Framework for: *"Enterprise Risk Management"*

Overview

USask faces external and internal factors and influences that make it uncertain whether strategic priorities and operational commitments will be met. Managing Risk is part of governance and leadership and is fundamental to informed decision making.

The Board of Governors approves USask's ERM Policy requiring a systematic ERM Framework. The ERM Framework includes defined and accepted Risk Tolerance and Appetite statements and ERM Procedures, which inform a routinely updated Risk Register for reporting.

Objective

To support the advancement of USask's mission, strategic priorities and operational commitments, management and the Board of Governors have committed to develop systematic and effective Risk Management processes across USask. The ERM Framework is designed to:

- Establish common risk language and direction related to risk management.
- Describe responsibilities for risk oversight among Members.
- Differentiate key risks and Opportunities in USask's strategy and activities.
- Increase the likelihood that risks are managed, and strategic priorities will be achieved.
- Evaluate USask's risk management processes and whether they are functioning effectively'
- Facilitate open communication between management, the Audit and Finance Committee, and the Board of Governors with respect to risk.
- Build an appreciation for risk management and a culture of risk awareness.
- Encourage proactive decision making.
- Improve operational efficiency and effectiveness.

Framework Design

The effectiveness of USask's ERM will depend on its integration into the governance of the organization, including decision making. This requires support from all members, particularly senior management and the Board of Governors. The key components of the framework design include:

- **Leadership and Commitment** – Senior management and the Board of Governors integrate risk management across USask activities by adopting an ERM Policy and setting USask's risk tolerance and appetite.
- **Integration** – The ERM is customized to USask's organizational structure.
- **Design** – The ERM is adaptable to USask's evolving external and internal context.
- **Implementation** – Training is provided, and learning through consistent practice and dialogue supports an evolving continuous improvement and risk aware culture.
- **Evaluation** – Periodic performance measures of the ERM against its purpose, indicators, and expected behaviours occur to support ERM maturity plans.
- **Improvement** – The ERM is designed to adapt to changing contexts and continually improve.

Process

Communication and Consultation

Communication and consultation with members:

- Builds a broader understanding of risk and the basis to how priorities are established.
- Ensures different views are considered when defining and evaluating risks.
- Provides sufficient information to support Risk Assessment by senior management or others.
- Builds a sense of inclusiveness and ownership among those affected by Risk.

Risk Assessment

Conducting the Risk assessment should be systematic, based on best available information, supplemented by further Risk Owner explanation, as necessary. Risk assessment is the overall process of risk identification, analysis and risk evaluation, each described as:

Risk Identification – Identifying risks that might help or prevent USask in achieving is mission, strategic priorities, and operational commitments. Risks should be defined and described by an appropriate risk owner.

The description of a risk should include a case example developed by the risk owner and Risk Analyst to promote broader understanding across senior management.

To identify risks the following factors, and the relationship between those factors, should be considered whether their sources are under USask's control:

- Tangible and intangible sources of risk.
- Causes and events.
- Threats and opportunities.
- Vulnerabilities and capabilities.
- Changes in the external and internal context.

- Indicators of emerging risks.
- The nature and value of assets and resources.
- Consequences and their impact on priorities.
- Limitations of knowledge and reliability of information.
- Time related factors.
- Biases, assumptions, and beliefs of those involved.

Risk Analysis – Comprehending the nature of risk, its characteristics, and level of risk involves consideration of many factors. Risk analysis should consider factors such as:

- The likelihood of events and consequences.
- The nature and magnitude of consequences.
- Complexity and connectivity.
- Time-related factors and volatility.
- The effectiveness of existing controls.
- Sensitivity and confidence levels.

Risk analysis should first be prepared by the risk owner with support of the risk analyst for broader Review by senior management. Risk analysis can be further influenced by divergent opinions, biases, perceptions of risk and judgments.
Additional influences can relate to the quality of information used, the assumptions made, and limitations of techniques and how they are executed. These influences should also be considered with the objective of generating a generally informed and accepted risk analysis.

Risk Evaluation - The results of risk analysis, including risk deliberations, provide insight for decisions and options for risk treatment based on the generally informed and accepted risk analysis.
The risk evaluation involves comparing the results of the risk analysis with USask's established risk appetite and tolerance criteria to determine where additional attention and action is required.
The risk evaluation can take many forms, USask will deploy a quarterly information package and risk survey approach to collecting the initial senior management risk evaluations. Those results will be presented back to senior management for additional discussion and deliberation, and where appropriate, an opportunity to re-evaluate risks will be provided.
The outcome of the risk evaluation is recorded, communicated, and validated at further appropriate levels within the organization, such as the President's Executive Committee, the Audit and Finance Committee, and the Board of Governors.

Risk Action – the risk evaluation supports USask's assessment of residual risk and can lead to:

- Accept the risk - Do nothing further.
- Maintain existing controls.
- Consider risk treatment options.
- Undertake further risk analysis to better understand the risk.
- Reconsideration of strategic priorities.

Risk Treatment

The objective of risk treatment is to select and implement appropriate options for lowering residual risk. Risk treatment involves:

- Formulating and selecting risk treatment options.
- Planning and implementing risk treatment.
- Assessing the effectiveness of the treatment.
- Deciding whether the remaining risk is acceptable.
- If not acceptable, initiating further treatment.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options for treating risk may involve one or more of the following:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the Risk.
- Taking or increasing the risk to pursue an opportunity.
- Removing the Risk Source.
- Changing the likelihood.
- Sharing the risk (such as, insuring the risk).
- Accepting and retaining the Risk by informed decision.

Risk Register

The Risk Register is the consolidated list of Enterprise Risks, with definitions, example cases, risk assessment, risk action plans, and risk ranking based on USask's risk appetite and/or tolerance (ERM Policy – Appendix 1).

Quarterly Monitoring, Review, and Reporting

Monitoring and reviews are to assure and improve the quality and effectiveness of the ERM process, design, implementation, and outcomes.

USask will conduct its risk process at minimum each quarter (Q). Each cycle, the following workflow outline will generally be followed to monitor, review and report risk.

May

- Annual Risk Universe review and validation.

June (Q1) | September (Q2) | November (Q3) | March (Q4)

- Risk owner review and update risk description, case, and risk assessment.
- Senior management receive risk overview package and complete the risk survey.

July (Q1) | October (Q2) | December (Q3) | April (Q4)

- Senior management review and deliberate the risk survey results with an opportunity to re-evaluate risks, if appropriate, to arrive at the generally informed and accepted risks.
- President and Executive Committee review and deliberate the risk assessment.

September (Q1) | December (Q2) | February (Q3) | June (Q4)

- Audit and Finance Committee and Board of Governors Review and discuss the ERM report and progress on the ERM maturity plan.

During the year an emergent risk may arise at any time, in this situation the President's Executive Committee can initiate adding a risk to the risk universe, identifying a risk owner and initiating the risk process for the risk.
The result of the risk process will be recorded and reported through appropriate levels of management and governance. Recording and reporting will:

- Communicate key risk management activities and outcomes across USask.
- Provide information to support informed decision making.
- Improve risk management activities.
- Assist with communication across members, including those responsible for risk management activities.

Definitions

The source of institutional approved definitions is in the Academic and Curricular Nomenclature.

Consequence – The outcome of an event affective USask strategic priorities or operational commitments.

Control – A measure or measures that maintains or modifies risk, which could take the form of a policy, process, practice, device, or other conditions or actions.

Enterprise Risk – Is the potential for an event or action to adversely affect USask's strategic priorities, operational commitments, which may involve stakeholders, finances, and/or impair USask's reputation.

Enterprise Risk Management (ERM) – Is the logical and systematic process to manage risks and seize opportunities within USask's risk appetite.

Enterprise Risk Management Framework – is a set of components that provide the foundation for designing, implementing, monitoring, reviewing, and continually improving risk management throughout USask.

Event – The occurrence or change of a set of circumstances, which can be a risk source.

Exposure – Extent to which an organization and/or stakeholder is subject to an event.

Impact - Is the severity of consequences that can have a positive or negative effect on strategic priorities or operational commitments, as well as cascading and cumulative consequences.

Inherent Risk – The risk of an event occurring in the absence of internal controls and/or a risk management process to mitigate the risk. Risk that exists by virtue of USask's existence in the absence of any action being taken by management to alter the risk likelihood or impact.

Likelihood – The chance or probability of something happening, whether defined, measured or determined subjectively or objectively, qualitatively or quantitatively, and described using general terms or mathematically (such as frequency over a given time).

Members – Individuals engaged in university activities, including faculty, staff, board members, students, postdoctoral fellows, research affiliates, contractors, and agents, who are responsible for conducting university business and managing risk within their roles.

Objective – Result to be achieved whether it be strategic, tactical or operational for USask

Opportunity – A risk-related opportunity is a positive outcome that arises from an uncertainty or potential negative event.

Probability – Measure of the chance of occurrence expressed as a number from 0 to 1, where 0 is impossibility and 1 is absolute certainty.

Residual Risk – the risk that is left after it has been assessed after current controls and mitigation strategies in plan.

Review – Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

Risk - The effect of uncertainty on objectives, resulting in positive and/or negative impact on the University's mission and can address, create or result in opportunities or threats.

Risk Acceptance – An informed decision to accept the likelihood and impact of a risk occurring.

Risk Action Matrix – is a visual risk exposure into quadrants where the vertical axis is a function of impact plus likelihood divided by two and the horizontal axis is an assessment of management preparedness gap resulting in enterprise risks falling into the Improve, Test, Monitor, or Optimize action quadrants.

Risk Analysis - A systematic process to review available internal and external information to determine how often specified events may occur and the magnitude of their impact on USask.

Risk Appetite – Also referred to as risk tolerance, is the overall level of risk USask is prepared to accept to achieve its strategic priorities and/or meet its organizational objectives, often expressed as a Risk Tolerance Statement.

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 Map – Is the visual representation of risk likelihood, impact, and velocity.

Risk Management - Coordinated activities to direct and control the probability and/or impact of risk.

Risk Mitigation – The part of risk management that involves the implementation of policies, procedures, and actions to eliminate, minimize, or manage risk.

Risk Owner - a person with accountability and authority to manage a risk. This is a person who is both interested in resolving a risk, (i.e., someone who is very much interested in preventing such risks from happening) and positioned high enough in the organization, so that his or her voice would be heard among the decision makers, to do something about it.

Risk Register – The official record of risks facing the University, as established through the risk assessment process undertaken pursuant to the Enterprise Risk Management Policy and Procedures.

Risk Reduction – A selective action to reduce either the likelihood of an occurrence of 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 Source – An element either alone or in combination could give rise to risk.

Risk Tolerance - see Risk Appetite.

Risk Treatment – Is the management action that avoids, accepts, transfers, or reduces various risks.

Risk Universe – Is a categorized list of prioritized enterprise risks that USask has identified as key risks that could impact the ability to realize strategic priorities and operational commitments. Those risks are typically categorized by strategic, operational, financial, and compliance related risks.

Risk Velocity – Is the speed of onset in which a risk can have an impact.

Stakeholder – A person or organization that can affect, be affected by, or perceive themselves to be affected by an action.

Uncertainty – State, even partial, of deficiency of information related to understanding or knowledge.

Related Policies/Documents

Enterprise Risk Management Policy
Academic and Curricular Nomenclature