ENTERPRISE RISK MANAGEMENT STRATEGY

ENTERPRISE RISK MANAGEMENT STRATEGY – CEDERBERG MUNICIPALITY

INDEX **page**

1. INTRODUCTION

The risk management strategy outlines the plan on how the Municipality will go about implementing its risk management policy. This strategy is designed to provide all the role players with information to enable them to fully understand the roles and responsibilities of their office in terms of risk management and to effectively discharge such roles and responsibilities.

This Risk Strategy includes the risk assessment processes and methodologies, monitoring and reporting, control and environment activities to give the effect of the risk management policy.

2. ROLES AND RESPONSIBILITIES

All personnel within Cederberg Municipality have a responsibility for maintaining good internal control and managing risk in order to achieve the Municipality`s objectives. To assist personnel with understanding their roles and responsibilities, the following table of guidelines per role player have been included:

Executive Authority (Council)

Council is responsible for the governance of risk and will report to the community, on the Municipality`s system of internal control to provide comfort that the Municipality is protected against significant risk to ensure the achievement of objectives as detailed in the Service delivery and Budget Improvement Plan (SDBIP). To fulfil its mandate with regard to Enterprise Risk Management, Council must:

Ref.	Activity	Frequency
1	Determine the levels of risk appetite with guidance from the Accounting Officer (Municipal Manager), Manager: Integrated Risk Management and the Risk and Ethics Management Committee	Annually
2	Approve the risk management policy by council resolution;	Annually
3	Approve the risk management strategy by council resolution;	Annually
4	Approve the fraud prevention policy by council resolution;	Annually
5	Approve the fraud prevention strategy by council resolution;	Annually
6	Ensure that IT, fraud and Occupational Health and Safety (OHS) risks are considered as part of the Municipality`s risk management activities;	Annually
7	Ensure that risk assessments (strategic, operational and projects) are performed by reviewing the Risk and Ethics Management Committee reports;	Quarterly

8.	Ensure that management implements, monitors and evaluates performance through the Risk and Ethics Management Committee;	Quarterly
9.	Ensure that assurance regarding the effectiveness of the Enterprise Risk Management process is received from the Risk and Ethics Management Committee.	Quarterly

Audit Committee

The Audit Committee is vital to, among other things, ensure the financial, IT and fraud risk related to financial reporting are identified and managed. To fulfil its mandate with regard to Enterprise Risk Management, the Audit Committee must:

Ref.	Activity	Frequency
1.	Formally define its responsibility with respect to risk management in its charter;	Annually
2.	Meet on a quarterly basis (minutes of the Risk and Ethics Management Committee meeting should be a standard agenda item at these meetings)'	Annually
3.	Review and recommend disclosures on matters of risk in the annual report;	Annually
4.	Include statement regarding risk management performance in the annual report to stakeholders;	Annually
5.	Provide an independent and objective view of the Municipality`s risk management effectiveness;	Annually
6.	Evaluate the effectiveness of Internal Audit in its responsibilities for risk management; and	Annually
7.	Ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities;	Annually
8.	Review the internal and external audit plans and ensure that these plans address the risk areas of the Municipality; and	Annually
9.	Review the risk register/dashboard at each meeting.	Annually

Risk and Ethics Management Committee

The Risk and Ethics Management Committee is appointed by the Council to assist the Municipal Manager in discharging his/her duties. To fulfil is mandate the Risk and Ethics Management Committee must:

Ref	Activity	Frequency
1.	Formally define the roles and responsibilities with respect to risk management in its policies;	Annually

2.	Meet on a regular basis;	Quarterly
3.	Review and recommend for the approval of the Council, the risk appetite;	Every three (3) years
4.	Review and recommend for the approval of the Council, the risk management policy;	Every three (3) years
5.	Review and recommend for the approval of the Council, the risk management strategy;	Annually
6.	Review and recommend for the approval of the Municipal Manager, the risk management implementation plan;	Annually
7.	Review and recommend for the approval of the Council, the fraud prevention policy;	Every three (3) years
8.	Review and recommend for the approval of the Council, the fraud prevention strategy;	Annually
9.	Review and recommend for the approval of the Municipal Manager, the fraud prevention implementation plan;	Annually
10.	Arrange for top risk to be formally re-evaluated;	Annually
11.	Advise council on how to improve management of the municipalities risks;	Annually
12.	Review risk management progress within the Municipality	Quarterly
13.	Provide a timely and useful ERM report to the Municipal Manager and Audit Committee. The report should contain the state of ERM within the Municipality accompanied by recommendations i.e. • the key strategic risk facing the Municipality (All extreme and high inherent risk exposures); • the key operational risks per directorate/department (minimum the top 10 identified risks); • any risk developments (changes) / incidents / losses; and recommendations to address any deficiencies identified.	Quarterly
14.	Measure and understand the Municipality`s overall exposure to IT risks and ensure that proper processes are in place;	Quarterly
15.	Review the risk registers/dashboard at each meeting and update the register`s contents to reflect any changes without formally reassessing the risks; and	Quarterly
16.	Provide guidance to the Municipal Manager, Manager: Integrated Risk Management and other relevant risk management stakeholders on how to manage risks to an acceptable level.	Ongoing

Accounting Officer (Municipal Manager)

The Accounting Officer is ultimately responsible for ERM and is accountable for the overall governance of risk within the Cederberg Municipality. To fulfil its mandate with regard to Enterprise Risk Management, the Municipal Manager must:

Ref.	Activity	Frequency
1.	Appoint a Manager: Integrated Risk Management and/or Risk Champions;	As required
2.	Review and recommend to Council for approval the Risk and Ethics Management Committee Terms of Reference;	Every three (3) years
3.	Review and recommend to Council for approval the risk appetite;	Every three (3) years
4.	Review and recommend to Council for approval the risk management policy;	Every three (3) years
5.	Review and recommend for Council for approval of risk management strategy;	Annually
6.	Approve the risk management and fraud prevention implementation plan;	Annually
7.	Review and recommend to Council for approval the fraud prevention policy;	Every three (3) years
8.	Review and recommend to Council for approval the fraud prevention strategy;	Annually
9.	Ensure appropriate action in respect of recommendations of the Audit Committee, Internal Audit, External Audit and Risk and Ethics Management Committee to improve ERM; and	Annually
10.	Provide assurance to relevant stakeholders that key risks are properly identified, assessed and mitigated by reviewing the report issued by the Risk and Ethics Management Committee which should contain the state of ERM within the Municipality accompanied be recommendations i.e. • The key strategic risk facing the Municipality (All extreme and high inherent risk exposures); • The key operational risks per directorate/department (minimum the top 10 identified risks); • Any risk developments (changes)/ incidents / losses; and recommendations to address any deficiencies identified.	Quarterly

Internal Audit

Internal Audit should provide a written assessment of the effectiveness of the Municipality`s system of internal control and risk management. To fulfil its mandate with regard to Enterprise Risk Management, Internal Audit must:

Ref	Activity	Frequency

1.	Provide assurance on the Enterprise Risk Management process design and its effectiveness	Annually
2.	Provide assurance on the management of “key risks” including, the effectiveness of the controls and other responses to the “key risks”;	Annually
3.	Provide assurance on the assessment and reporting of risks and controls; and	Annually
4.	Prepare a rolling three (3) year strategic Internal Audit plan and a one (1) year operational Internal Audit plan based on its assessment of key areas of risk	Annually

Management

Management is accountable for designing, implementing, monitoring and integrating Enterprise Risk Management into their day-to-day activities. To fulfil its mandate with regard to Enterprise Risk Management, Management must:

Ref	Activity	Frequency
1.	Empower officials to perform effectively in their risk management responsibilities;	Ongoing
2.	Devote personal attention to overseeing the management of key risks within their area of responsibility;	Ongoing
3.	Maintain a co-operative relationship with the Manager: Integrated Risk Management and Risk Champions;	Ongoing
4.	Draft a risk management report for submission of the Risk and Ethics Management Committee; This will focus on the following: • the operational risks per directorate / department (approximately top 10 identified risks); and • any risk developments (changes) / incidents / losses;	Quarterly
5.	Report to the Risk and Ethics Management Committee regarding the performance of internal controls for those risks in the operational risk registers;	Quarterly
6.	Maintain the proper functioning of the environment within their area of responsibility;	Ongoing
7.	Continuously monitor the implementation of risk management within their area of responsibility; and	Ongoing
8.	Hold officials accountable for their specific risk management responsibilities.	Ongoing
9.	Report events of risks to the Manager: Integrated Risk Management	Ongoing

Manager: Integrated Risk Management

The primary responsibility of the Manager: Integrated Risk Management is to bring his/her specialist expertise to assist the Municipality to embed risk management and leverage its benefits to enhance performance. To fulfil its mandate with regard to Enterprise Risk Management, The Manager: Integrated Risk Management must:

Ref.	Activity	Frequency
1.	Assist the Municipal Manager determine/review the risk appetite (for Council approval)	Every three(3) years
2.	Draft and/or review the risk management policy;	Every three(3) years
3.	Draft and/or review the risk management strategy;	Annually
4.	Draft the risk management implementation plan;	Annually
5.	Draft and/or review the fraud prevention policy;	Every three(3) years
6.	Draft and/or review the fraud prevention strategy;	Annually
7.	Draft the fraud prevention implementation plan;	Annually
8.	Coordinate and facilitate the assessments;	As per the Implementation Plan
9.	Consolidate risks identified by the various Risk Champions;	As per the Implementation Plan
10.	Prepare Enterprise Risk Management registers, reports and dashboards for submission to the Risk and Ethics Management Committee and other roles players;	As per the Implementation Plan
11.	Ensure that all risk information is updated;	As per the Implementation Plan
12.	Ensure that all IT, Fraud and OHS risks are considered as part of the Municipality`s ERM activities;	As per the Implementation Plan
13.	Coordinate the implementation of action plans;	As per the Implementation Plan
14.	Ensure that risk assessments are performed and reported to the Risk and Ethics Management Committee; and	Quarterly
15.	Avail the approved risk registers to Internal Audit on request	Annually

Risk Champion

Risk Champions assist the Manager: Integrated Risk Management facilitate the risk assessment process and manage risks within their area of responsibility to be within the risk appetite. To fulfil its responsibilities with regard to Enterprise Risk Management, Risk Champions must:

Ref.	Activity	Frequency
1.	Facilitate all operational assessments;	As per Implementation Plan
2.	Ensure that each key risk has a nominated risk owner;	As per Implementation Plan
3.	Ensure that all risk information is updated;	As per Implementation Plan
4.	Co-ordinate the implementation of action plans for the risk and report on any developments regarding the risk; and	As per Implementation Plan
5.	Report events of risks to the Manager: Integrated Risk Management	Ongoing

Other Officials

Other officials are responsible for integrating risk management into their day-to-day activities. To fulfil its responsibilities with regard to ERM, other officials within the Municipality must:

Ref.	Activity	Frequency
1.	Take the time to read and understand the content in the risk management policy but more importantly their roles and responsibilities in the risk management process;	Ongoing
2.	Apply the risk management process in their respective functions;	Ongoing
3.	Inform their supervisors and/or the risk management unit (CRO) of new risks and significant changes;	Ongoing
4.	Co-ordinate with other role players in the risk management process; and	Ongoing
5.	Provide information as required.	Ongoing
6.	Report events of risks to the Risk Champions/Line Managers and/or the Manager: Integrated Risk Management	Ongoing

3. INTERNAL ENVIROMENT

The Municipality`s internal environment is the of all other components of risk management. There are 10 factors to consider with regard to the internal environment:

- Risk Management Philosophy;
- Risk Appetite

- Risk Culture;
- Integrity and Ethical Values;
- Commitment to Competence;
- Management`s Philosophy and Operating Style;
- Organisational Structure;
- Assignment of Authority and Responsibility;
- Human Resource Policies and Practices;
- Differences in Environment.

Risk Management Philosophy

The philosophy is the Municipality`s beliefs about risk and how it chooses to conduct its activities and deal with risks. It reflects the value the Municipality seeks from risk management and influences how risk management components are applied.

Cederberg Municipality`s risk management philosophy is clearly stated in its risk management policy. Importantly, management reinforces the philosophy not only with word but with everyday actions and the Manager: Integrated Risk Management will communicate the risk management philosophy effectively with the Municipality to ensure that all personnel understand the Municipality`s commitment to risk management.

Risk Appetite

Risk appetite is the amount of risk the Municipality is willing to accept in pursuit of value. The risk appetite is directly related to a Municipality`s strategy. It is considered in strategy setting, where the desired is return from a strategy should be aligned with the Municipality`s risk appetite. Cederberg Municipality`s risk appetite and risk tolerance is clearly stated in the risk management policy.

Risk Culture

Risk culture is the set of shared attitudes, values and practises that characterise how the Municipality considers risk in its day-to-day activities. Management considers how its risk culture affects and aligns with other elements of risk management. Where misalignment exists, management may take steps to reshape the culture perhaps by rethinking its risk philosophy and risk appetite or how it applies risk management.

Integrity and Ethical Values

Management integrity is a prerequisite for ethical behaviour in all aspects of the Municipality`s activities. Because the Municipality`s good reputation is so valuable, the standard of behaviour must go beyond mere compliance with law. Integrity and ethical values are essential elements of the environment, affecting the design, administration and monitoring of other risk management

components. Establishing ethical values is often difficult because of the need to consider the concerns of several parties.

Management values must balance the concerns of Cederberg Municipality, employees, suppliers and the public. Ethical behaviour and management integrity are by-products of the corporate culture, which encompasses ethical and behavioural standards and how they are communicated and reinforced. Ethical values are not only communicated but also accompanied by explicit guidance regarding what is right and wrong.

Commitment to Competence

Competence reflects the knowledge and skills needed to perform assigned tasks. Management decides 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. Management specifies the competency levels for particular jobs and translate those levels into required knowledge and skills. The necessary knowledge and skills in turn may depend on individuals` intelligence, training and experience.

Management Philosophy and Operating Style

Management`s philosophy and operating style affect the way the Municipality is managed, including the kind of risks accepted. The attitude and daily operating style of top management affect the extent to which actions are aligned with risk philosophy and appetite. For example, an undisciplined operating style often is associated with and might encourage an appetite for high risk. 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 Municipality`s operating environment, both internal and external.

Organisational Structure

An organisational structure provides the framework to plan, execute, control and monitor activities.

A relevant organisational structure includes defining key areas of authority and responsibility and establishing appropriate lines of reporting. For example, an internal audit function should be structured in a manner that achieves organisational objectivity and permits full and unrestricted access to top management and the audit committee, and the chief audit executive should report to a level within the Municipality that allows the internal audit activity to fulfil its responsibilities.

An organisational structure is developed to suit an institution`s needs. The appropriateness of an organizational structure depends, in part, on the Municipality`s size and the nature of its activities.

Assignment of Authority and Responsibility

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 sizing risks and weighing potential losses versus gains in arriving at good business decisions. Another challenge is ensuring that all personnel understand the Municipality`s objectives. It is essential that individuals know how their actions interrelate and contribute to achievement of the objectives.

Human Resource Policies and Practices

Human resource practices pertaining to hiring, orientation, training, evaluating, counselling, promoting, compensating and taking remedial actions send messages to employees regarding expected levels of integrity, ethical behaviour and competence. For example, standards of hiring the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behaviour, demonstrate s Municipality`s commitment to competent and trustworthy people.

It is essential that employees be equipped to tackle new challenges as issues and risks throughout the Municipality change and become more complex driven in part by rapidly changing technologies and increasing competition. Hiring competent people and providing one-time training are not enough. The education process is on-going.

Differences in Environment

The internal environment of an institution`s autonomous subsidiary, divisions and other units can vary widely due to differences in senior operating management`s preferences, value judgements and management styles.

Since operating units often are managed in different ways, it is unlikely their internal environments will be the same. It is important, therefore, to recognise the effect that varying internal environments can have on other risk management framework components. The impact of an ineffective internal environment could be far-reaching, possibly resulting in financial loss, a tarnished public image or a business failure.

4. OBJECTIVE SETTING

Objective setting is a precondition to event identification, risk management, and risk response. There must first be objectives before management can identify risks to their achievement and take necessary actions to manage the risks.

There are 5 factors to consider with regard to objective setting:

- Strategic Objectives;
- Related Objectives;
- Selected Objectives; and
- Risk Appetite and Risk Tolerance.

Strategic Objectives

The Municipality`s mission sets out in broad terms what the Municipality aspires to achieve. From this, management sets its strategic objectives, formulates strategy and establishes related objectives for the Municipality. Strategic objectives are high-level goals, aligned with and supporting the Municipality`s mission/vision. Strategic objectives reflect management`s choice as to how the Municipality will seek to create value for its stakeholders.

Related Objectives

Establishing the right objectives that support and are aligned with the selected strategy, relative to all the Municipality`s activities, is critical to success. By focusing first on strategic objectives and strategy, a municipality is positioned to develop related objectives at operational levels, achievements of which will create and preserve value.

Objectives need to be readily understood and measurable. Cederberg Municipality`s risk management requires that personnel at all levels have a requisite understanding of the Municipality`s objectives as they relate to the individual`s sphere of influence.

All employees must have a mutual understanding of what is to be accomplished and a means of measuring what is being accomplished.

There are three (3) categories of related objectives:
Operational Objectives - These pertain to the effectiveness and efficiency of the Municipality`s operations, including performance and profitability goals and safeguarding resources against loss.

Reporting Objectives – These pertain to the reliability of reporting. They include internal and external reporting and may involve financial of non-financial information.

Compliance Objectives – These pertain adherence to relevant laws and regulations.

Selected Objectives

As part of risk management, management ensures that the Municipality has selected objectives and considered how they support the Municipality`s strategy and mission/vision. The Municipality`s objectives should also align with the Municipality`s risk appétit. Misalignment could result in the Municipality not accepting enough risk to achieve its objectives or, conversely, accepting undue risks.

Risk Appetite and Risk Tolerance
Frequently, the terms risk appetite and risk tolerance are used interchangeably, although they represent related, but different concepts. Risk appetite is a broad based description of the desired level of risk that the Municipality will take in pursuit of its mission. Risk tolerance reflects the acceptance variation in outcomes related to specific performance measures linked to objectives the Municipality seeks to achieve.

5. EVENT IDENTIFICATION

An event is an incident or occurrence emanating from internal or external sources that could affect implementation of strategy or achievement of objectives. Events may have positive or negative impacts, or both. As part of event identification, management recognises that uncertainties exist, but does not know when an event may occur, or its outcome should it occur. To avoid overlooking relevant events, identification is best made part from the assessment of the likelihood of the event occurring, which is the topic of Risk Assessment. There are 5 factors to consider with regard to event identification:

- Factors Influencing Strategy and Objectives;
- Methodologies and Techniques;
- Event Inter-dependencies;
- Event Categories; and
- Risks and Opportunities.

Factors Influencing Strategy and Objectives

A myriad of external and internal factors influences how events could potentially affect strategy implementation and achievement of objectives. As part of risk management, personnel recognize the importance of understanding external and internal factors and the type of events that can emanate there from. Management considers current factors, as well as those that may occur in the future.
The table below lists the internal and external factors:

Internal	External
Infrastructure	Economic and Business
Personnel	Natural environment
Process	Political
Technology	Social
	Technological

Methodologies and Techniques

Event identification methodology may comprise a combination of techniques, together with supporting tools. For instance, management may use interactive group workshops as part of its event identification methodology, with a facilitator employing a variety of technology-based tools to assist participants.

Event identification techniques look both to the past and the future. Techniques that focus on past events and trends consider such matters as payment default histories, changes in commodity prices and lost time accidents. Techniques that focus on future exposures consider such matters as exposure to shifting demographics, new market conditions and competitor actions.

Event Inter-dependencies

Events do not occur in isolation. One event can trigger another, and event can occur currently. In event identification, management should understand how events interrelate. By assessing the interrelationships, one can determine where risk management efforts are best directed. For example, a change to a central bank interest rate affects foreign exchange rates and, in turn, a company`s currency transaction gains and losses.

Event Categories

It may be useful to group potential events into categories. By aggregating events horizontally across the Municipality and vertically within operating units, management develops an understanding of the interrelationships between events, gaining enhanced information as a basis for risk assessment. By grouping together similar potential events, management can better determine potential opportunities and risks. Event categorisation also allows management to consider the completeness of its event identification efforts.

Risk and Opportunities

Events may be a negative impact, a positive impact or both. Events with a potentially negative impact represent risks, which require management`s assessment and response. Accordingly, risk is 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. Events representing opportunities are channelled back to management`s strategy or objective-setting processes, so that actions can be formulated to seize the opportunities. Events potentially offsetting the negative impact of risks are considered in management`s risk assessment and response.

6. RISK ASSESSMENT

In risk assessment, management considers the mix of potential future events relevant to the Cederberg Municipality and its activities.

This entails examining factors including the Municipality`s size, complexity of operations and degree of regulation over its activities that shape the Municipality`s risk profile and influence the methodology it uses to assess risks.

This strategy is also underpinned by a fraud risk assessment. The fraud risk assessment is completed according to the same process as the other risk assessments.

However, the Municipality may wish to integrate the fraud risk evaluation together with the other risk profiles or to separately complete a fraud risk assessment. The fraud risk information will need to be categorised in order to develop and maintain the fraud prevention plan.

Inherent and Residual Risk

Management considers both inherent and residual risk. Inherent risk is the risk to the Municipality in the absence of any actions management might take to alter either the risk`s likelihood or impact. Residual risk is the risk that remains after management responds to the risk. Risk assessment is applied first to inherent risks. Once risk responses have been developed, management then uses risk assessment techniques in determining residual risk.

Impact and Likelihood

Uncertainty of potential events is evaluated from two perspectives likelihood and impact. Likelihood represents the possibility that a given event will occur, while impact represents its effect. Likelihood and impact are commonly used terms, although some institutions sue terms such as probability, and severity or consequence.

7. RISK RESPONSE

Identifying Risk Responses

Risk responses fall within the following categories:

- **Avoidance –** Action is taken to exit the activities giving rise to risk. Risk avoidance may involve exiting a produce line, declining expansion to a new geographical market, or selling a division. Example The best way to avoid flood risk is to locate the development outside areas of Flood Zones.
- **Reduction –** Action is taken to reduce the risk likelihood or impact, or both. This may involve any of a myriad of everyday business decisions.
- **Sharing –** Action is taken to reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common risk sharing techniques include purchasing insurance products, pooling risks, engaging in hedging transactions, or outsourcing an activity.
- **Accept-** No action is taken to affect likelihood or impact.

Evaluating Possible Risk Responses

Inherent risks are analysed and responses evaluated with the intent of achieving a residual risk level aligned with the Municipality`s risk tolerances.

Any several responses may bring residual risk in line with risk tolerance, and sometimes a combination of responses provides the optimum result. Similarly, certain responses will affect the risk of multiple potential events.

Because risk responses may address multiple risks, management may discover that additional actions are not warranted. Existing procedures may be sufficient or may need to be performed better. Accordingly, management considers how individual responses, or combinations of responses, interact to affect potential events.

Evaluating Effect of Response on Likelihood and Impact

In evaluating response options, management considers the affect on both risk likelihood and impact, and understands that a response might affect likelihood and impact differently. The potential response to assessment of likelihood and impact may consider past events and trends, and potential future scenarios. In evaluating alternative responses, management determines their potential affect typically uses the same units of measure for the objective and associated risks as established in the risk assessment component.

8. CONTROL ACTIVITIES

Control activities are policies and procedures, which are the actions of people to implement the policies, to help ensure that management`s risk responses are carried out.

Types of Control Activities

Many different descriptions or types of control activities have been put forth. Internal Controls can be preventative, detective or corrective by nature.

- Preventative Controls are designed to keep errors or irregularities from occurring in the first place;
- Detective controls are designed to detect errors or irregularities that may have occurred;
- Corrective Controls are designed to correct errors or irregularities that have been detected.

Internal Control

Internal control is an integral part of risk 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 organizational 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 trail 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 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 department arising from factors within the department and to changes in the environment;
- The cost of controls must be balanced against 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 and 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 department 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**

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 job descriptions, development plans, review and approval of an employee`s work. Employees should be provided 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.

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`s 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.

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

Controls over Information Systems

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 computerised 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

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

Application Controls

Application controls are designed to ensure completeness, accuracy authorisation and validity of data capture and processing. Individual applications may rely on effective operation of controls over information systems to ensure that data is captured or generated when needed, supporting applications are available and interface errors are detected quickly. One of the most significant contributions of computers is the ability to prevent errors from entering the system, as well as detecting and correcting them once they are present. To do this, application controls depend on computerised edit checks. These consist of format, existence, reasonableness and other checks on the data that are build into an application during development. When properly designed, they can provide control over entered data.

9. INFORMATION AND COMMUNICATION

The Municipality identifies and captures information financial and non-financial, relating to external as well as internal events and activities relevant to managing the Cederberg Municipality. This information is delivered to personnel in a form and timeframe that enable them to carry out their risk management and other responsibilities.

9.1 Risk Management Information System

In order to ensure that reports are compiled with, the Risk Management Office is to procure an appropriate ICT tool for use throughout the organization that will achieve the following primary objectives:

- Collate and aggregate (in electronic format) information relating to ERM;
- Provide a management information tool that analyses data entered in order to identify trends, patterns ect.;
- Functionally, as a performance management tool based on risk registers, controls and implementation of actions by risk owners
- Enable effective monitoring and evaluation of the ERM processes;

- Ensure the integrity of the data and provide an audit trail on actions and omission related to the implementation of the ERM processes; and
- Function as an integrated case management system for the Cederberg Municipality (CM);
- The risk management office shall procure (in line with CM procurement policy) an electronic system within twelve (12) months of the approval of this strategy.

10. MONITORING AND REPORTING

Risk management changes over time. Risk responses that were once effective may become irrelevant; control activities may become less effective, or no longer be performed; or the Municipality`s objectives may change. This can be due to the arrival of new personnel, changes in the municipality structure or direction, or the introduction of new processes. Monitoring can be done in two ways: through on-going activities or separate evaluations.

10.1 Ongoing Monitoring Activities

Many activities serve to monitor the effectiveness of enterprise risk management in the ordinary course of running the business. These include regular management and supervisory activities, variance analysis, comparisons, reconciliations and other routine actions.

10.2 Separate Evaluations

While ongoing monitoring procedures usually provide important feedback on the effectiveness of other risk management components, it may be useful to take a fresh look from time to time, focusing directly on risk management effectiveness. This also provides an opportunity to consider the continued effectiveness of the on-going monitoring procedures.

10.2 Reporting

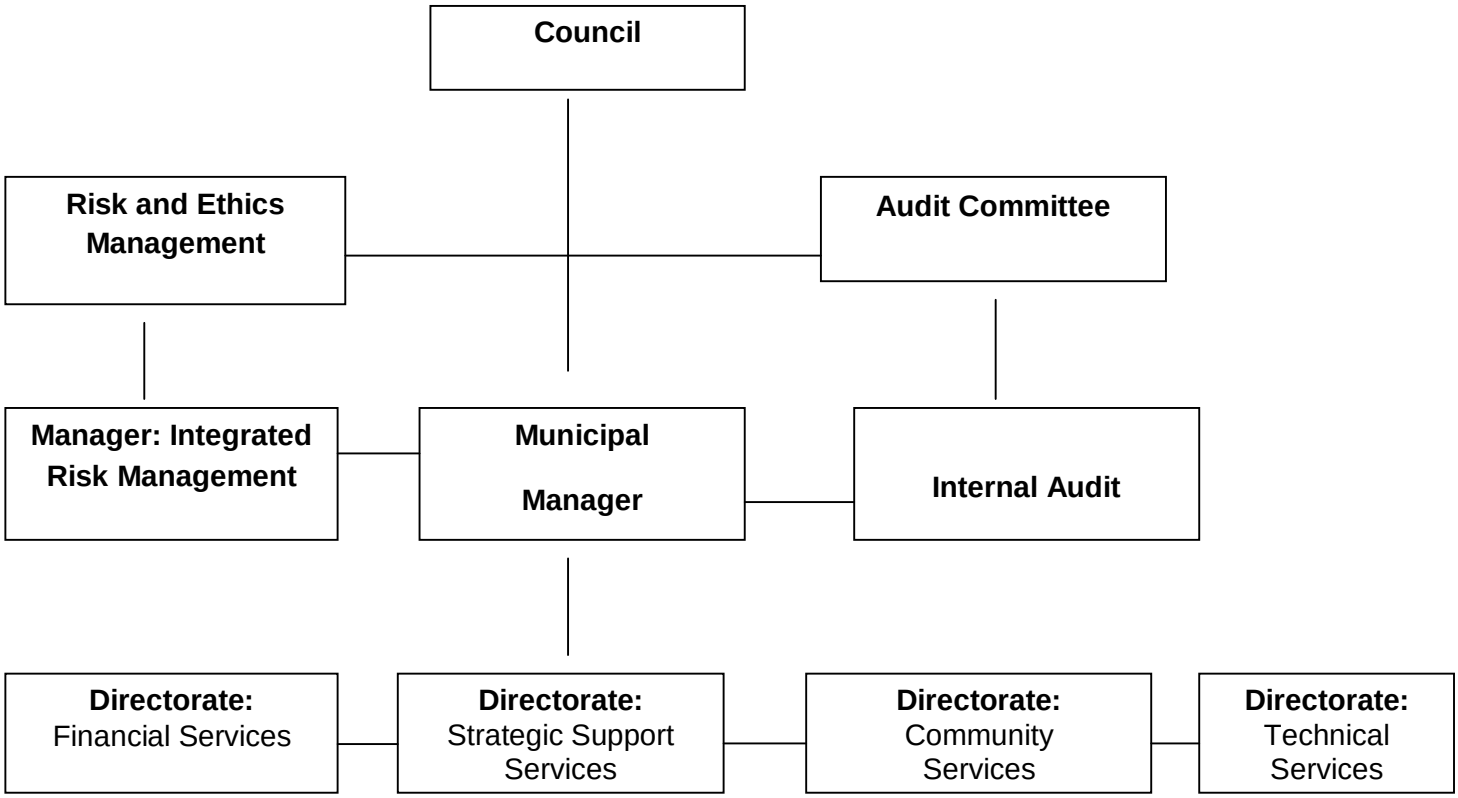
When it gets to reporting on risks and risk management processes, the following questions may arise, but not limited:

- How does the organisation report on risks?
- Who do they report to?
- How frequently do they report?
- What is the form of the reporting? (i.e. verbally)

Monthly and Quarterly reports should be generated to enable the processes of risk monitoring and the communication of action plans and the risk profiles as appropriate. Regular reporting to the relevant stakeholders, stakeholders, on status of risks and risk management processes within the departments. In order for risk management to work, it must be embedded into the everyday activities of the Municipality. It should be integrated into the reporting process. Risk should be part of everyday activities of the Municipality. It should be integrated into the reporting process. Risk should be part of every decision that is made, every objective that is set and every process that is designed. Risk

management will be integrated into the reporting process of managers in strategic planning meetings of the directorates / departments that are held.

The structures below set out the reporting lines through which risk management will be reported within the Cederberg Municipality:



11. REVIEW AND APPROVAL OF THE STRATEGY

The Risk and Ethics Management Committee must review this Policy every three (3) years and determine its adequacy and effectiveness for current circumstances and recommended to Council for approval.