CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Enterprise Risk Management

A PRACTICAL APPROACH TO MANAGING RISKS FOR SMALL- TO MEDIUM-SIZE ORGANIZATIONS

Bill Wesioly and Guenther Moeller

What is the issue?
According to a 2018 survey,[1] almost half of small- to medium-sized organizations do not have any kind of enterprise risk management (ERM) program in place.
These organizations operate in complex, demanding and ever-changing environments. To reduce unexpected major losses and achieve their objectives, they continually need to make informed, timely decisions about strategy and operations. Sound, holistic risk management practices can help.

Why is it important?
Practical, strategically-integrated risk management that meets operational needs can help small- to medium-sized organizations – including not-for-profits – achieve their objectives, increase value for stakeholders, and meet governance and compliance requirements.

What can be done?
This MAG® provides guidance to help you address internal and external dynamics (and associated risks) that impact your strategic objectives and day-to-day operations. You will learn to implement explicit, structured and integrated risk management practices; satisfy internal control needs; and create a risk culture that supports strong decision-making.
Many organizations institute a risk management program only after a negative event (e.g., loss of a key customer, large regulatory fine or major lawsuit). This MAG will help you anticipate and respond sooner to potential events, and then better manage and minimize their impacts.

Who is this guideline for and how can it be applied?
This guideline is for you if you are responsible for setting and achieving an organization's objectives, which often also means managing related risks (roles often filled by CPAs in small- to medium-sized organizations):

- board members with oversight of risk management
- senior leaders charged with strategy-setting and decision-making (e.g., CFOs, CEOs, chief auditors)
- line managers and other operations employees

This MAG defines a small- to medium-sized organization as having fewer than 100 employees; but this approach can also apply in some larger settings, and across industries and sectors.

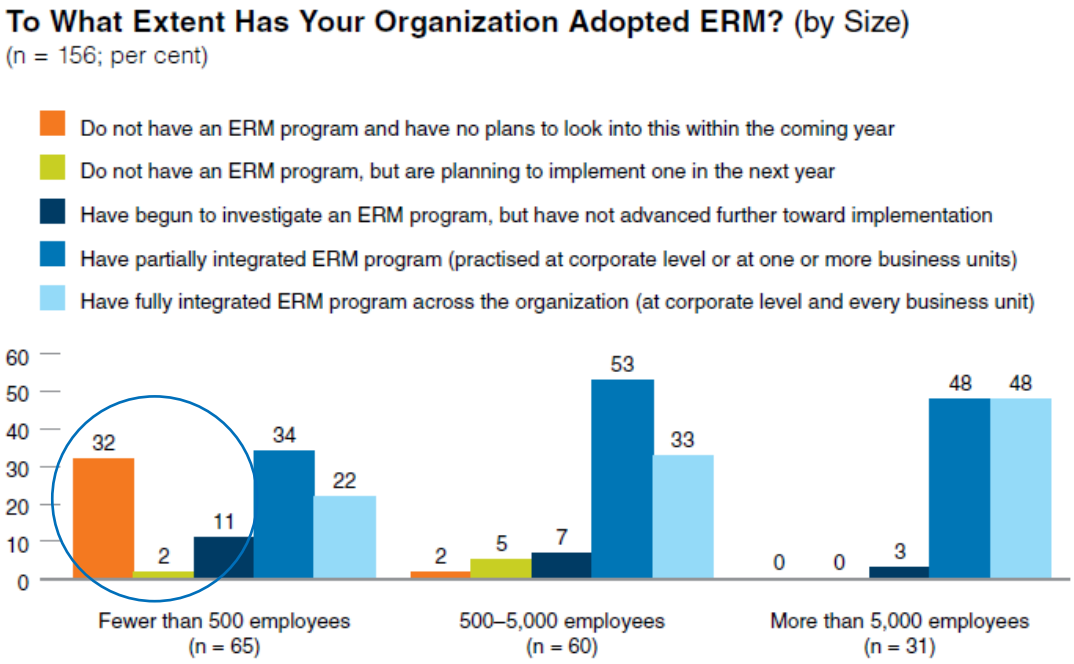
1 ***The State of ERM in Canada. A Benchmarking Study*** (2018) is a collaboration by the Conference Board of Canada, Chartered Professional Accountants of Canada, and the Global Risk Institute in Financial Services.

Overview

How emerging trends impact your organization

According to a 2018 Canadian survey, almost 50 per cent of small- to medium-sized organizations do not have a risk management or ERM program in place[2]; the survey defined this as a program that provides a structured approach to managing operational and strategic risks holistically and links risks with strategic and operational objectives (Figure 1).

FIGURE 1 – TO WHAT EXTENT HAS YOUR ORGANIZATION ADOPTED ERM?



This is striking, especially in the context of recent headlines that demonstrate the significant financial and reputational implications for the organizations involved. A few examples:

- City defrauded out of $503,000 due to phishing scam
- More charges laid in assaults at a private school after cell phone video goes viral
- Provincial government foundation $15M cut to make 'significant difference' to non-profit organizations, charities

Many organizations attempt to implement a risk management program after a negative event has occurred. This MAG will help readers provide a disciplined and holistic approach to managing the many current and emerging risks in their organizations.

2 *The State of ERM in Canada. A Benchmarking Study* (2018) is a collaboration by the Conference Board of Canada, Chartered Professional Accountants of Canada, and the Global Risk Institute in Financial Services.

The 2019 global pandemic has put business continuity to the test. The pandemic has been a significant risk event that required organizations to take immediate actions to manage risks impacting their people, operations and financial sustainability. These actions included testing business continuity plans, emergency management systems and disaster preparedness (Refer to Section 6.2, Worst Case Scenario Exercises). During these unprecedented times of uncertainty, constant change and business disruption, an organization's long-term viability hinges on its ability to:

- be resilient in the face of uncertainty
- adapt business practices to competing market pressures
- continuously innovate fresh and novel concepts to create long-term, sustainable value

CPA Canada's RAISE philosophy[3] was developed to help guide organizations to assess their level of resilience, adaptability and capacity to innovate in response to change to achieve continuity and sustainability. Implementing sound risk management strategies and practices supports this philosophy.

Taking a risk can also generate returns and value. This is the opportunity side of risk management. However, for the purposes of this MAG, the focus will be on mitigating the negative impacts of risk. For organizations that already have a mature ERM program and are moving toward a risk-optimized / opportunity mindset, refer to MAG® entitled *The CAM-I Risk-Value Curve: Understanding Your Risk Appetite to Create Value*.

Risk management overview

What is risk?

The word risk originates from the mid-17th century, from the Italian word *risco* and the French word *risqué*. Both roughly translate into the term *danger*.

For this MAG®, COSO's 2017 Enterprise Risk Management Guideline's definition of risk is used: "the possibility that events will occur and affect the achievement of strategy and business objectives."

Risk is measured in terms of the impact or consequence of a negative event occurring as well as the likelihood of that event occurring. These two dimensions are fundamental when assessing and responding to risks, because organizations should focus on the risks that have higher impacts and higher likelihoods. These are the critical risks.

3 CPA Canada, *RESILIENT + ADAPTABLE + INNOVATIVE = Sustainable Enterprises. A New Mindset to RAISE the Bar.* (2020 – coming soon)

What is enterprise risk management?

The study of risk management (RM) has been around since the end of World War II.[4] Organizations have always managed risks, though sometimes they have done so subconsciously, implicitly, or inconsistently.

Enterprise Risk Management (ERM) simply organizes risk management practices into a framework that enables organizations to manage risks in a more cohesive and coordinated manner.

Understanding the *E* in ERM is important. ERM is not just a financial risk view or an IT risk view, but also an enterprise- or organization-wide view of risk management. It involves all staff and all areas and processes of the organization, and it focuses on all critical risks. It is not ad hoc or one-off risk management.

This approach may seem overwhelming for smaller organizations, but it doesn't have to be. When smaller organizations plan and review their strategies and overall objectives, and as they operate daily, they can use the same risk management lens that larger organizations use. Indeed, small- to medium-sized organizations have the benefit of leveraging existing operational practices, lower coordination costs and more efficient internal communications networks when developing or enhancing risk management capabilities.

> "Enterprise Risk Management starts with a simple question: what are the major risks that can stop us from achieving our mission? The whole point is that you want to look at the big risks. And if you can build that into your culture, you can have a much more robust capacity to understand the vulnerabilities that you would otherwise run into without appreciating them."
>
> *Enterprise Risk Management - Thomas Stanton, Johns Hopkins University (Ted Talk, March 2017)*

For simplicity and consistency, this MAG will refer to the term "risk management," but note that the underlying discipline and fundamentals of enterprise risk management apply in all cases discussed here.

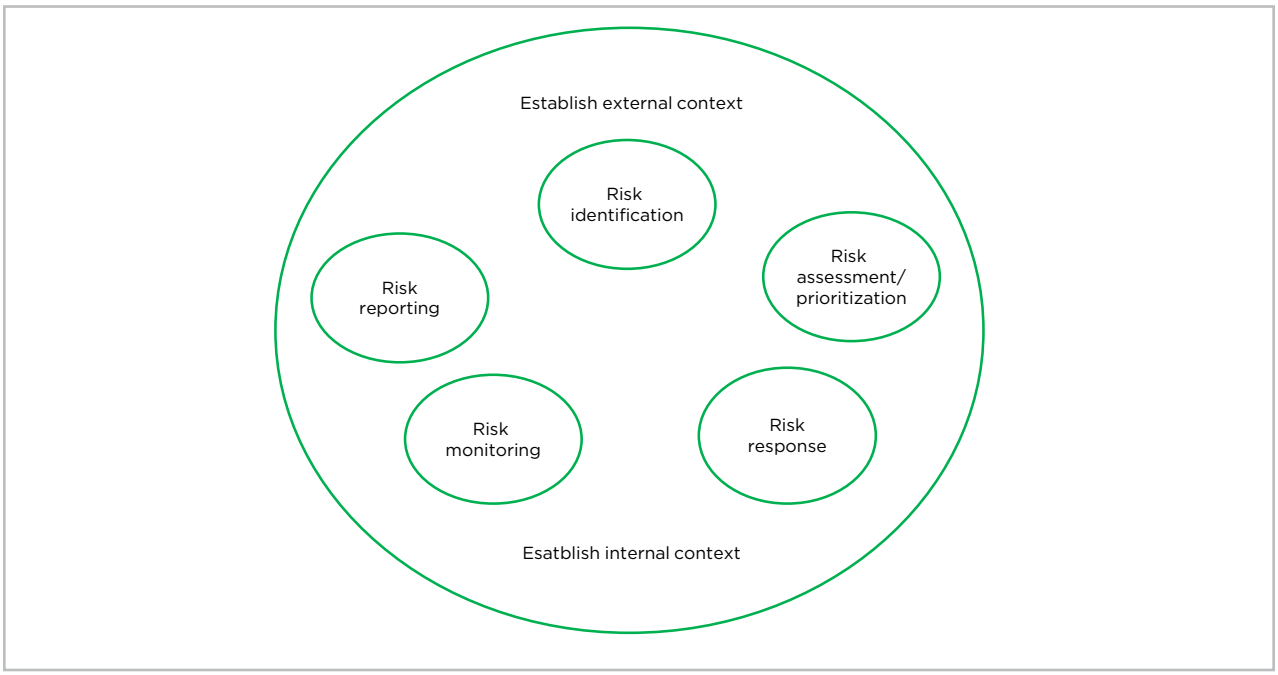
What are the basics of risk management?

As noted, organizations have always managed risks, but organizing and enhancing their risk management practices enables them to address those risks more and efficiently and effectively. Figure 2 illustrates a simple and practical way to conceptualize and organize such practices.[5]

4 Dionne Georges, "Risk Management: History, Definition and Critique." *Risk Management and Insurance Review.* (Wiley, 2013).

5 This framework aligns with the 2017 COSO guideline, *Enterprise Risk Management – Integrating with Strategy and Performance* (2017; an update to *Enterprise Risk Management – Integrated Framework*), and with the 2018 ISO 31000 Guideline.

FIGURE 2 – RISK MANAGEMENT FRAMEWORK



The components of the risk management framework in Figure 2 are defined as follows:

Establish external and internal context – Understand the environment within which the organization operates, along with external dynamics (e.g., regulatory compliance requirements, customer and stakeholder expectations, competitor and economic pressures) and internal dynamics (e.g., governance structure, culture, strategic objectives).

Risk identification – Understand all the risks that could impact the organization and could prevent it from achieving its strategic and operational objectives.

Risk assessment/prioritization – Determine the criticality of the identified risks by estimating the impact and likelihood of those risks occurring

Risk response – Determine the appropriate responses to critical risks using the CAAT approach:

- **C**ontrol the risk to minimize its impact or likelihood, or
- **A**ccept the risk, or
- **A**void the risk by not pursuing the underlying objectives, or
- **T**ransfer the risk (e.g., with insurance)

Risk monitoring – Review critical risks on an ongoing basis using key risk indicators (KRIs) to ensure that they do not increase to unacceptable levels and that the controls are working as expected. Also review the changing environment for any emerging risks.

Risk reporting – Communicate all relevant risk information (including the organization's risk profile) to all key stakeholders in a timely manner.

Process

There are six steps to effectively implementing (or enhancing) a risk management program. The timeline for implementing the program can generally vary from one to three years, depending on the organization's existing risk management practices, risk culture, and size and complexity.

These steps do not have to be followed sequentially. In fact, there may be times when an organization's risk management champion can carry out two or three of these steps concurrently.

Step 1

Engage the board and/or senior management – For the risk management program to be successful, it is imperative that the board of directors and/or senior management understand its value and are committed to it.

Step 2

Establish risk governance elements – As with any organizational function, it is important to provide some internal guidelines for managing risks. Formalizing a risk appetite, risk policy and risk responsibilities provides such guidance.

Step 3

Conduct a risk and control assessment with the board and/or senior management – Management must understand the organization's critical risks and manage them appropriately.

Step 4

Engage the staff – Since "risk is everybody's business," it is important that all staff understand risks. Communicating risk priorities and obtaining feedback is essential to managing risks appropriately.

Step 5

Enhance the value of risk management – Once fundamental practices have been established or enhanced, organizations should continue monitoring risks and consider additional monitoring and reporting steps.

Step 6

Embed risk management practices – The true value of risk management is that it keeps members of the organization engaged in key operational and strategy decisions. Aligning risk management with planning and strategy achieves this.

Guiding Principles

The following guiding principles help ensure the success of the six implementation steps:

- Start the conversation at the "top of the house" with the board, senior management and other key decision-makers to facilitate buy-in. Ensure these parties are seen as visible sponsors.
- Leverage existing practices, policies and documentation from other departments within the organization (including internal audit, legal, compliance).
- Communicate the benefits and expected outcomes of an organization-wide risk management program. Providing context (articulating how risk management affects the day-to-day work of employees) helps get employees on board.
- Look for initial change agents within the organization and leverage their enthusiasm and internal connections to build trust and collaborative relationships throughout the organization.
- Appoint a risk management champion who has the confidence of the board and senior management.
  - In a smaller organization, this role is often filled by the CFO, the CEO or the owner.
  - In NFPOs, this role would often be filled by the executive director.
  - In a medium-sized organization, consider the following areas when appointing a risk management champion:
    - Finance or CFO – This function often has an excellent internal and external oversight focus and a good understanding of internal controls and governance issues.
    - Business planning or strategy – This function (if applicable) already has responsibility for business planning and can support a more strategic approach to risk management.
    - Internal auditor or chief auditor – This function is used by some organizations to incubate risk management practices, given its expertise in governance and its understanding of the organization's systems, operational processes, risks and internal controls. After incubation, the risk management function would move to the most suitable corporate area.

Managing risks in your organization – The risk management implementation process

Step 1: Engage the board and/or senior management

The first step to implementing a risk management program is obtaining buy-in and ongoing commitment for the program from the board and/or senior management.

Note: Not all organizations are structured to have a board of directors, a CEO or senior management. The terms "board" and "senior management" in this MAG refer to the function within an organization that is responsible for significant organizational and strategic decisions and oversees risk.

1.1 Deliver risk education 101

In most cases, the board and/or senior management do not share a consistent understanding of risks facing the organization and strategies to manage risks. It is imperative to get everyone on the same page. Providing an introductory "Risk Management 101" session that involves an interactive discussion ensures that all parties have a solid understanding of risk management practices.

Topics to review and discuss in this session should include:

- the definitions of risk and risk management (i.e., what each of these mean to the organization)
- the benefits of an enterprise risk management program
- current and relevant examples of risks and their subsequent impacts related to the organization's specific industry or service sector
- generally-established risk management practices and how they are organized into a framework
- a risk "heat map" and how it ties together various risk management steps within the framework (see Section 3.4 for a detailed description of a risk heat map)
- the risk responsibilities and governance expectations of the board, line management and staff

Real-life example for introducing a risk management awareness session to the board and making it fun and interactive:

After discussing the components of the risk management framework, all participants who were asked to select a partner received hard copies of a risk heat map. Each group is asked:

- If you were going on a hike, what risks are there and how would you plot them on a heat map?
- If you were looking at implementing additional controls for each risk, what would the risk then look like on a heat map?
- How much risk is acceptable and what are the unacceptable risks?

A lot of good interaction occurred. A debrief amongst the larger group helped ensure that participants understood the concepts of impact and likelihood, how risks compared to one another and how implementing additional controls impacted the original inherent risk rating.

1.2 Obtain commitment from the board and/or senior management

At the end of the education session, it is critical to secure the board's commitment to the risk management program. Participants should come away from the session with a basic understanding of risk management concepts and practices. Next steps should include assurance that risk management will be part of the board's agenda. It is imperative that risk management remains on the board's agenda throughout the implementation of a risk management program and as operations move back into their steady state.

Step 2 – Establish risk governance elements

It may seem early in the implementation of a risk management program, but establishing governance elements like a risk appetite, a risk policy and risk responsibilities now will provide a foundation for the rest of the process later. These risk governance elements can be revisited and fleshed out throughout implementation.

2.1 Determine a Risk Appetite

"The key is to make informed and intelligent decisions that take the right level of the right risk, where it is justified on business and other grounds. Decision-makers need guidance so that they know what they are doing (taking risk) is consistent with the desires of top management and the board."

Norman Marks on Governance – Risk Management and Audit – March 2018

A risk appetite statement defines how much risk an organization is willing to accept when pursuing objectives: "Defining a risk appetite means assessing all the possible risks facing an organization, establishing the boundaries for acceptable and non-acceptable incidents, and creating the necessary controls that these limits require."[6]

Think about this concept as it applies to a financial investment: You can invest in a risky proposition (with the potential for a big payout or a big loss); or you can invest in a safe proposition (with a lower rate of return but little-to-no risk of losing your money). Which investment you choose to make is determined by your appetite for risk.

Risk appetite statements provide even more value when integrated with risk tolerances. Risk tolerances provide the thresholds and limits for taking on risk; they allow organizations to better monitor risks. Organizations will be alerted about any activity or event that breaches (or comes close to breaching) a risk tolerance threshold.

The following questions can help start an organization's risk appetite discussions:

- Which activities are absolutely unacceptable and must be avoided?
- What could irreparably harm our reputation?
- What would our customers, suppliers, regulators and other stakeholders consider too risky to take on?
- How much money are we prepared to lose relative to how much return we expect to make?
- Which objective, risk or business area would have a higher or lower risk appetite than another?

Risk appetite statements vary by organization, but the examples in Table 1 provide a guideline.

TABLE 1 – EXAMPLES OF RISK APPETITE STATEMENTS

Industry or sector	Examples of risk appetite statements
Credit unions and other financial services[7]	The X Credit Union has minimal desire to accept any material concentration of risk in a particular industry segment. Risk tolerance is rated as "low." The X Credit Union has a slightly higher tolerance with respect to borrower default for commercial loans. Risk tolerance is rated as "modest." The X Credit Union is unwilling to have a significant system outage. Risk tolerance is rated as "low."
Health care organization[8]	X organization will strive to treat all emergency room patients within two hours and critically ill patients within 15 minutes. However, management accepts that in rare situations (five per cent of the time), patients in need of non-life-threatening attention may not receive that attention for up to four hours.

6 Ariane Chapelle, *Operational Risk Management – Best Practices in the Financial Services Industry.* (Wiley & Sons: 2018)

7 Deposit Insurance Corporation of Ontario, ***Enterprise Risk Management – Application Guide***. (January 2018).

8 COSO Enterprise Risk Management, *Understanding and Communicating Risk Appetite.* (Rittenberg and Martens: 2012).

Industry or sector	Examples of risk appetite statements
Not-for-profits[9]	For X organization, endowment funds balance safety and possible low investment returns against the potential for higher income but higher risk. For X organization that operates in war-torn regions, it recognizes that it puts staff and volunteers at a higher risk than would be acceptable in their home countries, and the organization takes steps to minimize the risks.

2.2 Create a risk management policy

A risk management policy will provide guidance for developing and implementing risk management practices throughout the organization. The policy and its structure will vary from organization to organization depending on the nature of the business and its assets.

The following basic components should be included:

- purpose or objectives of the policy
- definitions of risk and of risk management
- types of broad risks or risk categories impacting the organization
- overview of risk management practices and framework components
- roles and responsibilities for managing risks (including those for the board and any committees)
- references to other related policies and/or standards

The risk management policy should serve as the overarching "umbrella" policy for the organization's other risk-related policies and standards (e.g., business continuity management, information security).

2.3 Outline risk management responsibilities

Outlining risk management responsibilities helps ensure that accountabilities are understood by all executives and staff. At a minimum, responsibilities should be defined for the following:

- The board – for its risk management oversight role. Both the latest ISO[10] and COSO ERM standards emphasize the increasing pressure for boards to recognize and fulfill this oversight role.
- Risk committees – for their oversight roles, if such a committee exists.
- Senior management – for their risk strategy and management roles.
- Line managers and staff – for their roles in executing the approved risk management practices and risk responses (e.g., internal controls) and for providing practical input at times of review.

9 Hugh Lindsay, *20 Questions Directors of Not for Profit Organizations Should Ask About Risk*. (2009).

10 *ISO 31000, Risk management – Guidelines*, provides principles, a framework and a process for managing risk. (2018).

Smaller organizations and NFPOs may not have this detailed set-up, but there should be a distinction between oversight and management roles.

Real-life example of establishing a risk committee within a risk management (RM) framework in a small- to medium-sized organization:

An independent school went through several steps in the beginning of its RM journey. After kicking off with a Risk Management 101 session that included an initial risk assessment of the school's critical risks, a decision was made to establish a risk advisory committee (RAC).

Members of the board and management team were selected to be part of the RAC. In an early meeting, the RAC tabled and approved a committee mandate. Next, the committee met to review critical risks from management's existing risk register. Soon, a risk appetite was developed. A summary of the key RM components and decisions was then taken forward to a full board meeting. At this time, the RAC is still in its infancy, but it is starting to add value.

Step 3 – Conduct a risk and control assessment with the board and/or senior management

After obtaining the board's commitment and developing key governance elements, the organization is ready to conduct a risk and control assessment with the board and/or senior management. This high-level task involves several practices outlined in the risk management framework (Figure 2): Identify risks, evaluate and prioritize their size or materiality, and determine the appropriate response.

To prepare for this, it is beneficial to draft a list of organizational objectives, critical risks and existing internal control programs. Listing organizational objectives, risks and internal control programs may involve external research.

Table 2 provides base guidance questions on conducting a risk and control assessment.

TABLE 2 – RISK DISCUSSION GUIDANCE QUESTIONS

Risk component	Guidance questions
Establish external and internal context	What is the internal and external context for our organization?
Identify risks	What are our strategic objectives? What risks can impact us and prevent us from achieving our strategic objectives?
Assess / prioritize risks	Of the risks that can impact us, which are the most critical?

Risk component	Guidance questions
Respond to risks	What are we doing to manage these critical risks? What else should we be doing?

Responses to these questions can be summarized on a risk heat map, providing a real-time visual overview of critical risks.

What follows is further detail on each of the Table 2 risk components.

3.1 Establish external and internal context

The objective of this step is to ensure that the board and/or senior management fully understands the external and internal drivers that determine the nature of the risks the organization will have to manage.

The "PESTEL" model can help an organization analyze and understand its macro environmental factors, or its external context. It summarizes the external factors that can impact an organization: **p**olitical, **e**conomic, **s**ocial, **t**echnological, **e**nvironmental and **l**egal.

The internal driver categories that can be used to establish an organization's internal context are governance, capital, people, processes and technology.

Understanding external and internal drivers can also help an organization refine its risk governance elements (i.e., risk appetite, risk management policy and risk responsibilities).

3.2 Identify risks

Once the organization establishes its internal and external context, it is ready to discuss its risks.

The objective of identifying risks is to identify and understand all the actual or potential risks that could impact the organization and could prevent it from achieving its strategic and operational objectives.

The starting point is understanding and stating the objectives before identifying risks. Properly determining risks is difficult if participants do not share a consensus or understanding of the organization's objectives.

Using the guidance questions in Table 2 along with the following examples of typical risks facing small- to medium-sized organizations (Table 3) can help the group develop a preliminary list of risks.

TABLE 3 – EXAMPLES OF RISKS AND EVENTS

Industry or sector	Types of risks
Non-industry specific small- to medium-sized organizations[11,12]	• Risks posed by customers, competitors, suppliers, or staff • Risks posed by business premises, location, or information technology • Risks posed by financial transactions, the market, or economy • Unexpected exit of a business partner or key employee • Threats to goodwill and reputation
Credit unions[13]	• Strategic risk: strategy implementation, depositor demographics, competition • Credit risk: default, concentration of lenders • Financial risk: liquidity, capital management • Operational risk: information technology, information security, outsourcing, fraud, personnel, cyber threats • Compliance risk: regulatory (e.g., money laundering)
Manufacturing[14]	• Supply chain delays and third-party vendors • Errors and omissions or defective parts • Equipment malfunctions • Cyber threats
Not-for-profits[15]	• Loss of a major source of funding, unsuccessful fundraising projects • Reduction in market value of investments, internal or external fraud • Failure of a project or strategic initiative • Irrelevance because programs or services are no longer in demand or distinctive • Reputation (e.g., actual or alleged misconduct by an employee or volunteer)

11 CPA Australia, *Risk Management Guide to Small and Medium Sized Businesses*. (2009).

12 Other risks may include: cashflow and insolvency risk, family business succession risk, protection of intellectual property, cyberattacks, fraud, supply chain and sustainability risk, and tax risk (Accountancy Europe Briefing Paper VIEWS, *SME Risk Management. How can your accountant help?*).

13 Deposit Insurance Corporation of Ontario, *Enterprise Risk Management – Application Guide*. (January 2018).

14 Northbridge Insurance, *Hidden risks that can damage your manufacturing business*. (July 2017).

15 Hugh Lindsay, *20 Questions Directors of Not for Profit Organizations Should Ask About Risk*. (2009).

3.3 Assess and prioritize the criticality of the risks

Not all risks can or should be fully mitigated once they have been identified. Organizations must choose carefully in allocating resources so that the investment of resources is justified by the improved outcome. Risks should therefore be categorized by size or significance to ensure they receive the appropriate level of coverage and oversight. This optimizes the value of risk management to the organization.

To assess and prioritize significant risks, organizations estimate the impacts and likelihoods of those risks occurring.

The impact of an event occurring can be defined not only in financial terms but also in regulatory and reputational terms. Table 4 provides an example of an impact rating scale.

TABLE 4 – GUIDANCE EXAMPLES OF EVENT IMPACT LEVELS

Rating	Financial impact	Regulatory impact	Reputational impact
Extreme	Loss of annual revenues or funding > 20 per cent	Loss of regulatory licence to operate	Long-term negative media coverage, game-changing loss of market share
Major	Loss of annual revenues or funding of 10 – 20 per cent	Major regulatory imposed fines	Significant negative media coverage, large impact to market share
Moderate	Loss of annual revenues or funding of 5 – 10 per cent	Regulatory formal written warning	Small, short-lived media coverage
Minor	Loss of annual revenues or funding of 5 per cent	Regulatory verbal warning	Minor media coverage

The *likelihood* of an event occurring is generally defined in terms of its probability and frequency of occurrence. Evaluating likelihood is, to a degree, a qualitative judgment and can be based on past experiences or on events experienced by similar organizations. The timeframe can vary depending on the organization or industry (10 years is a base timeframe). Table 5 provides an example of a likelihood rating scale.

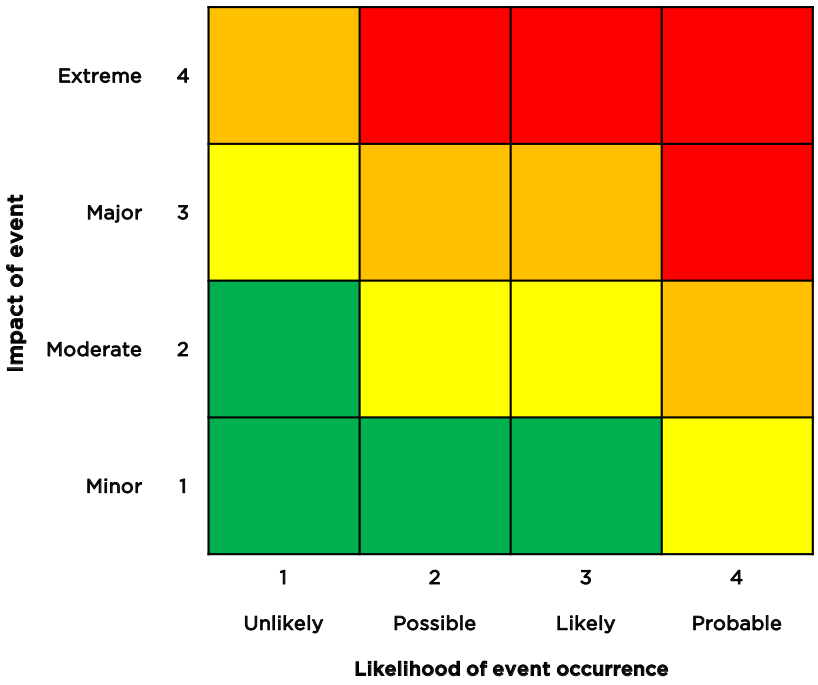
TABLE 5 – GUIDANCE EXAMPLES OF EVENT LIKELIHOOD LEVELS

Rating	Probability of occurrence	Frequency of occurrence
Probable	> 66 per cent in one year	An event will likely happen once or more in the coming year
Likely	> 33 to 66 per cent in one year	An event may happen once in the next one to five years
Possible	5 to 33 per cent in one year	An event may happen once in the next five to ten years
Unlikely	< 5 per cent in one year	An event is rare, and may occur in the next ten years or more

3.4 Plot the assessments on a risk heat map

Once organizations determine the impacts and likelihoods of risks, they can plot them on a risk heat map. A risk heat map illustrates the areas where each risk's impact and likelihood intersect (see sample in Figure 3). It is a powerful tool that provides the board and/or senior management with a visual risk rating for each risk the organization has identified.

FIGURE 3 – SAMPLE RISK HEAT MAP



Each risk's impact and likelihood rating will determine which cell the risk falls into on the heat map. Each cell is coloured (green, yellow, orange, or red) to represent how that particular intersection of impact and likelihood relates to the organization's risk appetite. Risks that fall into the green zone are considered low risk and just need to be monitored. Moving up the grid, risks that appear in a yellow or orange cell are more critical and should be carefully assessed to determine the most appropriate risk response. Risks in the red zone indicate a breach of the organization's risk appetite and must be addressed immediately.

Note that some organizations use a 5 x 5 grid for the heat map, which can be just as effective. As well, colours of some cells can vary, which is at the discretion of the organization.

3.5 Respond to the critical risks

With the risk heat map in place, the organization is ready to determine how best to respond to its critical risks and ensure the response falls within the organization's risk appetite. One possible response is to mitigate the risk with an appropriate form of control. Other common response options include avoiding the risk, accepting the risk or transferring the risk (e.g., via insurance).

If a risk is close to breaching or does breach the risk appetite, the organization should implement one or more of these responses until the residual risk level of a specific risk is deemed to fall within the risk appetite. Risk responses should be continuously monitored (and evaluated on their effectiveness) to ensure that risks are treated appropriately.

The estimated results of the responses can be plotted onto the risk heat map, which should show the risk level coming down from its original rating.

3.6 Use a risk register to document risk information

When identifying, rating and responding to risks, documenting risk information in a risk register preserves it for future monitoring and reporting.

The risk register can be used to summarize organizational objectives, identified risks, risk ratings and appropriate internal controls and action plans for critical risks. A risk register can be set up using a simple spreadsheet, as in Table 6.

TABLE 6 – SAMPLE RISK REGISTER

Risk	Risk category	Subcategory	Risk description	Inherent risk*			Risk response	Control program	Residual risk**			Further actions		
				Impact rating	Likelihood rating	Inherent risk rating			Impact rating	Likelihood rating	Residual risk rating	Specific action	Res'b'ty	Time-frame
1	Operational	IT Risk	Cyber hack	Extreme	Likely	Critical	Mitigate	ISO IT standards	Major	Possible	Major	• Look at innovative IT security practices such as the "honey pot"		
2	Strategic	Outsourcing	Misplaced third-party arrangements with AML information	Major	Likely	Major	Mitigate	Implement DICO AML standards	Moderate	Likely	Moderate	• Arrange for third-party audits • Review confidential information to determine if some can be held back		
3	Operational	Depositor satisfaction	Poor customer satisfaction	Major	Likely	Major	Mitigate	Work at "Always know your customers" (AYKC)	Major	Possible	Major	• Continuously review strategy, competitor's stragey • Focus on specific market niches		
4	Operational	Personnel	Top talent leaving	Major	Likely	Major	Mitigate	HR Attract and Retain program	Moderate	Possible	Moderate	• Develop a pipeline of qualified candidates • Implement new cross training initiatives		

*Inherent risk is the current level of risk in the absence of a risk response.

**Residual risk is the level of risk remaning after management's risk response.

Step 4 – Engage the staff

> "You have to ask the question: Who is saying these are the major risks and what is their natural bias or perspective? Unless you have a cross section throughout the organizational hierarchy of a large organization as opposed to merely a survey of senior management, then you're not going to have a good understanding of the true risks the organization faces."
>
> *Robert McFarlane - Corporate Director and former EVP and CFO, TELUS*[16]

After the discussions and risk assessments amongst the board and/or senior management, the task is to now take the risk management discussions to the rest of the organization. The objective is to build awareness of risk management practices, to gather the unique perspectives of all staff and to facilitate buy-in.

4.1 Build awareness and engagement in the organization

For many small- to medium-sized organizations, there should be several opportunities to conduct risk assessments at lower levels of the organization and to create additional departmental risk registers.

These lower level risk assessments may disclose additional risks that were not considered at the board or senior management level, which is understandable since the board and senior management view risk from a higher or strategic level. Operational areas, on the other hand, view risks from a practical day-to-day level. Both views are vital for providing a complete organizational risk profile.

Some organizations may initially state that there is no need for risk assessments at lower levels. That sentiment may be correct. However, there may be some important information related to risks that could be missed at a lower level, and morale could be negatively impacted as important ideas and voices would be excluded from contributing.

In creating awareness and engagement throughout the organization, it is important to build trust with all staff. Understanding and embracing the human impact of this process is essential and can be done by applying some basic change management practices.[17]

16 CPA Canada, *The State of Enterprise Risk Management in Canada*. (2016)

17 Refer to these Management Accounting Guidelines: *Engaging Change – Using a Learning Approach to put the Humanity back into Change Management* and *Organizational Change Management*. (2020 – coming soon) and ***The Change-Path Model for Ensuring Organizational Sustainability***. (2020).

Real-life example of conducting risk assessments at lower levels of the organization and building trust with individual units:

In one organization, the risk management (RM) team offered hands-on risk management training sessions that were integrated with risk assessment sessions. Throughout those sessions, the RM team asked questions and captured the business area's perspective on risks. This process included challenging the different business areas, especially when responses focused on funding limitations. The RM team acknowledged that funding was a challenge – the team treated funding as a potential root cause, rather than as a critical risk, in order to steer the conversation in a more focused direction.

The RM team also worked to build social capital and trust by helping the business areas with their issues and challenges going above and beyond risk management. The RM team completed some of the work and put some business areas in touch with others that could assist, which helped to forge strong relationships. RM is often more about relationship management than about a prescriptive science.

4.2 Provide ongoing education

Creating awareness of (and building engagement in) risk management concepts and practices can also be achieved by implementing ongoing education for management and staff.

Hands-on risk management training can be part of risk-assessment sessions. Tying risk management steps or practices back to the education primer can enable management and staff to better understand the concepts. Risk management education can also be emphasized in individual follow-up sessions.

Existing risk management practices such as annual code-of-conduct signoffs as well as privacy, safety, harassment and fraud awareness training can be considered as risk management education. Some organizations hold risk management town halls. These larger assemblies cover risk management topics that promote dialogue and interactive discussions, providing increased knowledge and problem-solving through the shared experience.

Step 5 – Enhance the value of risk management

As with any other organizational process, enhancing or refining risk management practices will help ensure they continue to meet the changing needs of an evolving organization.

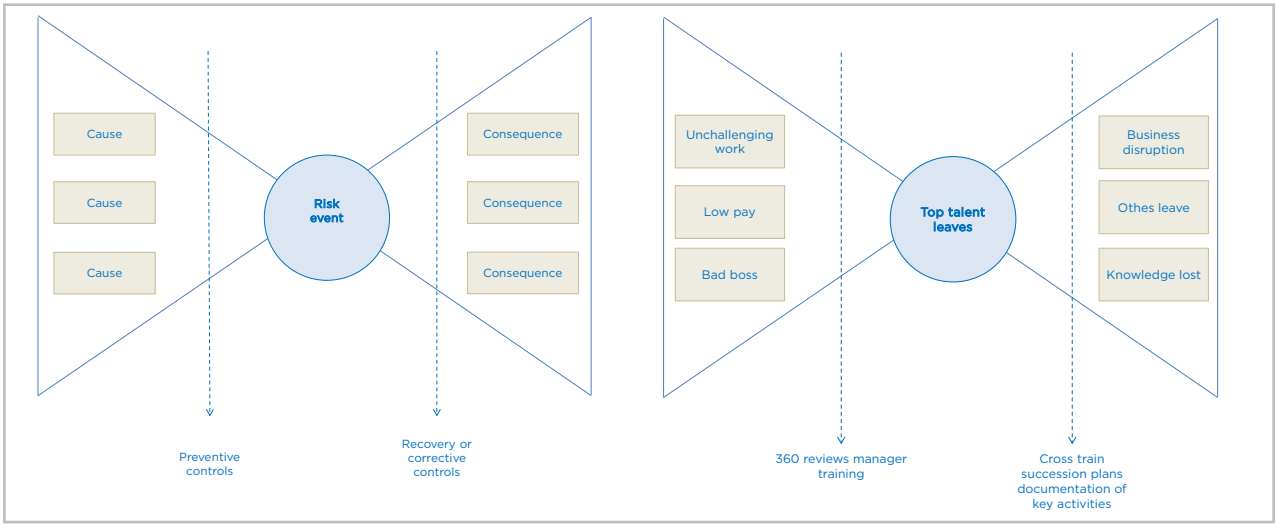
Reviewing and updating the various components of a risk management framework should be done at least once a year.

5.1 Perform root cause analysis – The 'risk bow tie'

A useful tool for identifying, understanding, and rating risks is the risk bow tie (see Figure 4), which is a visual representation of the relationship between a risk event and its causes and consequences.

Once the causes and consequences are discussed and documented, organizations can then establish controls to help prevent the risk event or to minimize its impact so that it remains within the risk appetite.

FIGURE 4 – RISK BOW TIE AND EXAMPLE



Here is an example from Ariane Chapelle's book, *Reflections on Operational Risk Management*: a company identifies "top talent leaving" as a risk event. That is the first step in risk bow tie analysis – identify the risk event, the "knot," of the bow tie. After the risk event is identified:

- Starting with the root cause analysis, the left side of the bow tie, identify major root causes of this risk event (e.g., a lack of challenging assignments or a poor manager). Consider how to mitigate this risk. For example, preventive controls to consider would include implementing "360 reviews" and/or focused manager training.
- Looking next at the major consequences, the right side of the bow tie, top talent leaving could include a huge loss of knowledge to the organization. Consider how to minimize this loss. For example, corrective controls to consider would include continuous cross-training and documentation of key processes and procedures.

5.2 Develop risk monitoring capabilities – Key risk indicators

The objective of this step is to ensure that critical risks do not increase to unacceptable levels (i.e., outside the organization's risk appetite) and to ensure that any implemented responses (e.g., internal controls) are working as expected. This can be accomplished by establishing key risk indicators (KRIs) for all critical risks.

KRIs, metrics that are tied to a specific risk, provide an indication of whether or not the implemented responses are functioning as intended. They can be predictors of important events or risks that can adversely impact an organization. As such, KRIs are aligned with risk appetite statements and risk tolerance levels.

Many organizations have some types of indicators that can be used as KRIs (e.g., safety measures, voluntary turnover, audit reviews). A major challenge is to develop predictive KRIs that provide an indication about the possibility of future adverse events. A mix of both "trailing / lagging" and "predictive / leading" KRIs should be developed.

TABLE 7 – EXAMPLES OF KEY RISK INDICATORS (KRI)[18]

Nature of risk	Key risk driver	KRI description	Limits (tolerances)		
Information security: sensitive data being compromised	Fraudulent intrusion (e.g., hacking, phishing)	Number of successful attempts of external intrusions	0	1	>1
		Number of persons with inappropriate system access profiles	0	1	>1
Regulatory compliance: non-compliance with regulations	Emerging regulations	Number of emerging regulatory issues rated "high risk"	<2	2 to 5	>5
People / staff: productivity and motivational decline	An unstable production work force	Voluntary turnover of high-performance staff	0%	0% to 5%	>5%
	An unmotivated work force	Scores on employee satisfaction surveys and scores on 360 surveys of supervisors and managers	>80%	60% to 80%	<60%
Customer retention: loss of market share	Customer complaints of product quality	Trending of nature and volume of customer complaints	0 to 2	2 to 4	>4
System availability: critical IT systems are not available	System outages	Percentage of time that critical systems are available during the month and month-over-month trending	>99.75%	99.0% to 99.75%	<99.0%
Internal controls	Internal or external audit issues	Number of major audit findings, audit grade	0 to 1	1 to 2	>2

18 Includes references from Institute of Operational Risk, *Key Risk Indicators*. (2010).

Using the "top talent leaving" example from the risk bow tie Section 5.1, a useful KRI for the "consequence" side would be the percentage of completed cross-training or succession plans. A useful KRI to develop on the "causal" side would be the percentage of poor 360-degree performance reviews for a manager versus the total reviews.

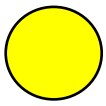
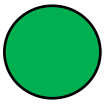
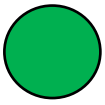
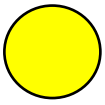
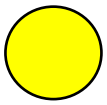
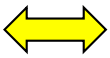
5.3 Develop risk reports – Risk management dashboard reports

It is important to communicate the organization's risk profile in a timely manner to all relevant stakeholders in relation to its strategic and operational objectives and to its risk appetite. Once the board and senior management understand the critical risks, it is important to report regularly on how the organization will manage them. And once risk management practices are enhanced and produce additional quality information, risk reports can also be further refined.

As well as communicating critical risks throughout the organization, a full summary of objectives and risks, along with an opinion on how well they are being managed, can be presented to the board and senior management on a regular basis (e.g., quarterly, semi-annually or annually, depending on board or stakeholder requirements). This helps ensure continued engagement and commitment to risk management.

Risk reports or dashboards should include a summary of strategic objectives, critical risks and KRIs, along with an insightful and detailed narrative. The level of sophistication in the report can increase over time.

TABLE 8 – EXAMPLE OF A RISK REPORT

Strategy	Risks		Risk assessment		Ability to manage risk	Key mitigating plan and status update	Risk outlook	Certainty of achieving strategic objective
	Type	Statement of risk	Current quarter	Prior quarter				
Strategy #1	Operational – HR	Brief description of why this is a risk/opportunity for division 's business objectives				Brief summary of key mitigation plans to address the high rated risk.		
	Operational – IT	Brief description of why this is a risk/opportunity for division 's business objectives				Brief summary of key mitigation plans to address the high rated risk.		
	Emerging risks							
	Operational – HR	Emerging risks from environmental scan		-		Summary of the management plans to continue to monitor and potentially prepare for		

Step 6 – Embed risk management practices

Embedding risk management into the organization's culture involves asking risk-related questions when setting strategies, evaluating the feasibility of establishing new products or services, or enhancing existing company offerings.

Real-life example of incorporating risk management practices into the daily operations of a not-for-profit organization:

In a major Canadian city, after homeless people received treatment in emergency rooms hospital staff would discharge and send them to the closest homeless shelters. The service manager responsible for shelters had a mandate to support homeless individuals in their search for safe and stable housing. Fulfilling this mandate was significantly more challenging for individuals with complex health care needs.

To better manage the risk of being overwhelmed with a number of homeless that had complex care needs, the service manager established and obtained approval for a "risk appetite" – a set of assessment criteria to be used when health care providers conducted an intake of clients and developed a discharge plan. The responses to those criteria enhanced the health care system's understanding of the capabilities of the shelter system and, most importantly, improved the service and care of those in need.

6.1 Align risk with planning and strategy

Risks are uncertainties that may arise as events that affect an organization's ability to achieve its strategic objectives. As such, it is imperative to explicitly link strategy planning processes with risk management processes.

Organizations can ask the following questions during annual strategy and planning sessions to stimulate conversation:

- What are the risks of having the wrong strategies? What are we doing to ensure we have the optimal strategies?
- What are the risks of misreading our "competitors?" What are we doing about this?
- What are the risks of not having the financial or organizational capacity and capabilities to implement our strategies correctly? What are we doing about these risks?
- What's the worst thing that could happen in terms of reputation?

Another way risk and strategy can be aligned is through a new product and service approval process. This includes a mini risk assessment for each new product or service offering. Senior management considers all applicable risks and signs off if they are within the company's risk appetite.

"Risk and strategy are the lynchpins of every business, with equal power to create or destroy value. They demand equal talent and attention. Management focus and board oversight must reflect this reality."

Olivia F. Kirtley Director – U.S. Bancorp; Papa John's International; Rangold Resources, Chairman of the AICPA Board of Examiners[19]

19 CIMA AICPA, *Enterprise Risk Oversight: A Global Analysis.* (September 2010).

6.2 Worst case scenario exercises

Stress testing (or a worst-case-scenario analysis) is a risk management technique that evaluates the potential effects on an organization's financial condition. Many organizations undertake scenario stress testing to ensure they are prepared for unexpected internal or external events that can significantly disrupt business operations and lead to significant financial losses. From a risk management perspective, a risk event such as the 2019 global pandemic is an example of an event that has a low probability of occurring; but if the risk event does materialize, it will have an extreme negative impact on the organization's ability to generate and sustain cash flow and operate as a going concern. Referring to the risk heat map (Figure 3), a tail risk event such as this would fall into the unlikely Likelihood and extreme impact cell.

The board and/or senior management along with relevant subject-matter experts should be involved in outlining potential scenarios and possible worst-case impacts on organizational operations. It is important to steer participants away from a "That could not happen" type of thinking and toward "What if it does happen?" type of thinking. Examples of worst-case scenarios include natural disasters and extreme weather, global trade wars, global pandemics, and large-scale fraud from cyberattacks.[20]

When working through the worst-case scenarios, the risk bow tie approach (Figure 4) can facilitate a discussion on the possible consequences of each scenario. The team should look at all the possible causes of each worst-case event, determine if current controls and processes should be strengthened, and consider whether additional preventative controls, plans, processes and systems (e.g., business continuity, disaster recovery and preparedness, emergency management systems, crisis management) are necessary. The benefits of having these plans in place in the event that the tail risk materializes include:

- addressing the health and safety concerns of the employees in the organization
- ensuring that critical operational processes continue to operate effectively
- maintaining financial sustainability in the worst-case scenario

Scenario planning[21] is another management tool that can be leveraged to make organizational decisions in uncertain, unpredictable and volatile environments where the pace of change is accelerating. Scenario planning is a valuable addition to an organization's risk management process to evaluate the effectiveness of strategies, tactics and plans based on a range of possible future environments.

6.3 Evaluate the risk management program

After a risk management program has been implemented and an appropriate amount of time has passed – generally anywhere from nine months to two years – the board and/or senior management should ask whether it is working as anticipated. Some steps to follow include:

20 World Economic Forum, *Global Risks Report 2020*. (2020).

21 Refer to the *Scenario Planning* MAG®. (2018).

- Developing qualitative feedback that would give some indication on whether the risk management program is providing value to the board, senior management, and other key stakeholders. Questions include:
  - Is there appropriate engagement by board members, and are they asking in-depth risk questions?
  - Does the board and/or senior management actively execute their defined risk oversight roles as noted in the risk policy?
  - Does strategic planning include identifying, assessing and responding to risks?
  - What do we know that will help us evaluate the quantitative and financial outcome of the risk management program?
    - Are there less surprises relative to previous years?
    - Are bottom line results more predictable?
    - Is the organization performing better?
- Reviewing risk management practices and components (e.g., risk appetite, key risk indicators) to the ongoing strategic and operational performance of the company, especially to specific events that may have occurred. Changes should then be made as appropriate.
- Comparing or benchmarking the risk management program against other, similar types of organizations and industries to determine areas for improvement. Exploring opportunities to connect externally with people in the risk management domain supports this.

Key Learnings

Summary

All organizations experience negative events, be they external or internal. However, organizations with risk management programs in place are more likely to identify these events sooner and more effectively manage or minimize their impacts.

Organizations of any size will benefit from implementing a risk management program. Enterprise risk management can help organizations increase their value, achieve their objectives and address many regulatory or stakeholder demands, such as the need to adopt best practices in governance, risk and compliance. The risk management steps and practices outlined in this guideline are designed to help organizations achieve resilience in the face of risk.

The tips and tools presented in this six-step framework should enable a small- to medium-sized organization to implement a risk management program that supports strategic and operational objectives in an ever-changing and often disruptive environment.

Resources

References

- Accountancy Europe (February 2020). *SME Risk Management. How can your accountant help?* [Briefing paper].
- Chapelle, A. (2019). *Operational Risk Management – Best Practices in the Financial Services Industry*. Wiley and Sons. Page 37.
- Chapelle, A. (2017). *Reflections on Operational Risk Management*. Risk Books.
- COSO. (2017). *Enterprise Risk Management – Integrating with Strategy and Performance*.
- COSO. (2012). *Enterprise Risk Management – Understanding and Communicating Risk Appetite.* Thought Leadership Series. Rittenberg and Martens.
- CPA Australia. (2009). *Risk Management Guide for Small to Medium Sized Businesses*
- Deposit Insurance Corporation of Ontario. (January 2018). *ERM Framework and ERM Application Guide*.
- Dionne, G. Social Science Research Network (SSRN). (2013). *Risk Management: History, Definition and Critique*. Wiley Online Library.
- FEI Canada. (2015). Leading Practices in Implementing Risk Management. Roundtable discussion, chaired by Steve Mallory.
- Institute of Operational Risk. (November 2010). *Key Risk Indicators*.
- International Standards Organization (ISO). (2018) *ISO 31000 – Risk management*.
- Marks, N. (March 2018). *Governance, Risk Management and Audit*.
- Northbridge Insurance. (July 2017). Hidden risks that can damage your manufacturing business [Blog post].
- Stanton, T.H. Enterprise Risk Management (March 2017) [Ted Talk].

CPA Canada resources referenced

- *20 Questions Directors of Not-for-Profit Organizations Should Ask about Risk* (2009)
- *A Framework for Board Oversight of Enterprise Risk* (2019)
- *From Bolt-On to Built-In: Managing Risk* (2015)
- Management Accounting Guideline, *Scenario Planning* (2018)
- *The State of ERM in Canada. A Benchmarking Study* (2018)

Additional CPA Canada resources

- *Drivers of Change: Navigating the Future* (2017)
- *Developing Robust Strategy for Uncertain Times: Parts I and II* (2015)

CPA Canada Management Accounting Guidelines®:

- *Engaging Change – Using a Learning Approach to Put the Humanity Back Into Change Management* (2020 – coming soon)
- *Organizational Change Management: The Change-Path Model for Ensuring Organizational Sustainability* (2020)
- *The CAM-I Risk-Value Curve: Understanding Your Risk Appetite to Create Value* (2020)

- *RESILIENT + ADAPTABLE + INNOVATIVE = Sustainable Enterprises. A New Mindset to RAISE the Bar* (2020 – coming soon)
- *The State of Enterprise Risk Management in Canada* (2016)

Other resources

- IFAC. (2019). *Enabling the Accountant's Role in Effective Enterprise Risk Management*
- World Economic Forum. (2020). *Global Risks Report 2020*

About the authors

Bill Wesioly is a risk management consultant and leadership coach. His goal is to improve the effectiveness of people and organizations.

His background is in the financial services industry: first with BMO, then with RBC. The last 15 years of his banking career have been in the field of risk management where he successfully built and led programs such as risk and control assessments, operational risk scenarios, and key risk indicators.

Bill currently teaches various risk management courses for CPA Ontario, CPA B.C., CPA Alberta, CPA New Brunswick, CPA Nova Scotia and CPA Newfoundland. He also teaches for the Centre of Outsourcing Research and Education (CORE) and has recently consulted on risk management for credit unions, independent private schools, and First Nations.

Guenther Moeller is a risk management consultant. His focus is on supporting organizations as they implement simple and practical risk management practices that help ensure they achieve their business objectives.

His background is in the financial services industry: first with BMO Nesbitt Burns, then with BMO Corporate, then with TMX. His risk management career spans 20 years and has focused on building successful and value-added risk management practices with organizations, and enhancing their risk management capabilities by developing and teaching risk management education modules.

DISCLAIMER

This paper was prepared by CPA Canada as non-authoritative guidance.

CPA Canada and the authors do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use, application or reliance on this material.