Governing in the Public Interest

RISK MANAGEMENT TRAINING
FOR BC PUBLIC SECTOR
BOARD MEMBERS
May 2019

BRITISH
COLUMBIA

MODULE 3 - RISK MANAGEMENT
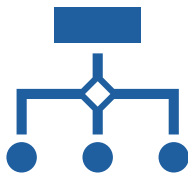
WHAT IS RISK MANAGEMENT?

Risk is the effect of uncertainty on objectives. Risk is inherent in everything we do, from governing an organization to crossing the road. Whether you are aware of it or not, you manage risk every day.

For example:

- You *avoid* risk by not drinking and driving,
- You *prevent* risk by wearing oven gloves to take a hot dish out of the oven,
- You *reduce* risk by having a smoke detector and testing it regularly,
- You *transfer* risk by buying insurance for your car, and
- You *accept* risk by waiting until next year to fix the loose railing on the back stairs.

> In plain terms, **risk management** refers to acting to reduce the likelihood of negative results, while increasing the likelihood of positive outcomes. Routine activities, such as the ones we encounter in daily life, rarely require formal risk management. Our intuitive processes are generally sufficient to anticipate and reduce our exposure to harm or loss.

The complex work of managing successful organizations, however, requires a formal approach to risk management. Organizations use physical, financial, intellectual and technological resources to achieve their goals. This creates uncertainty as organizations decide whether to pursue new opportunities or discontinue existing initiatives. Risk management considers the likelihood and consequences of each risk and considers what action, if any, should be taken to avoid or mitigate that risk.

Enterprise risk management[1] (ERM) is the coordinated, ongoing application of risk management across all parts of an organization, at all levels, from strategic planning to service delivery. An **ERM program** is the framework that an 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 as well as the effective reporting and communication of risk information throughout the organization.

The Government of B.C. has developed policy[2] and adopted an international standard[3] 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 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 that are shared across government;
> - Apply combined risk mitigation strategies;
> - Determine overarching priorities;
> - Facilitate discussion of the types and levels of risk government is prepared to accept; and
> - Make long-term plans for the future.

---

[1] Risk Management Guideline for the B.C. Public Sector, April 2019
[2] Core Policy and Procedures Manual 14: Risk Management
[3] CSA ISO 31000:2018
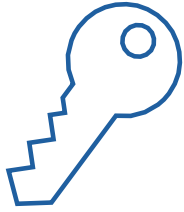
KEY MESSAGES

- *Risk is inherent in everything we do, from governing an organization to crossing the road.*
- ***Risk management*** *refers to acting to reduce the likelihood of negative results, while increasing the likelihood of positive outcomes.*
- ***ERM*** *is the coordinated, ongoing application of risk management across all parts of an organization, at all levels, from strategic planning to service delivery.*
- *The Government of B.C. has adopted an international standard to provide a structure for managing risk and implementing effective ERM programs across the B.C. public sector.*

WHAT ARE THE DIFFERENT ROLES AND RESPONSIBILITIES IN RISK MANAGEMENT?

Effective risk management is important for maintaining confidence in public institutions. Implementing an effective ERM program enables useful risk information to be communicated within your public sector organization, across the broader public sector and with external stakeholders. Since risk is the effect of uncertainty on objectives, accurate and timely communication of risk information is critical for a citizen-centred approach to governance.

> **Principles of Citizen-Centred Governance**
> 1. Put the interests of citizens at the centre of decision making.
> 2. Behave with integrity, demonstrate strong commitment to ethical values and respect the rule of law.
> 3. Ensure openness and respectful engagement with all citizens.
> 4. Strive for outcomes that support healthy communities in British Columbia, including social, economic and environmental well-being.
> 5. Implement actions to achieve the organization's mandate.

Risk management is also a key component to the four key areas of responsibility for every board in governing a public sector organization:

1. **Oversight and monitoring in the public interest:** The board is responsible for overseeing organizational performance and ensuring the activities of the organization align with the mandate. As a member or chair, how do you know what is happening with the organization? What processes are in place to monitor the impact and performance of the organization?

   Effective ERM programs help organizations anticipate and manage changes so that resources can be allocated wisely.

2. **Developing the organization's capacity and culture:** Together with the senior staff person, the board is responsible for building a common understanding of an organizational culture and philosophy that will best support your organization's mandate.

   The organization's culture determines whether risk information is communicated freely, enabling individuals at all levels of the organization to identify and manage risk appropriately.

3. **Effective leadership:** This entails ensuring that the organization's senior leadership has what it needs to succeed. It means there is a robust process for the *recruitment and selection* of the senior staff person that aligns with the current requirements of the organization, as well as ongoing *performance evaluation*, and *support* in the form of professional development opportunities, mentorship or coaching.

   Effective ERM programs identify both opportunities and threats. With this information, senior leaders can act to increase the likelihood of positive outcomes and reduce the likelihood of negative outcomes.

4. **External context and perspective:** As a diverse group of individuals, a public sector organization board can provide a variety of perspectives and insights to the work of the organization. As a board member you bring unique experiences, connections and knowledge that can inform your organization. Consider the economic, social and environmental impacts of the organization, and long-term sustainability of your work.

    a. Information and knowledge about current trends: *What external influences are relevant to your public sector organization?*
    b. Building public trust: *How can the board and the organization work to augment the relationships of the organization with key partners?*

Risk management involves asking questions such as "How do we know that this information is accurate and complete?" and "Are there other perspectives that could change our assumptions?" The process of identifying, mitigating and communicating risk information helps build public trust.
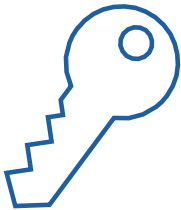
KEY MESSAGES

- *Risk management is also a key component to the four key areas of responsibility for every board.*
- *Effective ERM programs help organizations anticipate and manage changes so that resources can be allocated wisely.*

What is the board responsible for related to risk management?

As part of the board of directors, you are responsible for providing risk management oversight and determining what level and type of risks the organization is willing to accept (i.e., risk tolerance). The board is responsible for ensuring that the organization has an effective ERM program in place. Implementation of the program is largely the responsibility of the organization's senior management and staff.

Board responsibilities related to risk management include:

1. Ensuring that senior management has developed a comprehensive, organization-wide ERM program to identify, assess, and manage risks and opportunities,
2. Regularly reviewing the ERM program with senior management to understand key risks, how they are being managed, and implications for strategic and performance planning,
3. Working with senior management staff to ensure open and transparent communication and use of risk information,
4. Providing direction to senior management regarding the level and type of risk the organization is willing to accept, along with the rationale for the risk tolerance,
5. Contributing to the development of the strategic direction and approving the strategic plan with a thorough understanding of the risks that may affect the achievement of the strategic objectives,
6. Ensuring that the organization's key risks and related capacity considerations are disclosed in the strategic and performance planning documents and reports,
7. Proactively communicating key risk information with the ministry responsible and identifying what level and type of risk must be communicated,
8. Ensuring that the ERM program is evaluated periodically and is improved continuously, and
9. Ensuring that the organization has an appropriate risk financing program in place.

How do committees support the board in managing risk?

The **risk management** or **audit** committees support the board in fulfilling its risk management responsibilities. For some organizations, an audit committee will fulfill the risk management needs. However, for some medium-large sized organizations, a separate risk management committee may be deemed necessary. Regardless of the committee structure that is chosen, it is important for committees to have the necessary mandate, resources and independent expertise to fulfill its function.

The committee responsible for risk management regularly reviews the organization's risks and processes for managing risk and presents the pertinent information to the board for discussion and decisions.

While the terms of reference will vary, the committee is generally responsible for:

1. Regularly reviewing the organization's risk exposure and identifying signals that indicate problems,
2. Ensuring that the organization has appropriate systems in place to identify, assess, and manage risk,
3. Regularly reviewing the organization's internal control framework to ensure that the controls are valid and effective, and
4. Ensuring that all public reporting by the organization presents a complete, accurate and balanced picture of the organization's performance and risk exposure.

What is the role of individual directors related to risk management?

Each board member is responsible for understanding the organization's risk exposure. That means taking the time to satisfying yourself that the organization has taken the appropriate steps to manage risk.

What is the role of the senior management staff related to risk management?

The senior management staff of the organization have primary ownership and responsibility for operating an effective ERM program. It is management's job to provide leadership and direction to the employees related to risk management and to control the organization's overall risk-taking activities within the risk tolerance set by the board. Management is responsible for appropriately communicating risk information to the board and ensuring that the risk tolerance set by the board is communicated and actioned throughout the organization.

KEY MESSAGES

- *The board of directors is responsible for providing risk management oversight and determining what level and type of risks the organization is willing to accept (i.e., risk tolerance).*
- *The board is responsible for ensuring that the organization has an effective ERM program in place.*

Figure 1: The Connections Between Objectives and Risks Across the Levels of the Organizational Hierarchy

What is the role of the ministry with respect to risk management?

The ministry is responsible for following core policy and establishing a risk management framework within their ministry, which includes their associated public service organizations. The framework developed with public service organizations and their boards should complement and support the ERM framework of government and be integrated into existing ministry planning, reporting, operations and service delivery functions.

The ministry is responsible for implementing risk management strategies to address risks identified within their ministry. This includes working with their associated public service organizations to address key risks as identified and providing direction from the Minister responsible on key risks and mitigation strategies where appropriate.

WHAT DO RISK MANAGEMENT PROCESSES LOOK LIKE FOR PUBLIC SECTOR ORGANIZATIONS?

Risk management process

The B.C. public sector uses an internationally accepted eight step risk management process (CSA ISO 31000:2018) outlined in the diagram below. Three elements – *Communicate and Consult*, *Monitor and Review, and Record and Report*, occur continually throughout the process. The remainder are usually undertaken sequentially.

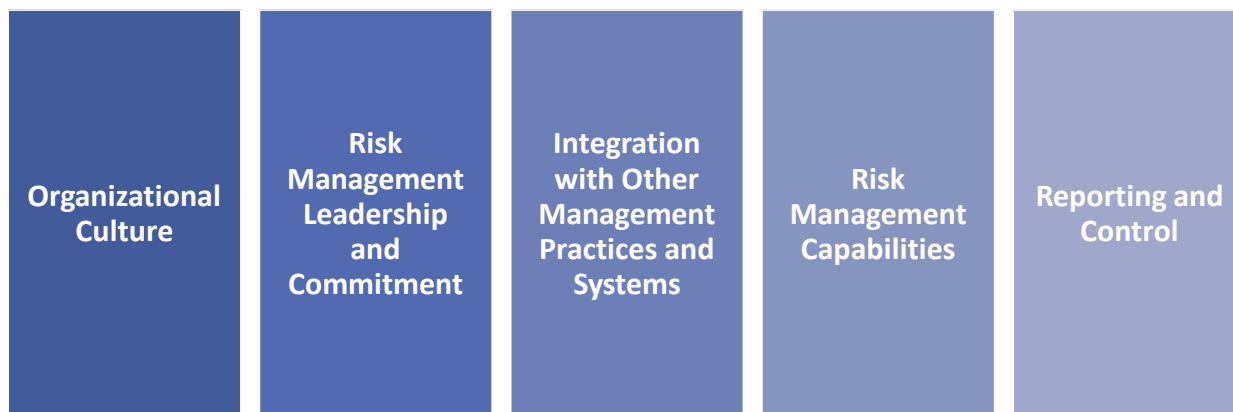**Figure 2: Adapted from CSA ISO 31000:2018 Risk Management Process[4]**

---
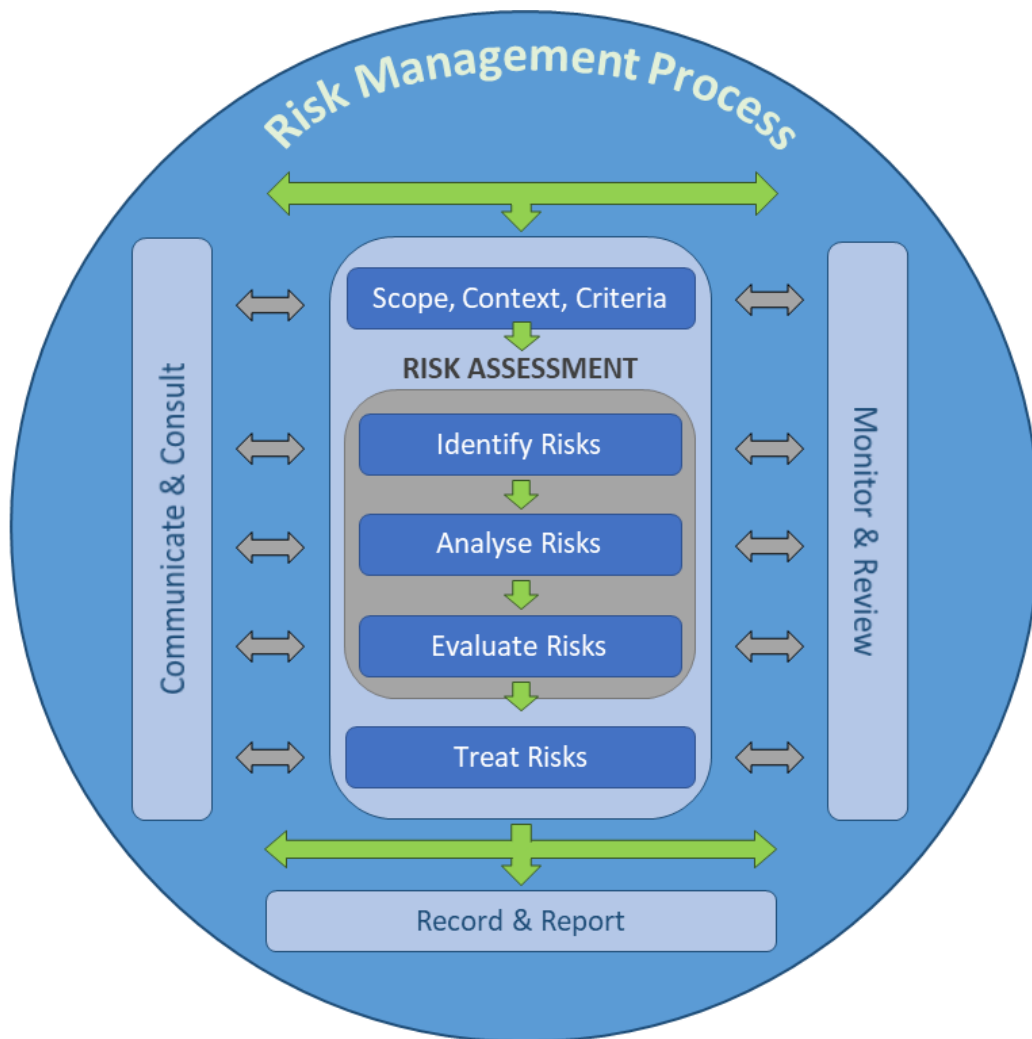
[4] Image taken from Risk Management Guideline for the B.C. Public Sector

1. **Establish the context.** Step 1 involves defining the scope and objectives for risk management. Define the situation, what you hope to accomplish, and identify who needs to be involved in the risk management process.

2. **Identify risks.** Step 2 involves determining what could occur that would have an impact on your objectives. This step involves identifying the *risk event*, or what could occur; the *risk causes,* or what could cause the risk event to happen; and *the risk impacts,* the positive and negative effects the risk event would have on your objectives.

3. **Analyze risks.** Step 3 involves ranking the *likelihood* that a risk will occur and ranking the *consequences* should it occur. Likelihood of a risk occurring is ranked from 1 – rare or improbable to 5 – almost certain. Consequences of a risk occurring are ranked from 1 – insignificant to 5 – catastrophic. The values are multiplied together to determine the risk.

4. **Evaluate risks.** Step 4 involves determining what level of risk is tolerable. This includes reviewing the effectiveness and appropriateness of current controls, asking if there is anything more that should be done, and determining what action (if any) to take.

5. **Treat risks.** Step 5 refers to the actions you are going to take to reduce the likelihood or consequence of something negative occurring. Generally, the costs of avoiding or mitigating a potential risk will not outweigh the potential loss.

6. **Communicate and consult.** It is important to keep key stakeholders informed throughout the process and to consult with affected groups. Step 6 ensures that risks are communicated up to higher levels in the organization and that the risk tolerances determined by the board are communicated to the rest of the organization.

7. **Monitor and review.** Regular review allows for progress in risk treatment to be monitored and new or emerging risks to be identified.

8. **Record and report.** The risk management process and its outcomes should be documented and regularly reported through appropriate communication mechanisms to support organizational decision-making.

Five pillars of risk maturity

The B.C. government's risk maturity model[5] helps government ministries and public sector organizations assess their risk management maturity and determine opportunities for growth and improvement to their ERM program. The board provides direction to the public sector organization on what risk maturity priorities should be focused on.

The risk maturity model includes five pillars:

Organizational Culture	Risk Management Leadership and Commitment	Integration with Other Management Practices and Systems	Risk Management Capabilities	Reporting and Control

Pillar 1: Organizational Culture

An optimal organizational culture for ERM is one where people are proactively encouraged for their contributions to risk management and where risk management is practiced regularly at every level of the organization. When this is achieved, an organization is more likely to identify and mitigate or manage risks.

Pillar 2: Risk Management Leadership and Commitment

Optimized ERM leadership and commitment are achieved when the leadership for risk management is embedded at all levels of the organization, an operational risk policy is in place and senior management have assumed a leadership role for implementing ERM.

Pillar 3: Integration with Other Management Practices and Systems

Optimal integration of ERM and management practices in an organization is achieved by using financial and non-financial information to assess risks; putting risk measures in place and monitoring them over time; providing online access to management information and tools; making internal best practices readily and easily shared; and working to gain stakeholders' respect for the organization's risk management practices.

---

[5] B.C. Government's Risk Maturity Model, 2018

Pillar 4: Risk Management Capabilities

Optimal risk management capabilities require an organization to commit to continually renewing ERM competencies among staff, working to integrate ERM tools throughout the organization and maintaining good access to ERM specialists.

Pillar 5: Reporting and Control

Optimal ERM in an organization uses state-of-the-art methodologies for environmental scanning, ensures that its control environment integrates risk management and measures and tracks its risk management performance over time.
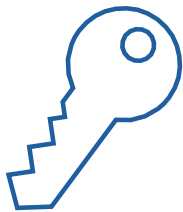
KEY MESSAGES

- *The B.C. public sector uses an internationally accepted eight step risk management process.*
- *The risk maturity model can help your organization assess risk management maturity and determine opportunities for growth and improvement to your ERM program.*

What does this mean for you?

Risk is the effect of uncertainty on objectives. As a board member, one of your key risk management responsibilities is to be curious and to ask questions. Some questions you might ask:

1. *Do you have the right information? Is the information accurate and complete? How do you know?*
2. *Are there other perspectives you should be considering?*
3. *Are your risk treatment strategies effective? Are there other strategies that might be more effective?*
4. *Is your organization allocating resources wisely and fairly?*

The board, as a whole (and sometimes in conjunction with the ministry), determines your organization's risk tolerance. As a board member, you want to satisfy yourself that your organization is doing enough to identify and manage risk. Managing risk can be expensive; therefore, you might also want to ask if your organization is doing too much to manage risk.

All public sector organizations are responsible for implementing an ERM program. As a board member, you should be familiar with your organization's ERM program: who does what, when, and how? One of the board's responsibilities is proactively communicating risk information with the minister. What information does your board need to communicate, and who is responsible for doing so?

ADDITIONAL RESOURCES

RM 100 Risk Management: Everyone is a Risk Manager, e-Learning course through the B.C. Government's Learning Centre

> link: https://gww.gov.bc.ca/groups/learning-bc-public-service/rm-100-risk-management-everyone-risk-manager (restricted access). For access to this document please contact Risk Management Branch.

Risk Management Guideline for the B.C. Public Sector

> link: https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/internal-corporate-services/risk-management/risk-management-guideline.pdf

Crown Agency Risk Management and Internal Controls: A Good Practices Checklist

> link: https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/public-sector-management/crown_agency_risk_management.pdf

Risk Maturity Model

> link: http://gww.fin.gov.bc.ca/gws/pt/rmb/ref/rrRiskMaturityTemplate.docx (restricted access). For access to this document please contact Risk Management Branch.

CSA ISO 31000:2018

> link: http://gww.fin.gov.bc.ca/gws/pt/rmb/iso31000tou.asp (restricted access). For access to this document please contact Risk Management Branch.

Core Policies and Procedures Manual, Chapter 14: Risk Management

> link: https://www2.gov.bc.ca/gov/content/governments/policies-for-government/core-policy/policies/risk-management

CONTACT RISK MANAGEMENT BRANCH AND GOVERNMENT SECURITY OFFICE

Ministry of Finance
3rd Floor, 617 Government Street, Victoria, BC
RMB@gov.bc.ca
(250) 356-1794

Internet: https://www2.gov.bc.ca/gov/content/governments/services-for-government/internal-corporate-services/risk-management

Intranet (Restricted access): http://gww.fin.gov.bc.ca/gws/pt/rmb/index.stm

Crown Agencies and Board Resourcing Office (CABRO)

tinyurl.com/BoardsofBC