Risk Management Policy

1. Introduction

The Safety Codes Council (Council) recognizes that **risk** occurs in all aspects of the operation and the delivery of programs and services that support the safety codes system in Alberta. The Council has established a formal **risk management** approach in order to proactively identify, assess, respond to, monitor, control, and report **risks**.

2. Purpose

The purpose of this policy is to provide guidance for the management of **risk** to create and protect value, improve performance, encourage innovations, and support the achievement of goals.

3. Definitions

employee: means a person engaged by the Council to perform a service in accordance with an employment agreement.

risk: means the effect of uncertainty on objectives. An effect is a deviation from the expected, either positive or negative.

risk management: means coordinated activities to direct and control the Council regarding **risk** to create and protect value, improve performance, encourage innovation, and support achievement of goals.

risk register: means a document that identifies **risks** and contains the results of **risk** analysis and **risk** response planning.

4. Policy

4.1. The Council will establish processes to understand and manage **risk**.

4.2. The Council recognizes that **risk** is inherent in all aspects of its operation, including inaction on the part of the Council where action may be required.

4.3. The Council will encourage a culture of **risk** awareness by ensuring that all **employees** are provided with **risk** awareness and identification training in order to support the identification of **risks** affecting the Council.

4.4. Council **employees** will identify and manage **risk** in order to create and protect value, improve performance, encourage innovation, and support the achievement of goals.

4.5. The Council will establish a **risk register** and provide a quarterly report on significant **risks** to the Board of Directors (Board).

4.6. Serious **risk** issues will be immediately escalated by the President and Chief Executive Officer (CEO) to the Board through the Board Chair.

4.7. The **risk management** framework and process utilized by the Council to manage **risk** are set out in Attachment A.

5. Authority

This policy is established under the authority of Corporate Governance Policy 1.4 which delegates authority to the President and CEO to establish policies and procedures for the management and operation of the Council regarding appeals, corporate operations, and operating programs, and Policy 1.10 which directs the President and CEO to establish **risk management** systems and processes to manage all Council **risks**.

6. Scope

The policy applies to all Council **employees**.

7. Related Policies and Procedures

- 1.10 Risk Oversight Policy

8. Version History

Date	Notes
December / 01 / 2019	New policy

Attachment A

Safety Codes Council

Enterprise Risk Management Framework

December 01, 2019

Version 1.0

Prepared in Collaboration with MNP

Contents

1. Introduction

Established by the Government of Alberta in 1993, the Safety Codes Council ("the Council") is responsible to the Minister of Municipal Affairs to administer portions of the safety codes system including:

- Accrediting the municipalities, corporations, and agencies that issue permits and inspect the work carried out under these permits
- Certifying and training safety codes officers who do the inspections
- Administering the Alberta Master Electrician Program
- Working with industry through its sub-councils to recommend codes and standards.

The Board of Directors ("Board") and Executive Committee ("EC") recognize that risk management is an important part of the Council's annual business planning and long-term strategic planning process. The Council defines risk as the effect of uncertainty on objectives. All risks with the potential to significantly impact the Council or the achievement of the strategic plan are considered enterprise risks. The purpose of this document is to outline the Program for identifying and managing the enterprise risks, although the approach and tools may also be applied to assess risks related to any plans, programs, services, divisions, or new initiatives.

2. The Risk Management Framework

The Council's Enterprise Risk Management ("ERM") Framework and overall ERM Program are based upon the International Organization for Standardization ("ISO") 31000:2018 Risk Management – Principles and Guidelines and the supporting Guide 73 Risk Management – Vocabulary (collectively referred to as "the Standard"). ERM is the coordination of activities to direct the Council and control risk thereby creating and protecting value, improving performance, encouraging innovation, and supporting the achievement of goals. ERM is more than an exercise in risk avoidance and helps to identify priorities. It is as much about identifying opportunities as avoiding or mitigating losses.

An effective ERM Program provides the following benefits:

- Greater confidence in achieving planned strategic or operational goals by applying risk management processes to identify and manage risks relative to the respective goals at all levels of the Council.
- Enhanced corporate governance and accountability by ensuring significant barriers, challenges, risks, and opportunities associated with policies, plans, programs, services, and operations are identified, evaluated, and managed while clearly identifying individuals accountable for the ongoing management of these risks. This information is used to provide the basis for ongoing decision making.
- Improved transparency in decision making by applying formal processes to identify, manage and communicate risks related to the achievement of the Council's goals, along with strategies to manage these risks.
- Formal integration of operational risk management programs across divisions (e.g. information technology, finance, operations, etc.), as well as integration with strategic risk management program for enterprise risks.
- Optimized resource allocation such that risks are prioritized, and resources are allocated to manage the risks based on this prioritization.
- A consistent approach to risk management, such that the Council is using common tools, language, and processes to evaluate and manage risks, as well as developing a common understanding of its risk appetite.

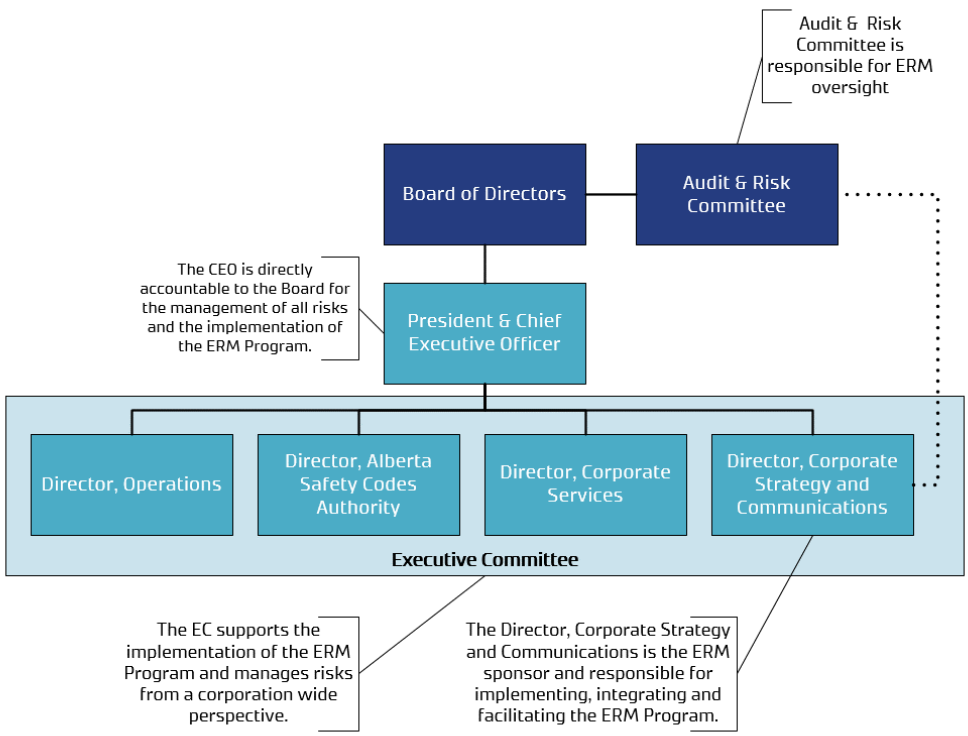
- Strategic issue resolution at its root cause, as opposed to applying tactical solutions that only address the symptoms of the problem.
- Recognizing synergies and interdependencies between risks, business decisions and their financial implications.
- Remaining highly adaptable and responsive.

Appendix A highlights some key definitions which will help in providing a better understanding of the terms used throughout this ERM Framework.

3. Roles and Responsibilities

The ERM oversight responsibility lies with the Board, which has delegated this responsibility to the Audit & Risk Committee. Ultimately, the President and Chief Executive Officer ("CEO") owns all risks and is responsible for the effective management of risk for the Council as a whole. The Director, Corporate Strategy and Communications is tasked with driving ERM implementation, including the integration and coordination thereof, and EC is responsible for managing the risks.

Figure 1: ERM Governance Structure



Every employee of the Council is impacted in some way, by risks, so every employee has an active role in being aware of risk and taking part in the risk management process. This involves understanding and applying the ERM Framework as well as identifying, analyzing, and managing risks.

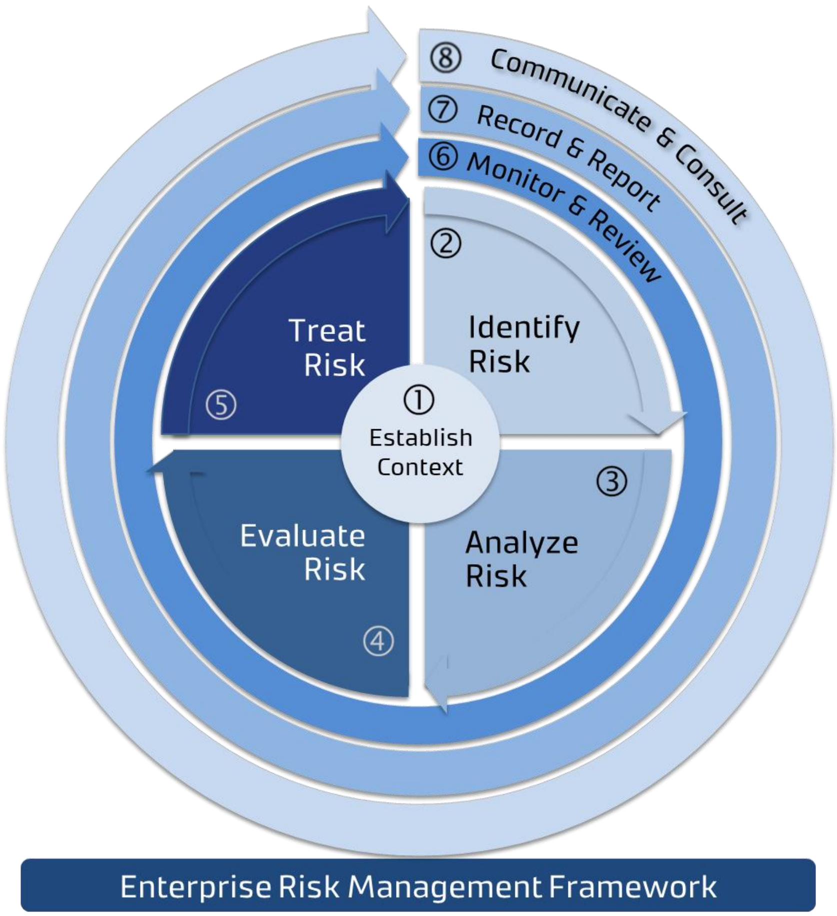
Every employee within the Council has responsibility for day-to-day management of risks, with some having more responsibilities than others. The detailed ERM roles and responsibilities are outlined in **Appendix B**.

4. The Risk Management Process

This ERM Framework has been developed to direct the risk management process for the Council, which is the identification and assessment of risks that may prevent the Council from achieving its strategic goals. The risk management process described herein is a structured approach to be integrated into broader management practices of the Council.

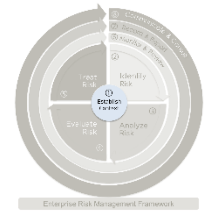
The typical process shown below and contained within this Framework is extracted from the Standard and can be applied to strategic goals, divisions, projects, or activities.

Figure 2: ERM Process



The sections below provide more detail on the steps outlined in **Figure 2.**

Step 1 – Establish the Context



Establish the context by identifying which part of the Council will be the focus of the risk assessment and subsequently, identify the objectives of the Council, plans, programs, services, divisions, or new initiatives. Consider the internal and external environment and parameters within which the risk must be managed.

The risk management process applies equally to risks that arise at an enterprise level, at an operational or day-to-day divisional level, or for new projects or activities. When embarking upon a risk assessment initiative, it is therefore important to have a clear understanding of the objectives / goals of the Council (or plans, programs, services, divisions, or new initiatives) for which the risk assessment is being completed. These objectives / goals should be clearly articulated and validated with the respective stakeholders prior to the initiation of the risk assessment initiative.

The Process:

i. Set the scope for the risk assessment by identifying which part of the Council is being assessed, whether it is an enterprise-wide risk assessment or an assessment of a plan, program, service, division, or new initiative.

ii. Identify all relevant stakeholders that are, or might be, impacted by the risk management process. Stakeholder input should be sought and will be required to validate objectives against which risk will be identified and assessed.

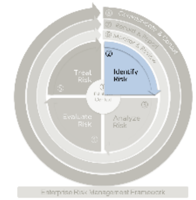
iii. Identify the goals against which risks (that may prevent the Council from achieving those goals) will be identified. It is important to have a clear understanding of the goals / objectives, such as strategic goals, division goals, project goals, etc. These goals should be clearly articulated and validated with the respective stakeholders.

iv. Gather relevant information to better understand the Council, plan, program, service, division, or new initiative for which a risk assessment is being conducted. Consider the following information:

- Strategic plans
- Business plans
- Organizational charts
- Annual reports
- Any other relevant information.

For the remainder of this document the steps will only reference strategic goals, but they remain applicable to the plan, program, service, division, or new initiative being assessed (should the Council choose to apply the risk management process at these levels).

Step 2 – Identify the Risks



Identify and describe the risks that might prevent the Council from achieving its strategic goals.

This step requires the identification of risks which arise not only from the external environment, but also from internal sources. While identifying risks, also consider the causes and sources of the risk as well as their potential consequences to the Council. It is important to consider the full range of risks, including those risks associated with not pursuing an opportunity. The risk universe (included in **Appendix C**) provides categories of risks to assist the Council in identifying those critical to the Council. This list is not meant to be exhaustive nor in exact alignment with how the Council conducts its business; rather, it is intended to be a thought starter in the identification process.

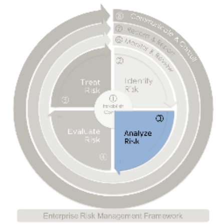
Risks may be identified through the following activities:

- Formal risk identification conducted annually (e.g. through a workshop, interviews, etc.) or as part of the strategic planning process.
- New, emerging, or changing risks identified and reported during the normal course of business.
- At any time by any individual within the Council using formal mechanisms (e.g. Code of Conduct and Ethics Policy) or informal mechanisms (e.g. regular meetings with a supervisor).

The Process:

i. Identify potential key risks for each strategic goal.
ii. Identify the source of the risks and specific context of the risk and consider the consequences to the Council.
iii. Document the risks (i.e. risk descriptions), risk categories, corresponding strategic goal(s) that is impacted, as well as the specific context of the risk, and potential impact to the Council using the strategic risk register (template provided in **Appendix D**).
iv. Risk owners responsible for managing the risk should be identified and included in the risk register.
v. Share the risk(s) as captured in the strategic risk register with EC and complete an initial validation with the EC.

Step 3 – Analyze the Risks



Analyze the likelihood and potential consequences of the risk to assist with the prioritization of risks and which risks are considered unacceptable or outside of risk appetite.

During this step, the levels of inherent and residual risk are determined by analyzing the likelihood (frequency or probability) and its consequence (magnitude of the impact), using the risk rating criteria, included in **Appendix E**.

Inherent risk is the risk before considering existing controls / mitigation strategies that are currently in place. Residual risk is the risk remaining after controls / mitigation strategies have been put in place to manage the inherent risk.

Likelihood and consequence should be viewed both in the absence of existing controls (inherent risk), as well as in the context of existing controls which may detect or prevent undesirable risks and events. This serves either to demonstrate the importance of existing controls/strategies and justify their continuation, or to identify those controls which are no longer necessary or cost-effective. This analysis also identifies the significance of the risk exposure should the existing controls/strategies fail.

To evaluate the level of residual risk, the Council must identify those existing controls that have been implemented to mitigate or manage the risk under consideration. It is important to ensure only existing (not planned) controls are identified to provide an accurate reflection of the Council's current risk exposure.

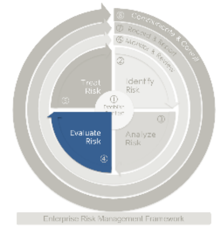
The Process:

i. Identify and document the existing controls already in place to manage risk.

ii. Assess the likelihood and consequence of the risks using the likelihood / consequence criteria included in the Risk Rating Tables in **Appendix E** as follows:
   - For each of the risks identified, rate each risk as to the likelihood of the risk occurring
   - For each of the risks identified, rate each risk as to the consequence should the risk occur
   - Complete the likelihood and consequence ratings first for inherent risks (without controls) and then repeat these steps considering current controls (residual risks)

iii. Document the likelihood and consequence ratings for both the inherent and residual risk assessments against each risk using the strategic risk register.

Step 4 – Evaluate the Risk



Using the likelihood and consequence ratings, determine the inherent and residual risk score and decide whether the risk is within the risk appetite of the Council.

To understand the relative priority of each risk, an overall inherent and residual risk score must be calculated and assessed against pre-established criteria (i.e. the Risk Matrix in **Appendix F**). The risk score is determined by multiplying the ratings for likelihood and consequence separately for inherent and then residual risk. Once the overall risk scores have been determined, the inherent and residual risk scores are compared against the Risk Matrix to determine the overall risk rating (i.e. extreme, high, moderate, or low).

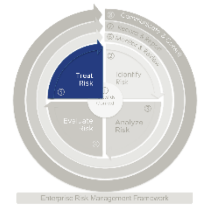
The Risk Matrix reflects the Council's risk appetite which is demonstrated by the coloring of each of the cells in the Matrix. Essentially, any high or extreme level risks (orange or red) are outside of the Council's risk appetite and require the selection of one or more risk treatment strategies and identification and development of a specific risk mitigation plan(s) on a timely basis. If the level of risk established is moderate or low (i.e. yellow or green risks, then the risk may be tolerable and additional risk management plans are not required).

At this point, the Council should also review and refine the risk scores to not only ensure they are appropriate, but to also ensure the prioritization of risks relative to one another aligns with EC expectations. Adjustments to risk scores should be made to more accurately reflect the prioritization of the risks. This final residual risk rating is then used in the following step (i.e. Risk Treatment) to determine the appropriate risk treatment strategy to manage the risk to an acceptable level.

The Process:

i. Calculate the overall risk score for both inherent and residual risk by multiplying the likelihood and consequence ratings determined in the previous step (i.e. Risk Analysis).
ii. Document the risk scores for both the inherent and residual risk assessments using the risk register in **Appendix D**.
iii. Share the risk analysis results as captured in the risk register and complete a validation of the risk assessments / prioritization and their relative risk ratings with EC.
iv. Adjust likelihood and consequence ratings, as well as the calculated risk scores as required.
v. Compare risks to risk appetite as included in the Risk Matrix (included in **Appendix F**) and identify which risks are in excess of risk appetite (as they will be subject to Step 5 - Treat the Risk).
vi. Document the risk appetite in the strategic risk register.

Step 5 – Treat the Risks



Determine how to treat the risks and develop risk mitigation plans.

As a result of completing the previous steps, risks have now been prioritized and risks outside of the Council's risk appetite have been determined. Management is now responsible for deciding how it will treat the risks that are in excess of its risk appetite. For risks with a residual rating that is within the Council's risk appetite, no further action is required. It is not the intent to minimize, avoid, or remove all risks that are identified; rather that the Council understands the significant risks (those outside of risk appetite) that could adversely impact the achievement strategic goals and, where appropriate, establish plans to address them. In addition, the Council should assess whether opportunities exist to exploit risks in support of achieving of its strategic objectives.

Various risk treatment strategies (or a combination thereof) are available for a given risk. Risk treatment strategies are not mutually exclusive (i.e. they can be combined) or appropriate in all circumstances. There are seven risk treatment strategies that can broadly be divided into the following four broad categories:

1. **Reducing the risks** – Modifying the risk through the following risk treatment strategies:
   - Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
   - Removing the risk source
   - Changing the likelihood
   - Changing the consequence
2. **Taking / increasing risk** – Modifying the risk to take on more risk; eliminate existing controls / mitigation strategies in pursuit of an opportunity
3. **Sharing the risk** – Limiting exposure to a risk by sharing the risk with another party or parties (e.g. through contracts, outsourcing, risk financing, insurance, etc.)
4. **Accepting the risk** – Retaining the risk by informed decision.

Selecting the most appropriate risk treatment strategy involves balancing the costs and efforts of implementation against the benefits derived, with regards to legal, regulatory, and other requirements such as social responsibility, stakeholder expectations, and the degree of control over each risk. More specifically, risk treatment decisions should consider the likelihood and consequence of the risk in determining the need for further treatment. For example, although a risk may have an extreme consequence, the potentially excessive cost of implementing a risk treatment strategy may not be justifiable given its low likelihood. Accordingly, the choice may be made to accept the risk, as opposed to taking further action to reduce or share it. In addition, the Council should also recognize that implementing a specific risk treatment strategy may reduce the likelihood or consequence of more than one risk, which may impact the cost-benefit analysis.

For all risk treatment strategies other than "accepting the risk", a risk mitigation plan should be developed to implement to the risk treatment strategy. Developing risk mitigation plans includes:

- Defining the specific risk mitigation action plans to support the implementation of the risk treatment strategy (i.e. what steps will be taken to mitigate the risk?)
- Assigning accountability to a risk mitigation plan owner
- Setting a timeline for implementation completion to facilitate tracking of progress.

The Process:

i. Select one or more risk treatment strategies to manage the risks in excess of risk appetite and ensure that the proposed benefit of the treatment strategy outweighs the costs to be incurred to implement the strategy. The risk treatment strategies should be documented in the strategic risk register.

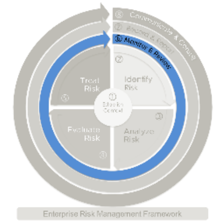
ii. The risk treatment strategies selected for each strategic risk should be validated with the EC.

iii. Develop and document the risk mitigation plan(s) in the risk register including the specific risk mitigation plan actions, accountability (mitigation owner), and timeline.

iv. Share the risk treatments and risk mitigation plans as captured in the strategic risk register and complete a final validation of the entire strategic risk register with EC.

v. Implement the risk mitigation plan(s).

Step 6 – Monitor and Review



Assess the effectiveness of the ERM Program through regular monitoring and review activities.

Once the ERM Program is implemented, it is important to monitor and review the effectiveness of the Council's ERM Program over a period of time. A well-crafted ERM Program is only as effective as the dedication of the Council's employees who adhere to the ERM principles and incorporate them into their daily decision-making processes. Monitoring and review mechanisms help to:

- Ensure the consistent application of the ERM Framework across the Council
- Ensure the effectiveness of the risk management process
- Identify weaknesses / enhancements within the ERM Program and develop corrective action plans.

Independent risk management evaluations are periodic reviews (typically every two to three years) of the effectiveness of the Council's ERM Program conducted by an independent party. Independent risk management evaluations provide the Council with an opportunity to gain an objective perspective of the effectiveness and maturity of the Council's ERM Program.

The Council should continually monitor risks and the effectiveness of the plans, strategies, processes, and management systems that have been established to manage risks and guide the implementation of risk treatment strategies. To assess the effectiveness of the ERM Program, the Council should consider annually whether risks are effectively identified and assessed and regularly monitored and reviewed thereby managing residual risk within the risk appetite of the Council. The Council should also ensure new and emerging risks are being considered and, where appropriate, integrated within the strategic risk register. Functions and processes change, as can the strategic goals of the Council. Accordingly, risks should be regularly re-examined to ensure the risks and the ways in which they are managed remain valid.

Ongoing monitoring and review are essential for managing risk and are the actions built into the normal operating activities of the Council and are performed by risk owners considering implications of information they receive. The presence of regular performance information or Key Risk Indicators ("KRIs") can assist in identifying likely trends, trouble spots and other changes which have arisen. The process of monitoring and review ensures that risk management strategies continue to be effective and a vital part of the Council business processes, while instilling a culture of continuous improvement.

The Process:

i. Develop KRIs for each risk to allow for the early identification of changes to the risk exposure of the Council. KRIs are developed considering the regular performance information of the Council.
ii. Once developed and agreed upon with EC, include the KRIs in the risk register and monitor them on a regular basis.
iii. Conduct regular independent risk management evaluations and implement recommendations for improvement.

Step 7 – Record and Report

Record and report on the risk management process and its outcomes.

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to:

- Communicate risk management activities and outcomes across the organization
- Provide information for decision-making
- Improve risk management activities
- Assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Factors to consider for reporting include:

- Differing stakeholders and their specific information needs, and requirements
- Cost, frequency, and timeliness of reporting
- Method of reporting
- Relevance of information to organizational objectives and decision-making.

Risk reporting is essential to ensure that key stakeholders are kept abreast of the significant risks and the actions resulting from risk management activities. In doing so, management and employees are better able to make informed decisions relative to risks and better support the achievement of the Council's objectives. The risk reporting requirements for the Council are outlined in **Appendix G**.

The Process

i. Develop and present risk reports as outlined in the reporting requirements (included in **Appendix G**).

Step 8 – Communicate and Consult

Pertinent information and effective communication are key components to successfully implement an ERM Program and necessary to increase the awareness of risks and risk management throughout the Council.

Effective communication and consultation are essential to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis upon which decisions are made and the reasons why particular risk treatment options are selected. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making. Close coordination between communication and consultation should facilitate factual, timely, relevant, accurate, and understandable exchange of risk-related information.

Continuous communication and consultation with internal and external stakeholders during all stages of the risk management process is pertinent, particularly when risk treatment strategies and risk management plans are first being developed and when significant decisions need to be made. Risk management is enhanced through effective communication and consultation when all parties understand each other’s perspectives and, where appropriate, are actively involved in decision making.

Communication and consultation aim to:

- Bring different areas of expertise together for each step of the risk management process
- Ensure different views are appropriately considered when defining risk criteria and when evaluating risks
- Provide sufficient information to facilitate risk oversight and decision-making
- Build a sense of inclusiveness and ownership among those affected by risk.

The Process:

i. Ongoing communication and support are provided from the CEO, Director, Corporate Strategy and Communications, and the EC across the Council as to the importance and benefits of risk management.

ii. Risk Management as a standing item on EC meeting agenda to review and discuss existing and emerging risks along with implementation progress of risk treatment strategies and risk mitigation plans.

iii. Develop and roll out risk management training to the Council employees. Also consider the need to deliver annual “refresher” training to employees reminding them of key risk management concepts / process and update them on the evolution of risk management within the Council.

Appendix A – Glossary

Consequence	Result or effect of a risk. The consequence can be certain or uncertain and can have positive or negative direct or indirect effects on the Council's goals.
Control	A measure that is modifying risk. Controls include any process, policy, device, practice, or actions which modify risk.
Cost Benefit Analysis	Cost benefit analysis is a systematic approach to estimating the strengths and weaknesses of alternatives that satisfy transactions, activities, or functional requirements for a business. In the context of ERM, it entails analyzing the costs involved in implementing additional risk management activities versus the additional benefit derived by implementing the risk management activities.
Divisions	The Council's group or functional units overseen by senior manager level staff.
Enterprise Risk Management	Coordinated activities to direct and control the Council regarding risk to create and protect value, improve performance, encourage innovation, and support achievement of goals.
ERM Framework	A set of components that provide the foundations and organizational arrangements for the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk throughout the Council.
ERM Program	ERM Program describes how the Council intends to manage risk. Typically, the Program includes the ERM Policy, ERM Framework, and processes. It describes the management components, the approach, and the resources that are be used to manage risk, including procedures, practices, responsibilities, and activities.
Governance	Processes by which an organization is directed, controlled, and held to account. It encompasses authority, accountability, stewardship, leadership, direction, and control exercised by the Council.
Inherent Risk	The risk to the Council in the absence of any actions taken to alter either the risk's frequency of occurrence and / or consequence.
Key Risk Indicator	A Key Risk Indicator, also known as a KRI, is an "early warning" indicator of a changing and emerging risks and should be aligned with the strategic priorities and key performance indicators ("KPIs") of the Council as set out in its strategic plan. In certain instances, a KRI can be the same as an existing KPI. KRIs help to identify potential risks that may impede the success of the Council and/or harm the continuity of operations.
Likelihood	The probability that the risk will occur within a fixed timeframe. Likelihood is usually expressed in terms of probability or frequency.
Residual Risk	The remaining risk after actions have been taken to alter the risk's frequency of occurrence and / or consequence.
Risk	Risk is the effect of uncertainty on objectives. An effect is a deviation from the expected, either positive or negative.
Risk Analysis	The process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment.
Risk Appetite	The amount and type of risk that the Council is willing to pursue or retain.
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Context	Risk context provides background information related to the risk to assist in understanding the nature, sources and causes of the risk.
Risk Evaluation	The process of comparing the results of risk analysis with risk criteria to determine whether the risk and / or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk treatment.
Risk Identification	The process of finding, recognizing, and describing risks. Risk identification involves the identification of risk sources, events, their causes, and their potential consequences.

Risk Management	See Enterprise Risk Management.
Risk Management Process	The systematic application of policies, procedures, and practices to the activities of communicating and consulting, establishing the context, and assessing, treating, monitoring, reviewing, recording, and reporting risk.
Risk Owner	The person with the accountability and authority to manage a risk.
Risk Tolerance	The level of variation around key performance indicators ("KPIs") and KRIs that the Council is willing to accept in the pursuit of strategic goals and the management of related specific risks. In defining risk tolerance, KPIs and KRIs should be in place for strategic goals and risks.
Risk Treatment Strategy	The process to modify risk. This involves the selection and implementation of appropriate options for dealing with risk, which may include: • Reduce the risk • Take / increase risk • Share the risk • Accept the risk
Stakeholders	Parties that are affected by the Council such as the Municipal, Provincial, or Federal government, employees, regulators, customers, suppliers etc.
Strategic Risk	Strategic risks are those risks that could prevent the Council from achieving its strategic objectives.
Turnover	**Turnover** is the act of replacing an employee with a new employee. Turnover rate is the percentage of employees in a workforce that leave during a certain period of time.

Appendix B – Roles and Responsibilities

Specific roles and responsibilities for each of the key roles identified in **Section 3 Roles and Responsibilities** are provided in the table below:

Stakeholder	Roles and Responsibilities
Board of Directors	***Role***: The Board provides oversight regarding ERM including direction, guidance, and monitoring. The Board may delegate the responsibilities outlined below to the Audit & Risk Committee. ***Responsibilities:*** • Provide risk management philosophy direction. • Provide leadership and guidance to the Council with respect to the ERM Program implementation and execution. • Promote high ethical and integrity standards and establish a culture within the Council that emphasizes to all levels of personnel the importance of risk management. • Develop and provide a strong environment to facilitate sound and prudent risk taking and risk managing activities. • Facilitate open communication between management and the Board with respect to risk. • Ensure integration of risk management into strategic objective setting, ongoing measurement processes and key decision-making points. • Review the Council's portfolio view of risks and consider it against its risk appetite. • Concur and approve risk appetite as determined by management.
Audit & Risk Committee	***Role***: The Audit & Risk Committee provides oversight of the ERM Program (when delegated to do so by the Board). ***Responsibilities***: • Provide leadership and guidance to the Council with respect to the ERM Program implementation and execution. • Promote high ethical and integrity standards and establish a culture within the Council that emphasizes to all levels of personnel the importance of risk management. • Facilitate open communication between management and the Board / Audit & Risk Committee with respect to risk. • Develop and provide a strong environment to facilitate sound and prudent risk taking and risk managing activities. • Provide guidance on risk appetite and recommend for approval by the Board. • Provide oversight of management's identification and mitigation of material risks. • Review the Council's portfolio view of risks and consider it against risk appetite. • The Audit & Risk Committee may delegate specific risks to a Board committee (e.g. a people risk to the Human Resources and Compensation Committee) for further analysis and oversight, as needed, to leverage the Committee's expertise. • Monitor the status of risk identification and risk management activities and ensures risk treatments strategies selected are in alignment with the Council's risk appetite. • Monitor and provide oversight of the effectiveness of the ERM Program. • May engage a third party or Internal Audit to assess the adequacy and effectiveness of the ERM Program.

Stakeholder	Roles and Responsibilities
President & Chief Executive Officer	***Role:*** The President and CEO is directly accountable to the Board for the management of all risks and the implementation of the ERM Program. The President and CEO may delegate the responsibilities outlined below: ***Responsibilities:*** • Promote high ethical and integrity standards and establish a culture within the Council that emphasizes to all levels of personnel the importance of risk management. • Approves the ERM Policy, including defining roles and responsibilities, and participate in setting goals for ERM implementation. • Oversee the implementation and maintenance of an effective ERM Program. • Oversee common risk management language that includes common measures around likelihood and consequence, and common risk categories. • Oversee and approve the processes, procedures, and tools for the communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk. • Promote an ERM competence throughout the Council, including facilitating development of technical ERM expertise. • Oversee and approve the development of risk appetite. • Review the portfolio view of risks and consider it against the Council's risk appetite. Ensure risk treatments strategies selected are in alignment with the Council's risk appetite.
Director, Corporate Strategy and Communications	***Role:*** The Director, Corporate Strategy and Communications is the ERM sponsor and responsible for implementing, integrating, and facilitating the ERM program. ***Responsibilities:*** • Provide leadership and guidance for the Council with respect to the ERM Program. • Establish and implement an ERM Policy, including defining roles and responsibilities and participate in setting goals for ERM implementation. • Establish a common risk management language that includes multiple measures around likelihood and consequence and agreed upon risk categories. • Establish the framework, processes, procedures and tools for the communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk. • Facilitate development of technical ERM expertise across EC and more general understanding of ERM for all employees. • Establish the Council's risk appetite and ensure that appropriate risk treatment strategies are selected. • Assist risk owners to develop appropriate risk mitigation plans to implement the selected risk treatment strategy. • Establish reporting requirements and risk management reports for various stakeholders. • Facilitate and report to the various stakeholders such as EC, the Audit, & Risk Committee, and the Board in line with established reporting requirements. • Ensure sufficient transparency of risk management practices through training, awareness programs, or communication. • Monitor effectiveness of the ERM Program and Framework. • Implement actions to address ERM Program deficiencies and enhancements.

Stakeholder	Roles and Responsibilities
	• Develop and provide a strong environment to facilitate sound and prudent risk taking and risk managing activities. • Promote high ethical and integrity standards and establishes a culture within the Council that emphasizes to all levels of personnel the importance of risk management. • Advocate and ensure the integration of risk management into strategy and goal setting, ongoing measurement processes, and key decision-making.
Executive Committee	***Role***: The EC supports the implementation of the ERM Program and manages risks from an enterprise-wide perspective. ***Responsibilities***: • Monitor status, effectiveness, and completeness of risk identification, assessment, treatments, and management activities. • Review the portfolio view of risks and consider it against the Council's risk appetite. Ensure risk treatments strategies selected are in alignment with the Council's risk appetite. • Develop and provide a strong environment to facilitate sound and prudent risk taking and risk managing activities. • Promote high ethical and integrity standards and establishes a culture within the Council that emphasizes to all levels of personnel the importance of risk management. • Advocate and ensure the integration of risk management into strategy and goal setting, ongoing measurement processes, and key decision-making.
Risk Owner	***Role:*** Responsible for the day-to-day management of the risks assigned to the risk owner. ***Responsibilities:*** • Implement the approved risk treatment strategy and develop appropriate risk mitigation plans to implement the selected risk treatment strategy in respect of the risk he/she is responsible for. • Execute risk management activities in accordance with the ERM Policy and Framework and the direction of their respective supervisors.
Safety Codes Council Employees	***Role:*** Responsible for the day-to-day management of the risks. ***Responsibilities:*** • Responsible for the day-to-day management of risks and, where appropriate, escalating significant risks to their respective supervisors for follow up. • Execute risk management activities in accordance with the ERM Policy and Framework and the direction of their respective supervisors.

Appendix C – Risk Universe

Internal Conditions

Strategy

- Governance
- Strategic Planning & Objectives
- Mandate
- Goal Alignment
- Organizational Performance Management
- Policies & Procedures
- Organizational Structure
- Reputation
- Collaboration & Coordination
- Value Proposition
- Transparency
- Alignment with Government
- Innovation

Culture

- Ethics, Values, & Diversity
- Social Responsibility
- Continuous Improvement
- Communication
- Change Management
- Accountabilities & Empowerment
- Cultural Alignment

Value Chain

Financial

- Cash Flow
- Funding
- Recording & Reporting
- Financial Reporting
- Internal Controls
- Investments
- Fraud & Corruption
- Capital
- Fiscal Sustainability & Prudence
- Insurance
- Budgets & Forecasts
- Management Reporting
- Liquidity
- Credit
- Interest Rates

Operations

- Staff Safety
- Security
- Process Efficiency & Effectiveness
- Operational Controls
- Business Continuity Planning
- Business Disruption
- Program / Service Delivery & Quality

Information Technology

- IT Strategy
- IT Infrastructure
- IT Integrity
- IT Capacity & Availability
- Data Reliability
- IT Security
- Access to Information
- Disaster Recovery Planning

Assets & Resource Management

- Capital Asset Planning and Management
- Asset Maintenance
- Intellectual Property
- Copy Rights

People

- Recruitment & Retention
- Training & Development
- Leadership
- Succession Planning
- Performance Management
- Compensation
- Knowledge Management
- Health & Wellness
- Employee Engagement

External Conditions

Stakeholders

- Federal, Provincial & Municipal Governments
- Industries
- Stakeholder Expectations
- Strategic Alliances

Compliance & Standards

- Regulations
- Legislation
- Contracts & Contract Management
- Litigation & Claims
- Taxation
- Privacy
- Policy Requirements

Appendix D – Risk Register Template

Included below is a sample summarized risk register template, which includes example risk information to illustrate the risk register template. The risk register is contained in a separate MS Excel document.

Risk Name	Risk Statement	Inherent Risk Score	Existing Controls	Residual Risk Score	Treatment Strategy
Recruitment & Retention	Risk that the Council is unable to recruit and retain sufficient, qualified staff.	20.0	• Performance management process is in place • Employee engagement survey conducted annually	9.0	Reduce

Appendix E – Risk Rating Tables

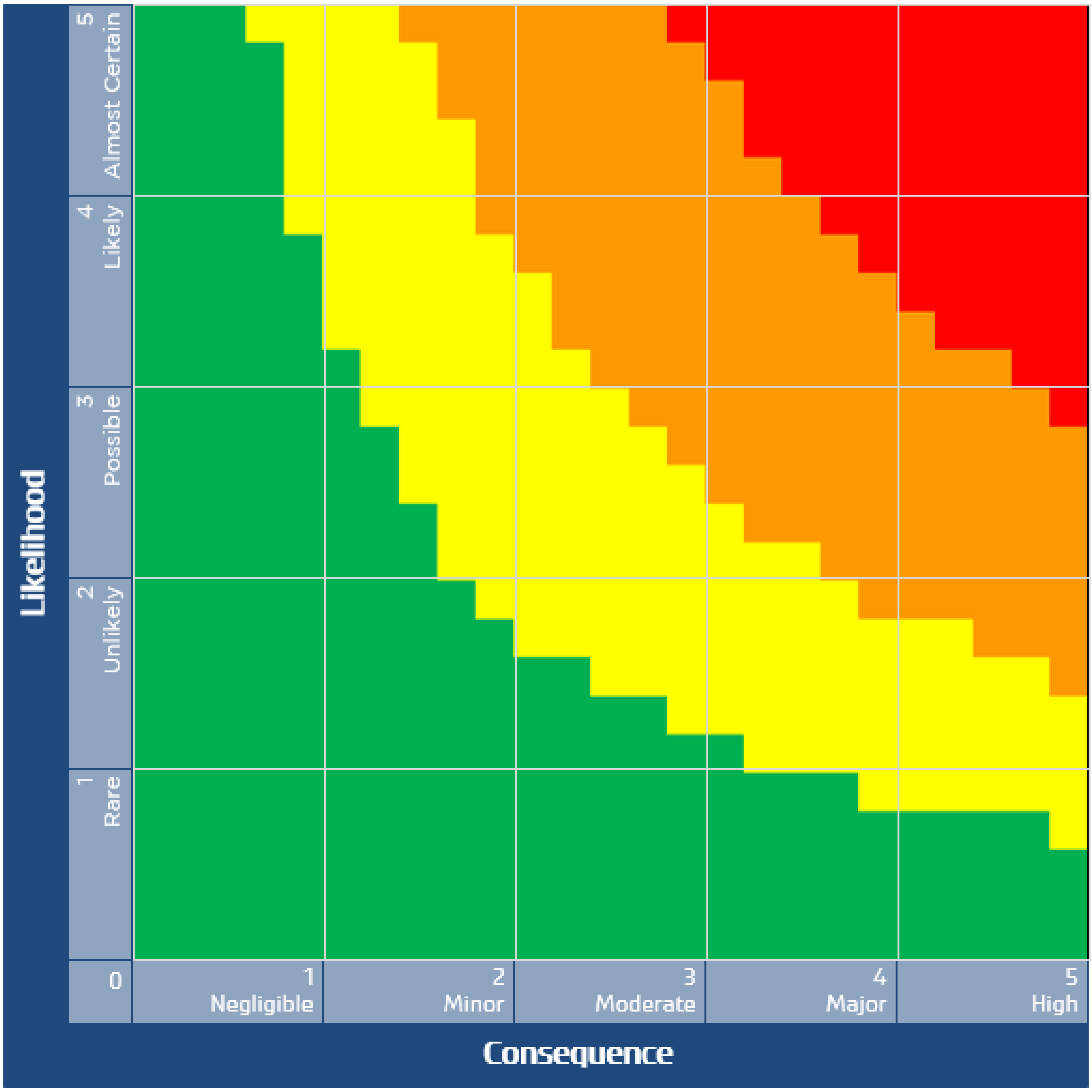
Likelihood Rating Table

Risk Management Likelihood Descriptors				
Risk Rating				
1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Event may occur in exceptional circumstances: • The event has not yet occurred in the past, but has occurred elsewhere, and is expected to occur once in a five-year period; or • Less than 10% chance of occurrence	Event could occur at some point in time: • The event has not yet occurred in the past, but is likely to occur once in a three-year period; or • 10% to 29% chance of occurrence	Event might occur at some point in time: • The event has occurred in the past and is likely to occur once in a two-year period; or • 30% to 59% chance of occurrence	Event is expected to occur in most circumstances: • The event has occurred in the past year and is likely to occur once in a one-year period; or • 60% to 89% chance of occurrence	Event is expected to occur frequently under most circumstances: • The event has occurred in the past and is likely to occur more than once in a one-year period; or • 90% or greater chance of occurrence

Consequence Rating Table

Risk Management Consequence Descriptors					
	Risk Rating				
	1 Negligible	2 Minor	3 Moderate	4 Major	5 High
Financial	• Financial impact or change in total budget of less than $25K.	• Financial impact or change in total budget between $25K and $74K.	• Financial impact or change in total budget between $75K and $150K.	• Financial impact or change in total budget between $151K and $250K.	• Financial impact or change in total budget of more than $250K.
Operations	• Delays in projects of up to one month. • Interruption to programs and services for up to one day. • Negligible interruption to non-critical technology and / or data and minor impact on normal operations for up to one day.	• Delays in projects of up to two months. • Interruption to programs and services for up to two days. • Interruption to non-critical technology and / or data and minor impact on normal operations for up to two days.	• Delays in projects of up to three months. • Interruption to programs and services for up to one week. • Intermittent loss of access to important data and intermittent effect on providing services for up to one week.	• Delays in projects of up to six months. • Interruption to programs and services for up to two weeks. • Prolonged loss access important data and inability to provide core services for up to two weeks.	• Delays in projects of more than six months. • Interruption to programs and services for more than two weeks. • Permanent loss of critical data and inability to provide core services for more than two weeks.
Regulatory	• Immaterial breach that does not attract regulatory attention. • No regulatory communication and no indicators of a more serious issue.	• Breach with minimal consequences that can be readily rectified. • The Council identified the potential or actual breach. Monitoring and correction is required by the Council.	• Breach with material consequences that can be readily rectified. • The Council receives regulatory communication or the Council initiates own plan to remediate with no fines or public notification.	• Breach with material consequences that cannot be readily rectified. • The Council is required by the regulator to develop action plans to remediate the breach, pay fines and / or regulator makes public notification.	• Breach with very significant consequences that cannot be readily be rectified. • The Council is required to immediately initiate action plans to remediate (likely to include board involvement and additional reporting to the regulator). The Council's viability is at risk.
Reputation	• Event has limited impact on the Council's reputation and stakeholder confidence. • No media attention.	• Modest impact on the Council's reputation and impact on stakeholder confidence fades over time. • Minor negative attention in local news / social media.	• Moderate impact on the Council's reputation and stakeholder confidence. • Moderate negative attention in local news / social media.	• Major impact on the Council's reputation and stakeholder confidence that is challenging to regain. • Limited negative attention in national and major attention in local news / social media.	• Serious, sustained, impact on the Council's reputation and stakeholder confidence. The Council's viability is at risk. • Intense negative attention in national and local news / social media.
People	• Staff turnover of less than 5% (annual rolling rate). • Position vacancy duration of less than a month. • Single preventable injury with no lost time.	• Staff turnover of between 5% and 10% (annual rolling rate). • Position vacancy duration of between one and three months. • Multiple preventable injuries with no lost time.	• Staff turnover of between 11% and 15% (annual rolling rate). • Position vacancy duration of between three and six months. • Multiple preventable short term disabling injuries.	• Staff turnover of between 16% and 25% (annual rolling rate). • Position vacancy duration of between six and nine months. • Single preventable long term disabling injuries.	• Staff turnover of more than 25% (annual rolling rate). • Position vacancy duration of more than nine months. • Single preventable fatality or multiple preventable long term disabling injuries.

Appendix F – Risk Matrix



Legend for Risk Matrix

Risk Rating			Risk Treatment Guidance
0 - 3	🟢	Low Risk	Manage by routine procedures.
4 - 7	🟡	Moderate Risk	Manage by specific monitoring procedures (monitoring required at least every 12 months).
8 - 14	🟠	High Risk	Management responsibility should be specified and appropriate risk treatment action taken and implemented within 12 months.
15 - 25	🔴	Extreme Risk	Immediate treatment action required, with SLT involvement, and implemented within six months.

Appendix G – Reporting Requirements

The table below outlines the reporting requirements, in terms of the type of information for each stakeholder, who delivers / presents the information, the frequency, and the forum for discussion.

Stakeholders	Type of Risk Management Information	Reporting Responsibility	Timing	Format of Report	Forum for Discussion
Board of Directors	Analysis of top 10 risks over a three to five-year period	CEO	Annually	Dashboard reporting	Board Meeting
	Summary of extreme and high risks, with key risk indicator analysis and trending.	CEO	Annually	Dashboard reporting	Board Meeting
	Review of risk register	CEO	Annually	Dashboard reporting	Board Meeting
Audit & Risk Committee	Analysis of top 10 risks over a three to five-year period	Director Corporate Strategy & Communications	Quarterly	Dashboard reporting	Audit & Risk Committee Meeting
	Summary of extreme and high risks, with key risk indicator analysis and trending.	Director Corporate Strategy & Communications	Quarterly	Dashboard reporting	Audit & Risk Committee Meeting
	Summary of extreme and high risks with updates on risk treatment implementation progress.	Director Corporate Strategy & Communications	Quarterly	Dashboard reporting	Audit & Risk Committee Meeting
	Summary of new risks	Director Corporate Strategy & Communications	Quarterly	Dashboard reporting	Audit & Risk Committee Meeting
EC	Analysis of top 10 risks over a three to five-year period	Director Corporate Strategy & Communications	Quarterly	Dashboard reporting	EC Meeting
	Summary of extreme and high risks, with KRI analysis and trending.	Director Corporate Strategy & Communications	Quarterly	Dashboard reporting and prioritized risk register	EC Meeting
	Summary of extreme and high risks with updates on risk treatment implementation progress.	Director Corporate Strategy & Communications	Quarterly	Dashboard reporting	EC Meeting
	Summary of new risks	Director Corporate Strategy & Communications	Quarterly	Dashboard reporting	EC Meeting

Safety Codes Council

Contact:

Erin Stroud
Director Corporate Strategy & Communications

Phone: 780.392.1366
Email: erin.stroud@safetycodes.ab.ca