ENTERPRISE RISK MANAGEMENT

Corporate Business Risk Planning

Risk Management Model

First Release: Nov. 26, 03
Last Update: Sep. 22, 05

Intentionally Left Blank

ENTERPRISE RISK MANAGEMENT
Corporate Business Risk Planning
Risk Management Model

Table of Contents

Click on blue arrows to return to the Table of contents

ENTERPRISE RISK MANAGEMENT 1

INTRODUCTION 1
CULTURAL IMPACT 2
ROLES AND RESPONSIBILITIES 3

CORPORATE BUSINESS RISK PLANNING 5

PHASE 1 – UNDERSTAND OBJECTIVES 6
PHASE 2 – RISK IDENTIFICATION 7
Step 1 – Preliminary Risk Identification and Risk Rating 7
Step 2 – Risk Identification for Higher Rated Risk Events 8
PHASE 3 – RISK ASSESSMENT 10
Step 1 – Quantitative Assessment of Higher Rated Risks 10
Step 2 – Subjective Assessment and Corporate Prioritization 12
Step 3 – Validation and Approval of Corporate Priorities 13
PHASE 4 – RISK RESPONSE 14
Risk Response Techniques 15
PHASE 5 – MONITORING AND REPORTING 17

APPENDICIES 18

DEFINITIONS 19
RISK MANAGEMENT ASSESSMENT FRAMEWORK 21
RISK AREAS AND EXAMPLES OF RISK EVENTS 23
EXAMPLE OF POTENTIAL SOURCES OF RISK 25
SAMPLE RISK QUESTIONNAIRE 26
DEVELOPING A RISK STATEMENT 27
RISK PROFILE FORM 28
SUMMARY BY HIGHER RATED RISKS 30
RISK CRITERIA AND TOLERANCES 31
Business Area Perspective 31
Corporate Perspective 32
Citizen Perspective 34
PRIORITIZED LIST OF RISKS - QUANTITATIVE 36
PRIORITIZED LIST OF RISKS SUBJECTIVE AND QUANTITATIVE ASSESSMENT 37

THE CITY OF Edmonton

Intentionally Left Blank

ENTERPRISE RISK MANAGEMENT

Introduction

Everyday managers and employees practice risk management by making decisions on what to do, how to do it and when to do it. Managing risk has become increasingly complex. Technological innovation, globalization, complex regulation and increased accountability have all combined to significantly change the landscape of risk management today. Organizations cannot afford to let new, unforeseen areas of risk remain unidentified. Communication with interested stakeholders is essential, it must occur at all stages of the risk management process and at all levels of the organization. It is not whether to engage stakeholders, but who and how.

Since its passage in 2002, Sarbanes-Oxley has become the driving force for organizations to implement controls with the hopes of avoiding the negative publicity surrounding corporate scandals (e.g., Enron, WorldCom). In 2004 guidance on the implementation of a consistent Enterprise Risk Management (ERM) framework was provided through the Commission of Sponsoring Organizations of the Treadway Commission's (COSO). The framework strives to define and describe ERM and provides a standard against which businesses can assess their ERM program and determine how to improve it. An executive summary of the framework can be downloaded from http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

The risk that something bad will happen (e.g., decreased customer satisfaction) or something positive will not happen (e.g., a missed opportunity) is a part of daily operations. Because different stakeholders place different values on things, they also view risk differently; consequently, attempts to manage risk informally may not be fully effective from an organizational perspective. In response, the City adopted ERM and developed the Corporate Business Risk Planning (CBRP) risk management model to supplement and coordinate existing risk management activities. Definitions of ERM and other risk management terms are provided in Appendix A.

The goal for ERM in the City of Edmonton is to have a self-sustaining process that is an integral element of the Corporation's business process.

The objectives for ERM are to:

- Implement an integrated risk management approach to ensure all significant areas of risk are identified, understood and effectively managed,
- Promote a shared vision of risk management and encourage discussion on risks at all levels of the organization to provide a clear understanding of risk/benefit trade-offs,
- Deploy appropriate risk management methodologies and tools for use in identifying, assessing, managing and reporting on risks, and
- Determine the appropriate balance between cost and control of risk and deploy appropriate resources to manage/optimize key risks.

The ultimate goal of the Corporate Business Risk Planning (CBRP) project is to identify current and potential risks to the Corporation, categorize them, and ensure that each one is being appropriately managed.

The adoption of the CBRP model will result in:

- Endorsement or enhancement of existing risk management activities (such as the City's Infrastructure Strategy, insurance, security, etc.),
- Development of a process to address risks not previously identified or not yet identified at an appropriate level of the organization, and
- Development of a framework to prioritize all risks, for multiple types of service, within the context of corporate business planning.

Cultural Impact

For an organization to achieve the maximum benefit from ERM it must recognize that it is not just a bureaucratic process, it is a risk management culture in which attitudes, behaviours and activities together form an environment in which risk considerations are part of what we routinely do.

The implementation of ERM can have a significant impact on the risk culture of the corporation with the process combining an inward looking (operational) focus with a forward thinking (strategic) initiative. In this new "risk smart" culture, managers will be more aware of business risks the corporation faces, and will have better information for improved management of risks and more informed decision making. This will ultimately improve the corporation's strategic planning process and reduce the overall level of risk we face as an organization.

As ERM principles are adopted and applied the traditional reactive risk culture will change to a proactive risk smart culture for more cost effective risk management. Table 1 sets out key traits of each culture.

Table 1 – Risk Culture Traits

Traditional	Risk Smart
• Ad hoc or informal processes • Segregated risk management, risks are considered in isolation of each other • No formal measures or reporting • Reactive decision making, risks are not optimized • Narrowly focused risk assessments • Risks considered as negative	• Formal and structured processes • Integrated risk management, risk linked to business objectives • Formal measurement and reporting. • High level of risk awareness • Proactive risk identification and assessment • Open communication on risk related matters

Progress in implementing ERM will be impacted by the ability for the Corporation to change its risk management culture. The following questions from a Risk Management Assessment Framework tool provide a basis for assessing risk management performance and progress in improving risk management capabilities.

- Does senior management support and promote risk management?
- Is there a clear risk strategy and risk policies?
- Are people equipped and supported to manage risks well?

- Are there effective arrangements for managing risks with partners?
- Do the organization's processes incorporate effective risk management?
- Are risks handled well?
- Does risk management contribute to achieving outcomes?

This framework should be applied periodically to evaluate performance and progress in improving risk management capabilities and its impact on improved risk handling. Performance levels for each of these questions are set out in Appendix B. The detailed framework is available on the UK Government website at http://www.hm-treasury.gov.uk/media/17A/81/17A8166B-BCDC-D4B3-16668DC702198931.pdf

Roles and Responsibilities

The **Audit Committee** is responsible to **City Council** for oversight of the ERM process. The results of the corporation's efforts and an evaluation of the risk management process, will be periodically reported to the Audit Committee.

Employees are responsible for**:**

a. Staying aware of risk management issues and practicing risk-smart behaviours.

Business Risk Planning Team is responsible for:

a. Documenting results of activities for periodic review and assessment by SMT and to ensure consistency with corporate goals,
b. Ensuring appropriate planning, training, monitoring and documentation processes are in place to support the ERM program,
c. Ongoing coordination of risk management activities both within their departments and at the corporate level,
d. Conducting a subjective assessment of higher rated risks, and
e. Identify enhancements to the CBRP process.

Corporate Services Department is responsible for:

a. Providing guidance and a centre of expertise in support of the ERM framework.

Department Management is responsible for:

a. Identification and assessment of risks that involve their department,
b. Ensuring risk consideration is part of the decision-making process,
c. Monitoring external and internal environments to identify changes that may impact departmental or corporate risk exposures, and
d. Development and implementation of risk management strategies for risks.

Senior Management Team is responsible for:

a. Championing ERM by visibly supporting the process and promoting a risk smart culture throughout their department,
b. Approval of the CBRP model, risk appetite and risk tolerances,
c. Evaluation, confirmation and approval of risk assessments, and
d. Ensuring ERM strategies are adequately implemented.

City Manager is responsible for:

a. The consistent administration and communication of the ERM program, and
b. Reporting results to the Audit Committee

City Auditor is responsible for:

a. Periodic examination and evaluation of the effectiveness of the ERM program and providing assurance to the Audit Committee on the risk management process,
b. Review management of key risks, and
c. Assisting, on a request basis, with facilitation of risk identification and assessment workshops. The extent of assistance will depend on the availability of resources.

CORPORATE BUSINESS RISK PLANNING

Corporate Business Risk Planning is one of the processes or functions that make up the ERM environment in the City (Figure 1). The CBRP process was developed to document of all types of risks regardless of their source or level (Figure 2). The CBRP risk management model is depicted as a cyclical rather than linear process with risks being reassessed on a periodic basis in order to confirm their status relative to current business objectives (Figure 3).

Figure 1 – The ERM Environment

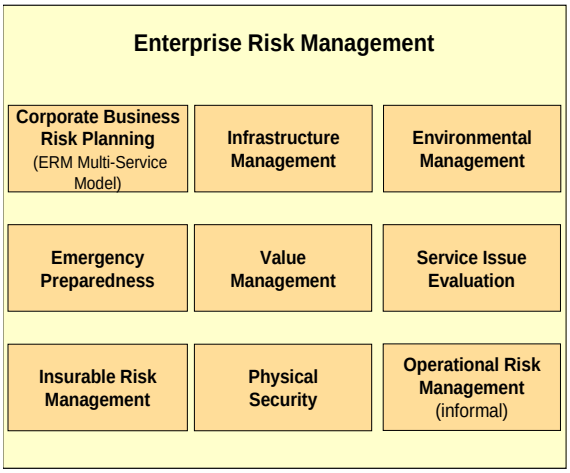


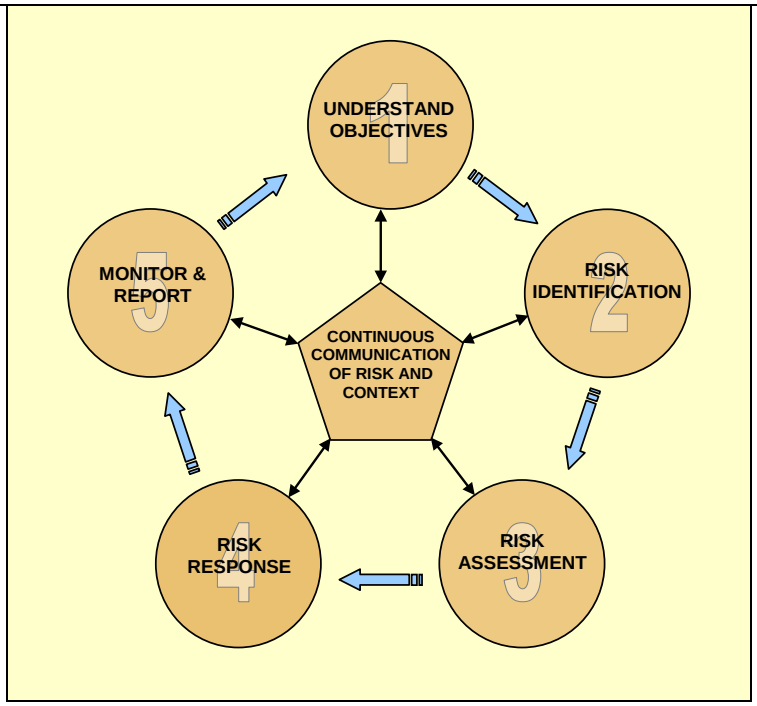
Figure 2 –The CBRP Environment

Figure 3 –The CBRP Risk Management Model.

Phase 1
Understand the organization's objectives, strategic direction, stakeholders, and structure.

Phase 2
Identify the consequence a risk event will have on the stated objectives and existing mitigating measures.

Phase 3
Systematic assessment of risks against established criteria and setting of priorities.



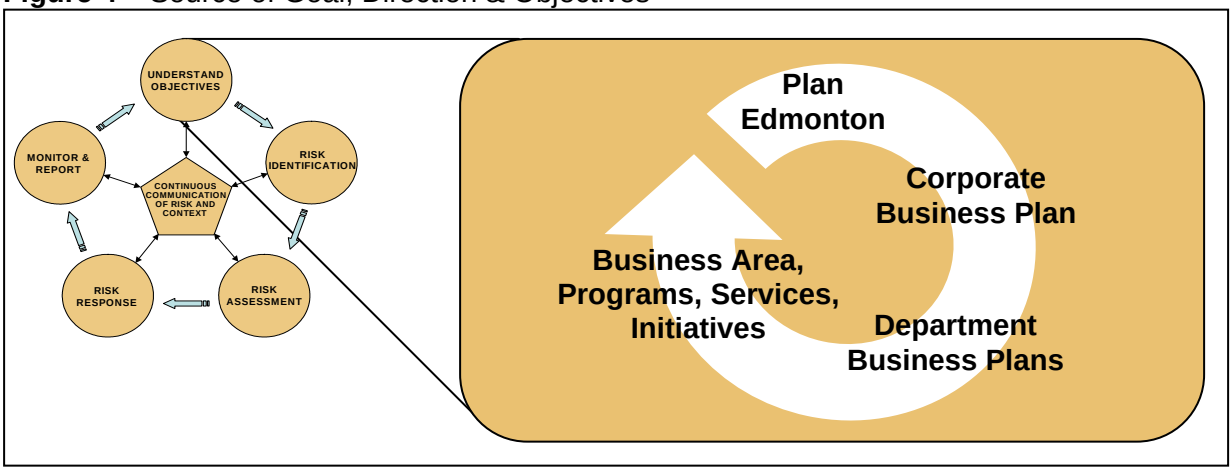
Phase 4
Identification, evaluation and implementation of actions to address risks identified as priorities.

Phase 5
Establish a monitoring process, evaluate effectiveness of decisions and recommend revisions.

PHASE 1 – UNDERSTAND OBJECTIVES

The first phase of the risk management model is to understand the organization's objectives, strategic direction, stakeholders, and structure (Figure 4). This understanding includes both the corporate goals and the specific business area objectives.

Figure 4 – Source of Goal, Direction & Objectives



The City of Edmonton's Corporate Business Plan outlines priorities and the longer-term strategies required to preserve the future health of this city. It follows the vision for our city described in Plan Edmonton:

- A culturally diverse city where people choose to live, learn, work and play,
- An international smart city with a vibrant economy,
- A capital city where businesses want to locate and expand, and
- A welcoming city where citizens take pride in their community and their contribution to its quality of life.

The City Administration takes its goals from the five key municipal responsibility areas in Plan Edmonton and adds a sixth to meet citizen expectations for a well-managed Administration.

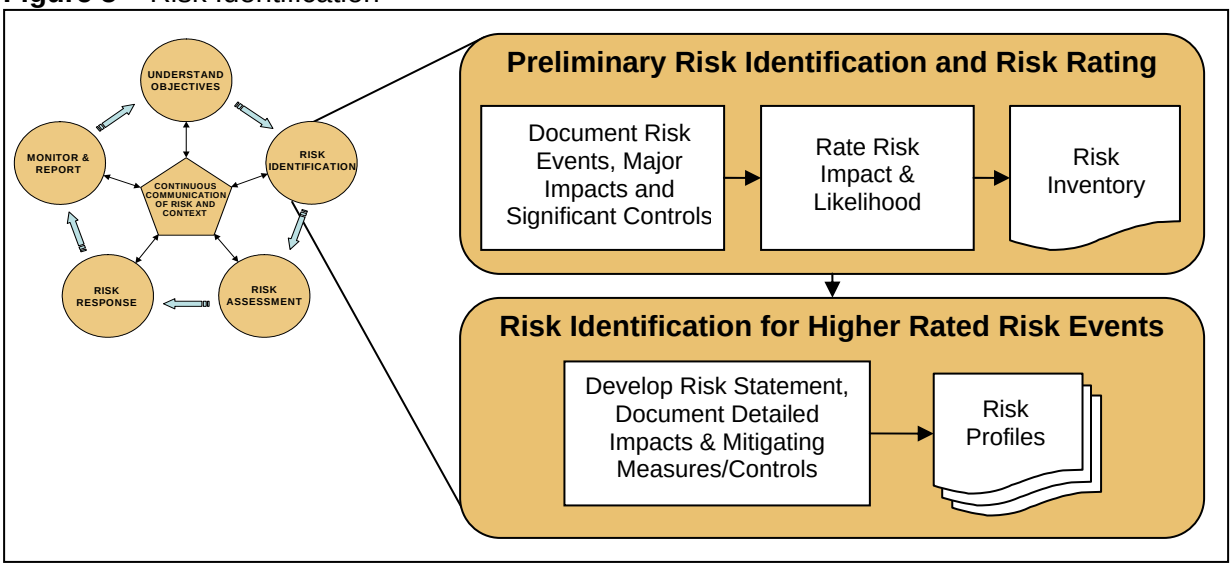
- **Services to People –** Quality, best value services that contribute to Edmonton's safety, security, well-being and enjoyment,
- **Planned Growth –** A well-planned urban environment,
- **Economic Development –** A dynamic, best value business climate,
- **Infrastructure and Physical Environment –** Prudent stewardship of environment, infrastructure and technology,
- **Leadership, Regional Cooperation and Planning –** A strong partner in regional affairs including other orders of government, and
- **Administrative Excellence –** Quality public service in a cost-effective manner.

Business areas need to identify and document their specific business objectives prior to identifying risks. Business areas must ensure that specific objectives are aligned with the corporate goals.

PHASE 2 – RISK IDENTIFICATION

The second phase of the model is to document the impact a risk event will have on specific business objectives identified in phase 1 and existing mitigating measures. There are two steps in this phase. The first step "Preliminary Risk Identification and Risk Rating" is to identify all risks and determine which have the greatest potential to prevent the achievement of business objectives. The second step is the completion of detailed documentation for higher rated risks.

Figure 5 – Risk Identification



Step 1 – Preliminary Risk Identification and Risk Rating

This step may be completed at the branch level, section level or a lower level depending on the organizational structure and delegated authority.

The first part of this step is to briefly document all risk events that could prevent the achievement of business objectives, the major impacts that would result if the risk event took place and the significant controls that are in place to mitigate the risk event. The exercise should be undertaken in a team setting comprised of the head of the business unit and a number of individuals familiar with the operations. Where possible a facilitator should be engaged to guide the process. The following are examples of tools available to assist in completing this exercise:

- Areas of Risk and Examples of Risk Events (Appendix C)
- Potential Sources of Risk (Appendix D)
- Sample Risk Questionnaire (Appendix E)

The second part of this step is to assign a rating to the impact of the event and to the likelihood that the event would occur. Table 2 sets out the criteria for rating the impact and likelihood in the preliminary identification step.

An example of documentation for the preliminary identification step is provided in Figure 6.

Table 2 – Preliminary Risk Rating Criteria

Rating	High	Medium	Low
Impact	If this happens it would cause major problems & delays.	If this happens it would cause problems & delays.	If this happens it would cause only minor problems & delays.
Likelihood	Surely will happen	Might happen	Not very likely to happen

Risks should be assessed in both their inherent state (without considering the impact of controls) and residual state (with controls in place) to assess the impact of controls. The rating for the residual risk is documented and used to determine which risk events require further documentation.

Figure 6 – Example of a Risk Inventory

Business Unit A

Risk Identification				Residual Risk Rating	
	Risk Event	**Major Impacts**	**Controls**	**Impact**	**Likelihood**
1	Employees are absent due to sickness, extended leave, etc.	• Need to backfill - not easy to do this because of the knowledge required.	• None	High	Medium
2	Dangerous situations to staff	• Physical harm to staff	• Special training • Special tools • Warning system - Red Flag Protocol	Low	Low
3	Use of technology affects productivity	• Expectation is an increase in productivity • Decreased productivity - software is not user friendly • Customer satisfaction decreases. • Staff frustration	• On-going training	Medium	Medium

Any risk event with a high rating for either the impact or likelihood or a medium rating for both the impact and likelihood should be carried forward to step 2 for further analysis. In figure 6 risks 1 and 3 would be carried forward to step 2. Risk events that are common to a number of business units should be consolidated and re-assessed from a branch or department perspective.

Step 2 – Risk Identification for Higher Rated Risk Events

The next step in the risk identification process is to prepare a risk statement that clearly and concisely describes the risk that is to be assessed. A tool for developing a risk statement is set

out in Appendix F. Analysis of risk statements will be undertaken to identify relationships that may exist among risks.

Once the risk statement has been prepared, the detailed impacts or concerns related to the risk are to be identified along with the measures or mechanisms that are in place to mitigate the impact and/or the likelihood of an occurrence of the risk event.

The information noted in the previous paragraphs needs to be documented on the Risk Profile included in Appendix G. For risks impacting more than one business area multiple Risk Profiles will initially be required. A consolidated Risk Profile will be developed as the risk assessment process progresses to higher levels in the organization.

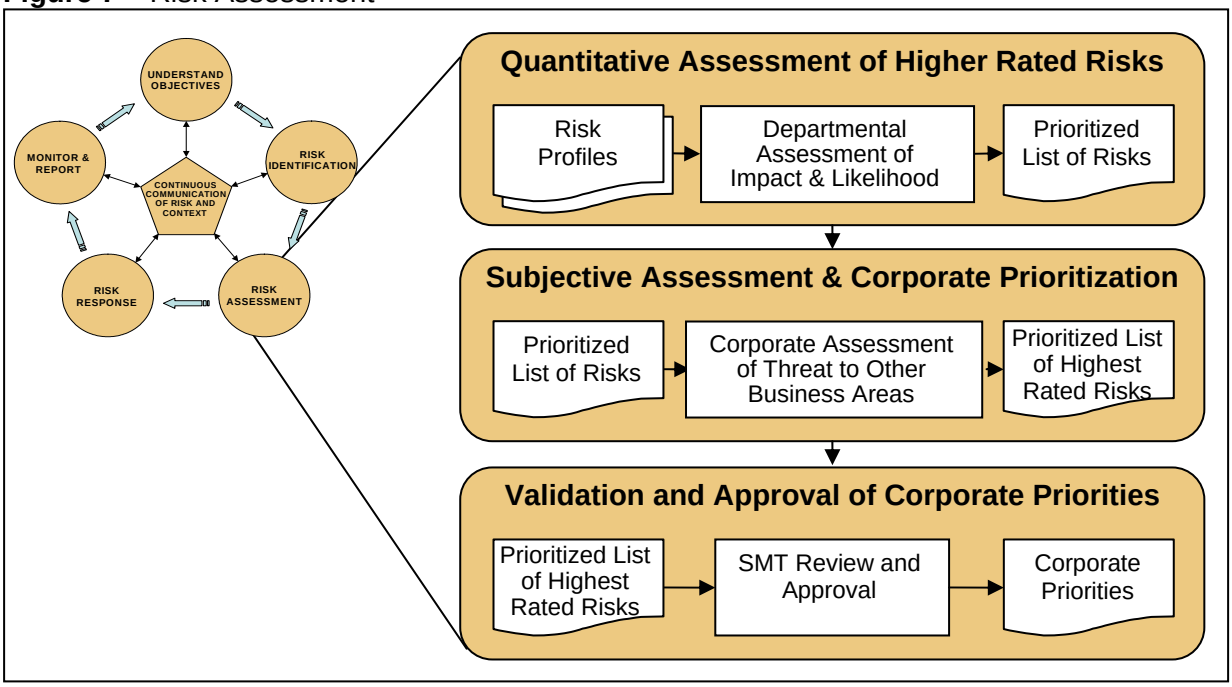
Initially the focus will be on events that are considered highest risk. A complete inventory will likely take a few years to complete. As higher rated risks are identified and risk statement developed they will be summarized and reported to ensure that proper assessments can be undertaken. An example is illustrated in Appendix H.

To ensure that no significant risks are overlooked and to minimize duplication the CBRP process will be coordinated and interfaced with purpose-specific assessment processes that are currently in place (e.g., Emergency Preparedness, Infrastructure Strategy, Workforce Planning).

PHASE 3 – RISK ASSESSMENT

Risk assessment is a snapshot at a specific point in time. Assessments are to be undertaken or updated annually as part of the business planning process. Risk assessment is a three step process, first at the department or business area level, second by a corporate team and finally by the Senior Management Team.

Figure 7 – Risk Assessment



Step 1 – Quantitative Assessment of Higher Rated Risks

The inputs to this step are the Risk Profiles that have been completed for any new risks as well as the documentation of risks identified and assessed in prior years.

Assessments of both inherent risk and residual risk are to be completed by the department or business that could be affected by the risk. The assessment includes consideration of the magnitude or impact the risk event will have on business objectives should it occur as well as the likelihood that the impact described in the risk statement will occur.

The assessment tool developed for the City will be used to facilitate the quantitative assessment of the identified risks. Table 3 sets out the six levels for assessing the magnitude or impact on objectives if the risk were to occur.

Table 3 – Magnitude/Impact

Descriptor	Explanation	Value
Unacceptable	The impact is totally unacceptable to the organization	1000
Severe	Serious threat to the organization, public, etc.	100
Substantial	Considerable impact	50
Moderate	Moderate impact	10

Descriptor	Explanation	Value
Marginal	Small impact	5
Negligible	Trivial impact	1

The magnitude/impact of risks will be assessed from three perspectives, that of the business area, the corporation and the citizen. The assessment will be conducted using the Risk Profile, the criteria set out in Table 4, and the tolerances set out in Appendix I.

Table 4 – Magnitude/Impact

Business Area Criteria	Corporate Criteria	Citizen Criteria
• Service delivery • Employee safety • Infrastructure capacity	• Financial • Environment • Economy • Legislated/legal requirements	• Citizen Feedback • Phone calls, letters, rallies, survey results, etc. • Media attention • Public safety

Table 5 sets out the six levels for assessing the likelihood or probability that the impact described in the risk statement will occur.

Table 5 – Magnitude/Impact

Descriptor	Explanation	Probability	Value
Highly Likely	Almost certain that it will happen, frequent occurrence	over 70%	20
Likely	More than a 50 – 50 chance	50% – 70%	15
Somewhat Likely	Less than a 50 – 50 chance	15% – 50%	10
Unlikely	Small likelihood, but could well happen	1% – 15%	5
Very Unlikely	Not expected to happen	0.01% – 1%	2
Extremely Unlikely	Just possible, but would be very surprising	less than 0.01%	1

The total risk score is calculated by adding the values of the magnitude/impact associated with each of the three perspectives and multiplying the result by the likelihood value. Based on the total risk score, risks will be categorized as follows:

Table 6 – Risk Categories

Risk Score	Category
Over 2000	Unacceptable
500 – 1999	Undesirable
50 – 499	Marginally Acceptable
10 – 49	Acceptable
Less than 10	Negligible

The output from this step will be:

- A listing of all risks that have the potential to impact business area objects along with the assessment results. This listing can be sorted by department, risk area or risk event (see Appendix J for an example).
- Risk Profiles updated with the results of the assessment.

Step 2 – Subjective Assessment and Corporate Prioritization

The inputs for this step will be:

- The list of risks from the quantitative assessment
- The Risk Profiles for residual risks with the highest risk scores.

The voting members of the Business Risk Planning Team will complete this step using the information contained in the risk definition worksheet including the results of the quantitative assessment. This subjective assessment will be conducted on all risks assessed as either "Unacceptable" or "Undesirable" and, if the number of risks identified is not too great, "Marginally Acceptable."

There are two objectives for this assessment:

- First, to provide a corporate perspective on the risks departments have rated the highest.
- Second, to prioritize identified risks corporately for presentation to SMT.

Following is a description of the technique that will be used to prioritize the risks.

1. The list of risks to be assessed and the risk profiles will be circulated to all BRPT members in preparation for a facilitated workshop.

2. BRPT members are to prepare for a facilitated session by:
    - reviewing the Risk Profiles,
    - obtaining additional information or clarification as required from subject matter experts, and
    - assigning an order of importance to each risk statement using the criteria set out in Table 7.
        - High Importance – 3
        - Medium Importance – 2
        - Low Importance – 1

Table 7 – Subjective Assessment Criteria

High	Medium	Low
• Significant threat with potential to impact other departments. • SMT awareness and direction is required.	• Significant threat with impact limited to the identifying department. • Moderate to low threat with potential to impact other departments. • SMT awareness is required. • General Manager direction is required.	• Moderate to low threat with impact limited to the identifying department. • General Manager awareness and direction is required.

3. During a facilitated workshop, each risk will be discussed prior to collecting information on assigned importance. Importance scores for each risk will be averaged with risks being ranked in descending order based on the average score as illustrated in Appendix K.

4. Results of this subjective assessment will be prioritized into a High, Medium or Low category. High priority will have an average score equal to or greater than 2.5, Medium an average score between 1.5 and 2.49, and Low an average score less than 1.5.

The output from this step will be:

- A corporate prioritized list of risks
- Risk Profiles updated with the results of the assessment

Step 3 – Validation and Approval of Corporate Priorities

The inputs for this step will be:

- The corporate prioritized list of risks from the subjective assessment,
- A listing of risks categorized as negligible from the quantitative assessment, and
- The Profiles for risks rated as high.

Documentation will be provided to the SMT for review followed by a facilitated session at which time the assigned ratings will be validated. The process will take into account the quantitative assessments, subjective assessments and factors which may not have been apparent to the individuals and groups conducting assessments in steps 1 and 2.

SMT will also be provided with risks categorized as negligible for discussion to determine if the effects of the mitigating measures are cost effective.

The output of this review will be the identification of risks considered to have the greatest potential impact on the corporation and assessment of the appropriate level of resources to address each of the risks.

PHASE 4 – RISK RESPONSE

Based on the priorities established by SMT and the total risk scores assigned by departments in the assessment phase the following risk responses are suggested.

Figure 8 – Risk Response

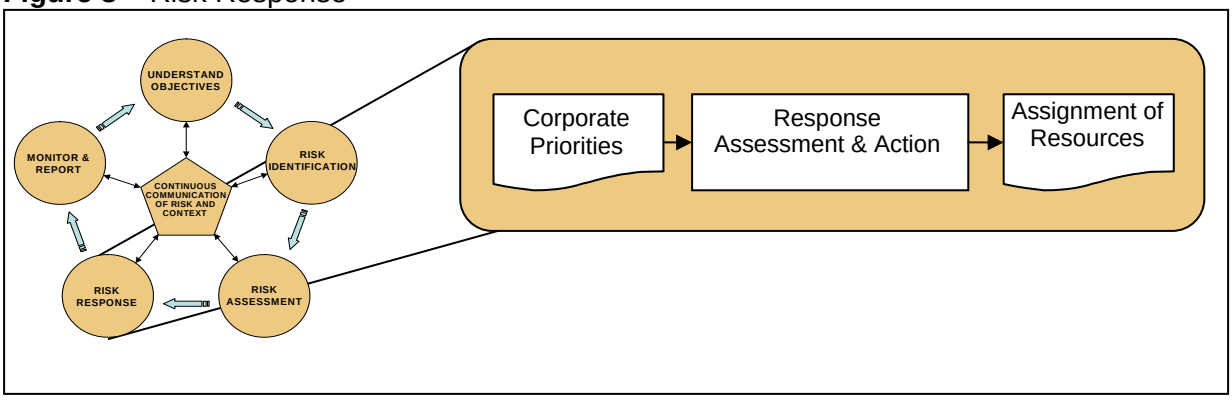


Table 9 graphically represents how risks area categorized.

Figure 9 – Risk Response Score

	MAGNITUDE					
LIKELIHOOD	Negligible	Marginal	Moderate	Substantial	Severe	Unacceptable
Highly Likely						Unacceptable
Likely					Undesirable	
Somewhat Likely				Marginally Acceptable		
Unlikely			Acceptable			
Very Unlikely	Negligible					
Extremely Unlikely						

Table 8 describes the suggested risk response for each category.

Table 8 – Risk Response

Total Risk Score		Category	Suggested Response
1	Over 2000	Unacceptable	Resource to be dedicated to ensuring risk is properly managed and monitored.
2	500 – 1999	Undesirable	Resources to be assigned to ensure risk management measures are in place and periodically monitored.
3	50 – 499	Marginally Acceptable	Risk management measures to be in place and reviewed periodically.

Total Risk Score		Category	Suggested Response
4	10 – 49	Acceptable	Acknowledge and monitor risk with appropriate resourcing.
5	Less than 10	Negligible	Accept risk and evaluate the need for resourcing.

Risk Response Techniques

Following assignment of corporate priority and responsibility for managing the identified risk, an appropriate risk management technique will need to be applied. Each of the following risk management techniques can be applied to a risk either singularly or in combination.

- Terminate or Avoid
- Transfer
- Treat or Reduce
- Tolerate or Accept

Each risk needs to be reviewed to determine the most appropriate technique to be applied. The decision regarding which technique to use should take into account the potential cost of an occurrence as well as the cost of implementing the mitigating measures.

Whatever decision is made needs to be documented. Following implementation, the measure or mechanism is to be recorded on the appropriate risk definition worksheet.

Terminate or Avoid

Whenever an organization cannot offer a service while ensuring a reasonable level of risk and exposure, it should choose avoidance as a risk management technique. Avoiding the risk means that the condition that is creating the risk is eliminated. Risk can sometimes be avoided by simply ceasing the business activity or by not undertaking a part of a project that has high risk associated with it.

This technique has obvious difficulties and limited application. Always ask, "Is there something we could do to deliver this program/project within the tolerance level set by the organization?"

Transfer

Risk transfer allows the company to transfer responsibility for aspects of its operations to another party, perhaps in the form of outsourcing and service agreements, in return for an agreed fee.

Another form of transfer is risk sharing with another organization through a contract. Two common examples are:

- Insurance contracts that require an insurer to pay for claims expenses and losses under certain circumstances, and
- Service contracts whereby a provider agrees to perform a service and assume liability for potential harm occurring in the delivery of that service.

This technique may not be appropriate in circumstances that result in creation of a higher net risk for the organization.

Treat or Reduce

If a risk has been identified that cannot be reasonably avoided or transferred, steps must be taken to ensure that the frequency or impact of any occurrence is minimized.

Reduction can be either through preventative measures, which attempt to reduce the probability and frequency of occurrence, or through controls that attempt to reduce the severity of losses.

Policies and procedures, training, non-slip surfaces at swimming pools and sprinkler systems in buildings are examples of risk reduction measures.

Tolerate or Accept

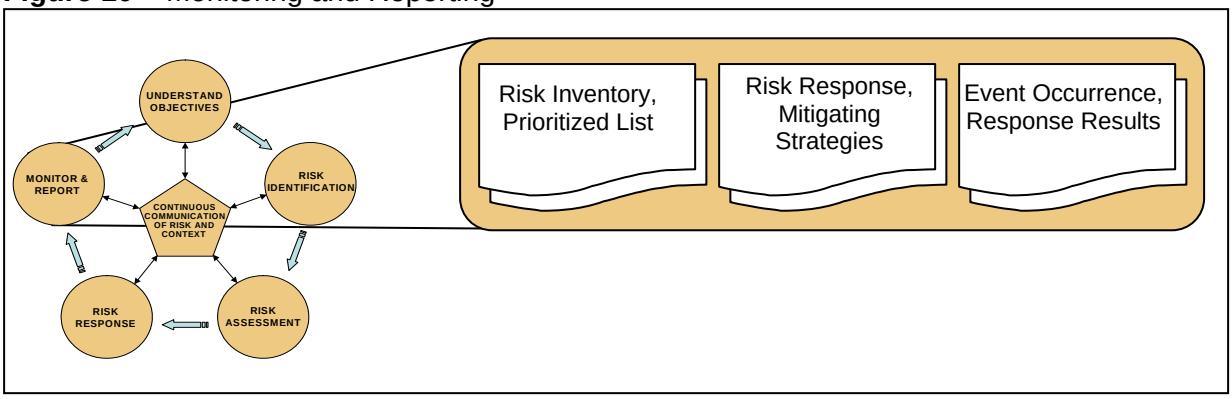
Risk acceptance is exercised when the cost of avoidance, transfer or reduction is not reasonable, or where the risk is so insignificant that the cost of resources to manage it exceeds the potential impact.

Risk acceptance should only be chosen where risks are known and can be monitored. Unintentional acceptance of risk can be the result of insufficient understanding of the scope of risk an organization faces or because the risk has not been fully evaluated.

PHASE 5 – MONITORING AND REPORTING

Monitoring and reporting mechanisms for risk management activities are developed to provide feedback to management and other interested parties (e.g., audit committees, governing bodies, etc). The results of these activities ensure that enterprise risk management is effective in the long term.

Figure 10 – Monitoring and Reporting



Some of these activities could be assigned to functional groups in the organization that are responsible for review and audit. Responsibility may also be assigned to operational managers and employees to ensure that information affecting is risk collected as part of local reporting or monitoring practices and is incorporated into the environmental scanning process. Reporting could also take place through normal management channels (performance reporting, ongoing monitoring, or appraisal).

Reporting facilitates learning and improved decision-making by assessing both successes and failures, monitoring the use of resources, and disseminating information on best practices and lessons learned throughout the organization. Organizations should evaluate the effectiveness of their enterprise risk management processes on a periodic basis to ensure sustained progress in building a risk-smart workforce and environment.

APPENDICIES

Definitions A
Risk Management Assessment Framework B
Risk Areas and Examples of Risk Events C
Potential Sources of Risk D
Sample Risk Questionnaire E
Developing a Risk Statement F
Risk Profile G
Summary of Higher Rated (example only) H
Risk Criteria and Tolerances I
Prioritized List of Risks – Quantitative J
Prioritized List of Risks Subjective and Quantitative K

Corporate Business Risk Planning

Definitions

The following definitions provide an understanding of risk concepts that form the basis of a risk management framework.

Citizen

For external services it includes individuals and corporations. For internal services it includes anyone or any group requesting or benefiting from services.

Corporate Business Risk Planning (CBRP)

A comprehensive process to manage the impact of identified risks on the total operations of the City, allowing it to reasonably achieve its stated business objectives. This process is the City of Edmonton's adaptation of Enterprise Risk Management.

Enterprise Risk Management

Enterprise risk management is a **continuous**, **proactive** and **systematic** process to understand manage and communicate risk from an **organization-wide perspective**. It is about making strategic decisions that contribute to the achievement of an organization's overall corporate objectives.

Key features include:

- Organization-wide focus
- Systematic, proactive, continuous
- Understanding risk profile
- Integrated into existing practices
- Stakeholder focus
- Framework, policy and functional support
- Explicit understanding of level of risk for three main categories: Strategic Risk, Operational Risk and Project Risk

Incident Response

Plans that are in place to respond after an incident has occurred.

Inherent Risk

"Pure" risk without consideration of any mitigating effects of controls.

Operational Risk

Risks that can generally be controlled. These risks arise in relation to areas such as operational processes, human resources, integrity, liability, information processing and technology and financial issues.

Corporate Business Risk Planning

Project Risk

Risks that focus on technical, development, implementation and management aspects that can lead to cost, schedule and performance issues arising from a long list of potential sources including unclear roles, contractor competency, micro-management, environment-related events, etc.

Residual Risk

Risk remaining after taking into account the effectiveness of existing controls.

Risk

Risk refers to uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event that has the potential to influence the achievement of an organization's objectives (e.g., low chance of a major earthquake in Edmonton).

Risk Area

A risk area is a general term that can be used to describe a number of related events or circumstances (e.g., environment).

Risk Event

A risk event is a specific event or circumstance that could affect the ability to achieve a stated objective (e.g., an earthquake).

Risk Response

Mechanisms that are in place to appropriately address the likelihood or impact of an occurrence.

Risk Statement

A sentence or concise phrase that describes the objective, the risk event and the likely or potential consequence should the risk event occur (e.g., inability to respond appropriately to a major earthquake resulting in multiple deaths).

Risk-smart

Risk-smart refers to an environment that supports responsible risk management, where risk management is built into existing governance and organizational structures, and into planning and operational processes. An essential element of a risk-smart environment is to ensure that the workplace has the capacity and tools to be innovative while recognizing and respecting the need to be prudent in protecting the public interest and maintaining public trust.

Strategic Risk

Issues of significant sensitivity, issues that are not easy to address because they cannot be directly controlled, and significant risks common to multiple operating areas or projects.

Corporate Business Risk Planning

Risk Management Assessment Framework

Level 1 Awareness & Understanding	Level 2 Implementation Planned & in Progress	Level 3 Implemented in Key Areas	Level 4 Embedded and Improving	Level 5 Excellent Capability Established
1. Leadership – Does senior management support & promote risk management?				
Top management are aware of need to manage uncertainty and risk and have made resources available to improve.	Senior Managers take the lead to ensure that approaches for addressing risk are being developed and implemented	Senior Managers act as role models to apply risk management consistently and thoroughly across the organization.	Top down commitment with embedding and integrating risk management as routine business practice.	Senior Managers re-enforce and sustain risk capability, organizational & business resilience and commitment to excellence. Leaders invited to speak at conferences about their success.
2. Risk Strategy & Policies – Is there a clear risk strategy and risk policies?				
The need for a risk strategy and related risk policies has been identified and accepted.	A risk management strategy and polices have been drawn up and communicated and are being acted upon.	Risk strategies and policies are communicated effectively and made to work through a framework of processes.	A separate risk strategy and policies not necessary. Risk handling is an inherent feature of all policies and strategy making processes.	Risk management capability in strategy and policymaking helps to drive the risk agenda and is reviewed and improved. Role model status.
3. People – Are people equipped and supported to manage risk well?				
Key people are aware of the need to assess and manage risks and they understand risk concepts and principles.	Suitable guidance is available and a training program has been implemented to develop risk capability.	A core group of people have the skills and knowledge to manage risk effectively.	People are encouraged and supported to be more innovative. Regular training is available for people to enhance their risk skills.	All staff are empowered to be responsible for risk management and see it as an integrated part of the Departments business. They have a good record of innovation and well managed risk taking.
4. Partnerships – Are there effective arrangements for managing risks with partners?				
Key people are aware of areas of potential risk with partnerships and understand the need to agree approaches to manage these risks.	Approaches for addressing risk with partners have been developed and implemented.	Risk with partners is managed consistently for all key areas and across organizational boundaries.	Sound governance arrangements established, partners and suppliers selected on basis of risk capability and compatibility.	Excellent arrangements in place to identify and manage risks with all partners and to monitor and improve performance. Organization regarded as a role model.

Corporate Business Risk Planning

Level 1 Awareness & Understanding	Level 2 Implementation Planned & in Progress	Level 3 Implemented in Key Areas	Level 4 Embedded and Improving	Level 5 Excellent Capability Established
5. Processes – Do the organization's processes incorporate effective risk management?				
Some stand-alone risk processes have been identified.	Recommend risk management processes are being developed.	Risk management processes implemented in key areas. Risk capability self assessment tools used in some areas.	Risk metrics are collected. Risk management standards applied in some areas.	Management of risk and uncertainty is well integrated with all business processes. Best practice approaches are used and developed. Selected as a benchmark site by other organizations.
6. Risk Handling – Are risks handled well?				
No clear evidence that risk management is being effective.	Limited evidence that risk management is being effective in at least most relevant areas.	Clear evidence that risk management is being effective in all relevant areas.	Very clear evidence that risk management is being very effective in all areas and leading to the production of very good results.	Very clear evidence of excellent results due to risk management being highly effective in all areas and that improvement is being pursued.
7. Outcomes – Does risk management contribute to achieving outcomes?				
No clear evidence of improved outcomes	Limited evidence of improved outcome performance consistent with improved risk management.	Clear evidence of significant improvements in outcome performance demonstrated by measures including, where relevant, stakeholders' perceptions.	Very clear evidence of very significantly improved delivery of all relevant outcomes and showing positive sustained improvement.	Excellent evidence of markedly improved delivery of outcomes which compares favourably with other organizations employing best practice.

Corporate Business Risk Planning

Risk Areas and Examples of Risk Events

Return to Risk Identification

Events (conditions or circumstances) that could lead to risks that could positively or negatively impact the achievement of business objectives.

1. **External Environment** (events originating outside the organization)

• Decisions made by all levels of government • Public reaction or confidence • Demographic changes • Social factors	• Environmental damage • Economic factors • Natural Disasters • Terrorism/vandalism

2. **Legal/compliance** (events related to compliance and legal agreements)

• Legislation • Regulatory changes • Health and Safety laws • Environmental laws • By-laws	• Administrative directives • Policies • Contracts (documented and enforceable) • Publicity from legal action

3. **Culture** (intangible events that shape the way business is conducted)

• Leadership or management philosophy • Stewardship, fiduciary or policy responsibilities • Tone at the top • Governance • Level of trust • Lines of authority • Communications • Ethics and values	• Decision model • Integration across organization • Change management practices • Ability to apply learning and redirect energies • Monitoring/performance measures • Adaptability to change • Activities affecting public perception

4. **Operations** (events related to business processes)

• Assumptions/methodologies • Quality of planning • Process/service quality • Process/service efficiency • Business continuity • Fraud (employee, customer, vendor) • Security of assets	• Policies and procedures • Reliance on third party • Operational capacity • Internal controls • Customer Needs (Ease of doing business, customer expectations)

5. **Financial Resources** (events related to the financial heath of the organization)

• Return on investment • Asset valuation • Protection from loss • Sources of revenue • Alternate funding mechanisms (new taxes, fees, charges)	• Ability to meet financial obligations • Capital funding • Operational funding • Material price fluctuations • Pricing or market positioning • Level and type of insurance

6. **Physical Assets** (events relate to tangible assets)

• Suitability • Breakdown • Level of maintenance	• Misuse • Obsolescence • Theft

7. **Human Resource** (events related to staffing)

• Training and development programs • Changing resource needs • Authority, accountability and responsibility • Staffing levels • Staff competencies	• Recruitment/retention decisions • Performance incentives & compensation • Staff turnover • Job action • Succession planning

8. **Information Resources** (events related to the storage and use of information)

• Availability (information/communication/ computer systems) • Infrastructure (capacity and ability to support business initiatives) • Freedom of Information and Privacy Legislation (FOIP)	• Security • Information quality (relevance, integrity) • Integration/coordination • Performance information

Corporate Business Risk Planning

Example of Potential Sources of Risk

	Strategic Perspective	Business Line Perspective	Corporate Management Perspective	Compliance Perspective	Government Agenda Perspective
Description of Views or Perspective	*Sources that can impede the achievement of mandate and objectives*	*Sources that can impede the achievement of business line or program objectives*	*Sources that may not effectively support the achievement of results*	*Sources that could embarrass the organization or cause liabilities for not complying with laws and regulations*	*Sources that are critical to ensure alignment with government-wide commitments*
Sources of Risk	***Strategic***	***Business Line***	***Corporate Management***	***Compliance***	***Government Agenda***
	➢ policy and strategy ➢ corporate reputation ➢ political factors ➢ public expectations ➢ stakeholder relations ➢ media relations ➢ industry developments ➢ changing demographics ➢ globalization ➢ national security threats ➢ business continuity ➢ emergency preparedness ➢ technology trends ➢ economic trends ➢ competitive trends	➢ business line activities ➢ program activities ➢ program delivery ➢ client services ➢ service delivery ➢ alliances, partnerships ➢ major projects	➢ structure and reporting relationships ➢ planning & priority setting ➢ budgeting and resource allocation ➢ expenditure mgmt. ➢ revenue/ cost recovery ➢ transfer payments ➢ procurement and contracting ➢ financial management ➢ performance mgmt. ➢ project management ➢ change management ➢ inventory management ➢ asset management ➢ human resources ➢ information and knowledge ➢ information technology ➢ communications ➢ risk management	➢ funding and appropriations ➢ statutory reporting ➢ compliance with laws and regulations ➢ compliance with central agency policies ➢ agreements and contractual obligations ➢ workplace health and safety ➢ environmental protection ➢ security, privacy and confidentiality ➢ legal liabilities and litigation	➢ citizen focus ➢ values and ethics ➢ accountability ➢ transparency ➢ responsible spending ➢ client satisfaction ➢ Government On-Line ➢ improved reporting ➢ modern comptrollership ➢ fairness and equity ➢ Results for Canadians ➢ modern HRM ➢ integrated risk management

Corporate Business Risk Planning

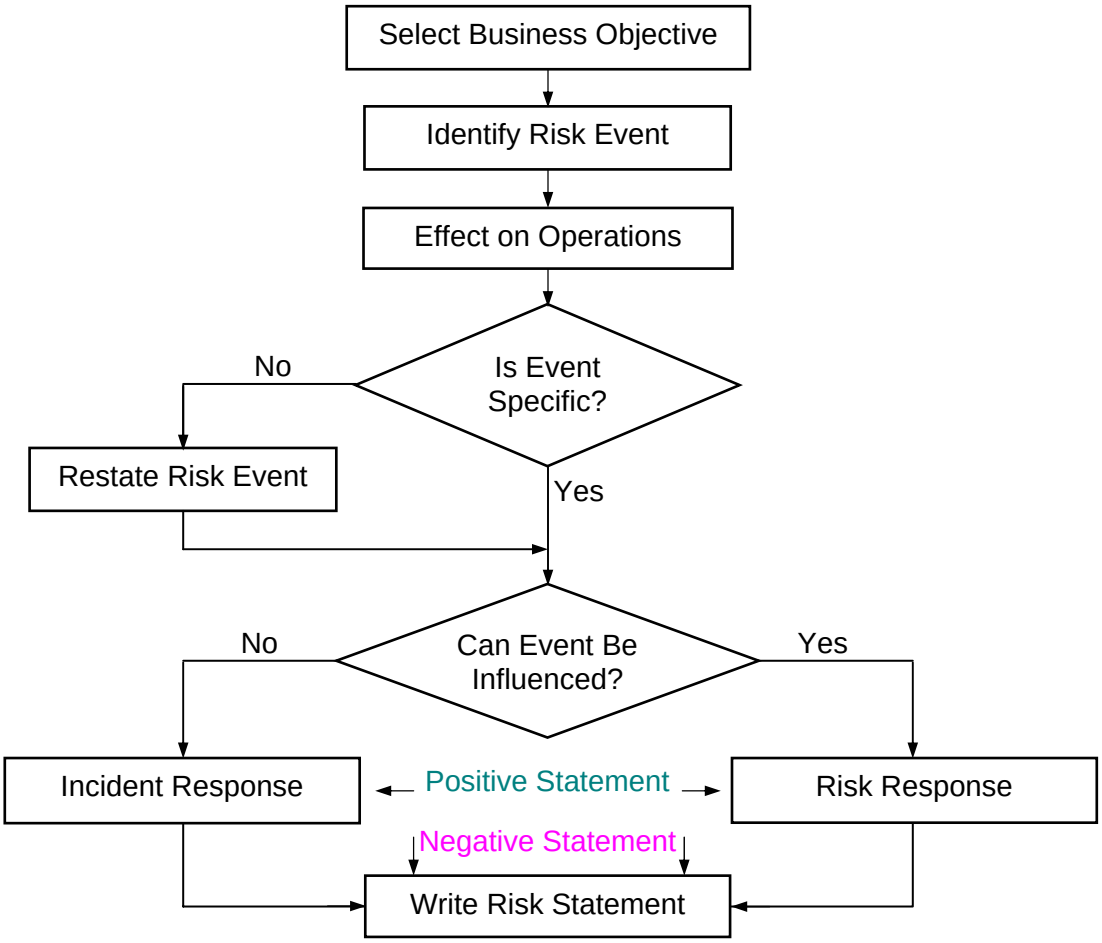
Sample Risk Questionnaire

- In terms of your business environment, what do you perceive as risks facing your business area?
- What risks exists that might lead to reduced efficiency or effectiveness in your business area?
- What legal risks does this business unit face?
- What risks do you see to the quality of services you provide?
- Describe events or risks that could lead to the interruption of your business?
- What are the impacts of a information systems interruption?
- What is the potential for fraud or misrepresentation with your business unit?
- What risks exist to the people within your operations?
- What risks does this business unit face in regards to reliance on third party work?
- What risks exist in relation to operational capacity and the inability to meet demand for services?
- What risk exists in relation to misuse of physical assets that the corporation owns?
- What risks exist in relation to human resourcing within your business unit?
- What risks exist in technological changes for this business unit?
- What departmental or corporate level risks exist that directly or indirectly impact your business unit?
- How do changes in other levels of government affect risk to this business unit?

Corporate Business Risk Planning

Developing a Risk Statement

Return to Risk Identification



Corporate Business Risk Planning
Risk Profile Form

Return to Risk Identification

Return to Risk Assessment

Corporate Business Risk Planning
Risk Profile

Business Area		**Risk ID**	
Business Objective:			
Risk Area:		**Risk Event**:	
Risk Statement:			

Prepared by: _____ **Date**: _____

Inherent Risk
Impact/Concerns:

Inherent Risk Score

Impact	Negligible - 1	Marginal - 5	Moderate - 10	Substantial - 50	Severe - 100	Disastrous - 1000
Likelihood	Extremely Unlikely - 1	Very Unlikely - 2	Unlikely - 5	Somewhat Likely - 10	Likely - 15	Highly Likely - 20

Business Area Impact	**Corporate Impact**	**Citizen Impact**	**Total Impact**	**Likelihood**	**Total Risk Score**
+	**+**	**=**	**X**	**=**	

(See page 2 for Residual Risk)

Corporate Business Risk Planning
Risk Profile

(See page 1 for Inherent Risk)

Residual Risk

Existing Mitigating Measures:

Step 1 – Quantitative Assessment of Residual Risk

Business Area Impact	Corporate Impact	Citizen Impact	Total Impact	Likelihood	Total Risk Score
Inherent Risk Score					

Impact	Negligible - 1	Marginal - 5	Moderate - 10	Substantial - 50	Severe - 100	Disastrous - 1000
Likelihood	Extremely Unlikely - 1	Very Unlikely - 2	Unlikely - 5	Somewhat Likely - 10	Likely - 15	Highly Likely - 20

+ + = x =

Response Category	NEGLIGIBLE less than 10	ACCEPTABLE 10 – 49	MARGINALLY ACCEPTABLE 50 – 499	UNDESIRABLE 500 – 1999	INTOLERABLE over 1999

Response Category	

Step 2 – Subjective Assessment	
Step 3 – Validation & Approval	

Action Plan to Reduce Risk

Corporate Business Risk Planning

Summary by Higher Rated Risks

Return to Risk Identification

EXAMPLE – FOR ILLUSTRATIVE PURPOSES ONLY

Emergency Response Department					
Branch	**Corporate Objective**	**Business Objective**	**Risk Area**	**Risk Event**	**Risk Statement**
Emergency Planning	Leadership	Coordination of the response to a disaster	Natural Event	Tornado Hit	Inability to effectively coordinate the City's first response to damage and injury caused by a tornado.
Emergency Medical Service	Service to People	Preserve life and alleviate suffering	Natural Event	Tornado Hit	Inability to respond in a timely manner to a tornado resulting in unnecessary suffering.
Fire Rescue	Service to People	Contain fires and rescue victims trapped in structures	Natural Event	Tornado Hit	Fire Rescue is not prepared for multiple responses to a major incident such as a tornado.

Corporate Business Risk Planning

Risk Criteria and Tolerances

Return to Risk Assessment

Business Area Perspective

Impact Level	Service Delivery	Employee Safety	Infrastructure Capacity
Unacceptable (1000)	Long-term disruption or removal of citywide services.	Multiple employee deaths in one incident with potential for more deaths and injuries.	More than 30% of current demands cannot be serviced with existing and approved planned infrastructure.
Severe (100)	Short-term disruption or removal of citywide services.	Multiple employee deaths and/or life threatening injuries in one incident.	Between 20% and 30% of current demands cannot be serviced with existing and approved planned infrastructure.
Substantial (50)	Long-term disruption or removal of services to a large segment of the City.	Single employee death or multiple serious injuries to employees resulting in permanent disabilities.	Between 10% and 20% of current demands and projected short-term growth cannot be serviced with existing and approved planned infrastructure.
Moderate (10)	Short-term disruption or removal of services to a large segment of the City.	Multiple serious injuries resulting in temporary disability.	Up to 10% of current demands cannot be serviced with existing and approved planned infrastructure.
Marginal (5)	Long-term disruption or removal of services to a neighbourhood.	Single serious injury to an employee resulting in permanent disability or multiple minor injuries requiring attention or report.	Projected long-term growth cannot be serviced with existing and approved planned infrastructure.
Negligible (1)	Short-term disruption or removal of services to a neighbourhood.	Minor injury requiring attention or report.	Projected short-term growth cannot be serviced with existing and approved planned infrastructure.
No Impact (0)	Business area objectives are not at risk		

Corporate Business Risk Planning

Risk Criteria and Tolerances

Corporate Perspective

Impact Level	Financial	Environment	Economic	Legislated/Legal
Unacceptable (1000)	Annual tax levy impact in excess of $50 million. or Infrastructure failure/damage in excess of $500 million.	Long-term environmental impact (decades) with indefinite time for remediation, or the extent of damage is widespread and covers a large area.	The loss of a significant level of business activity for a long period of time with out-migration to surrounding areas.	Multiple major violations of legislation with significant penalties. or Multiple claims against the City totaling in excess of $50 million that are not covered by insurance.
Severe (100)	Annual tax levy impact between $30 million and $50 million. or Infrastructure failure/damage between $100 million and $500 million.	Long-term environmental impact (years) with long time for remediation and extent of damage is significant but not large, or short time for remediation and extend of damage is large.	The loss of a significant level of business activity for a short period of time with out-migration to surrounding areas.	A major violation of legislation with significant penalties. or Multiple claims against the City totaling between $30 million and $50 million that are not covered by insurance.
Substantial (50)	Annual tax levy impact between $15 million and $30 million. or Infrastructure failure/damage between $30 million and $100 million.	Long-term environmental impact (months) with long-time for remediation and extent of damage is significant but not large, or short time for remediation and extent of damage is large.	The loss of a moderate level of business activity for a long period of time and out-migration to surrounding areas.	Multiple violations of legislation with minor penalties. or Multiple claims against the City totaling between $15 million and $30 million that are not covered by insurance.

Corporate Business Risk Planning

Corporate Perspective

Impact Level	Financial	Environment	Economic	Legislated/Legal
Moderate (10)	Annual tax levy impact between $10 million and $15 million. or Infrastructure failure/damage between $10 million and $30 million.	Short-term environmental impact (weeks) with short time for remediation and the extent of the damage is small.	The loss of a moderate level of business activity for a short period of time with out-migration to surrounding areas.	A violation of legislation with minor penalties. or Multiple claims against the City totaling between $10 million and $15 million that are not covered by insurance.
Marginal (5)	Annual tax levy impact between $5 million and $10 million. or Infrastructure failure/damage between $5 million and $10 million.	Short-term environmental impact (days) with short time for remediation and the extent of the damage is limited.	The loss of a small level of business activity for a long period of time.	Multiple infractions of legislation with no penalties. or Multiple claims against the City totaling between $5 million and $10 million that are not covered by insurance.
Negligible (1)	Annual tax levy impact less than $5 million. or Infrastructure failure/damage less than $5 million.	Limited environmental impact (hours) with minimum time for remediation and the extent of damage is minimum.	The loss of a small level of business activity for a short period of time.	An infraction of legislation with no penalties. or Multiple claims against the City that are less than $5 million.
No Impact (0)	Corporate objectives are not at risk			

Corporate Business Risk Planning

Risk Criteria and Tolerances

Citizen Perspective

Impact Level	Citizen Feedback	Media Coverage	Public Safety
Unacceptable (1000)	High volume of calls to Citizen Action Centre and City Council offices for an extended period of time. or Large public rallies/protests directed against the City for an extended period of time. or Substantial negative feedback on surveys indicating loss of confidence in the corporation.	Significant amount of negative media coverage for an extended period of time.	Multiple deaths in one incident with potential for more deaths and injuries.
Severe (100)	High volume of calls to Citizen Action Centre and City Council offices for short period of time. or Large public rallies/protests directed against the City for short period of time. or Substantial negative feedback on surveys indicating dissatisfaction with service delivery.	Significant amount of negative media coverage for short period of time.	Multiple deaths and/or life threatening injuries in one incident.
Substantial (50)	Moderate volume of calls to Citizen Action Centre and City Council offices for an extended period of time. or Moderate public rallies/protests directed against the City for an extended period of time. or Moderate negative feedback on surveys indicating dissatisfaction with the administration of the corporation.	Moderate amount of negative media coverage for an extended period of time.	Multiple serious injuries resulting in permanent disability.

Corporate Business Risk Planning

Citizen Perspective

Impact Level	Citizen Feedback	Media Coverage	Public Safety
Moderate (10)	Moderate volume of calls to Citizen Action Centre and City Council offices for a short period of time. or Moderate public rallies/protests directed against the City for a short period of time. or Moderate negative feedback on surveys indicating dissatisfaction with service delivery.	Moderate amount of negative media coverage for an short period of time.	Single death or multiple serious injuries resulting in temporary disability.
Marginal (5)	Small volume of calls to Citizen Action Centre and City Council offices for an extended period of time. or Small public rallies/protests directed against the City for an extended period of time. or Low level of negative feedback on surveys indicating dissatisfaction with the administration of the corporation.	Small amount of negative media coverage for an extended period of time.	Single serious injury resulting in permanent disability or multiple minor injuries requiring attention or report.
Negligible (1)	Small volume of calls to Citizen Action Centre and City Council offices for a short period of time. or Small public rallies/protests directed against the City for a short period of time. or Low level of negative feedback on surveys indicating dissatisfaction with service delivery.	Small amount of negative media coverage for a short period of time.	Minor injury requiring attention or report.
No Impact (0)	Customer objectives are not at risk		

Corporate Business Risk Planning

Prioritized List of Risks - Quantitative

Return to Risk Assessment

EXAMPLE – FOR ILLUSTRATIVE PURPOSES ONLY

Risk Area	Natural Event	**Risk Event**	Tornado Hit

Dept./ Branch	**Corporate Objective**	**Risk Statement**	**Business Area Impact**		**Corporate Impact**		**Customer Impact**		**Total Impact**		**Likelihood**		**Total Risk Score**
ERD/Fire Rescue	Service to People	Fire Rescue is not prepared for multiple responses to a major incident such as a tornado.	5	+	0	+	10	=	15	x	15	=	225
ERD/ Emergency Medical Service	Service to People	Inability to respond in a timely manner to a tornado resulting in unnecessary suffering.	10		1		5		16		5		80
Corp. Serv./Risk Management	Leadership	The insurance needs of the corporation do not address the damage and/or claims resulting from a tornado.	0		10		5		15		5		75
ERD/ Emergency Planning	Leadership	Inability to effectively coordinate the City's first response to damage and injury caused by a tornado.	5		1		1		7		10		70
Comm. Serv./ Parkland Services	Infrastructure and Physical Environment	Funding is not available to restore parkland to a usable state after being hit by a tornado.	1		1		1		3		20		60
T&S/Traffic Operations	Service to People	Alternate safe traffic routes are not identified resulting in significant delays in traffic movement.	1		0		10		11		2		22

Corporate Business Risk Planning

Prioritized List of Risks Subjective and Quantitative Assessment

Return to Risk Assessment

EXAMPLE – FOR ILLUSTRATIVE PURPOSES ONLY

			Quantitative Assessment		Subjective Assessment by BRPT			
Ranking	**Priority**	**Risk Statement**	**Total Risk Score**	**Category**	**Member #1**	**Member #2**	**Member #3**	**Average Score**
1	High	Risk Statement 1	2800	Intolerable	3	3	3	3.00
2	High	Risk Statement 2	2700	Intolerable	3	2	3	2.67
3	High	Risk Statement 3	1800	Undesirable	3	3	2	2.67
4	Medium	Risk Statement 4	2400	Intolerable	2	3	2	2.33
5	Medium	Risk Statement 5	1680	Undesirable	2	2	3	2.33
6	Medium	Risk Statement 6	2100	Intolerable	2	2	2	2.00
7	Medium	Risk Statement 7	1560	Undesirable	2	2	2	2.00
8	Medium	Risk Statement 8	1290	Undesirable	1	2	2	1.67
9	Medium	Risk Statement 9	1080	Undesirable	2	1	2	1.67
10	Low	Risk Statement 10	900	Undesirable	2	1	1	1.33
11	Low	Risk Statement 11	780	Undesirable	1	2	1	1.33
12	Low	Risk Statement 12	600	Undesirable	1	1	1	1.00