



First Nations University of Canada

tradition innovation leadership

Name: Enterprise Risk Management Framework

Responsibility: Associate Vice President, Academic

Complements: Policy XXX: Enterprise Risk Management Policy

Date: March 2015

Revision Date(s):

Approved:

Overview

First Nations University of Canada (FNUUniv) is committed to establishing an institution that ensures risk management is a core capability and an integral part of all FNUUniv's activities. FNUUniv has developed an Enterprise Risk Management (ERM) Framework based on the internationally recognized principles from ISO 31000 to manage change and uncertainty. The ERM framework applies to all academic and administrative levels, and assists in achieving the FNUUniv's strategic objectives by bringing a leading practice and a systematic approach to identifying, analyzing, mitigating and reporting risk and control. The ERM process will lead to enhanced and proactive decision making and improve FNUUniv's performance, since it combines governance, risk and opportunity management, compliance, and financial reporting. This framework is divided into components describing: What Enterprise Risk Management is; why it is beneficial; who is responsible; how it is executed, and what management actions are required.

Objective

To meet the strategic goals FNUUniv has set, management and the Board of Governors (the 'Board') have committed to develop a rigorous, structured and effective risk management processes across the institution. The risk management framework is developed to:

- Establish common risk language and direction related to risk management;
- Assign responsibilities for risk oversight among the full Board and its committees;
- Understand critical risks and opportunities in the University's activities and strategy;
- Increase the likelihood that strategic objectives will be achieved;

- Evaluate FNUniv's risk management processes and whether they are functioning effectively;
- Facilitate open communication between management and the Board with respect to risk;
- Build an appropriate culture of integrity and risk awareness;
- Encourage proactive decision making; and
- Improve operational efficiency and effectiveness

Key ERM Definitions

FNUniv has adopted internationally accepted definitions from ISO 31000, the internationally accepted risk management standard¹.

Risk – effect of uncertainty on business objectives. Simply risk is an event that would deter the institution from achieving its objectives. Risk is often described in terms of a combination of the impact and the associated probability.

Risk Management – the identification, assessment and response to risk to a specific objective or within a specific risk category.

Risk Management Framework – provides a direction and guidance to strengthen risk management practices within FNUniv.

Risk Owner – person or entity with the responsibility and authority to manage a risk.

Risk Tolerance – or sometimes known as risk appetite is described as the level of risk the institution is willing to accept in relation to a threat that may cause loss or an opportunity in the day-to-day business activities. The risk tolerance of an institution may be different for different events. FNUniv's risk tolerance and the alignment between its risk appetite and its objectives form part of the overall strategy.

Control – measure or management action to mitigate risk. It includes the policies, procedures, reporting and initiatives performed by FNUniv to ensure that the desired risk response is carried out. These activities take place at all levels and functions of the institution.

¹ International Standard ISO 31000; 2009 Risk Management Principles and Guidelines

Likelihood – the probability of an event occurring. Likelihood of an event occurring is rated as low, medium, or high.

Impact – the severity of an event. Impact or severity of an event is rated as minor, moderate or significant.

Risk Communication – the process of identifying risk and communicating broadly to enable all personnel to deliver on their responsibilities.

Risk Register – official recording of the identified risks facing the institution. A catalogue of the full spectrum of risks (with impact and likelihood assessed) forms FNUniv risk register.

Stakeholders

Roles and Responsibilities

Risk Management is the responsibility of every employee of FNUniv. Different stakeholders have different objectives and levels of accountability with respect to risk management. An effective risk management framework includes a comprehensive and defined accountability for risks, controls and risk treatment tasks. The risk management framework documents the roles and responsibilities of the various components of a risk management process. FNUniv ensures that those who are responsible are equipped to fulfil their role by providing them with the appropriate authority, training and resources.

Board of Governors

Canadian Securities Administrator (CSA) National Policy 58-201, Corporate Governance Guidelines, and National Instrument 58-101 Disclosure of Corporate Governance requires that the Board²:

- Establish a strategic planning process
- Ensure the strategic plan considers potential corporate risks and opportunities
- Identify corporate risks and their mitigation strategy, and
- Ensure the corporations internal controls are working effectively.

² Ontario Securities Commission - National Policy 58-201. Corporate Governance Guidelines http://www.osc.gov.on.ca/documents/en/Securities-Category5/rule_20050415_58-201_gov-practices_2.pdf

FNUniv's Board of Governors, through its Audit, Finance and Risk Management Committee, is accountable for the oversight of risk management and the results of the institution. The Board is responsible to ensure the risk management framework and corresponding results work towards achieving the strategic objectives.

Audit, Finance and Risk Management Committee

The Audit Finance and Risk Management Committee of the Board is responsible for:

- Determining the institution's approach to risk
- Approving the risk management policy/framework
- Identifying the risks inherent in the FNUniv's strategy
- Monitoring and evaluating the effectiveness of risk management activities, and
- Ensuring FNUniv has effective crisis management systems and contingency plans.

Executive Team

The University Leadership Team is responsible for:

- Providing top down support
- Identifying emerging strategic and operational risks and assessing them based on likelihood and impact
- Setting a risk tolerance level
- Reporting on key risks and the effectiveness of the corresponding mitigation strategies
- Ownership and day-to-day oversight and management of individual risks, and
- Ensuring alignment between the institution's strategic objectives and risk management.

Enterprise Risk Management Steering Committee

The Enterprise Risk Management Steering Committee is responsible for:

- Reviewing and providing advice on the risk management framework, ensuring appropriate consultation, and recommending it to the Audit and Risk Management Committee

- Evaluating and/or supporting academic and administrative units in the identification and reporting of material risks
- Ensuring that business units are assessing their risks based on likelihood and impact to the institution
- Determining whether material risks being accepted across the University are consistent with the institution's risk tolerance level
- Reviewing and assessing processes, controls and mitigation strategies, and
- Overseeing the development of the risk register and reporting to Executive Team and the Audit and Risk Committee.

Enterprise Risk Management Coordinator

The Enterprise Risk Management Coordinator is responsible for:

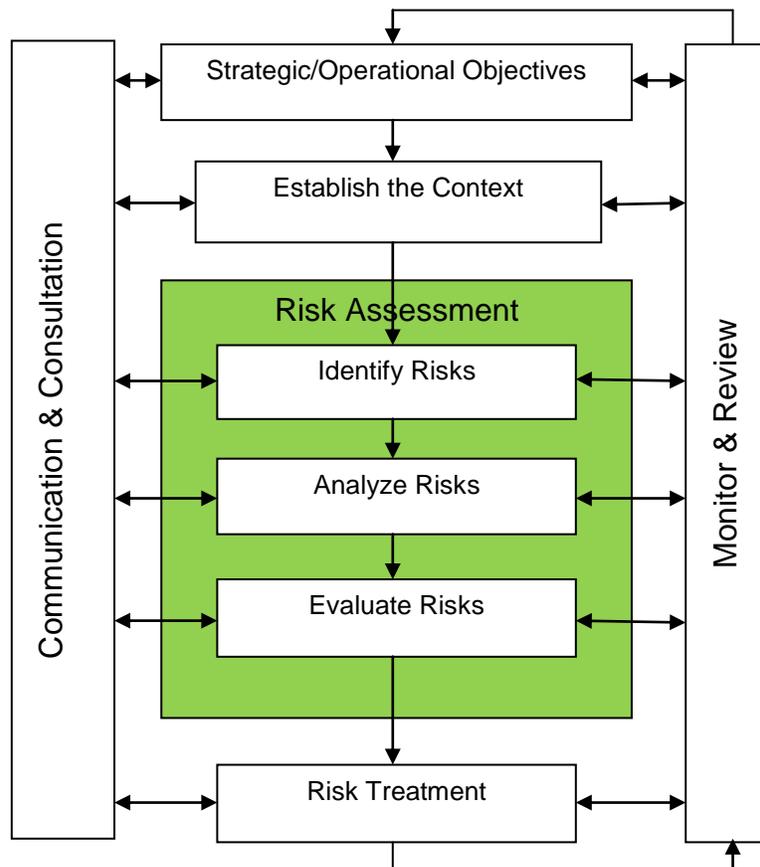
- Assisting the Audit and Risk Management Committee in the oversight of risk management by leading the development and implementation of the ERM framework
- Providing risk assessment training and workshops to University officials as required
- Conducting risk assessments, both internal to the University and within the Canadian post-secondary education system, to identify material risks to the University
- Bringing a systematic approach to evaluating and improving the effectiveness of risk management and control
- Ensuring accurate and reliable risk documents exist, and relevant information is provided to the Audit and Risk Management Committee, and
- Participating in the drafting and review of the University's annual report related to risk management and oversight.

ERM Methodology

FNUniv's methodology for risk management is shown in Figure 1³ and is simply a flow chart expression of the risk management activities. The process is continuous and can be applied at both the institution (enterprise) level or at an individual academic and administrative unit level.

³ International Standard ISO 31000; 2009 Risk Management Principles and Guidelines

Figure 1
Risk Management Process



The eight interrelated components form the basis for establishing and putting ERM into practice at FNUniv. Each component is described in more detail as follows:

- a. *Objective Setting* is the process of determining the strategic objectives for FNUniv and its risk strategy. The strategic planning process also requires all divisions and business units define their key business/operational objectives and targets.

- b. *Establishing the context* consists of the internal and external environment of the University. They form the foundation for defining the institution's risk approach and risk appetite. *Internal Environment* comprises FNUniv's history, culture, values, organizational structure, strategy, policies or procedures. *External Environment* comprises the social, cultural, political, legal, regulatory, financial, economical or technological environment in which the institution operates.
- c. *Risk, Event and Trend Identification* describes those developments either internal or external to the institution that could significantly affect its ability to meet its strategic objectives, either positively or negatively. In order to assure that the full scope of the institutions is considered, event and trend identification is done broadly engaging a cross-section of FNUniv members.

There are two approaches utilized for identifying key risks at FNUniv:

1. Top-down approach: starts by identifying enterprise-wide risks that affect FNUniv's strategic objectives. This approach involves executive management and the Board.
 2. Bottom-up approach: starts by identifying business unit level or operational risks. This approach usually involves middle management.
- d. *Risk Analysis* describes the extent to which potential events and trends might affect FNUniv's objectives. Events and trends are assessed by two criteria – impact and likelihood. Figure 2 displays a matrix known as a Risk Heat Map that graphically represents the impact and likelihood of each risk, as well as the corresponding management action. The color gradient from green (low) to red (high) provides a comparative level of priority when evaluating the institution's risks. This matrix is used to evaluate risk at both the inherent (without management or control) and residual (with management or control) levels. The corresponding management action suggests the appropriate response or treatment for risks assessed in that area of the matrix. Risk analysis can be done by qualitative and/or quantitative methods.
 - e. *Risk Evaluation* is the process of prioritizing risks (based on the result of risk analysis) for making a decision which risks require immediate treatment. The decision takes into consideration the risk tolerance level of FNUniv.
 - f. *Risk Treatment* means that once the risks are clearly identified assessed and prioritized, it is essential to recognize existing mitigation plans. Management may determine what

specific measures are currently in place to mitigate identified risks. ERM leading practices suggest listing first those mitigation plans and controls that already exist. Second, brain storm and propose additional mitigation plans. Third, it is important the Board and executive management team assess the adequacy of existing mitigation plans in relation to the significance of the risk⁴. Typical risk response considered for a risk event includes avoidance, reduction, transferring, sharing, or acceptance.

- g. *Communication and Consultation is required for an effective ERM program and requires information to be obtained from all levels of the institution for identifying, assessing and responding to risk. Consultation will be as broad as possible within FNUniv community and use a variety of approaches. FNUniv personnel will be encouraged to identify risks that are both internal and external to the institution. The knowledge gained through ERM will be communicated in a relevant form and appropriate timeframe enabling FNUniv personnel to carry out their responsibilities while incorporating risk management.*
- h. *Monitoring and Review refers to managing risk in the course of day-to-day operations. Periodic evaluations where management defines the scope, methodology and frequency of the risk assessment are done to ensure the currency of information in the FNUniv's risk register.*

Integration

Universities are complicated institutions generating a risk register that is broad and diverse, while several laws, regulations, policies and agreements also affect the operating environment. Good managers address risk by implicitly building it into their programming and decision-making. It is also important to re-iterate that risk management practices are an integral part of strategic planning, budget planning and audit planning. The ERM framework is a methodology that formalizes risk management and provides an all encompassing view of risk management process in order to aid in the operation of the institution. A systematic and integrated risk management approach creates efficiency and effectiveness by promoting team work, strengthening trust, reducing redundancies, and sharing responsibility. Working within FNUniv:

- a. The following elements are essential when managing risk:

⁴ Risk Management Guideline for the BC Public Sector:
http://www.fin.gov.bc.ca/pt/rmb/ref/RMB_ERM_Guideline.pdf

- i. **Assurance:** Stakeholders are assured that risk is being managed within FNUniv's risk tolerance and receive information regarding the quality and type of control in place.
 - ii. **Oversight and responsibility:** All critical risks facing FNUniv have been identified, managed and reported on a level and frequency that support FNUniv's risk tolerance.
 - iii. **Ownership:** Risk owners are assigned and understand their responsibility for management, oversight and assurance.
- b. Risk response for identified risks will be assessed according to FNUniv's risk appetite. The five possible risk responses are to:
 - i. Avoid (eliminate) the risk;
 - ii. Reduce (mitigate) the risk;
 - iii. Transfer the risk (e.g. insurance);
 - iv. Share the risk; or,
 - v. Accept the risk.
- c. A formal or informal evaluation of risk will be considered depending on the scope of the decision or action taken at the institution. This will be done both at the onset and throughout the life of the decision or action. Where applicable and quantifiable, the expected cost of the risk will be considered in the business case used in the decision and evaluation process.
- d. There will be a desire to learn from events that have transpired - the risk management process is a cycle where experience provides key information for new decisions and actions. Open and appropriate communication of results and lessons learned is required to facilitate learning.
- e. The institution's risk register will be evaluated regularly. New risks will be considered, and risks no longer relevant will be removed. The risk register will be refreshed by rating the likelihood and impact for each risk. This information is used to prioritize the risks and this, in turn, flows into the institution's planning cycle.

References

1. International Standard ISO 31000; 2009 Risk Management Principles and Guidelines
2. Treasury Board of Canada. Integrated Risk Management Framework.
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/rmf-cgr01-1_e.asp
3. Risk Oversight Inc. www.riskoversight.ca