. The risk manager must deal with business risks, not just insurable risks. In this way, their importance within the organization increases.

7. Communicating risk management performance

A handful of organizations report to management and stakeholders/shareholders on risks and risk management performance. Ways of reporting are:

The Internal Control department presents two reports annually to the Executive Authority.

The reports communicate the results of monitoring risk. Each Operating Division is also required to prepare an annual report on its monitoring results for the Internal Control Department;

Managers are required to report three times annually to the Finance and Risk Committee.

The reports outline the units' top ten risks and how they are managed;

Managers advise the Board on the risks of their ventures and key shareholders/stakeholders have their say.

8. Internal Audit and/or the Audit Committee assist in implementing risk management

The internal audit function plays a key role in facilitating risk management throughout an organization.

Examples of this practice are:

Facilitating self-assessment workshops;

Monitoring and reporting on the management of significant risks;

Providing advice;

Raising awareness of risk management among managers;

Identifying critical risks and preparing "watching briefs" on them;

Monitoring compliance in key areas, such as legislative requirements;

Reviewing processes for managing risks;

Communicating objectives for managing risk;

Sitting on the risk management committee meetings.

9. Guidance

Providing guidance is an important practice for integrating risk management. Guidance is provided indirectly (documents) or directly (advice).

Examples of this practice are:

A tool kit for agencies of the government.

The kit enables agencies to self-assess their position relative to current best practices. It also helps them move to the best practice using generic improvement strategies; Internal consulting services provided by the risk management unit;

A forum of managers.

Managers are able to identify their problems/risks. The forum allows the sharing of best practices. Action items are proposed to deal with the risk. Another advantage is all line managers are now aware of the risk and the action items;

A legislative agency that makes recommendations to agency management for reducing risk. The recommendations have been proven successful in other agencies.

10. Risk management training

Risk management training helps integrate risk.

Topic areas include:

Risk assessments;

Best practices;

Legislative requirements;

Safety; objectives for managing risk;

Risk-awareness training to ensure that all managers consider risk.

Annexure C: Risk Assessment Templates, tools and documents

The availability of certain documents and templates simplifies the risk management process by automating some of the activities. Tools, templates, and documents were developed to assist organizations in performing risk management activities. These are summarized as follows:

1) Risk Management Plan

The risk management process is complemented by a risk management plan/strategy. The purpose of this plan is to document the individual responsibilities and the steps that need to be taken in undertaking risk management activities and giving effect to risk management policies. It also details the schedule and budget for risk management activities as well as the methods, tools and techniques to be employed in the risk management process. Risk management plans are composed of six main components summarized below.

1.1) Roles and responsibilities

This section outlines the roles and responsibilities of all individuals who will participate in a particular project or program. It also outlines the major lines of authority and accountability as well as reporting from top management to operational staff.

1.2) Documentation

It contains information about individual risks that are relevant for the department, program, or project. The information contained here is that which is commonly found in the risk register. As such, it can also be presented in a separate document or even a database. In such a case, this section contains information about the various fields in the database as well as directions on how to use it.

1.3) Risk management process tasks or activities

Risk identification

A list of techniques that should be used in identifying risks are outlined and explained. The techniques include brainstorming, interviews, checklists, etc. Additional information is provided about those who will participate in the risk identification exercise. In general, everybody participating in the project has the power to identify new risks. In some cases, the steps involved in the risk identification process are outlined.

Risk assessment

The most urgent risks are ranked according to their degree of importance and presented in this section. This is usually based in the department's risk tolerance levels. Each of the risks is then allocated or assigned to the individual project members who are responsible for putting risk contingency and action plans in place.

Risk management planning

The risk mitigation plans are recorded in this section containing the recommended actions that will either reduce the probability of the risk materializing or its impact if it materializes. During the course of the year, individuals who have been assigned responsibilities exercise their risk management powers. The contingency action plans are usually advanced to the control phase after the risks have materialized. This allows for evaluation of the effectiveness of decisions, which were taken.

Risk monitoring and review

This section details the methods that are used in monitoring the status of risks over time. It also provides information on the periodicity of risk reviews to determine whether their status has not changed. Steps are outlined on how the risks should be handled if their status has changed or if there are new risks that were identified during the monitoring and review period.

Reporting of risks

This outlines the format and periodicity of risk related reports. It also details the persons to whom reports should be submitted. The lessons learned from managing certain risks can also be detailed in this section. If lessons are stored in a different database, the section provides information about the database including how to access it. Usually reported are provided on the categories of risks that are worth reporting to different levels of management.

Timetable for risk management activities

This section serves as a year planner and details all the dates at which various risk management activities will take place. This may include dates for risk identification sessions, reporting dates, and review dates. This suggests that risk management should be a forward-looking process.

1.4) Risk management budget and contingency fund

This section outlines the sources of funds for performing risk management activities. Information about the maximum budget available for the whole year is also provided. This information is usually provided for various levels of management as well as individual programs.

The contingent fund is related to the work areas of the program to be managed. This must not be made in an ad hoc manner, since it then does not provide a target of financial benefits to be derived from implementing risk management. As such, the allocation of funds for risk management is usually done based on allocating funding sufficient to cover the estimated risk exposure that is identified within a particular program or project. This is based on formal risk identification and analysis of the probability and impact.

1.5) Risk management tools, methods, and techniques

Information is provided on tools, techniques, and methods that are used to identify, evaluate and track risks during the year. Where databases and templates are present, information about them is also provided in this section.

Business risk mapping

Organizations are developing business risk maps to identify key business risks to the organization. This helps the organization understand and address its risks. Management must quantify the magnitude of the risks and measure their potential impact. The use of a broad scope framework permits the consideration of different types of potential risk in risk mapping. The use of a framework can influence a discussion on the sources and types of risks, for example, external, economic, market, credit, information, human resources and strategic. This brings a multi-disciplinary perspective for looking at the risks.

Examples of this practice are:

Listing of the various business risks. Then, the risks are charted into four quadrants depending on whether an event has a high or low probability of occurrence and whether it could result in a highly severe loss or a low severity loss.

Developing a risk map on one sheet of paper. The map provides a comparative evaluation of all operational, financial, hazard and strategic risks that the organization faces. By comparing risks on a single matrix of severity and frequency, senior managers can see a complete picture of all the risks facing the company and their interrelationship.

Developing a 'major matrix of risks'. It captures the most damaging threats to the corporation. Senior management and the Board can use it in decision-making.

Simplicity underlies these approaches.

Modeling tools

Modeling tools enable managers to manage uncertainty. Scenario analysis and forecast models are the predominant tools. Examples of using modeling tools are:

Using scenario analysis, decision makers can see the range of possibilities and consider changes that they would otherwise ignore. These scenarios can also be built into the organization's contingency plans. Scenarios can be documented and analyzed using computer spreadsheet software.

Using statistical analysis and Value at Risk techniques, managers can estimate the variability of future losses. They measure the impact of a potential loss on earnings or cash flow, include sensitivity analysis, stress testing, and various types of simulations.

Financial models which dynamically simulate the various financial risks and the impact of various scenarios on portfolios of debt and equity.

Anticipating hazards in the production process that could make the product defective, and then identifying the points at which they can be controlled.

Assessing technical risks during new product development by identifying, early on in the project, the potential errors in the manufacturing process. This gives the time to address the consequences.

Accumulating past project experience and extrapolating it to provide a synthesis of the likely risk impact of a particular project.

Some tools, such as scenario analysis, modeling, technical risk analysis, have broad applicability to management areas. Others, such as financial models, are less applicable to other disciplines.

Risk identification and assessment techniques

Techniques for identifying and assessing risks help managers identify where they should be focusing their attention and resources. There is no predominant technique.
Various techniques are:

Brainstorming groups. Staff from multiple business units meets to brainstorm issues.

Workshops. Organizations are starting to develop risk-focused facilitated workshops that help operating personnel determine and prioritize their objectives and identify and assess risks. Management in attendance would generally span a variety of areas.

Questionnaires. Operating units are tasked with completing questionnaires on objectives and risks. For example, managers may annually update risks and progress on managing them.

Self-assessment. Managers self-assess with support from Audit, Finance and an external accountant.

Control self-assessment (CSA). CSA provides assurance that an end-point business objective will be met, taking into account controls and risks. Risk-focused workshops help operating managers determine and prioritize their objectives.

Filters. Risks are evaluated against four filters: non-core function, low impact, risk well-managed, and low probability of occurrence.

Boston Squares. Boston Squares is used to chart the impact/severity of risks.

Risk Quick Scan. This is a technique for presenting risks (cost, timing, specifications, etc.) in such a way that the risks can be easily compared to each other in terms of probability and consequences. This is especially useful in projects.

Matrix to assess supplier capability. The matrix is used to make an overall assessment of the ability of a potential supplier to deliver successfully the services/products specified in a contract. The matrix considers: the history and development of the supplier's business; legal background and capital structure; critical performance elements of the contract; management and employees; commitment, contingencies and litigation; financial viability.

Assessment matrix. The matrix consists of a series of questions covering elements of risk management and internal controls. It also includes descriptions of best practices.

Risk identification templates. Business units are given templates. These assist them in identifying and evaluating risks during their business planning process.

"Bottom up" risk assessments. Operating managers identify and evaluate risks. These are then rolled up at the corporate level.

Value at Risk (VAR) model and worst case model. These models are used to assess risk. The (VAR) model looks at the estimated potential loss in value of a position or portfolio within a specified period based on market factors. It allows the simultaneous trend comparison of, for example, currency fluctuations.

Prioritizing risks. Based on their rank, the risks are addressed.

1.6) The internet/intranet

The internet/intranet is increasingly being used to manage risks. It is used to: promote risk awareness and management; obtain information on risk in specific areas; communicate with employees; share information on risk management across agencies; and communicate risk management objectives.

2. Risk Assessment Template

Activity	Risk	Impact	Like-lihood	Control	Method assessed/ source	Priority	Responsible person	Due date
1. Timeliness and accuracy of information and the delivery thereof by the departments in the financial reporting on National Accounts process								
1.1 Accounting policies, standards and support services	Incomplete data capturing in the general ledger of departments and this information is then submitted to National Treasury.	3	3	Each department is required to prepare and sign a monthly compliance certificate that information submitted is accurate.	Internal audit review/procedures	High	XYZ	
	Inadequate management and enforcement of month-end closure procedures which result in the inability to extract information.	3	3	System month-end force closure 5-7 days after month end. In addition, dates for month end closure are set at the beginning of the financial year.	Internal audit review/procedures	High	XYZ	
	Month-end closure delayed by untimely interfaces with the bank, Telkom, etc.	3	3	Bank statements are received on a daily basis. Enhancements to the Telkom Interface System will be made in November 2003.	Internal audit review/procedures	Medium	XYZ	

3) Risk register

A risk register is a very important tool in identifying, analyzing, and documenting potential risks. It serves as an up-to-date information database about the status of individual risks. It also provides information about the effectiveness of certain risk management actions.

The fields of a risk register or log should be as follows:

Risk reference number.
This number serves to identify the risk and avoids the use of actual names that can be quite confusing. The reference number can be composed of letters, digits, or a combination of both.

Risk description
This describes the identified risk and gives additional information about its nature. A brief description of the context of risk should also be provided here.

Risk attributes
Information about the frequency and severity of each of the risks identified are provided in this field. The time over which the action needs to be taken and the amount of money at risk are also detailed. Providing an estimate of the amount of money at risk allows the risk level to be quantified.

Preventive controls
This field details the internal controls that are currently available in the department. It also details persons responsible for making sure that such controls are effective. This information is useful for determining the effectiveness of controls by establishing the extent of loss that could result assuming the controls were not in place.

Contingency plans
This field details the actions that should be taken in the case of the risk materializing. The actions are necessary for minimizing the adverse effects of risks. This field also provides information about the person responsible for contingency actions as well as the log of actions taken and their effectiveness.

Frequency of reporting
This field details the frequency with which risk management reports are generated and submitted to top management. This can be weekly, monthly, or quarterly depending on the nature of risks under consideration. This is important for the early warning systems.

4) Risk Impact Matrix

These are used for classifying and ranking or prioritizing various risks that the organization is more likely to face. The ranking of consequences and likelihood differs from organization to organization depending on the nature of risks each of them faces. For instance, Australia has put in place a framework that allows the classification of risks based on five possible degrees of occurrence and consequences. For consequences, the ranking includes extreme, very high, medium, low, and negligible. On the other hand, likelihood includes almost certain, likely, moderate, unlikely and rare.

The above allows risks to be prioritized for all public sector organizations according to whether they are severe, high, major, significant, low, moderate, or trivial. Responsibilities are then defined for each prioritized category of risk as follows:

Category of risk	**Level of Management required**
Severe risks	Actively managed by senior management
High Risks	Require detailed research and management planning at all levels
Major risks	Require senior management attention
Significant risks	Must be assigned to individuals who would be responsible for managing them
Moderate risks	Need to be monitored although detailed plans are not necessary
Low risks	Managed by routing procedures such as internal control and quality assurance procedures,
Trivial risks	Risks do not need specific application of resources but need to be reviewed at specified points in time to ensure that their status has not changed

5) Risk Information Sheet

This template provides detailed information about individual risks that are recorded in the risk register. The fields of this sheet cover at least those contained in the risk register (see 2 above). The following is a summary of the most common fields in the risk identification sheet used by other countries and organizations.

Example: Risk Information Sheet

Risk ID (The number that uniquely identifies risks from others in the risk database**.)**	**Report date** (The date at which the report or sheet was last updated.)
Classification	The category of risk as assigned during the risk assessment exercise.
Description	A risk statement including both the condition and consequence of the risk should it happen.
Risk context	Details the context within which risk originates
Risk attributes	The information about the probability and impact of the risk as well as the consequent risk exposure or level applicable to that risk
Risk indicator	Specifies the trigger conditions that will prompt action from the person responsible for managing risk
Mitigation strategies or contingency actions	Details the actions that has to be taken to mitigate either the probability of the risk occurring or its impact after it has occurred
Dates of implementation	Specifies the dates during which the mitigation plan will begin and the date at which it is expected to be fully implemented
Risk owner	The person who is responsible for the management of the risk
Risk status	Describes the status of the risk and effectiveness of the actions that were taken to mitigate the risk
Contingency plan	List the actions that will be taken in case the risks materialize
Contingency plan trigger	Details the conditions under which the department will commence with the implementation of the contingency plan

Annexure D: Case study: Effective utilization of assets to achieve effective service delivery

The following example indicates the risks attributable to a transport function. The measurement of both the risks might not be realistic, and serves as an example only.

Strategic goals and objectives

The following strategic goal and objective has been identified in a Public Sector Health Department

***Strategic Goal**: Effective utilization of the Department's finance and assets to achieve effective service delivery.*

Strategic Objective: *Efficient financial and asset management as well as financial controls.*

Related objectives:

Operational objectives: *Improved service delivery due to increased availability of assets to assist staff to achieve their objectives.*

***Reporting objectives**:* *Establishment of key performance and risk indicators.*

Comprehensive system for producing performance information to assist management with its evaluation of the effectiveness of internal control and risk management.

***Compliance objectives**:* *Develop policies and procedures for asset management.*

Monitoring of compliance with the standards documented in the policy and procedure manual.

Demonstrable improvement in the compliance with standards against baseline self assessment.

Comprehensive controls assurance statement in the annual report.

The risks that might prevent management from achieving the objectives are then analysed to identify the impact (consequence) and likelihood of the risk materializing.

The following criteria and risk categories were applied in assessing and classifying identified risks:

IMPACT (CONSEQUENCE)

Score	Rating	Description
5	Catastrophic	Loss of ability to sustain ongoing operations. A situation that would cause a standalone business to cease operation
4	Major	Significant impact on achievement of strategic objectives and targets relating to organisational plan.
3	Moderate	Disruption of normal operations with a limited effect on achievement of strategic objectives or targets relating to organisational plan.
2	Minor	No material impact on achievement of the organisation's strategy or objectives.
1	Insignificant	Negligible impact.

LIKELIHOOD (FREQUENCY, PROBABILITY)

Score	Rating	Description
5	Common	The risk is almost certain to occur more than once within the next 12 months. (Probability = 100% p.a.)
4	Likely	The risk is almost certain to occur once within the next 12 months. (Probability = 50 – 100% p.a.)
3	Moderate	The risk could occur at least once in the next 2 – 10 years. (Probability = 10 – 50% p.a.)
2	Unlikely	The risk could occur at least once in the next 10 - 100 years. (Probability = 1 – 10% p.a.)
1	Rare	The risk will probably not occur, i.e. less than once in 100 years. (Probability = 0 – 1% p.a.)

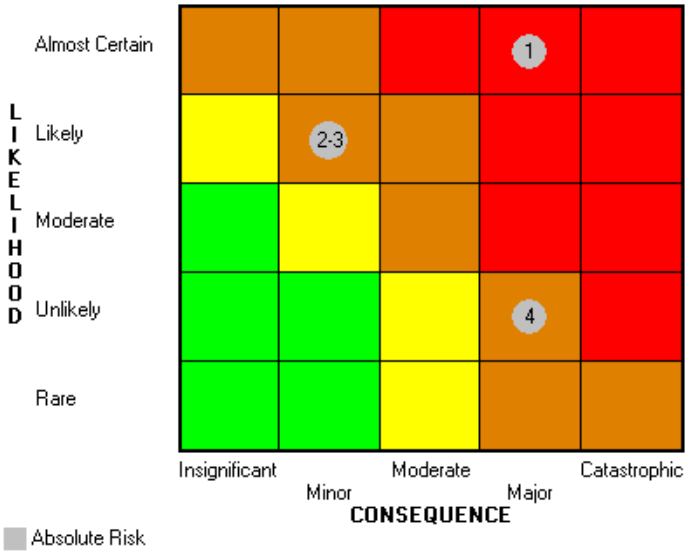
Risk assessment ratings are the product of likelihood and impact and are ranked as follows:

From 13 to 25	High
From 8 to 12	Medium
From 1 to 7	Low

Operational risks relating to transport control

Operational objectives: *Improved service delivery due to increased availability of assets to assist staff to achieve their objectives.*

The following sample of operational risks were identified and plotted on the risk grid based on the assessment of impact and likelihood:



Risk ref	Name	Consequence	Likelihood
O - 1	Inadequate skills assessment and training to provide staff with needed competency.	Major	Almost certain
O - 2	Inadequate planning of maintenance of vehicles.	Minor	Likely
O - 3	Unauthorised use of a government allocated vehicles.	Minor	Likely
O - 4	Unavailability of vehicles for effective service delivery.	Major	Unlikely

The inherent risks are then evaluated individually. Each risk is analysed in terms of consequence and likelihood, with a corresponding risk rating. It is critical to identify the reasons for the specific impact and likelihood assessment as this will focus management attention in their effort to reduce the residual risk (exposure).

Risk	**Inadequate skills assessment and training to provide staff with needed competency.**			**Reference O - 1**		
	Lack of skills assessment, job descriptions, training needs analysis and training.					
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Major	Almost certain	High	20	0.0	20.0
	Evaluation	Factors influencing consequence will include: Staff lacks competence, service delivery negatively affected and limited improvement in quality of service. Factors influencing likelihood will include: High volume of transactions, large geographical area to monitor, and decentralised nature of operations.				

When controls are being identified, it should be linked directly to the risk to determine the change in residual likelihood (exposure). The remaining risk should then either be accepted by management, or reduced by implementing further controls. It is extremely important to ensure at this stage if further controls would be cost-effective.

Control assessment	**Inadequate skills assessment and training to provide staff with needed competency.**			**Reference O - 1**		
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Major	Almost certain	High	20	12	8
	Controls in place	Minimum performance criteria identified for all processes. Staff skills assessment performed to determine current skill levels. Training planned and aligned to address skill shortages. Quarterly performance management to measure improvement of skills				

Risk	**Inadequate planning of maintenance of vehicles.** **Reference O - 2**
	Vehicle lifetime not optimised, vehicles broken down and not available for service delivery, possible fraud and corruption with maintenance contracts.

Consequence	Likelihood	Severity	Risk	Control	Exposure
Minor	Likely	Extreme	8	0.0	8.0

Evaluation	Factors influencing consequence will include: Incurring wasteful expenditure, service delivery negatively affected and vehicles not in running condition. Relatively insignificant effect on the budget. Legal impact – high costs if client dies because of poor service delivery. Cost of replacement exceeds cost of a proper maintenance plan. Factors influencing likelihood will include: High incidence of accidents, roads not in good condition, vehicles needs regular maintenance to prolong life. Lack of management information indicating service regularity. Vehicles not licensed.

When controls are being identified, it should be linked directly to the risk to determine the change in residual likelihood (exposure). The remaining risk should then either be accepted by management, or reduced by implementing further controls. It is extremely important to ensure at this stage if further controls would be cost-effective.

Control assessment	**Inadequate planning of maintenance of vehicles.** **Reference O - 2**

Consequence	Likelihood	Severity	Risk	Control	Exposure
Minor	Likely	Extreme	8	4	4

Controls in place	All vehicles are listed in a fleet management system. Maintenance are schedules as per manufacturers requirements. Exception reports generated when vehicles not sent for maintenance within 500 km of manufacturers requirements.

Risk	**Unauthorized use of a government allocated vehicles**				Reference O - 3
	Misappropriation of government vehicles, by using vehicles intended for official trips for private use.				
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Minor	Likely	Extreme	8	0.0	8.0
	Evaluation	Factors influencing consequence will include: Incurring wasteful expenditure, service delivery negatively affected and reputation risk. Relatively insignificant effect on the budget. Factors influencing likelihood will include: High volume of transactions, large geographical area to monitor, and decentralised nature of operations. Inadequate accountability chain. Inaccurate completion of log sheets.				

When controls are being identified, it should be linked directly to the risk to determine the change in residual likelihood (exposure). The remaining risk should then either be accepted by management, or reduced by implementing further controls. It is extremely important to ensure at this stage if further controls would be cost-effective.

Control assessment	Unauthorised use of a government allocated vehicles				Reference O - 3
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Minor	Likely	Extreme	8	0.0	8.0
	Controls in place	Internal audit issued a report of no reliance on control. Several recommendations not implemented to date. No change in the exposure.				

Risk	Unavailability of vehicles for service delivery				Reference O - 4	
	Available vehicles in good working condition not sufficient to ensure effective service delivery.					
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Major	Unlikely	High	8	0.0	8.0
	Evaluation	Factors influencing consequence will include: Lack of service delivery, reputation risk. Factors influencing likelihood will include: Large rural area serviced by the department, prevalence of road accidents, private contractor functioning nationally.				

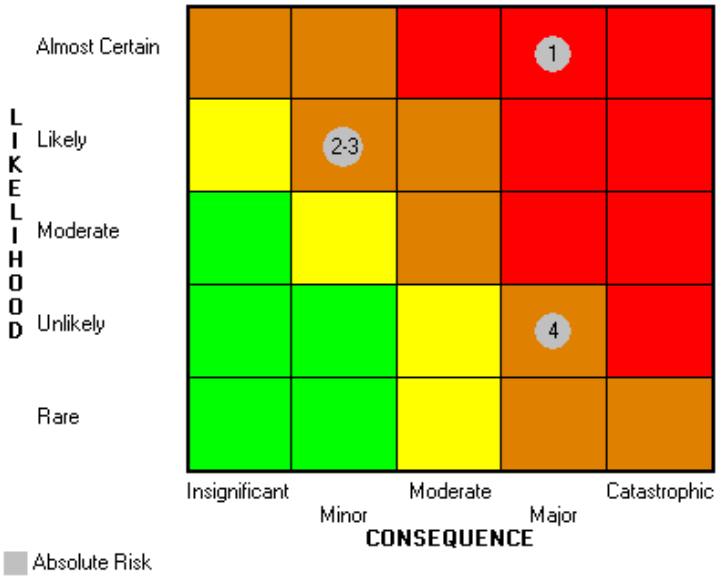
When controls are being identified, it should be linked directly to the risk to determine the change in residual likelihood (exposure). The remaining risk should then either be accepted by management, or reduced by implementing further controls. It is extremely important to ensure at this stage if further controls would be cost-effective.

Control assessment	Unavailability of vehicles for service delivery				Reference O - 4	
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Major	Unlikely	High	8	0.0	8.0
	Controls in place	No specific controls in place – several findings of Auditor-General not implemented. No change in exposure.				

Reporting risks relating to transport control

***Reporting objectives**:* *Establishment of key performance and risk indicators.*

Comprehensive system for producing performance information to assist management with its evaluation of the effectiveness of internal control and risk management.



A sample of the risks identified above, and relating to vehicles are reflected below:

Risk ref	Name	Consequence	Likelihood
R - 1	Invalid transport charges paid by the department.	Major	Almost certain
R - 2	Inadequate management information system to assist management with the evaluation of internal controls	Minor	Likely
R - 3	Incorrect allocation of transport expenses to cost centers.	Minor	Likely
R - 4	Lack of performance indicators	Major	Unlikely

The inherent risks are then evaluated individually. Each risk is analysed in terms of consequence and likelihood, with a corresponding risk rating. It is critical to identify the reasons for the specific impact and likelihood assessment, as this will focus management attention in their effort to reduce the residual risk (exposure).

Risk	**Invalid transport charges paid by the department**				**Reference R - 1**
	Invalid expenditure appropriated against the departmental budget, resulting in irregular expenditure. This includes charges for fuel, maintenance, km tariffs and daily tariffs.				
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Major	Almost certain	High	20	0.0	20.0
	Evaluation	Factors influencing consequence will include: Modifications of the AG's report, if undetected could result in over-spending. Transport budget relatively small. Factors influencing likelihood will include: Large volume of transactions, relatively low value per transaction, decentralised nature of operations.				

When controls are being identified, it should be linked directly to the risk to determine the change in residual likelihood (exposure). The remaining risk should then either be accepted by management, or reduced by implementing further controls. It is extremely important to ensure at this stage if further controls would be cost-effective.

Control assessment	Invalid transport charges paid by the department				Reference R - 1
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Major	Almost certain	High	20	8	12
	Controls in place	All invoices signed off by the user department/function. Charges compared and reconciled to log sheets.				

Risk	Inadequate management information system to assist management with the evaluation of internal controls			Reference R - 2		
	Lack of exception reporting to indicate ineffective internal controls. Lack of performance information to measure quality of service delivery.					
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Minor	Likely	High	8	0.0	8.0
	Evaluation	Factors influencing consequence will include: Service delivery not measured in terms of quality. Mistakes committed/made by the service provider would not be detected. Transport budget relatively small. Factors influencing likelihood will include: System relatively new and complicated. Lack of reconciliations of actual expenses to recorded expenditure. No reviewing of management information and exception reports. Controls not delegated to responsibility level. Lack of performance management.				

When controls are being identified, it should be linked directly to the risk to determine the change in residual likelihood (exposure). The remaining risk should then either be accepted by management, or reduced by implementing further controls. It is extremely important to ensure at this stage if further controls would be cost-effective.

Control assessment	Inadequate management information system to assist management with the evaluation of internal controls			Reference R - 2		
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Minor	Likely	High	8	0.0	8.0
	Controls in place	New system in the process of being developed. Contract outsourced to external service provider. Exposure remains unchanged.				

Risk	Incorrect/invalid kilometer readings used to calculate charge				Reference R - 3	
	Incorrect charges against expenditure could result if the km variable was incorrect.					
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Minor	Likely	Extreme	8	0.0	8.0
	Evaluation	Factors influencing consequence will include: Inaccurate allocation of costs to user, inaccurate financial reporting for planning purposes, inaccurate recovery. Transport budget relatively small. Factors influencing likelihood will include: Large volume of transactions, relatively low value per transaction, decentralised nature of operations. Service stations record kilometer reading incorrectly.				

When controls are being identified, it should be linked directly to the risk to determine the change in residual likelihood (exposure). The remaining risk should then either be accepted by management, or reduced by implementing further controls. It is extremely important to ensure at this stage if further controls would be cost-effective.

Control assessment	Incorrect/invalid kilometer readings used to calculate charge				Reference R - 3	
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Minor	Likely	Extreme	8	0.0	8.0
	Controls in place	Internal audit issued a report of no reliance on control. Several recommendations not implemented to date. No change in the exposure.				

Risk	Lack of key performance indicators				Reference R - 4	
	No standard setting to establish the minimum level of performance required from staff to assist with the achievement of objectives					
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Major	Unlikely	Extreme	8	0.0	8.0
	Evaluation	<u>Factors influencing consequence will include</u>: Lack of standards and performance criteria, Staff not informed of minimum standards and/or objectives to be achieved. Poor service delivery. Opportunity for fraudulent transactions. Cost of recovery exceeds cost of prevention. <u>Factors influencing likelihood will include</u>: System relatively new and complicated. No review of transactions by decentralized users. Fraud recovered too late.				

When controls are being identified, it should be linked directly to the risk to determine the change in residual likelihood (exposure). The remaining risk should then either be accepted by management, or reduced by implementing further controls. It is extremely important to ensure at this stage if further controls would be cost-effective.

Control assessment	Lack of key performance indicators				Reference R - 4	
	Consequence	Likelihood	Severity	Risk	Control	Exposure
	Major	Unlikely	High	8	0.0	8.0
	Controls in place	No specific controls in place – several findings of Auditor-General not implemented. No change in exposure.				

Annexure E: Bibliography

Guidelines for Managing Risk in the Australian Public Service (1996).
COSO report on Enterprise Risk Management, published as a draft in July 2003.
Integrated Risk Management Framework, published by the Treasury Board of Canada in April 2001.
King report on Corporate Governance, 2002.
Public Finance Management Act, 1999 and related regulations.
Municipal FinanceManagement Act 2003
Draft Risk Management Framework – National Treasury