



TEXAS TECH™

Operating Policy and Procedure

OP 40.13: Enterprise Risk Management

DATE: September 5, 2025

PURPOSE: The purpose of this Operating Policy/Procedure (OP) is to establish a comprehensive framework for Enterprise Risk Management (ERM) at Texas Tech University (TTU), in congruence with Texas Tech University [System \(TTUS\) Regulation 1.1.1](#), Enterprise Risk Management – Standards of Practice.

REVIEW: This TTU OP will be reviewed every two years after publication by the TTU Office of Institutional Compliance and the TTUS Office of Risk Management, with substantive revisions forwarded to the Office of the President.

POLICY/PROCEDURE

1. Introduction

ERM assesses and defines actions taken to identify, assess, mitigate, monitor, and communicate risks that threaten the achievement of strategic plan goals and/or continuing operational activities. Through the implementation of an ERM framework, TTU aims to:

- Promote effective governance by aligning risk management with institutional priorities;
- Enhance decision-making by providing consistent risk analysis tools and processes;
- Safeguard the university's people, assets, and reputation while enabling innovation and strategic growth; and
- Ensure compliance with all applicable laws, regulations, and institutional policies.

This policy applies to all risks (strategic, operational and information technology, financial, and compliance) that may affect TTU and its stakeholders.

2. Statement of Risk Attitude

TTU will continuously seek out innovation in the way we deliver our mission while ensuring that all decisions are informed by an understanding of the uncertainties we face as an institution. We will continuously seek out those opportunities that can best strengthen our core values. While it is not possible or even desirable to eliminate all risk, we will not tolerate any risks that:

- Willfully expose students, employees, or other people to unsafe environments or activities;
- Intentionally violate laws, regulations, contractual obligations, or other externally imposed requirements; or
- Result in unethical behavior.

3. Definitions

- a. Enterprise Risk Management – Assesses and defines actions to be taken by the Board of Regents, Texas Tech University System Administration, and/or the component institutions to identify, mitigate, and monitor risks that threaten the achievement of strategic plan goals and/or continuing operational activities.
- b. ERM Subcommittee – A group comprised of a cross-section of executive risk owners and risk coordinators, whose purpose is to discuss and evaluate the growth and success of the ERM program. This group will meet twice per semester (fall and spring).
- c. Executive Risk Owner – A senior administrator who is responsible for the oversight of a specific high-level risk category with the TTU ERM framework.
- d. Risk – The possibility that an event or condition will negatively (or positively) impact TTU's ability to achieve its strategic goals.
- e. Risk Coordinator – An individual who facilitates the implementation of risk management practices within a particular university department or area.
- f. Strategic Risk Update – Annual briefing designed to inform executive risk owners and risk coordinators about emerging risks that could impact TTU's objectives and operations.

4. Major Categories of Risk

The TTUS Office of Risk Management has provided four major categories of risk for use by component institutions.

- a. Strategic – Risks threatening organizational reputation, constituent relationships, ability to generate funds, goal achievement, etc.
- b. Operational and Information Technology – Risks threatening continuity of activities, safety and security, information technology operations, physical infrastructure, process efficiency, program effectiveness, etc.
- c. Financial – Risks threatening resources, financial structure, ability to meet future financial needs, financial reporting, etc.
- d. Compliance – Risks of non-compliance with legal, regulatory, contractual, accreditation body, NCAA, or other requirements.

5. Rating Scales

The TTUS Office of Risk Management has provided rating scales by which risk can be ranked and assessed.

- a. Impact – The potential consequences to TTU should the risk occur. Impacts may range from negligible to significant across the four risk categories, and one event could generate multiple impacts.

- b. **Likelihood** – The chance that a risk will occur. This may range from extremely likely to very likely and should be assessed considering the effectiveness of existing controls, as they are known.
- c. **Velocity** – How quickly a risk could impact TTU. For example, an information technology cyberattack could have an instantaneous impact, while a legislative change may only impact the organization months or even years later.
- d. **Preparedness** – TTU’s readiness to deal with a risk. Preparedness should be assessed based on the existence and effectiveness of such aspects as prevention or detection controls, recovery arrangements, backups, response plans, communication plans, insurance, notifications to constituents, emergency management planning, etc.

6. Roles and Responsibilities

Defining roles and responsibilities in an ERM framework ensures accountability, clear communication, and effective risk management. It prevents confusion, reduces overlap, and aligns risk efforts with institutional goals. Regular reporting should flow upward, ensuring that leadership is aware of key risks, while guidance and policies should flow downward to ensure effective risk management at all levels.

- a. **President and Executive Risk Owners**
 - Promote a culture of risk awareness and accountability; and
 - Integrate risk management into strategic planning and decision-making processes.
- b. **Office of Institutional Compliance (OIC)**
 - Develop, implement, and maintain the ERM framework;
 - Conduct regular risk assessments; and
 - Monitor emerging risks and report findings to leadership.
- c. **Risk Coordinators**
 - Identify and assess risks within their respective departments;
 - Develop and implement mitigation strategies; and
 - Monitor and report risks to the OIC.

7. Procedure

TTU follows a structured timeline for ERM to ensure that risks are monitored and reported on a continuous basis. This timeline shows the ERM lifecycle over a two-year span.

- a. **Odd-Numbered Years**
 - March (second Friday): Internal responses due to OIC.
 - Spring Semester: OIC presents institutional status at President’s Executive Council.
 - September (second Friday): OIC distributes Strategic Risk Update.
 - November (second Friday): OIC initiates internal update process.

b. Even-Numbered Years

- March (second Friday): TTU submissions due to TTUS Office of Risk Management.
- May: Report presented to the TTU System Board of Regents.
- September (second Friday): OIC distributes Strategic Risk Update to executive risk owners and risk coordinators.
- November (second Friday): OIC initiates risk update process.

8. Right to Change Policy

TTU reserves the right to interpret, change, modify, amend, or rescind any policy, in whole or in part, at any time without the consent of workforce.