CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Enterprise Risk Management

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

Bill Wesioly and Guenther Moeller

MANAGEMENT ACCOUNTING GUIDELINE | CASE STUDY

Case Study
Key Learnings

Case Study

Premier Advantage Credit Union – Company background

Premier Advantage Credit Union[1] was founded in 1986 as the result of the vision, effort and perseverance of a core group of concerned community members (the "members") in Green River, Ontario, who did not want to be beholden to big banks but wanted a community bank for Green River. The idea was to put money back into the community and support growth in small- to medium-sized businesses.

The growth of Premier Advantage Credit Union has paralleled that of Green River. There are now eight branches in prominent locations around the community.

Financially, the credit union has been strong for some time. It has a good customer base, but it consists mostly of older clientele. Its biggest concerns tend to reflect what is happening with other credit unions: external fraud and cyber-attacks, both of which Premier Advantage has experienced recently. As well, there are new regulatory compliance requirements around money laundering, which Premier Advantage is just beginning to address.

Choosing a holistic risk management program

The board of Premier Advantage Credit Union acknowledges that an Enterprise Risk Management (ERM) program would be extremely beneficial. Not only would it satisfy regulatory requirements, but a holistic ERM program would also greatly help to handle the multitude of risks arising from the increasing complexity of banking and the broader political, societal and technological changes.

First steps

Once the board agreed that it would move forward with an ERM program, its first task was to select an internal ERM champion, someone who was familiar with the organization and had risk management knowledge and experience.

The board selected Jenna Altreca, a senior manager from Finance. Jenna's credentials were excellent: a good base knowledge of risk management, excellent teamwork and leadership skills, and a positive relationship with the board.

Jenna's first meeting with the board resulted in agreement on some basic guiding principles for implementing an ERM program. The board indicated its commitment to making the program a success. This commitment included providing time at board meetings to discuss risk management topics as well as periodically dedicating entire board meetings to risk management. The board also agreed to support any communications to the rest of the organization to demonstrate their commitment and support.

[1] Premier Advantage Credit Union is a fictitious company.

Case Study
Key Learnings

The basic guiding principles for implementing a risk management program include:

- Start at the "top of the house" with the board, to get its buy-in and commitment.
- Keep the program simple, and begin with a straightforward framework to keep the steps manageable.
- Leverage existing risk management processes in various organizational departments (e.g., Internal Audit, Compliance / Legal).
- Clearly communicate the benefits of a successful risk management program.
- Build relationships along the way.

Also, at this time it was decided that the term "enterprise risk management" would be referred to as "risk management" – the former descriptor seemed too all-encompassing for a small credit union such as Premier Advantage.

Initial risk assessment with the board – Preparation

Once the board provided its commitment to the program, Jenna scheduled a three-hour interactive risk management education session (henceforth referred to as the "education session") for board members, which included a risk management fundamentals presentation and a risk and control assessment exercise.

The risk management fundamentals presentation – Part 1 of the education session

After the first meeting with the board, Jenna realized that different board members had different levels of understanding of risk management, so she decided to provide an introductory education session that would cover:

- defining risk and risk management
- benefits of a risk management program
- examples of risk events in similar organizations
- introducing risk management framework steps
- defining risk management roles, responsibilities, governance and oversight
- introducing a risk heat map

She would employ an interactive exercise when introducing the risk heat map, where board members would be asked to list the risks of a hypothetical activity – in this case, hiking. They were asked to plot the risks on a risk heat map and consider what additional controls would help bring them within an acceptable level.

The risk and control assessment exercise – Part 2 of the education session

Immediately following the presentation on risk management fundamentals, Jenna executed a risk and control assessment exercise on the organization's risks. The goal of this exercise was to make board members aware of the critical risks facing Premier Advantage. This included understanding how the risks were currently managed and determining further risk management practices the organization should implement.

To prepare for the risk and control assessment exercise portion of the education session, Jenna documented Premier Advantage's strategic objectives:

- Achieve positive organizational growth (with a minimum of 5 per cent growth in each major portfolio).
- Extend the reach of Premier Advantage into new demographics (e.g., young urban professionals) and increase its customer base.
- Offer innovative new products and services.
- Maintain a positive relationship with the community and customers.
- Ensure regulatory compliance requirements are met.

Jenna then executed an external business assessment where she concluded that the organization's major drivers were political, regulatory and economic. This enabled her to draft some initial critical risk areas for Premier Advantage.

Jenna identified key risks faced by other credit unions that also apply to Premier Advantage:

Types of risks facing credit unions

- Strategic risks – strategy implementation, depositor demographics, competition
- Credit risks – default, concentration of lenders
- Financial risks – liquidity, capital management
- Operational risks – information technology, information security, outsourcing, fraud, personnel, cyber threats
- Compliance risks – regulatory (e.g., money laundering)

As a next step, Jenna documented her findings in an initial "risk register," outlining some of the key risks facing Premier Advantage. She believed that a draft list (as opposed to a blank template) would stimulate and facilitate discussion.

Before sending out the draft risk register, Jenna shared it with senior management for their input. The resulting draft register listed a number of key risks, four of which are noted here:

TABLE 1

Risk category	Sub-category	Risk description	Impact rating	Likelihood rating	Inherent risk rating	Control program
Operational	IT risk	Cyber hack	Extreme	Possible	Critical	• IT department with latest IT security protocols • Shared IT knowledge and assessments with others

Case Study
Key Learnings

Risk category	Sub-category	Risk description	Impact rating	Likelihood rating	Inherent risk rating	Control program
Operational	Regulatory compliance risk	Money laundering	Major	Likely	Major	• Annual money laundering training for all staff • Quality checks on “know your customer” transactions
Credit	Industry concentration risk	Too much concentration in residential real estate market	Moderate	Probable	Major	• Quality reviews on all new real estate loans • Business intelligence on future trends, recommendations to diversify
Strategic	External environment risk	Aging customer demographics	Major	Likely	Major	• Strategies aimed at younger demographic including digital • Advertising at nearby university / college market fairs

To determine risk ratings for the register, Jenna used the following likelihood rating scale:

Rating	Likelihood 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

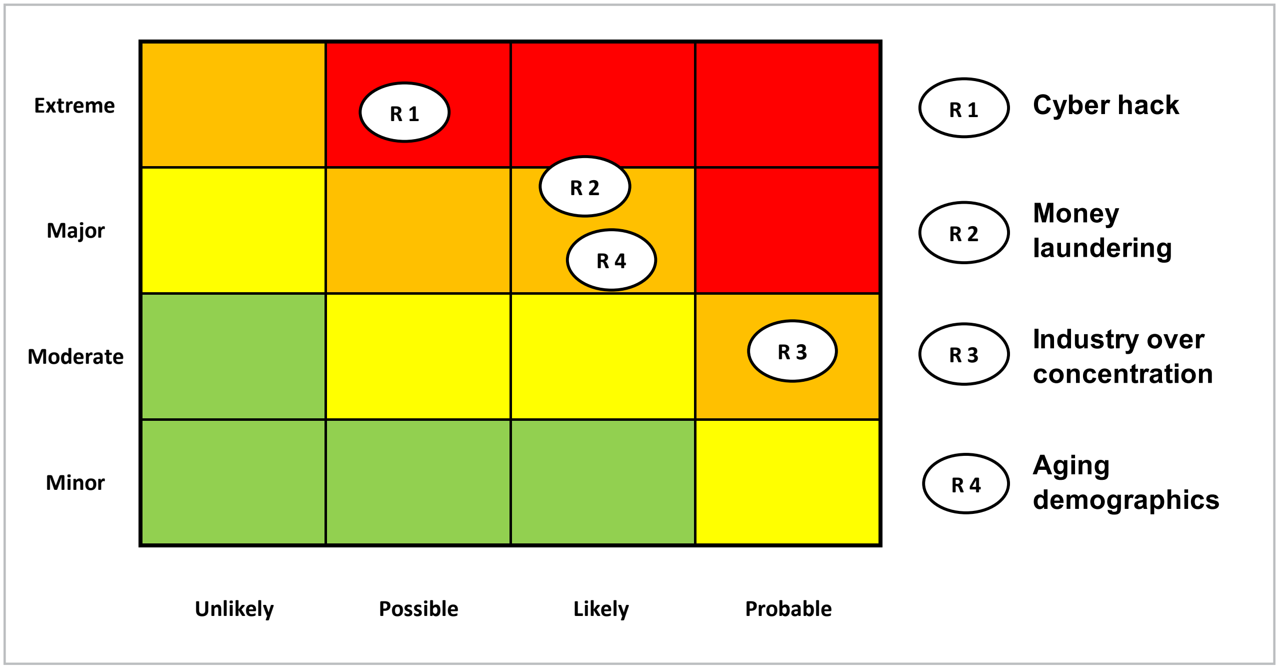
She also used the following severity rating scale:

Rating	Financial impact	Regulatory impact	Reputational impact
Extreme	Loss of annual revenues or funding > 20 per cent	Loss of regulatory license to operate	Long-term negative media coverage, game-changing loss of market share

Case Study
Key Learnings

Rating	Financial impact	Regulatory impact	Reputational impact
Major	Loss of annual revenues or funding of > 10 to 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 to 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

Jenna also plotted the results from the risk register on a risk heat map. She knew that many of the board members connected with visual overviews. The following four risks from the risk register are noted as follows:



Jenna circulated all four documents to board members one week before the three-hour education session, along with all appropriate details and instructions. This ensured that board participants had sufficient time to review materials. She also ensured that the CEO, CFO and other key members of the senior management team would be in attendance.

Case Study
Key Learnings

Education session with the board – Delivery

Risk management fundamentals presentation

Jenna started the meeting by thanking board members for their attendance and upcoming participation. She moved onto the risk management fundamentals presentation, which had the following objectives:

- Provide the board with a better understanding of risk management (including board oversight responsibilities).
- Determine the major risks facing Premier Advantage and how they are currently being managed.
- Consider whether the major risks must be further managed (and what additional actions could be taken).
- Determine next steps for continuing to engage the board on risk management.

The risk management fundamentals presentation went very well, stimulating a lot of good discussion and eliciting considerable participation.

Risk and control assessment exercise

For the risk and control assessment exercise, Jenna carefully walked through the pre-circulated materials to ensure that board members had a thorough understanding of the objectives and the steps in the exercise.

Jenna then went through each risk and asked each person for their own assessment of the risk impact, risk probability and ultimate inherent risk rating. She discussed each risk, focusing on the controls, the on effectiveness of the controls, and on the residual risk ratings.

Jenna asked board members to list additional key risks, which sparked a more in-depth discussion. These additional risks and their controls were assessed and then added to the draft risk register.

The last discussion item centered on the updated risk register. Members were asked to consider whether additional controls should be added for controls rated as “Not fully effective” or where residual risks were considered to be too high. The group discussed suggestions for improvements as well as next steps for bringing the level of those risks down.

At the end of the education session, Jenna requested immediate feedback on whether or not board members felt the meeting achieved its objectives. Many members commented on the richness of the information and indicated that the discussion was extremely valuable. Jenna thanked the board for these comments and ended the meeting by asking for their continued commitment throughout the risk management program.

Case Study
Key Learnings

Post-meeting and developing the initial risk framework and governance activities

Immediate follow-up

Two days after the session, Jenna summarized and the results of the meeting with a risk-assessment matrix and accompanying heat map. The updated risk register is below. The circled areas denote action plans that Jenna will take forward to the responsible parties and whose progress she will monitor and report on to the board in subsequent meetings.

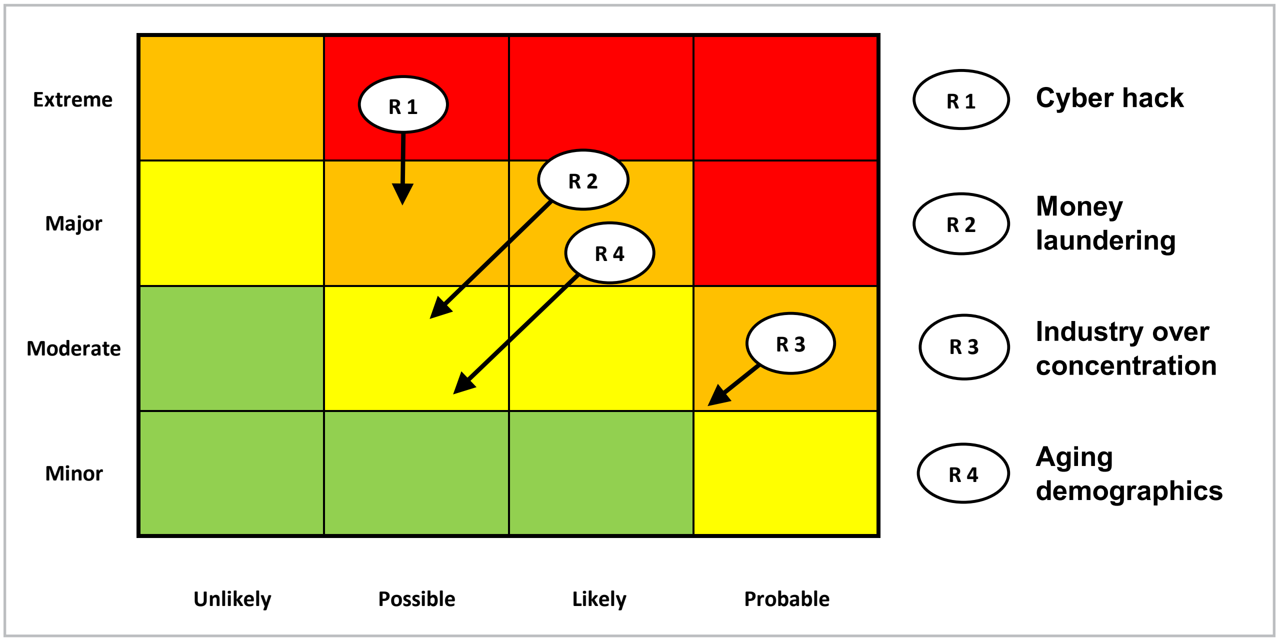
TABLE 2

Sub risk category	Risk description	Impact rating	Likelihood risk rating	Inherent risk rating	Control program	Impact rating	Likelihood rating	Residual risk rating
IT risk	Cyber hack	Extreme	Possible	Critical	• IT Department with latest IT Security protocols • Shared IT knowledge and assessments with others	Major	Possible	Major
Compliance	Money laundering	Major	Likely	Major	• Annual money laundering training for all staff • Quality checks on "know your customer" transactions	Moderate	Likely	Moderate
Credit risk	Industry concentration risk	Moderate	Probable	Major	• Quality checks on all new real estate loans • Business intelligence on future trends, recommendations to diversify	Moderate	Likely	Moderate
Environment review	Unfavourable customer demographics	Major	Likely	Major	• Strategies aimed at younger demographic including digital • Advertising at university market fairs	Major	Likely	Major

Case Study

Key Learnings

The risk heat map reflects the residual risk results for these same four risks. With further discussion on additional controls, Jenna depicted how those risk levels could come down.



In the distribution of the assessment results, Jenna asked the board to verify the information. As well, she assured them that she would continue working with senior management on outstanding action plans and report back on progress.

Introducing key risk indicators

The next step for Jenna was to develop potential tracking indicators for the first major risk, cyber hack, with senior IT managers. The discussions with senior IT managers centred on possible control failures in the IT area and identified two controls that could be tracked: vulnerability patching and penetration tests.

Jenna and the senior IT managers developed some initial key risk indicators (KRIs) for overdue vulnerability patching and failed penetration tests.

She depicted the initial KRIs with the following template. She would introduce the concept of monitoring risks through KRIs at the next board meeting and start to work on KRIs for the other critical risks.

Case Study
Key Learnings

Risk appetite	Key risk driver	Key risk indicator	Tolerance limits		
			Green	Yellow	Red
External cyber hacks will not impact the organization	Overdue vulnerability patching	Vulnerability patching overdue against pre-determined schedule	> sch. time	= sch. time and up to 1 day overdue	> 1 day overdue
External cyber hacks will not impact the organization	Failed penetration tests	Number of failed penetration tests	0	NA	1 or more

Next steps – Developing risk governance elements

Once the risk and control assessment exercise and follow up were complete, Jenna then started work on building the risk governance pieces of the framework. She knew that the board would find this exercise extremely important for starting to build the foundation of risk management.

Jenna started first to build a risk management policy that would provide guidance for people in the organization in understanding risk management practices. She drafted the key components as follows:

- Objective of the risk management policy
- Definitions
  - of risk and risk management, as well as the different sub-risk categories (e.g., IT risk and compliance)
- Risk management guiding principles
  - including ongoing support from the board and alignment to industry risk management standards
- A summary of the risk management framework – context of risk, identification of risk, assessment and prioritization of risk, treatment of risk, monitoring of risk and reporting of risk
- Policy structure
  - alignment to other organizational policies, as well as the risk management policy being the overarching policy to lower-tier risk management-related policies and standards
- Governance structure
  - structure of designated sub-board committees and their decision-making and oversight responsibilities
- Risk management roles and responsibilities

After adding more detail, Jenna then planned to introduce it to senior management for their input and agreement, then to the board for final approval.

Another risk governance element that Jenna wanted to start putting in place was the risk appetite statements from the related discussion started in the risk and control assessment exercise with the board.

Jenna wanted a set of statements that could provide boundaries for risk-taking relative to generating profits for the business, something that everyone could understand. They could understand what risks could harm Premier's reputation, and what risks would be considered too sizeable for customers and regulators. She came up the following draft statements that she planned to take first to senior management for their input and additions, and then finally to the board for their approval:

Credit risk	Operational risk	Reputational risk
• There is minimal desire to accept any material concentration of risk in any particular industry segment. • We shall maintain lending policies that place conservative limits on loan-to-value ratios.	• We will not accept any breach of confidential customer information. • We will comply with all applicable regulatory and statutory requirements. • We will maintain a robust risk management and internal control framework.	• We will only engage in activities and transactions where we possess the expertise and ability to ensure effective risk management. • We will not engage in any activities that could be damaging to our brand. • We will not engage in any activities that are illegal.

Jenna knew from her external research that a fully developed and accepted risk appetite statement would take time, but she also knew it was necessary to start the development process up-front.

Key Learnings

Moving ahead with ERM – One year later

After one year, Jenna and the board felt positive about the pace and results of the ERM implementation. She had started scaling risk assessments to the rest of the organization, and she continued to work on the risk governance pieces: The risk policy and risk appetite statements were finalized and approved, and she consistently reported to senior management and the board on risk assessment results, KRIs and emerging risks.

Jenna knew that continued education and board commitment were key for the continued success of the ERM program. The hands-on training throughout the risk and control assessment sessions would be supplemented with semi-annual risk management town halls, involving all senior people involved in risk and control assessments. Her next steps were to continually ensure that risk management implications were considered, understood and managed with all major decisions throughout Premier Advantage.

cpacanada.ca/MAGs

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.