Athabasca University

PROCEDURE

Enterprise Risk Management Procedure			
Parent Policy	Enterprise Risk Management Policy		
Policy Sponsor	Vice President, Finance and Administration & Chief Financial Officer (CFO)	**Category**	Board
Policy Contact	Vice President, Finance and Administration & CFO	**Effective Date**	March 27, 2020
Procedure Contact	Director, Strategic Initiatives and Services	**Review Date**	March 27, 2025

1. Purpose

Enterprise Risk Management is inherently part of planning, budgeting, audits and day to day operations. This procedure will assist in decision-making processes that support the Board's Risk Tolerance Statement.

2. Scope

It is imperative that all members of the University Community – from the Board to the University's stakeholders – are actively engaged in Enterprise Risk Management. Responsibility for assessing risks and appropriately addressing them exists at all levels of the organization. These procedures will guide the University Community's actions.

3. Definitions

Board	The Governors of Athabasca University
Board Audit Committee	Assists the Board in fulfilling its due diligence, fiduciary, financial reporting and audit responsibilities and to approve, monitor, evaluate and provide advice on matters affecting the external audit, internal audit, risk management, legal and regulatory compliance, and the financial reporting and accounting control policies and practices of the University.
Impact	Defined by the ISO 31000: 2018 Standard in terms of severity of consequences that can have positive or negative effects on institutional objectives, incorporating broader analysis of positive and negative impacts as well as cascading and cumulative consequences.
Inherent Risk	Risk that exists by virtue of an organization's existence in the absence of any action being taken by management to alter the risk likelihood or impact.

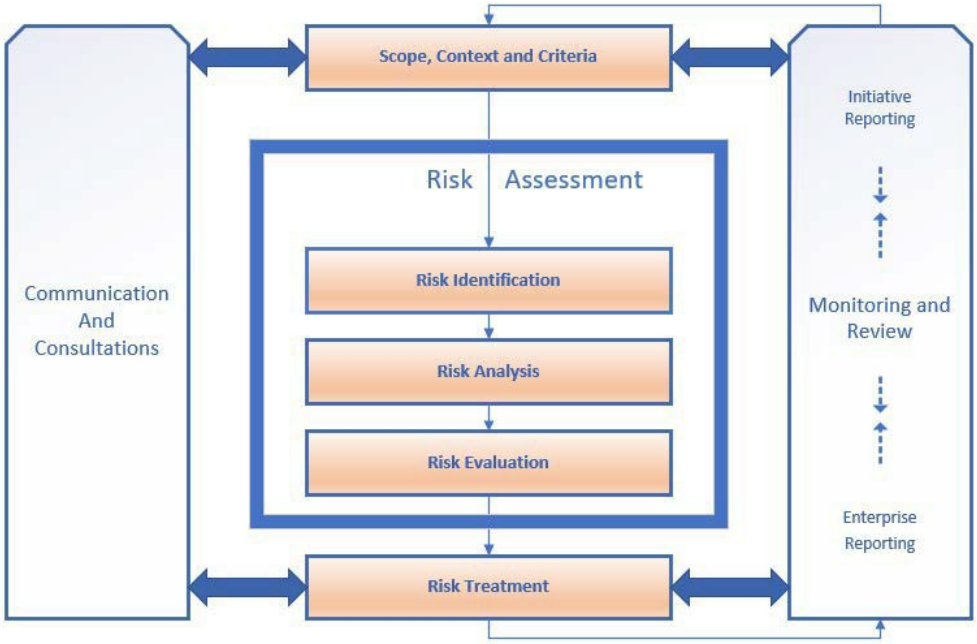
Likelihood	Defined by the ISO 31000: 2018 Standard as the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency). The University characterizes likelihood within a defined timeframe of 24 months.
Primary Risk Owner	A member of the Executive Team who is accountable for the implementation of mitigation strategies for an assigned risk.
Residual Risk	The risk that is left after it has been assessed within current controls and mitigation strategies in place.
Risk	Defined by the ISO 31000: 2018 Standard as the effect of uncertainty on objectives, as well as the chance or probability of loss.
Risk Acceptance	An informed decision to accept the likelihood and impact of a risk occurring.
Risk Analysis	A systematic use of available internal and external information to determine how often specified events may occur and the magnitude of their impact on the entity.
Risk Appetite	See Risk Tolerance
Risk Assessment	A comprehensive approach towards identifying risks, undertaking a risk analysis to determine consequences and likelihood, and completing a risk evaluation by determining which risks need mitigation or harm reduction.
Risk Avoidance	An informed decision to not become involved in a risk situation.
Risk Management	The process of identifying, assessing and developing management strategies to deal with risk(s) facing an organization.
Risk Mitigation	That part of risk management which involves the implementation of policies, standards, procedures and physical changes to eliminate, minimize or manage risk.
Risk Reduction	A selective application of appropriate techniques of management principles to reduce either the likelihood of an occurrence of the risk, or the impact, or both.
Risk Register	The University's formal record of identified Risk exposures that are being addressed for mitigation and management.
Risk Sharing	Sharing the responsibility for a loss with another party through legislation, contract, insurance, waivers, or other means.
Risk Tolerance	The willingness to accept risk in pursuit of objectives; often expressed in a Risk Tolerance Statement.

Stakeholder	A person or organization that can affect, be affected by, or perceive themselves to be affected by, a decision or activity.
University Community	All faculty and staff, students, Board Members, contractors, postdoctoral fellows, volunteers, visitors and other individuals who work, study, conduct research or otherwise carry on business of the University.

4. Guiding Principles

4.1. Athabasca University will implement an Enterprise Risk Management (ERM) Program as described in ISO 31000:2018. The ERM Framework and the Risk Tolerance Statement provide additional guidance to the University Community.

4.2. Under the direction of the Director, Strategic Initiatives and Services, key processes associated with the ERM Program are implemented as per the following diagram:



ERM Key Processes

4.3. Risk Assessment

a) Risk Identification
   i. Each risk will be assigned a Primary Risk Owner.
   ii. The process of risk identification begins with clarifying and articulating the primary strategic objectives and priorities of the University in order to generate a comprehensive list of risks based on events which could affect achievement of objectives.
   iii. This is accomplished through annual engagement and surveying of Executive Team members and/or identified delegates and careful review of the University's strategic, academic, research and capital planning activities.

b) Risk Analysis and Evaluation:
   i. Each of the identified institutional level risks, are to be evaluated by Executive Team members and/or identified delegates on the basis of their likelihood and impact using the risk criteria and evaluation tools in the ERM Risk Tolerance Statement. The initial assessment is to be done in order to generate an inherent risk assessment.
   ii. This analysis will enable assessment of the risks among the risk levels of Low Risk, Normal Risk, High Risk, and Critical Risk as defined in the ERM Risk Tolerance Statement based on inherent risk levels, as per the Risk Level Matrix in Appendix A.

4.4. ERM Primary Risk Register

a) Based on the risk assessment processes a Risk Register will be developed and maintained by the Director, Strategic Initiatives and Services.
b) The ERM Primary Risk Register must be reviewed and updated at least annually to anticipate and respond to changing internal and external realities.
c) The review should enable the identification of new and emerging risks and will be carried out as outlined in 4.3 Risk Assessment section.
d) All evaluated risks should be heat mapped according to the Risk Mitigation Matrix in Appendix B which identifies expected behaviors by Risk Owners based on the level of risk.
e) All Risks in the ERM Primary Risk Register should have a Control Record that identifies the Risk, Risk Description, Risk Drivers, Risk Owner and an inherent and residual risk level based upon a likelihood

and impact assessment as outlined in the ERM Risk Tolerance Statement.

f) A comprehensive review of the ERM Primary Risk Register should occur annually. The timing of the annual review should be aligned with the integrated planning cycle.

g) The ERM Primary Risk Register will be presented to the Board annually for approval through the Audit Committee.

4.5. Risk Mitigation

a) The Board defines risk tolerance related to key areas of the University's educational, learner support and business operations and with regard to the achievement of the University's strategic objectives.

b) Mitigation procedures for each category are as follows:

i. Critical Risk – Continuance of a risk with an inherent risk level assessed as a Critical Risk is not acceptable given existing circumstances without application of mitigation strategies that reduce the residual level of the risk to Normal Risk or Low Risk.

ii. High Risk – Continuance of a risk with an inherent risk level assessed as a High Risk is not acceptable under existing circumstances unless mitigation strategies are applied that reduce the level of residual risk to Normal Risk or Low Risk.

iii. Normal Risk – Continuance of a risk with an inherent risk or residual risk level assessed as Normal Risk is acceptable as long as the current mitigation strategies remain in place.

iv. Low Risk – Continuance of a risk with an inherent risk or residual risk level assessed as Low Risk is acceptable.

c) The approval authorities responsible for determining if a risk is acceptable for the University are as follows:

i. The Board must approve acceptance of any risks categorized with an inherent risk of Critical, contingent on management's implementation of mitigation strategies that result in a Residual Risk level of Normal or Low.

ii. Executive Team has authority to approve acceptance of any risk categorized with an inherent risk of High, contingent on management's implementation of mitigation strategies that result in a Residual Risk level of Normal or Low.

iii. Executive Team has authority to approve acceptance of any risk categorized with an inherent risk of Normal, contingent on management's implementation of mitigation strategies that result in a Residual Risk level remaining at Normal or being reduced to Low.

iv. Acceptance of a risk with an inherent risk level of Low, may be further delegated to members of Administrative Council to manage.

4.6. Quarterly Monitoring, Review and Reporting

a) An ERM Summary Report shall be compiled by the Director, Strategic Initiatives and Services, based upon input from the Primary Risk Owners and presented quarterly to the Board of Governors thought the Audit Committee

b) The ERM Summary Report should provide management and the Board of Governors with the confidence the ERM program is implemented as designed:

i. monitor and report on status and effectiveness of identified risk mitigation strategies;
ii. advise of new or emerging risks, as appropriate;
iii. advise of a change in risk assessment level; and,
iv. consider the effectiveness of the overall risk management process at the University.

5. Applicable Legislation and Regulations

Financial Administration Act, Chapter/Regulation: F-12 RSA 2000
Government Accountability Act, Chapter/Regulation: G-7 RSA 2000
Post-Secondary Learning Act, Chapter P 19. 5 2003, Banking and Investment, 75(3)
Governors of Athabasca University General By-Laws

6. Related Procedures/Documents

Enterprise Risk Management Policy
ERM Risk Tolerance Statement
ERM Framework
IT Risk Management Procedure

NOTE: The subject matter and scope of this procedure are also supported by internal-use only Standard Operating Procedures, including SOPs unique to AU business areas.

History

Date	*Action*
March 27, 2020	Associated Policy Approved (The Governors of Athabasca University Motion #242-03)

APPENDIX A: RISK LEVEL MATRIX

The intersection of a risk's likelihood and the severity of its impact categorizes the risk level for consistent application across the University.

LIKELIHOOD

IMPACT	RARE	UNLIKELY	NORMAL	LIKELY	ALMOST CERTAIN
SEVERE	HIGH RISK	CRITICAL RISK	CRITICAL RISK	CRITICAL RISK	CRITICAL RISK
MAJOR	NORMAL RISK	HIGH RISK	HIGH RISK	CRITICAL RISK	CRITICAL RISK
NORMAL	NORMAL RISK	NORMAL RISK	NORMAL RISK	HIGH RISK	HIGH RISK
MINOR	LOW RISK	LOW RISK	NORMAL RISK	NORMAL RISK	HIGH RISK
INSIGNIFICANT	LOW RISK	LOW RISK	LOW RISK	LOW RISK	NORMAL RISK

Note: If a risk falls into several categories, it is always placed in the category with the highest risk level. For example, if an activity could result in a major reputation impact as well as a Normal financial/ physical Infrastructure impact, it should be considered a major impact.

APPENDIX B: MITIGATING THE RISK – MITIGATION MATRIX

The Mitigation Matrix below identifies the requirements for mitigation expected of members of the University Community based on the level of risk.

RISK LEVEL TOLERANCE AND MITIGATION REQUIREMENTS	
RISK LEVEL	**MITIGATION REQUIREMENTS**
CRITICAL RISK	Level of Risk is not acceptable given existing circumstances and must be mitigated immediately. Risk poses non-recoverable, immediate and/or lasting threat of loss. Risk exposure requires immediate, continued, mitigation and/or cessation of activity giving rise to the Risk. Should be monitored constantly and reviewed monthly.
HIGH RISK	Level of Risk is not acceptable given existing circumstances unless is it reduced to a lower level. Risk poses significant but recoverable (with effort) loss. Requires mitigation measures to immediately reduce Risk Level and /or continued effort with additional mitigation strategies to reduce risk exposure to acceptable levels in the midterm. Should be constantly monitored and reviewed every 3 months.
NORMAL RISK	Level of risk exposure is known and is being successfully managed. Continuation of planned/existing mitigation strategies is expected and managed by specific monitoring or response procedures. Should be monitored and reviewed annually.
LOW RISK	Level of Risk is acceptable and planned for, such as a risk inherent to approved business operations. Manage by routine procedures and operations and does not require additional mitigation, but should be reviewed annually.