

| Enterprise Risk Management Policy | | | |
|--|--|-----------------------|----------------|
| Policy Sponsor | The Office of the President | Category | Board |
| Policy Contact | Vice President, Finance and Administration and Chief Financial Officer (CFO) | Effective Date | March 27, 2020 |
| Approved By | Board | Review Date | March 27, 2025 |
| Approved Date | March 27, 2020 | | |

1. Purpose

Enterprise Risk Management is an integral, essential expectation associated with the University's intention to take risks, seek out new ideas and adopt innovations to clearly define value-added outcomes. Successful management and oversight of institutional activities must comply with legislative requirements, promote operational efficiencies and mitigate or reduce the implications of risk as appropriate within risk tolerance expectations. All activity has an element of inherent risk associated with it. It is imperative to assess risks at all levels of the organization in order to effectively identify and appropriately address them.

2. Scope

Application of this policy is complemented by a Risk Tolerance Statement and Enterprise Risk Management (ERM) Framework. The Board is responsible for describing its tolerance for acceptable risks and for approving the ERM Framework. All members of the University Community share responsibility for practicing effective risk management based on these guidance documents and associated procedures.

3. Definitions

| | |
|----------------------|--|
| Board | The Governors of Athabasca 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. |
| 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 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. |
| University | Athabasca University |
| 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. The purpose of Enterprise Risk Management (ERM) at Athabasca University is to identify and manage the risks that could influence the achievement of the organization's strategy and operations. The ERM program provides a structured, consistent, and continuous process for the proactive identification and reporting of risks to senior management and the Board of Governors. The policy and procedures establish the principles of the program, assign roles and responsibilities for risk management and establish a common risk language.
- 4.2. ERM informs decision making and action regarding strategic and operational activities by providing decision-makers with informed choices to plan for and manage through uncertainty.
- 4.3. The University is committed to incorporate a systematic approach to risk management that can be applied consistently across all levels of the organization, including proactive maintenance of its ERM Framework.
- 4.4. Adherence to risk management practices are expected of all members of the University Community. The Vice President, Finance and Administration and CFO is responsible for building increased awareness and understanding of this shared responsibility.
- 4.5. ERM business processes employed by the University are embedded within routine planning and evaluation activities to ensure continual improvement, including working in a coordinated manner with internal audit in the identification and assessment of risks and mitigation strategies.
- 4.6. The University, where appropriate, will engage third parties in Risk Sharing in order to protect both the University Community and its assets.
- 4.7. Management will carry out ongoing identification and assessment of risks and provide regular reporting on mitigation strategies as required by the Monitoring and Review business processes in the ERM Framework, in order to provide assurance that enterprise risks are being managed proactively at all times.

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

[ERM Framework](#)

[ERM Risk Tolerance Statement](#)

[Enterprise Risk Management Procedure](#)

[Information Technology Risk Management Procedure](#)

NOTE: The subject matter and scope of this policy and its related procedures are also supported by internal-use only Standard Operating Procedures.

History

| <i>Date</i> | <i>Action</i> |
|----------------|--|
| March 27, 2020 | Policy Approved (The Governors of Athabasca University Motion #243-03) |