NDSU | FOUNDATION

Enterprise Risk Management Policy

Purpose

The purpose of NDSU Foundation's ("Foundation") enterprise risk management (ERM) program is:

1) To identify, assess, manage and mitigate key risks across the enterprise
2) Align strategy and risk

Policy

It is the policy of the Foundation to proactively assess and respond to any risks that may affect the achievement of the Foundation's mission, goals, and strategic objectives. The Foundation is also committed to compliance with all relevant laws, regulations and policies. The Foundation's commitment to managing risk and supporting compliance efforts is implemented through the Foundation's ERM program.

The Foundation recognizes that there is exposure to risk inherent in its programs and activities. Taking risks provides the opportunity to find innovative and more efficient ways to operate, to achieve higher returns on investments, and to protect business continuity. It requires a balanced approach to minimize hazards, influence and control uncertainties and manage opportunities so that negative outcomes are acceptable or mitigated and chances of good outcomes are increased.

The Foundation regularly engages in comprehensive, strategic risk assessment to identify major risks to mission success, to establish risk tolerances, to establish plans for management of risks outside of tolerance, to monitor results, and to provide reasonable assurance to the Executive Governing Board ("Board") of the achievement of Foundation objectives.

Procedures

The Foundation will implement and maintain a disciplined process to ensure that comprehensive risk assessment occurs at least annually and addresses strategic risks, financial risks, operational, compliance risks and reputational risks. It is understood that as an institutionally related foundation, the Foundation's risks are deeply shared with the University. Identified risks should be prioritized. Prioritization should include a discussion of likelihood, impact, complexity, preparedness and any past or existing problems. Both the identification and prioritization of risk should be reviewed annually.

High-priority risks require a documented mitigation plan. Appropriate plans for management of risk are to avoid, accept and monitor, reduce the likelihood, reduce the impact, or risk transfer and may include business process improvement, policy and procedure development, greater resource allocation, deploying skilled resources, and technological improvements. The Foundation will review industry best practices on managing and controlling key risks. Plans should be documented and monitored for implementation and effectiveness.

While the primary responsibility for institutional risk management is assigned by the President/CEO to the Chief Financial Officer, senior leadership is responsible to ensure all staff have an understanding and are using information about risk in decision making. This awareness should be promoted through education, training, and information sharing.

To meet Board legal and fiduciary responsibilities, at least semiannually, the Finance & Audit Committee will review with senior leadership the Foundation's major policies and processes with respect to Enterprise Risk Management, including but not limited to the identification of risks and the efforts being taken to manage, mitigate and insure the Foundation against such risks. The Finance and Audit Committee provides the Risk Report to the Board semiannually.

Process

- **Step 1 – Risk Identification (Annually – Senior leadership team responsible)**
  - Identify list of top risks (approximately 20)
    - Focus on big risks that have potential to derail ability to execute strategic plan
    - Remember risks are not just bad events, but also missed opportunities
    - Review problems that could have been prevented
    - Review areas that have caused concern for peer institutions
    - Review best practices and regulations that have recently been implemented
  - CFO compiles organization's Risk Report
  - Develop a disciplined process to consider risk in strategic discussions
- **Step 2 – Risk Assessment (Annually – Senior leadership team responsible)**
  - Prioritize top risks with a framework using financial impact and likelihood
    - Assess reputational impact as it relates to financial impact
    - Assess preparedness, potential for mitigation, and tolerance
  - Assign ranking of High/Probable (red), Medium (yellow), or Low (green)
    - Immediacy of Risk
    - How likely is it that this will occur in our organization?
    - How bad will it be if it does?
    - Identify and analyze loss exposure and safety hazards
    - The goal is to arrive at a shared understanding of each risk's impact and likelihood relative to other important risks.
  - Approximately 5-10 should be reported to the Board/Finance and Audit Committee
    - Experience shows that focus is diluted and follow-through is weak if an institution's risk register is larger than that.
- **Step 3 – Risk Mitigation Plan (Ongoing – Subject-area staff member responsible)**
  - Regular reports are required for each high-priority risk being monitored
  - Assign staff and potentially Board committee ownership to top risks based on subject-area (limit to 10 or less)
  - Develop mitigation plan for risks that is regularly shared with senior leadership
    - Plan should be informed by appropriate staff at every level and across functional teams
    - The plan will identify specifically how the risk will be dealt with and required action steps to implement including, but not limited to:
      - Preventive controls,
      - Detective controls, and
      - Potential internal controls to improve/implement
    - Senior leadership recognizes that some level of residual risk will always exist due to limited resources and future uncertainty. The risk should be managed to the acceptable tolerance, not necessarily to elimination. The best risk management mitigation plans

should strive to reduce the likelihood and impact to a level that would not disrupt the institution's plans and seriously damage its reputation.

  - Involve all staff. Many serious risks are first spotted by those closest to the work. It is incumbent upon each person who is monitoring risk to involve staff at all levels and in all relevant departments. Staff should view risk management as an integrated part of daily activities rather than an event.
  - Monitor the results produced or achievement of change
- **Step 4 – Report to Board (Semiannually – Finance and Audit Committee responsible)**
  - Review the risks identified by senior leadership via the Risk Report
  - Ask questions on the process and scope of the risk identification process
  - Discuss and agree on the institution's risk tolerance for high priority risks
  - Review risk mitigation plans or treatment proposed by the senior leadership
  - Regularly monitor the senior leadership's identification, assessment, and mitigation plans
  - Finance and Audit Committee provides Risk Report to the Board semiannually
- **Step 5 – Reassess risks and prioritization (Annually – Senior leadership team responsible)**
  - Annual reviews will focus on reviewing prior year risks that were being monitored, updating prioritization of previously identified risks and identification of new risks
  - Look for blind spots. Using the prior years' experience, share any process in risk mitigation that revealed new aspects to the risk or impacted the prioritization of the risk. Integrate, as appropriate, this experience into anticipated risk monitoring for upcoming year.
- **Step 6 – Maintain the process (Ongoing – Chief Financial Officer responsible)**

Definitions

Term	Definition
Risk	Any issue that has the potential to affect the organization's ability to meet its objectives
Enterprise Risk Management	A business process, led by senior leadership, that is holistic approach to risk management and includes: • Identifying risks across the entire enterprise; • Assessing the impact of risks to the operations and mission; • Developing and practicing response or mitigation plans; and • Monitoring the identified risks, holding the risk owner accountable, and consistently scanning for emerging risks.
Types of Risk:	
Strategic	Puts the organization at risk for meeting its long-term organizational goals
Operational	Exposure to uncertainty related to day-to-day risks
Financial	Risk of financial impact to the organization that may result in a loss of assets
Compliance	Exposure related to laws and regulations, also includes compliance with donor intent
Reputational	The threat of negatively impacting the external perception and image of the organization or institution

Effective Date: September 29, 2023

Responsible Parties

- Policy Owner:
    - Governance: Finance and Audit Committee
    - Staff: Sr. Vice President of Finance & Operations/Chief Financial Officer