STANDARD ADMINISTRATIVE PROCEDURE

24.01.99.M0.02 Enterprise Risk Management

Approved March 1, 2011
Revised February 28, 2016
Revised June 6, 2023
Next scheduled review: June 6, 2028

SAP Statement and Reason for SAP

Texas A&M University is committed to identifying and managing risks in a proactive manner. As such, Texas A&M University implemented an Enterprise Risk Management (ERM) process to establish a systematic organization-wide approach to identify risks and mitigation strategies.

ERM is an on-going process designed to identify and manage potential risks that may adversely affect the University's ability to achieve its objectives. ERM assesses and documents actions to be taken by the University to identify, mitigate, and monitor risks that negatively impact the achievement of the University's mission, strategic plan, goals, and/or continuing operational programs. The University's ERM process includes 1) identifying and ranking risks, and 2) documenting and reviewing mitigation activities related to those risk areas.

The ERM process requires an annual risk assessment for the University as a whole. To enhance risk management oversight, other major functions and units throughout the University (i.e., Vice Presidents, others reporting to the President, Deans, major functions and operating units, etc.) may apply the process, at their discretion, to enhance the oversight of their units.

Definitions

Enterprise Risk Management: A process applied across the entity that is designed to identify potential risks that may affect the entity, manage risks within the entity's risk tolerance, and support the achievement of the entity's objectives.

Mitigating activities/strategies: Actions, procedures, and processes used to manage (limit, reduce, avoid, accept, transfer, and/or share) and monitor risks.

Risk: Any event or action that adversely impacts the entity's ability to achieve its objectives. Types of risks include strategic, operational, reputational, financial, technology, compliance, fraud, etc.

Risk assessment: The process used to identify and rank risks, and document mitigating strategies, monitoring, and/or reporting processes.

Risk ranking: A qualitative process to prioritize risks using a high, medium and low scale considering both the potential impact (consequences) and probability of occurrence (likelihood of happening).

Official SAP/ Responsibilities/ Process

---

1. Roles and Responsibilities

   1.1 A university-wide risk assessment that considers significant risks from across the university will be performed on an annual basis. Executive management, with input from their direct reports (i.e., Vice Presidents, Deans, Directors, etc.) shall identify and rank significant risks. To assist with strategic planning and oversight, major units within the University are encouraged to perform periodic internal risk assessments or other measures to identify significant risks.

   1.2 The Division of Risk, Ethics, and Compliance (DREC) coordinates the ERM process and maintains the university-wide ERM records. DREC is responsible for conducting and facilitating the university-wide risk assessment, and performing a review of significant mitigating and monitoring activities. Results of the ERM process shall be reported to executive management and System Risk Management, as appropriate. In addition, DREC personnel are available to university units to facilitate risk assessments. This includes identifying and ranking risks and documenting mitigation and monitoring processes.

   1.3 Every Texas A&M University employee has a responsibility to manage and mitigate risks.

2. When performing a risk assessment, the process includes the following steps:

   2.1 Review the mission, vision, goals, objectives and/or strategic plan and any major activities and/or functions.

   2.2 Identify and prioritize risks. When prioritizing or ranking risks, consider the risk's consequence and the probability of occurrence.

   2.3 Identify the significant mitigating activities. Document the evidence of the mitigating activity occurring and the designated accountable person/position.

   2.4 Document the significant monitoring and executive reporting processes, such as supervisory reviews, oversight, communication flow, and assurances gained by management that risks are effectively managed.

2.5 Review the overall effectiveness of the mitigating, monitoring and/or reporting processes significant in managing the highest ranked risks. Develop action plans and implement new mitigating activities/strategies to enhance effectiveness, as needed.

2.6 Maintain a copy of the current risk assessment documents and provide a copy to DREC.

Related Statutes, Policies, or Requirements

System Policy 24.01 Risk Management

Appendix or Forms

Additional information regarding Enterprise Risk Management is available at https://orec.tamu.edu/erm-compliance/.

Contact Office

Division of Risk, Ethics, and Compliance
http://orec.tamu.edu