BRITISH COLUMBIA

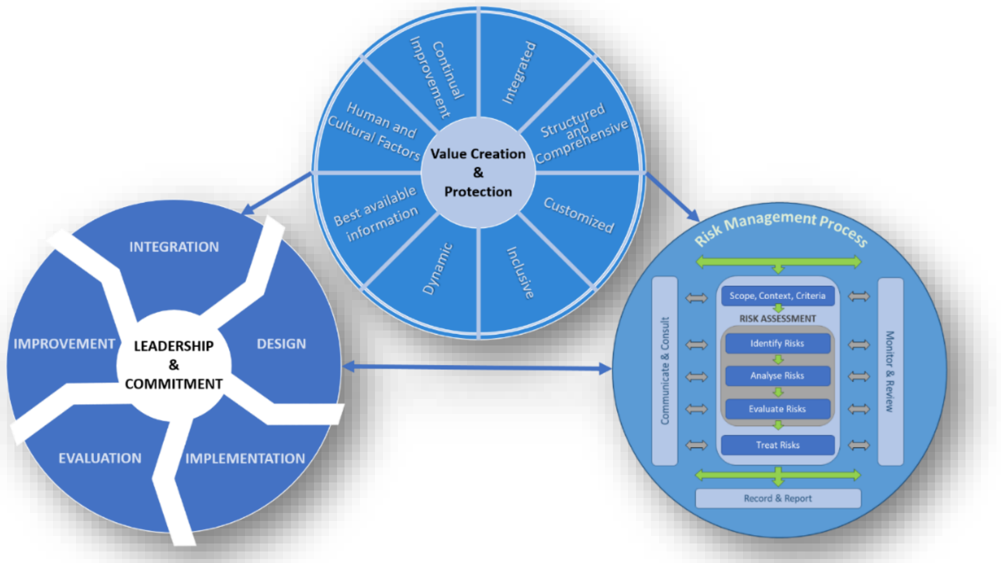
# CHIEF RISK OFFICE

RISK MANAGEMENT BRANCH & GOVERNMENT SECURITY OFFICE

# Risk Management Guideline for the B.C. Public Sector

**August 2022**

*(Supersedes April 2019 version)*



## FORWARD

Risk is defined as "the effect of uncertainty on objectives." If we could see into the future, we could prepare accordingly and there would be no need for risk management. Unfortunately, there are no crystal balls, and both internal and external forces create uncertainty. Some of these forces are within our control, but many are not.

Every day, we manage risk in an informal way. Consider a simple evening walk. You weigh the risks and take actions to ensure your safety, such as looking both ways before crossing the street or bringing an umbrella in case of rain. These daily personal decisions may not require formal risk management; however, for those working in the public service, a formal risk program may be required, for instance, to improve pedestrian safety within a community. A program could assess risks and implement priority treatments such as installing additional cross walks or adding signage or signals at busy intersections where required.

Enterprise Risk Management (ERM) provides an effective way for organizations to identify and manage risks that may require cross-departmental collaboration and senior level decision-making. As public servants, we strive to uphold the mission statement and vision of our organizations on behalf of the citizens of British Columbia. The ability to recognize and proactively manage the uncertainty that unfolds as we implement our strategies is crucial to our ultimate success.

British Columbians rely on the B.C. government and its public sector organizations to provide essential services and programs that are relevant, effective and resource conscious. Government takes ownership of some of the biggest risks in society and provides critical services where mistakes can be costly. As a result, a more formal approach to risk management is required.

Some explicit examples of formalized and enterprise-level risk management include legislation, regulations, policies and practices. These "rules" guide people and processes. They work as risk treatments, reducing the likelihood of loss and providing a framework for compliance audit.

Even with these strategies in place, you still need to consider some uncertainties could have an impact (positive or negative) on your organization's goals and objectives. How can decision-makers utilize risk information to make informed decisions? This guideline provides internationally adopted practices and principles to help B.C. public sector organizations establish effective risk management programs.

## TABLE OF CONTENTS

# SECTION 1 – GENERAL

## 1.1 RISK STATEMENT

The B.C. public sector accepts risk as an integral part of doing business; manages risk by monitoring, treating, and transferring it; and consciously retains residual risk at an appropriate level.

## 1.2 OBJECTIVES

- Recognizing risk management as critical to the achievement of government's goals and governance responsibilities.
- Encouraging a culture that embraces innovation and opportunity, informed risk-taking and acceptance of risk as inherent in all activities of government.
- Providing common and consistent risk management processes and practices that:
    - offer assurance that risks are identified and appropriately managed, and
    - support ministries in operational and strategic decision making.

## 1.3 ABOUT THIS GUIDELINE

This Risk Management Guideline is an update to the version that was released in 2019 and assists in the application of consistent risk management practices across the B.C. public sector. This guideline works in conjunction with:

1. ***ISO 31000:2018***, the international standard for risk management adopted by the B.C. government. This suite of resources includes:
    - ***CSA ISO 31000:18 Risk management – Guidelines*** (CSA ISO 31000) provides guidance for the provincial risk management framework and process.
    - ***CSA ISO/TR 31004:14 (R2019) Risk management – Guidance for the implementation of ISO 31000*** provides detailed guidance for the implementation of the provincial risk management framework**.**
    - ***CSA IEC 31010:20 Risk management – Risk assessment techniques*** provides guidance on selection and application of systematic techniques for risk assessment**.**
    - ***ISO Guide 73:2009 Risk management – Vocabulary*** provides risk management terminology to be consistently applied throughout risk management activities.
2. ***Core Policy and Procedures Manual (CPPM),*** Chapter 14: Risk Management provides risk management direction to ministries. It assigns specific risk management roles and responsibilities, establishes the Enterprise Risk Management (ERM) framework for the B.C. public sector, and details specific risk management and reporting processes and tasks. Provincial crown corporations and B.C. public sector agencies must follow the spirit and intent of CPPM and can use this policy as a guide to implement their own risk management policies.

3. ***Supporting tools and documents***, such as the ISO Guidelines above, Standard Risk Register, Risk Maturity Model, and guides to loss reporting, insurance, indemnities, and financial guarantees are available at the Risk Management Branch intranet site (government access only). Provincial crown corporations and other B.C. public sector agencies may contact the Risk Management Branch (RMB@gov.bc.ca) for access to these resources.

## 1.4 DEFINITIONS

The B.C. government utilizes definitions for risk management as included in this guideline and, if not defined in this guideline, then as defined in the ***ISO Guide 73:2009 Risk Management – Vocabulary***.

**Risk**: the effect of uncertainty on objectives.

**Risk Management***:* the structured and disciplined efforts to understand and treat risk, reduce uncertainty and better meet or exceed goals and objectives.

**Enterprise Risk Management (ERM)***:* the coordinated, ongoing application of risk management across all parts of an organization, at all levels, from strategic planning to service delivery.

**ERM Program**: the framework that the organization has in place to govern risk management activities. This includes how risk is assessed, the roles and responsibilities of senior leaders and all employees in managing risk, and the effective reporting and communication of risk information throughout the organization.

## 1.5 ADDITIONAL INFORMATION

To support the B.C. public sector, and to provide risk management advice from a government-wide perspective, the Risk Management Branch offers advisory services in areas as diverse as security and loss prevention, insurance, procurement risk, project management risk, health and education risk financing programs, and claims and litigation.

For more information or to engage the services of a Risk Management Consultant, contact the Risk Management Branch at 250-356-1794, or email RMB@gov.bc.ca.

## SECTION 2 – RISK MANAGEMENT IN THE B.C. PUBLIC SECTOR

The BC Government has adopted an international standard, CSA ISO 31000, to provide a structure for managing risk and implementing effective ERM Programs across the B.C. public sector. In this context, enterprise is defined as the whole of government, including B.C. government ministries and all public sector organizations that work together to provide services to British Columbians. Strong ERM Programs enable senior leaders to:

- identify and communicate risks shared across the B.C. public sector;
- apply combined risk mitigation strategies;
- determine overarching priorities;
- facilitate discussion of the types and levels of risk government is prepared to accept (tolerance); and
- make long-term plans for the future.

All ERM Programs are comprised of three components: principles for managing risk, the risk process that guides the identification and assessment of risk (see Figure 1), and a framework which governs the reporting and communication of risk information.

The CSA ISO 31000 was updated in 2018 and considers shifts in global risk management practices and to address new challenges faced by organizations. This version places more emphasis on the involvement of senior leadership and the integration of risk management with organizational business processes. This updated standard is integrated within the B.C government as these enhancements represent two of the five pillars that comprise our risk maturity assessment framework.

B.C. government ministries and public sector organizations are encouraged to build an ERM Program based on the three key components, but tailored to their decision-making structure and encompassing the elements found within the standard.

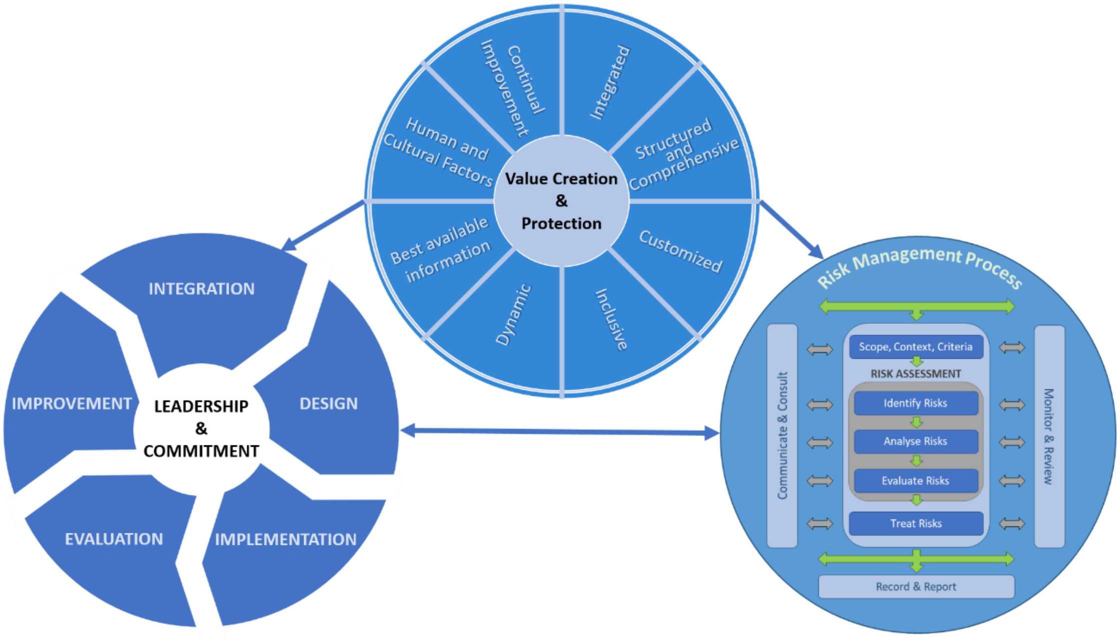


*Figure 1: CAN/CSA-ISO 31000 Principles, Framework and Process*

## 2.1 RISK MANAGEMENT PRINCIPLES

An ERM Program should improve performance, encourage innovation and support the achievement of objectives. CSA ISO 31000 provides a set of principles to consider when establishing your organization's framework and related processes (see Figure 2). These principles are centred around the ERM Program creating and protecting value for the organization.

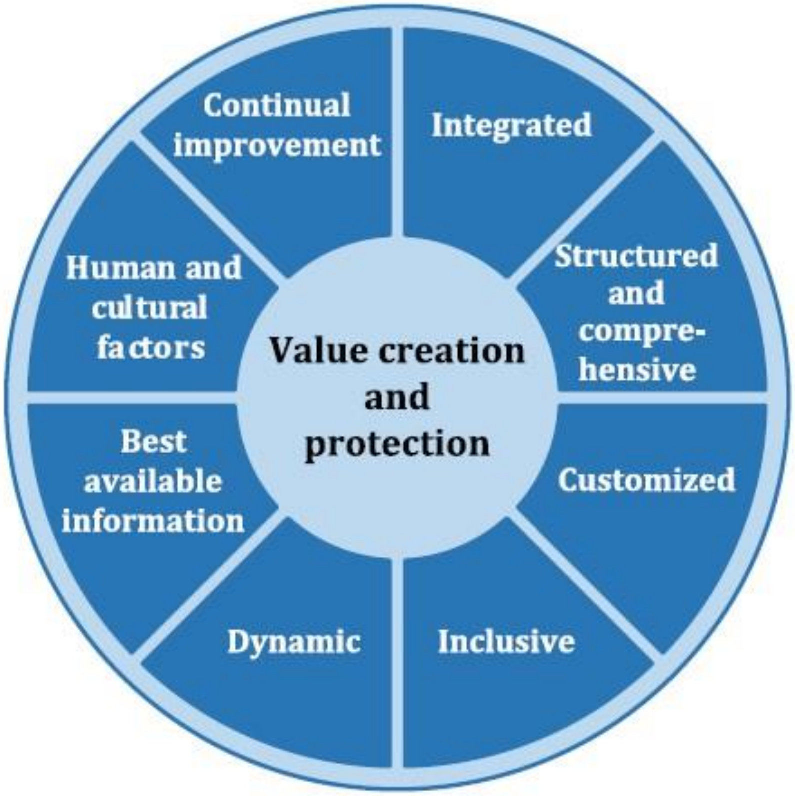

Value creation and protection
Integrated
Structured and compre-hensive
Customized
Inclusive
Dynamic
Best available information
Human and cultural factors
Continual improvement

*Figure 2: CSA ISO 31000 Principles*

## 2.2 RISK MANAGEMENT FRAMEWORK

An ERM Program should include a risk management framework that governs risk management practices and is tailored to the organization. A framework ensures that information about risk collected through the risk management process is adequately utilized and is considered as a basis for decision-making at all relevant organizational levels.

This requires the establishment of the right structure to assign responsibility and facilitate the gathering and communication of risk information.

**REFLECTION:** How do you know your ERM Program is effectively contributing to decisions?

CSA ISO 31000 provides a framework that should be tailored to the organization's business processes. Risk management is not a separate exercise that is conducted periodically, it should be regularly integrated into business processes accordingly to inform decision-making (see Figure 3).

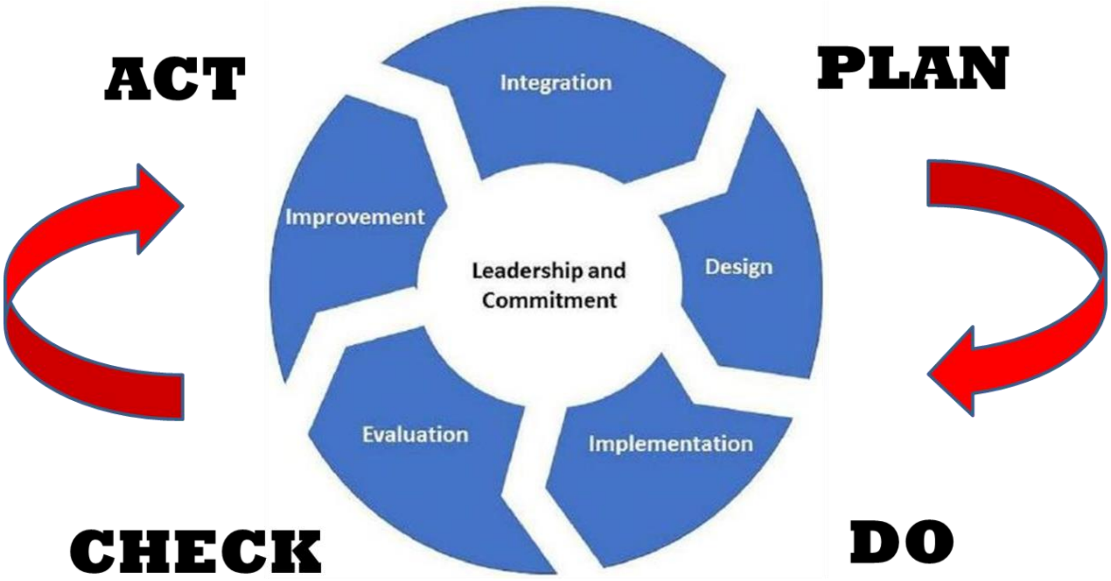


*Figure 3: CSA ISO 31000 Framework*

**Leadership and Commitment:** Top management and oversight bodies should ensure that risk management is integrated into all organizational activities and should demonstrate leadership and commitment.

**Integration:** Integrating risk management relies on an understanding of organizational structures and context. Structures differ depending on the organization's purpose, goals and complexity. Risk is managed in every part of the organization's structure. Everyone in an organization has responsibility for managing risk.

**Design:** When designing the framework for managing risk, the organization's ERM Program should:

- Understand the organization and its context
- Articulate risk management commitment
- Assign the organization's risk management roles, authorities, responsibilities and accountabilities
- Ensure allocation of appropriate resources
- Establish an approach to communication and consultation

**Implementation:** Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all activities throughout the organization, including decision-making, and that changes in external and internal contexts will be adequately captured. A risk management framework is implemented by:

- Developing an appropriate plan including time and resources.
- Identifying where, when and how different types of decisions are made and by whom.
- Modifying the applicable decision-making process where necessary.
- Ensuring that that arrangements for managing risk are clearly understood and practised.

**Evaluation:** To evaluate the effectiveness of the risk management framework, performance must be periodically measured to determine if it remains suitable to support achieving the objectives of the organization.

**Improvement:** The risk management framework should be continually monitored and adapted to address external and internal changes. As relevant gaps or improvement opportunities are identified, plans and tasks can be assigned to those accountable for implantation and enhanced risk management practices.

**REFLECTION:** How do you know your organization's ERM Program is effective and creates value?

The B.C. government's Risk Maturity Model helps B.C. government ministries and public sector organizations assess their risk management maturity (see Figure 4). By assessing within twenty attributes across five pillars, organizations can determine where they land on the risk maturity continuum and determine opportunities for growth and improvement to their ERM program.

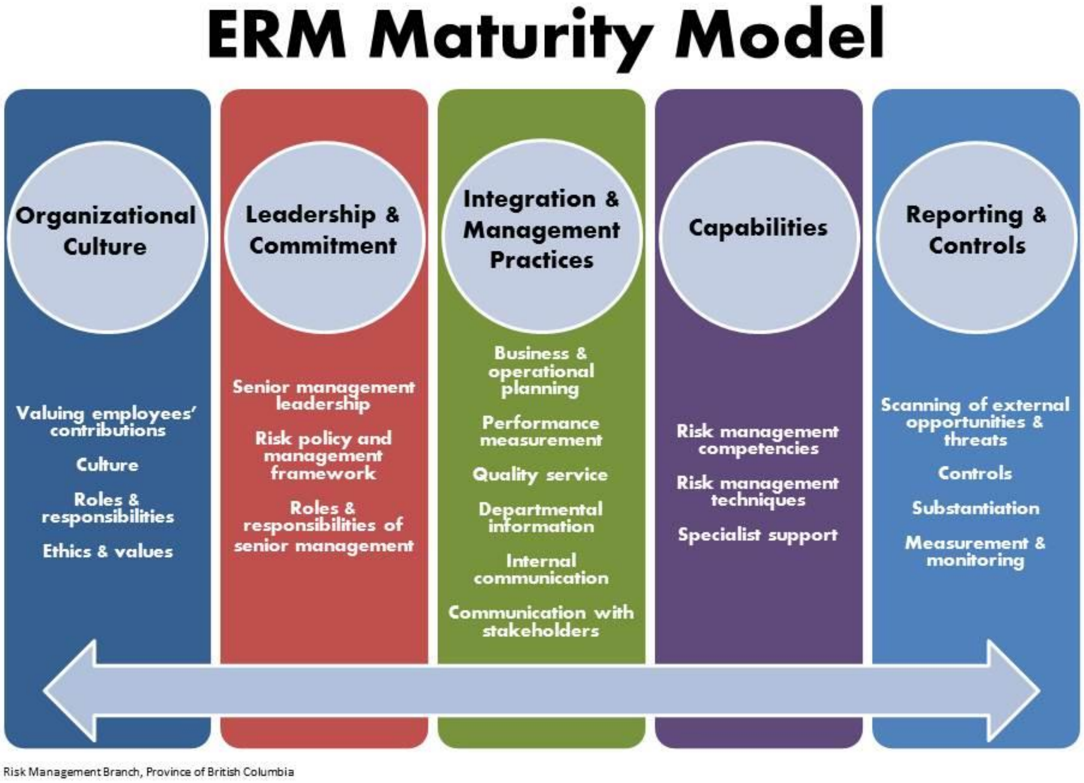

ERM Maturity Model
Organizational Culture
Valuing employees' contributions
Culture
Roles & responsibilities
Ethics & values
Leadership & Commitment
Senior management leadership
Risk policy and management framework
Roles & responsibilities of senior management
Integration & Management Practices
Business & operational planning
Performance measurement
Quality service
Departmental information
Internal communication
Communication with stakeholders
Capabilities
Risk management competencies
Risk management techniques
Specialist support
Reporting & Controls
Scanning of external opportunities & threats
Controls
Substantiation
Measurement & monitoring
Risk Management Branch, Province of British Columbia

*Figure 4: B.C. government's Risk Management Maturity Model*

## 2.3 ROLES AND RESPONSIBILITIES

The following roles and responsibilities enable the effective application of risk management throughout the B.C. public sector.

**Ministries are responsible for:**

a. ensuring their ministry's compliance with government's risk management policy as established in CPPM Chapter 14: Risk Management, including the appointment of an Assistant Deputy Minister responsible for ERM implementation;

b. establishing a ministry-specific ERM Program, which includes their associated public sector organizations that align with this guideline and CSA ISO 31000; i

c. integrating the risk management process into existing ministry planning, reporting, operations, and service delivery functions; and

d. implementing risk management strategies to address identified risks within their ministry, which includes working with their associated public sector organizations to address key risks identified and provide the minister responsible' s direction on key risks where appropriate.

**Risk Management Branch is responsible for:**

a. performing the functions of a government-wide Chief Risk Office as outlined in CPPM Chapter 14;
b. providing central risk management programs, advice and consultation services to all B.C. public sector organizations; and
c. operating the Government Security Office, including the role of Chief Security Officer, with overall responsibility for security within government.

**Internal Audit and Advisory Services is responsible for:**

a. using ERM to inform the annual Internal Audit & Advisory Services risk-based government-wide annual audit work plan;
b. reviewing risk management practices across government; and
c. assessing the effectiveness of established risk mitigation strategies/controls within ministries and across government.

**Every manager is responsible for:**

a. integrating sound risk management planning and process into the business processes they are responsible for; and
b. reporting risks with causes, impacts, or mitigations beyond their scope of responsibility to executive.

**Every employee is responsible for:**

a. applying sound risk management within the scope of their duties and responsibilities; and
b. reporting risks with causes, impacts, or mitigations beyond their scope of responsibility or available resources to their manager.

**REFLECTION:** Do your employees know what their responsibilities are in relation to generating and communicating risk information?

# SECTION 3 – THE RISK MANAGEMENT PROCESS: HOW TO DO A RISK ASSESSMENT

## 3.1 OVERVIEW OF THE PROCESS

CSA ISO 31000 outlines the risk management process, (see Figure 5) and provides a step-by-step guide to identify, assess and treat risk. This process is scalable and can be applied at strategic, operational, program or project levels.

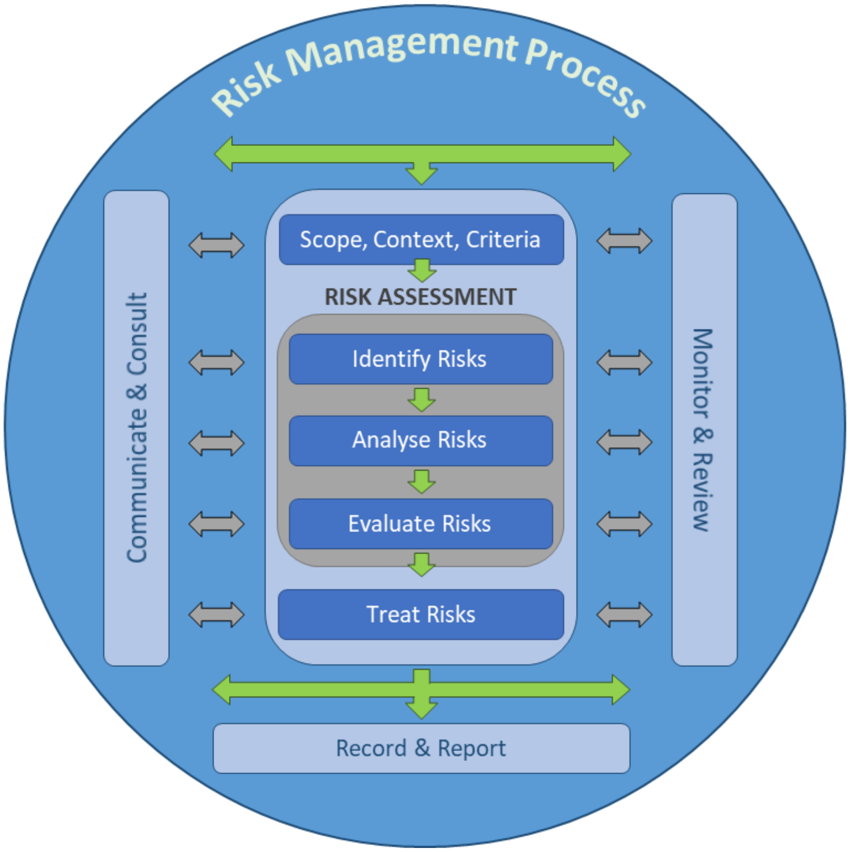


*Figure 5: CSA ISO 31000 Risk Management Process*

The risk management process should be an integral part of business management. The risk information that is gathered through this process should be shared throughout the organization as prescribed by the organization's ERM Program to support decision-making.

**REFLECTION:** How does your ERM Program gather and communicate risk information using the risk management process?

## 3.2 COMMUNICATE AND CONSULT

*"Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process" (CSA ISO 31000, Section 6.2)*

The consultative team approach means that the assessment of risk is proactive and inclusive and involves those who understand the risks and are best able to manage them. Communication and consultation must be used to ensure that risk reporting goes up to higher levels, and that executive decisions regarding tolerance of risk and priorities for action get communicated back down to the business unit level.

Depending upon the context, the organization conducting the risk assessment must determine the correct balance of and limits to direct participation. We recognize that it is not always practical or productive to bring all stakeholders to the table. Still, you are seeking a full range of perspective - advocacy, systems, budget, policy, senior leaders, front line delivery and so forth.

Wider participation brings the benefits of greater expertise, experience and buy-in balanced against the requirements for confidentiality, timely action, and strategic scope. RMB can provide advice when deciding which stakeholders should be included in a risk assessment.

## 3.3 ESTABLISH THE SCOPE, CONTEXT AND CRITERIA

*"The purpose of establishing the scope, the context and criteria is to customize the risk management process, enabling an effective risk assessment and appropriate risk treatment. Scope, context and criteria involve defining the scope of the process and understanding the external and internal context" (CSA ISO 31000, Section 6.3)*

"Establishing the scope, context and criteria" for a risk assessment performs a number of functions. It confirms the subject of the risk assessment, the subject's goals and objectives, and the goals and objectives of the risk assessment itself; identifies stakeholders; and acknowledges constraints and limitations imposed on the subject and on the risk management process.

Factors influencing context may be internal, such as executive direction, government policies, budget, regulations and culture; or external, such as other government jurisdictions, national or international economic forces, climate and natural events, or citizens and special interests.

When applying the risk management process to day-to-day decision making, it may be sufficient to establish the scope, context and criteria informally. Formal risk assessments, however, benefit from a thorough examination and detailed recording of these elements. A written document will ensure all stakeholders involved in the process have a clear understanding of the scope, context and criteria. It also proves invaluable for recording the environment in which the risk management decisions are made and can demonstrate due diligence if those decisions are revisited later.

For this reason, the B.C. government has established the Context Paper Template to record these elements:

1. ***Subject of the risk analysis:*** What is being reviewed e.g., is it a strategic plan, service plan, project, program, policy, process or procedure? State the scope with respect to organization, hierarchical level, and time frame. Specify whether the context is strategic or operational.

*Hint: If there is no plan or policy yet created, and there is a need for a risk profile on a particular issue, then the subject of the risk analysis may be the status quo i.e., the organization's current approach to the issue. If general goals or values are provided, the team can generate a risk profile.*

2. ***Goals and objectives*****:** You should clearly establish what the risk assessment seeks to do because there may be multiple sets of related goals and objectives:

   - Those of the ministry, division or branch sponsoring the risk assessment. Clearly establishing those higher goals and objectives will help ensure the subject of the risk assessment is aligned with strategic direction.
   - Those of the program, policy or plan in question. Risks are best identified in relation to either broad strategic goals (at the highest level of planning) or in relation to objectives and specific activities. The list of goals, objectives and strategies (activities) can serve to structure the discussion of risk.
   - Those of the risk assessment process itself. For example, a risk assessment may be used to inform whether a proposal or project should proceed, or to ensure the success of a new initiative.

*Hint: If there is no program of activities yet designed, state the highest overall goals, and sketch the main components of a draft plan. This will provide a basis to generate a risk profile and mitigations to inform a final plan*

3. ***Value criteria:*** These are the guiding principles of the organization, such as a professional ethical code, business practices, political priorities, or operating principles found, for example, in existing vision and mission statements. They might take the form of special rules (e.g., how to conduct business in a specific context). Participants refer to value criteria to help to identify and assess risks.

*Hint: It is important to keep value criteria in plain view during the session. They serve as a common point of reference to aid in formulating and assessing risks. If controversy arises, or conversation deviates, anchor points or parametres can help refocus the conversation to what needs to be assessed.*

4. ***Stakeholder*** analysis***:*** This involves the identification of internal and external stakeholders and their respective roles, degree of influence, interests and motives and position with respect to value criteria. They can be both bearers of risk, and/or sources of it.

*Hint: Refer to existing consultation papers. A diverse range of session participants, where appropriate and within the limits of facilitation, lends rigour to the process and leads to a*

> *better quality result. Tools to assist in the conduct of a stakeholder analysis are available from Risk Management Branch.*

5. ***Assumptions*** and ***constraints:*** These include fixed deadlines, executive directives, resources or other limiting conditions.

> *Hint: Legislation, regulation and policy are part of the context in which the risk assessment will take place. Not only do they often address the risks identified, but they also guide the implementation of proposed mitigation strategies.*

6. ***Deliverable for the session:*** This is the intended product of the session. A typical deliverable statement might be *"*a comprehensive list of risks, with rankings and summary treatments arrived at by consensus, to inform an improved business plan/policy/program".

### 3.3.1 Specialized Contexts and Criteria: Sub-disciplines within Risk Management

Do not let the identification of risk stray out of scope of the defined context. Recognize, too, that certain perils or exposures call for a *specialized risk analysis* as a *separate exercise*. For example, earthquake, hurricane or flood hazards create risk exposures in almost any context. Those risks belong to a specialized analysis for *emergency and business continuity planning*. Similarly, security risks with respect to physical dangers, facilities, and procedures, require a *security review*, which is an expertise unto itself. These specialized areas may bring their own criteria and resources to bear upon the process.

Risk Management Branch can assist with many of these specialized sub-disciplines and can refer client ministries to other experts across government, such as Emergency Management B.C., Government Chief Information Officer, and Treasury Board Staff.

**Examples of Risk Management Sub-Disciplines**

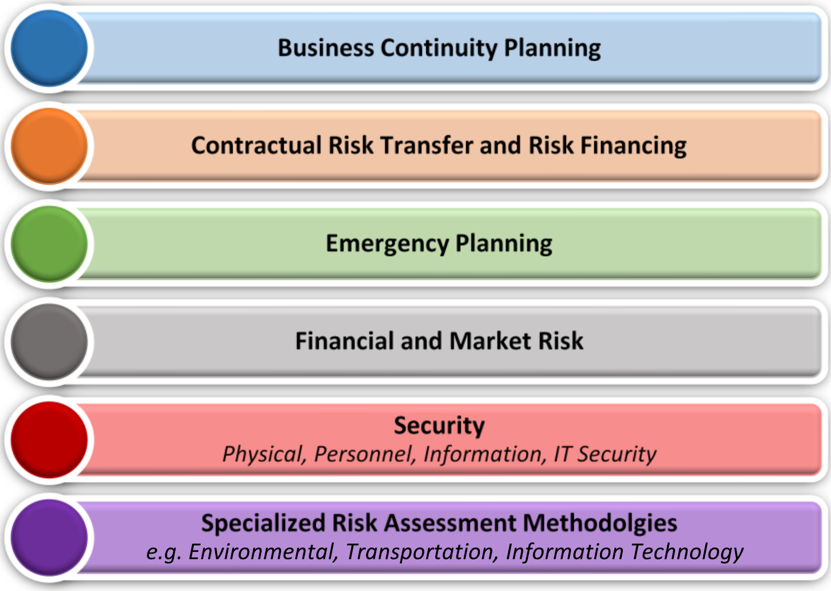

Business Continuity Planning
Contractual Risk Transfer and Risk Financing
Emergency Planning
Financial and Market Risk
Security
Physical, Personnel, Information, IT Security
Specialized Risk Assessment Methodolgies
e.g. Environmental, Transportation, Information Technology

*Figure 6: Provincial Risk Treatment Specialized Disciplines*

## 3.4 IDENTIFY RISKS

*"The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieve its objectives. Relevant, appropriate and up-to-date information is important in identifying risks." (CSA ISO 31000, Section 6.4.2)*

### 3.4.1 Risk Identification Methods

Typically risk assessments rely on expertise, knowledge, and experience, but there are other tools and methodologies that can aide teams in the risk assessment process. These include:

- interview/focus group discussions;
- audits or physical inspections;
- questionnaires or surveys;
- networking with peers, industry groups and professional associations;
- incident, accident and injury investigation;
- loss history analysis (such as government's General Incident or Loss Reports (GILRs));
- scenario analysis (what ifs);
- process analysis;
- strengths, weaknesses, opportunities, threats (SWOT) analysis; and
- flow charting, system design review, systems analysis.

***CSA IEC 31010:20 Risk management – Risk assessment techniques*** also offers a variety of risk assessment techniques for various stages of the risk assessment process, including root cause analysis, scenario analysis and Monte Carlo simulation.

Many ministries and public agencies have designated risk management positions or employees with risk management experience. Consult with internal risk management resources and inform ministry risk management experts of your risk management activities. In their absence, Risk Management Branch's consultants are trained facilitators and can assist your organization with the risk assessment process.

### 3.4.2 Risk Categories

When identifying risk, it is important to take an enterprise-wide view of all potential threats and opportunities that may have an impact on objectives. RMB has researched industry best practice and collaborated with government central agencies to develop risk categories to consider when identifying risk. The major categories are Hazard, Operational, Financial, and Strategic. For more details about these categories and resources available to assist with risk assessment, in particular categories or sub-categories, please refer to the B.C. Enterprise Risk Categories Tool.

### 3.4.3 How to State Risks

Once you've identified all possible risks, the recommended method for stating risk involves considering its three elements: event, causes, and impacts. Being articulate about defining the risk event will help develop tangible, treatable strategies.

You can test your risk event statements. As with the fire triangle, fuel, oxygen, and a source of ignition are required. When one element is removed, the fire is prevented or extinguished. By identifying risk by its three elements (Figure 7) provides treatable options: by acting on one of the elements, the risk can be affected.

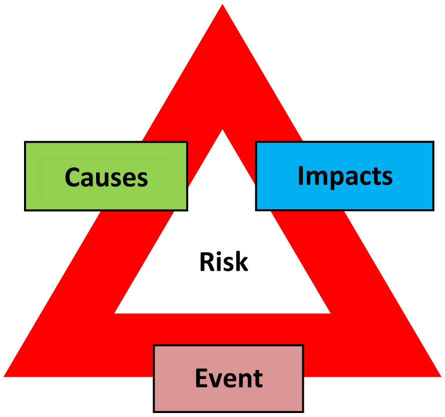


*Figure 7: Risk Elements*

Since we define risk as "*the effect of uncertainty on objectives*", it is helpful to link your organization's objectives to the risk identification. Define the event as something that could prevent achievement of an objective, milestone or target, or create an opportunity to exceed them. From there, the causes and impacts become easier to identify.

Use of a bowtie diagram, as illustrated below (Figure 8), can be helpful in identifying multiple causes and impacts of a single event:

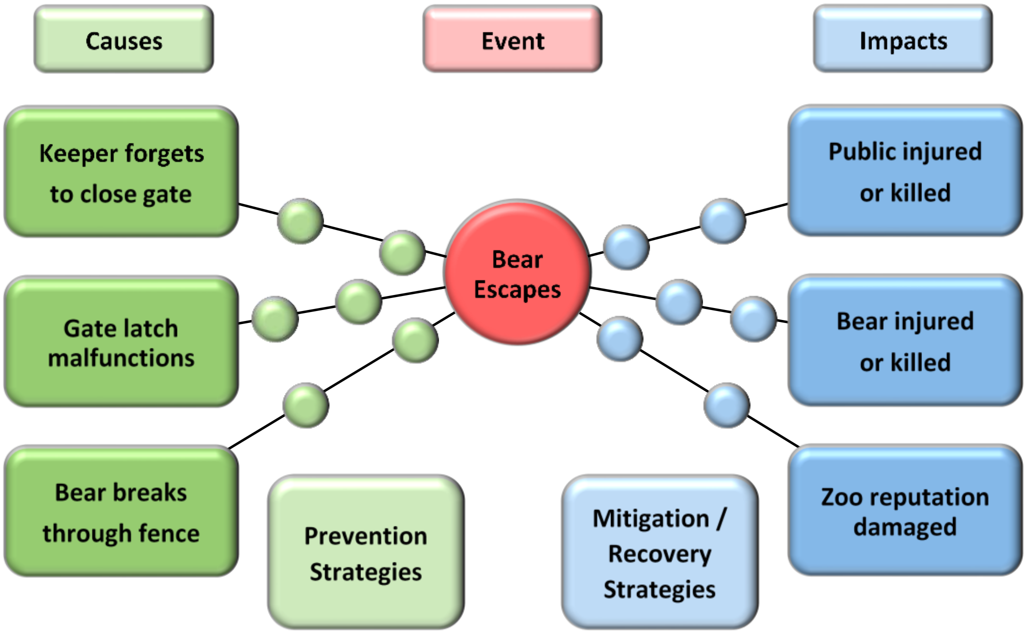


*Figure 8: Risk Management Bowtie Diagram*

A generic example of a negative risk tied to a goal of a fictitious entity – a zoo. In this case, a strategic organizational objective is *"safe and secure stewardship of their animal exhibits"*. A risk event that could influence that is *"escape of the bear"*. Causes and impacts flow from this event:

1. Identify a risk event related to an in-scope objective. Do not state general unfavourable conditions, in and of themselves, as risk events.
2. List the potential causes of such an event. There are often multiple causes for a given risk event. Ask yourself "why" the event might happen. Use of root cause analysis methods (such as the *Five Whys* tool) can be effective.
3. Identify the impacts of the event, should it happen. Ask yourself, "So what if the event were to occur?" Keep asking "so what" to the chain of impacts until all realistically potential impacts are identified.

***Example***

**Event**: Failure to secure project objective #1: Treasury Board approval for required project funding.

**Causes**:

a. Possible 10% budget cut across government.
b. TB submission fails to link project goals with Ministry objectives.
c. Failure to meet submission deadlines.

**Impacts**:

a. Possible termination of project.
b. Resubmission to Treasury Board and costly delays.
c. Funding of project from within existing operational budget, leading to service reductions elsewhere.

The Standard Risk Register is the tool that the B.C. government uses to document the risk assessment and manage the risk management process. We do not recommend using risk registers pre-populated with generic risks as this may stifle the brainstorming process. Refer to section *3.4.1 Risk Identification Methods and Categories* above for examples of sources of risk.

### 3.4.4 Existing Treatments

Once the risk is clearly identified and details the risk event, causes and impacts, it is important to identify existing treatments (i.e., mitigations). Ask what measures are currently in place (if any) to treat this risk. In the risk register, list only those treatments that already exist. Identification of additional proposed treatments (if required) happens later, after the group has evaluated the adequacy of existing treatments and the significance of the risk.

## 3.5 ANALYZE RISK

*"The purpose of the risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives." (CSA ISO 31000, Section 6.4.3)*

### 3.5.1 Risk Rating

Risk analysis is the process of calculating the likelihood of an event and the consequence if it were to occur. The product of these two variables is the *Risk Rating (see Figure 9)*.

LIKELIHOOD

| | | | | | |
|---|---|---|---|---|---|
| 5 | LOW | MED | HIGH | EXT | EXT |
| 4 | LOW | MED | HIGH | HIGH | EXT |
| 3 | LOW | MED | MED | HIGH | HIGH |
| 2 | LOW | LOW | MED | MED | MED |
| 1 | LOW | LOW | LOW | LOW | LOW |
| | 1 | 2 | 3 | 4 | 5 |

CONSEQUENCE

| LIKELIHOOD X CONSEQUENCE | | | |
|---|---|---|---|
| SCORE | 0 – 5 | = | LOW |
| SCORE | 6 – 10 | = | MEDIUM |
| SCORE | 12 – 16 | = | HIGH |
| SCORE | 20 – 25 | = | EXTREME |

*Figure 9: Risk Rating Matrix*

***Likelihood:*** is the chance that the risk event identified will actually occur. When available, statistical data can support estimates of likelihood and severity. In practice, however, often we do not have historical data. Instead, we often rely on the experience of those around the table; therefore, likelihood rarely implies mathematical certainty; rather it is a subjective estimate.

| Likelihood = Probability of the risk event actually occurring | | |
|---|---|---|
| **Score** | **Criteria** | **Probability (%)** |
| 5 | Almost Certain | 80%-99% or Once a year or more frequently |
| 4 | Likely | 61%-79% or Once every three years |
| 3 | Possible | 40%-60% or Once every five years |
| 2 | Unlikely | 11%-39% or Once every 15 years |
| 1 | Almost certain not to happen | 0%-10% or Once every 25 years |

***Consequence:*** is the outcome of an event affecting objectives. A B.C. government ministry or public sector organization can adjust the consequence criteria appropriate to their lines of business (perhaps quantifiable in terms of budget dollars), and risk appetite. Many organizations develop a "scorecard" with several categories of consequence.

| Consequence = Degree of severity, with respect to goals/values, should the risk event occur | | |
|---|---|---|
| **Score** | **Impact** | **Descriptor** |
| 5 | Catastrophic | • Major problem from which there is no recovery.<br>• Significant damage to ministry credibility or integrity.<br>• Complete loss of ability to deliver a critical program. |
| 4 | Major | • Event that requires a major realignment of how service is delivered.<br>• Significant event which has a long recovery period.<br>• Failure to deliver a major political commitment. |
| 3 | Moderate | • Recovery from the event requires cooperation across departments.<br>• May generate media attention. |
| 2 | Minor | • Can be dealt with at a department level but requires Executive notification.<br>• Delay in funding or change in funding criteria.<br>• Stakeholder or client would take note. |
| 1 | Insignificant | • Can be dealt with internally at the branch level.<br>• No escalation of the issue required.<br>• No media attention.<br>• No or manageable stakeholder or client interest. |

### 3.5.2 Risk Rating Terms

The terms associated with the ranking of risks vary across the risk management discipline; therefore, some clarification is required. *Inherent Risk, Initial Risk, Residual Risk, Current Risk, and Risk Tolerance* are common terms used within the B.C. public sector. It is not necessary to use all the different risk ratings for any particular risk assessment, but as a minimum, the rating of *initial risk* is required, and *residual risk* is recommended.

***Inherent risk:*** involves rating the exposure in the absence of existing controls. When seeking to understand inherent risk, we are considering a hypothetical condition free of all controls, like locks, rules, procedures, ethics and so forth. This can be difficult to imagine. However, there is value in assessing risk this way as it can identify whether an exposure is over- or under-controlled. This is of particular interest to ministry executive and auditors. Strategic risk assessments, of ministry business plans, for example, often benefit from an assessment of inherent risk.

***Initial risk***: involves rating the exposure within its current control environment (i.e., now). Initial risk is a baseline against which you can measure progress. Reviews of loss histories, reviews of similar sectors' loss histories, and consultation with stakeholders can support the assessment process.

***Residual risk:*** involves rating the exposure after the development of additional mitigation/treatment strategies. It is important to establish a residual risk rating because it is a prediction of the efficacy of proposed treatments. It also serves as a start point for an informed discussion of acceptable risk with senior decision-makers.

***Current risk:*** is a measure of progress. Later, regular updates on the progress of risk treatment strategies can be valuable in helping to demonstrate progress or to secure additional resources for stalled mitigation efforts. The tracking of current risk over time allows efficient shifting of resources to problem areas or to areas of opportunity. In addition, tracking the progress of current risk can help demonstrate the effectiveness of the organization's risk management program.

***Risk tolerance:*** is the maximum level of risk the organization is willing to accept for a particular exposure. Executive should provide this once briefed on the nature of the risk, existing controls and the implications of planned mitigations. Ideally, residual risk and risk tolerance are equal. This would confirm that senior executive has committed to the planned additional treatments and has consciously retained the remaining residual risk.

## 3.6 EVALUATE RISK: EXISTING CONTROLS, TOLERANCE AND ACTION

*"The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required." (CSA ISO 31000, Section 6.4.4)*

Risk evaluation consists of considering the ranked risk in relation to existing controls and the organization's tolerance for the particular risk in question. The purpose is to arrive at a decision as to how to respond to risks – guided by specific value criteria and cost/benefit. There are three considerations when evaluating existing controls. Enter the following into the risk register columns (see Standard Risk Register).

1. **Characterize, in qualitative terms, the existing controls**:
   *Non-existent, Inadequate, Adequate, Robust, Excessive (this latter indicates over-controlling and so possibly overspending).*

   How would you describe the process, policy, device, practice or other action already in place that mitigates the risk in question?
2. **Characterize the risk in relation to the organization's degree of tolerance:**
   *Unacceptable/ Acceptable with treatment/ Acceptable*

   It is possible to have 'zero" tolerance for certain risks (assuming one can avoid them). A risk may be "Acceptable" either because it is inevitable and too prohibitive to treat, or because it is immaterial and not worthwhile to treat. Over time, ministries may develop risk criteria or measures of risk tolerance or risk thresholds. Expressing tolerance for an unexpected financial loss over a certain percentage of operating budget as "unacceptable" might be one way executive can quantify their tolerance of certain risks.
3. **Decide on consequent action, based on steps 1 and 2:**
   *Avoid/ Treat/ Monitor only (tolerate)*

   You may avoid a risk altogether, if unacceptable, by not doing the action that would incur it in the first place. We tolerate and monitor risk when treatment is impracticable or prohibitive. We monitor risks that are inconsequential, but whose status might change.

## 3.7 TREAT RISK

*"The purpose of risk treatment is to select and implement options for addressing risk." (CSA ISO 31000, Section 6.5)*

If the current level of risk is unacceptable or acceptable with treatment, you should recommend a treatment strategy.

***Risk Avoidance:*** It may be possible to eliminate a risk event entirely by ceasing the activity associated with the event. Given that government delivers society's riskiest services to its most vulnerable members, this is not often possible. It is worth asking though "if this activity is something that government needs to be doing?" Risk *avoidance* is the term given to the elimination of risk by ceasing the associated activity, but it often introduces new risks, especially reputation loss.

***Prevention and Treatment Strategies:*** Other than avoidance, risk treatments work to prevent the event by addressing the causes or decrease its impacts by treating the negative effects and preparing for post-event recovery. Ask the group "what might be done to prevent the event from happening", then ask, "If it were to happen, how can we limit the damage done and get back to business?"

### 3.7.1 Diversity of Risk Treatment (Mitigation)

As discussed in section 1, existing legislation, regulation, policies and procedures effectively mitigate many government risks. These legal and administrative controls effectively reduce to tolerable levels most risks associated with routine activities. The first risk management priority of a ministry should therefore be a review of procedural controls and remedial action to educate and encourage compliance. Internal Audit is an excellent resource to assist in assessing compliance with policy.

Should existing treatments be inadequate, the subject be new, or if the context in which it is applied should change, a risk assessment and consideration of additional treatments may be appropriate.

Treatments (risk mitigations) can consist of virtually any sort of administrative action, as well as the application of specialized disciplines – where a separate analysis may be required, e.g., emergency planning, business continuity planning, security planning, risk financing, financial controls, and human resources management. Grouping risks in categories can help in the design of cost-effective treatments.

### 3.7.2 Ensuring Effective Risk Treatment (Mitigation)

In B.C. public sector work, three points are necessary to underscore:

1. ***Treatments are new measures undertaken to mitigate identified risk***. At times, participants fall into familiar thought patterns and merely repeat the list of existing controls and say there is nothing more to be done. Alternatively, they may say that the implementation of their planned program activities constitutes mitigation of risk. It is just here where the facilitator or risk champion may add value:
   - A facilitator can lead off by asking (either naïve or well-informed) questions about possible treatments and stimulate discussion;
   - A facilitator can draw attention to the ranking of the risk – if participants are reminded that it is high or extreme, and threatens the viability of the program, they will feel less inclined to rank it lower or leave the matter unattended. It is always best to rank the risk at the appropriate level. Public sector employees are often risk averse by nature. If a risk is ranked high by consensus of subject matter experts, that is how it should be recorded (e.g., healthcare is a good example where risks can be inherently high even with current treatments. Additional treatments are then factored (a form of gap analysis) to best manage the risk;
   - A facilitator can introduce categories of implementation risk (well-documented, common reasons for program failure) to inform the analysis;
   - The necessity to study the issue and develop treatments “off-line” or in a separate session can be flagged;
   - The possibility of inviting expertise from outside the immediate group can be raised; and
   - At a minimum, the action of documenting the risk and bringing it to the attention of a higher authority or other entity constitutes an improvement in the management of the risk.
2. ***Document treatments.*** During the latter part of a risk identification and analysis session, make summary statements of treatments. They might have to be elaborated upon elsewhere, but briefly summarizing them allows the facilitator to cover a maximum amount of material. A measure of due diligence is achieved by recording both the risks *and* how they will be managed.
3. ***Translated treatments into action.*** Suggested treatments (mitigation of either a risk likelihood or degree of consequence) are subject to cost-benefit analysis. The facilitator must challenge the participants to commit to acting upon mitigation strategies. If the risk management initiative is an enhancement to existing processes, then the treatments must become new items in the list of project tasks or business plan strategies. Assigning an individual by name to the development of a treatment strategy, identifying a specific deliverable, assigning a due date, and listing required resources all bring value and practicality to the risk assessment, and help transform planned

mitigations into action. The Standard Risk Register is formatted in such a manner and is an excellent option for initiating the process.

## 3.8 MONITOR AND REVIEW

*"The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined." (CSA ISO 31000, Section 6.6)*

### 3.8.1 Monitor: Regular Management of Risk Information

Monitoring has to do with managing your risk information as a regular practice. Risks themselves undergo change and can require revision in terms of their description and ranking. New risks appear. Old material requires striking through (~~striking through~~ but not deleting) and archiving. Therefore, we recommend a periodic updating of risk information, using the risk register as a management tool – perhaps as the first agenda item in regular meetings. When used to track the implementation of mitigation strategies and the resultant impact on risk ratings, the risk register becomes a valuable communication tool by informing executive on the progress or lack thereof, and any additional resources required.

A note on risk management software: initial trials with software designed to assist with the risk management process showed that simple spreadsheets are often more appropriate to support the early proof of concept. Start by defining your processes and information needs. A mature practice of integrated service planning, performance, and risk management may eventually warrant the use of a specialized application, and Risk Management Branch can provide some advice on products that may be available or attributes that should be included. Many risk management software programs are based on a pre-determined platform for another area (e.g., claims, security, occupational health & safety) then adapted, meaning they may not be the best approach for a public sector organization and may also be costly. Decide what approach is best for your individual organization.

### 3.8.2 Review: Historical Risk Information

In a mature practice of risk management, a growing body of information can inform analysis of the risks themselves, their most common sources, their frequency and impacts /costs of actual occurrence, the efficacy of treatments, and the occurrence of unforeseen events. All of this serves to better manage risks and inform planning. Audits, complaints investigations, legal judgements, and retrospective cost/benefit analysis are some sources of historical risk information.

Another tool in ministries that facilitates the collection and analysis of historical information is the General Incident or Loss Report (GILR). The GILR is a core government reporting tool for a loss, or incident with the potential to lead to a loss. It allows for tracking of property losses and "near misses", identification of trends, and development of treatments. As such, it is one of the tools available to assist in assessing risk. Ministries use of the GILR is mandated by CPPM Chapter 20: Loss Management and CPPM Procedure L: Loss Reporting.

## 3.9 RECORD AND REPORT

*"The risk management process and its outcomes should be documented and reported through appropriate mechanisms." (CSA ISO 31000, Section 6.7)*

Recording risk management activities enables the organization to effectively document and measure risk assessment outcomes. This improves the governance of risk management and provides evidence to validate risk management decisions or to back recommendations to senior executive. Documentation may include:

- ***Your organization's policies and framework*** for your ERM Program. These documents set risk management goals and expectations, establishes the ministry risk management framework, assigns responsibilities and resources, establishes executive's risk tolerances and appetite, and gives guidance for organization-specific processes, reporting structures, etc. Risk Management Branch can help B.C. government ministries and public sector organizations develop and implement ERM Programs.
- ***Your organization's risk assessment documentation***, including context analyses, risk registers complete with treatment strategies, and supporting historical data.
- ***Ministry's responsibilities to report risk to Risk Management Branch,*** including the direction outlined in CPPM Chapter 14: Risk Management. Other B.C. public sector organizations must follow the spirit and intent of CPPM policy and work with their oversight bodies, including their board of directors and the ministry responsible, to implement an ERM program and report risk appropriately.

The **Risk Management Branch** provides assistance in interpreting and implementing these guidelines.

Please contact the **Risk Management Branch**
at 250-356-1794 or RMB@gov.bc.ca