

**ENTERPRISE RISK
MANAGEMENT
PROGRAM**



TEXAS A&M
UNIVERSITY
CENTRAL TEXAS

CHARTING A PATH TO EXCELLENCE

Texas A&M University – Central Texas is a member of The Texas A&M University System which is governed by a nine-member Board of Regents. The mission of Texas A&M University – Central Texas (the “University”) is to be an upper-level institution committed to high-quality, rigorous and innovative learning experiences that will prepare its students for lifelong learning through excellence in teaching, service, and scholarship. To fulfill that mission, the University has embarked on an ambitious strategic planning initiative which is outlined in a five-year strategic plan that was initiated in 2011. This plan is designed to focus University commitment on three imperatives essential to building a quality institution of higher learning:

- a. Academic Excellence through Accountability and Classroom Rigor
- b. Building an Environment to Foster Scholastic Achievement
- c. Fostering a Sense of Community

The plan not only articulates these imperatives, it describes specific outcomes to be accomplished, and it details performance measures to chart progress.

The complex and rapid changes in today’s world place unprecedented pressures on the University, especially one as relatively young as the Texas A&M University – Central Texas. Events occur that have the potential to adversely affect the University’s ability to achieve its goals. The possibility that an adverse event will occur is called “risk”. Risks can be financial, operational, technological, environmental, regulatory, competitive, strategic, legal, reputational, and political in nature. They can affect the entire University, specific programs and individual departments.

To facilitate its commitment to excellence and support the achievement of its strategic plan, the University has decided to implement an Enterprise Risk Management (ERM) program to establish a systematic organization-wide approach that will allow it to proactively manage risks. Managing risks involves identifying risks, assessing their potential impact, and exercising prudent judgment to accept, avoid, reduce or share the risks.

AUTHORITY

A&M System Policy 03.01 – System Mission, Vision, Core Values, and Strategic Planning requires the development of an enterprise risk management process. This ERM program is designed to fulfill this requirement.

ENTERPRISE RISK MANAGEMENT PROGRAM

The goal of the ERM program is to address risks in a centralized, holistic approach rather than independently within operational units and functional areas. Addressing risks from a University-wide perspective gives personnel the opportunity to understand how their individual actions affect not only their specific goals, but also the achievement of the University's goals.

The University's ERM program will follow the Enterprise Risk Management Framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The COSO Enterprise Risk Management Framework is designed to create a consistent risk and control consciousness throughout an enterprise and establish the model for discussing and evaluating the organization's risk management processes.

Framework

The Enterprise Risk Management Framework is made up of eight separate components:

1. **Internal Environment.** The internal environment forms the basis for how risks are viewed and addressed. It includes:
 - a. Vision and mission
 - b. Organizational structure
 - c. Management's operating style
 - d. Assignment of authority and responsibility
 - e. Competence and development of personnel
 - f. Ethical values
 - g. Policies and procedures
 - h. Risk management culture

2. **Goal Setting.** ERM ensures that a formal process is in place to establish goals and that those goals support the University's mission and strategic plan and are consistent with its risk appetite. Risk appetite is the amount of risk the University is willing to accept in pursuit of its goals. It affects the risk management philosophy and in turn affects the University's culture and operating style. Risk management philosophy is the set of shared beliefs and attitudes that characterize how risks are considered from strategy development and implementation to day-to-day activities. It reflects the University's values, influences its culture and operating style, and determines how risks are identified, assessed, and managed.

3. **Event Identification.** Events have the potential to positively or negatively impact the University's ability to achieve its strategic goals. A variety of internal and external factors drive events. Examples of internal factors are infrastructure, people, processes, and technology. Examples of external factors are social, political and economic conditions, laws and regulations, technological changes, weather, and natural disasters. It is important to understand these internal and external factors and develop methods for identifying and monitoring these factors and related events.

4. **Risk Assessment.** Risk assessment is the process of identifying the risk level for events based on an assessment of vulnerabilities, likelihood of occurrence, and potential impact. Risk assessment is both a point-in-time activity and a continuous and iterative process. It involves a determination of both inherent risk and residual risk. Inherent risk is the risk to the University in the absence of any actions that may be taken to alter the likelihood, vulnerability, or impact related to that risk. Residual risk is the risk that remains after the risk mitigation activities occur.
5. **Risk Response.** After risks are identified and assessed, the University must decide how it will respond to those risks in order to bring the residual risk within the desired tolerance level (i.e., within its risk appetite).

Risk responses include:

- a. Accepting the residual risk associated with an event or activity
- b. Avoiding the event or activity that causes the risk
- c. Reducing the likelihood, vulnerability or impact associated with a risk
- d. Sharing a portion of the risk with others (e.g., insurance, outsourcing)

Risk responses should be evaluated according to the relative costs and benefits of possible responses so that decisions can be made to determine the best course of action.

6. **Control Activities.** Control activities are policies and procedures that help ensure risk responses are properly executed so that the University's goals can be accomplished. Control activities involve the University's structure, people, information systems, and operational processes. They are the means by which resources are directed, monitored, and measured.
7. **Information and Communication.** Financial and non-financial Information is needed at all levels throughout the University to identify, assess, and respond to risks. Information is available from internal and external sources, in quantitative and qualitative forms, and can be both formal and informal in nature.

Having and communicating the right information at the right time is essential to enterprise risk management. An inventory must be developed of the information needed for the ERM program and processes put in place to ensure that this information is effectively produced, aggregated, analyzed, and communicated to those involved in risk management.

The communication process should convey:

- a. The importance and relevance of effective enterprise risk management
- b. The roles and responsibilities of personnel at all levels in supporting and carrying out enterprise risk management
- c. The process for identifying existing and emerging risks to the University's goals
- d. The risks that have been identified and how those risks can impact the achievement of the University's goals
- e. The University's risk appetite and risk tolerances related to those risks
- f. Existing controls that address identified risks
- g. New controls or changes to existing controls that are designed to improve risk postures
- h. The process for determining the cost/benefit proposition for new and changed controls
- i. Sources of information and key indicators related to identified risks
- j. The process for monitoring and reporting the effectiveness of controls in maintaining and reducing risk exposures

8. **Monitoring.** Monitoring is the process of assessing the ongoing operating effectiveness of the ERM program and related activities. Monitoring can be accomplished through day-to-day management oversight and reporting and through separate control evaluations.

Monitoring should include these key activities:

- a. Identifying early warning indicators that signal changes in the risk environment
- b. Making changes to the details of the risks already documented in the risk register
- c. Adding new risks to the risk register
- d. Determining the effectiveness of risk control activities so that corrective action can be initiated when needed
- e. Reporting on the success of the ERM program

Benefits and Limitations

An effective ERM program will give the University a consistent and systematic approach to managing risks. It will allow the University to critically review its activities, assess new ideas, and seize opportunities. It is expected to provide tangible benefits, including:

- a. Greater confidence in decision making
- b. Fewer operational surprises, disruptions and losses
- c. Improved operational effectiveness and efficiency
- d. More effective deployment of resources
- e. Increased cross-institutional awareness and involvement in the achievement of strategic goals

While ERM provides important benefits, some limitations do exist, such as:

- a. Not all risks can be foreseen
- b. Sudden changes may not allow sufficient time to mitigate risks
- c. Sufficient resources may not be available to address all key risks
- d. Resources may not be correctly allocated due to limited information and/or the lack of control over external factors
- e. Errors and mistakes may occur in the control environment
- f. Controls may be circumvented and decisions overridden

The goal of the ERM program will be to maximize its benefits while addressing its limitations.

BUILDING AN EFFECTIVE ERM PROGRAM

One of the frequent reasons that ERM program implementations fail is that organizations try to implement all the components of ERM at one time, making the program too broad and overly complex. The University has elected to take an incremental approach by beginning with the basic components of the ERM framework and adding additional elements and complexity as the program matures over time.

Initially, the University will identify and focus on those risks that can directly impede the achievement of the business goals outlined in the University's Strategic Plan. The University will then determine specific actions designed to address those risks, and put in place targeted practices that will help it reduce the impacts of those risks and improve the likelihood that the goals listed in our Strategic Plan can be realized. This will allow the University to experience early "wins" and incorporate the ERM program into operational processes. As the program matures, we will apply the ERM framework in a more targeted manner at the program and department level.

PROGRAM IMPLEMENTATION

ERM program planning began in March 2012. ERM program introduction meetings were held with University leadership, department directors and other key personnel to introduce the concept of enterprise risk management, discuss why ERM is important to the University, and describe their roles and responsibilities in the program.

An ERM risk survey form was distributed to the University's executive team and department directors which requested the following information for compilation into the University's risk register:

- Department name, description and mission
- Three to five primary department goals
- Five to eight primary department processes
- Three University goals that were most relevant to the department
- Risk information for each department and University goal:
 - Short description for a risk that would impact the goal
 - One or more risk category names from the list below to designate the type of risk:
 - ◁ Strategic – events that affect the ability to make good decisions and respond appropriately to changes in critical internal and external factors such as social trends, economic trends, technological trends, industry trends, political changes, regulatory changes, etc.
 - ◁ Compliance – events that affect compliance with laws and regulations
 - ◁ Operational – events that affect ongoing business and educational processes
 - ◁ Technological - events that affect electrical and electronic systems
 - ◁ Financial – events that affect the sources/uses of funds and the achievement of financial goals
 - ◁ People – events that affect the availability, quality, health and safety of staff and students
 - ◁ Facility – events that affect the availability and quality of facilities
 - ◁ Reputational – events that affect public perception
 - Risk background – why the risk might occur

- Risk likelihood rating
 - ◁ High – happens frequently, occurs often, and is common or predictable
 - ◁ Medium – happens infrequently, sometimes occurs, or is unpredictable
 - ◁ Low – seldom happens, infrequent, rare, or has not happened before
- Risk proximity rating
 - ◁ Immediate (risk exists now)
 - ◁ Near-term (<1 year)
 - ◁ Mid-term (1-3 years)
 - ◁ Long-term (>3 years)
- Risk impact rating
 - ◁ High – consequence include termination of business area or program, significant injury or loss of life, termination of funding, significant financial loss/cost (including legal liability), and criminal penalties
 - ◁ Medium – consequences include inefficiencies and extra workloads, fines, minor injuries or property loss
 - ◁ Low – consequences have little or no effect on the organization; include warnings and/or reprimands with no other actions taken
- Risk impact description – a description of the effect the risk will have on the attainment of the specified goal
- Risk history
 - ◁ Has this risk occurred before? If so, when and what was the impact?
- Risk indicator – events or data that can indicate that the risk is likely to or about to occur
- Existing controls to reduce the likelihood and/or impact of the risk
- Risk acceptance level
 - ◁ Is the current level of risk acceptable? If not, why not?
- Recommended controls or changes to existing controls

Meetings were held with the University’s executive team and department directors to discuss the information provided in the risk surveys, and to clarify and expand the information provided in the surveys. The results of the risk surveys and meetings were compiled and presented in summary form to the executive team and department directors. Key risks were selected for which new or modified risk management control activities will be implemented and the ERM program plan was finalized (the Key Risks summary begins on page 12).

RESPONSIBILITIES AND OVERSIGHT

The University has established an ERM Steering Committee to oversee its efforts to identify, assess, measure, respond, monitor, and report risks. This committee will establish ERM program goals, assess progress toward those goals, and provide reports to the President and other key stakeholders as requested. It will be the responsibility of the ERM Steering Committee to revise the program as needed to accommodate the emerging needs of the University and address the current risk environment. While the President and ERM Steering Committee are responsible for enterprise risk management, it is critical that all employees support the University's risk management philosophy, promote compliance with its risk appetite, and manage risks within their spheres of responsibility.

INFORMATION REQUESTS

For additional information about the ERM program, please contact Gaylene Nunn, Vice President for Finance and Administration, at nunn@ct.tamus.edu.



TAMUCT Enterprise Risk Management Matrix FY18

Description of Risk	Likelihood	Impact	Mitigation and Control Mechanisms	Monitoring Activities	Reporting Mechanism
Funding of Operations	High	High	<ol style="list-style-type: none"> 1. Build a compelling Legislative Appropriations Request (LAR) 2. Implement measures for cost containment 3. Increase tuition and fees 4. Build an endowment and planned giving strategic plan 	<ol style="list-style-type: none"> 1. Conduct internal and external assessments of LAR prior to submission 2. Assess cost containment measures 3. THECB Report of Affordability 4. Affordability of educational expenses compared to other state institutions 5. Assessment of endowment and planned giving strategic plan 	President's Cabinet
Information Technology Infrastructure, Information Resources (IR) Security,	Medium	Medium	<ol style="list-style-type: none"> 1. Manage the IR risk assessment process 2. Annual IR Security Awareness training 3. Create the required security standards to maintain compliance with TAMUS Reg. 29.01.03 4. Train all departments responsible for information resources on their responsibilities regarding IR security and their roles 5. Role based security assessment and training as required for staff 	<ol style="list-style-type: none"> 1. Virus detection monitoring and alerting, and electronic audit trails on critical systems 2. Monitoring of servers, networks, firewalls, IPS and data loss prevention systems 3. Participate in TAMUS Network Security Operations Center network monitoring services 4. Annual disaster recovery plan updates and testing. 	<p>Annual Information Resource Risk assessment to the University President</p> <p>Annual Security Assessment for Texas Dept. of Information Resources</p>

Description of Risk	Likelihood	Impact	Mitigation and Control Mechanisms	Monitoring Activities	Reporting Mechanism
			<ul style="list-style-type: none"> with system administration duties. 6. Monitor and review critical IR systems 7. Review and classify all data sources 8. Expand efforts to locate backup servers off-campus and continue the failover Internet path through Tarleton State University 9. Enterprise Application Steering committee will review requests for enterprise application functions and new applications 	<ul style="list-style-type: none"> 5. University Technology Advisory Council and Enterprise Applications Steering Committee review of major technology initiatives 	
Technology Enhanced Learning	Low	Medium	<ul style="list-style-type: none"> 1. Prepare Technology Enhanced Learning needs analysis and budget 2. Negotiate better pricing on Technology Enhanced Learning technology and services and seek Technology Enhanced Learning partnership arrangements with other institutions 3. Acquire and implement additional instructional delivery technology 4. Follow established procedures for accessibility of academic technology systems 5. Provide faculty training on 	<ul style="list-style-type: none"> 1. Assess results of Technology Enhanced Learning needs analysis 2. Review the applications for grants and other sources of funding that can be applied to Technology Enhanced Learning 3. Assess results of price negotiation activities and Technology Enhanced Learning partnering discussions and negotiations 4. Assess results of expenditures related to instructional delivery 	<p>Academic Affairs</p> <p>Technology Enhanced Learning</p>

Description of Risk	Likelihood	Impact	Mitigation and Control Mechanisms	Monitoring Activities	Reporting Mechanism
			<p>accessibility and compliance, course design, and teaching quality</p> <ol style="list-style-type: none"> 6. Establish course review policy and procedure for accessibility of content 7. Increase the utilization of shared instructional technology and distributed learning resources 8. Monitor LMS system 9. Evaluate all building blocks for compatibility 10. Expand use of Quality Matters for all courses 11. Adopt and implement Online Learning Consortium Quality Scorecard for all programs and Colleges 12. Prepare for the migration from LMS Blackboard to Canvas 	<p>technology</p> <ol style="list-style-type: none"> 5. Evaluation of academic technology systems for accessibility 6. Review faculty training plans for accessibility 7. Author proposed policy and procedures for accessibility of course content 8. Assess the utilization of shared instructional computing and distributed learning resources 9. Monitoring LMS server load 10. Review and evaluate all requested building blocks 11. Conduct evaluation of other hosting models 12. Review faculty training plans 13. Review QM reports 14. Conduct faculty and student course quality surveys 	
Student recruitment, retention and success	Medium	Medium	<ol style="list-style-type: none"> 1. Implement the Client (Customer) Relationship Management (CRM) module to track student prospects and increase student communication 2. Implement a student recruitment and retention plan to promote student success, retention, and 	<ol style="list-style-type: none"> 1. Assess the results of student recruitment and retention plan including the A&M System Student Success Measures and incorporate findings into the Continuous Improvement cycles 	<p>Academic Affairs</p> <p>Graduate Studies</p> <p>Student Affairs</p> <p>Enrollment Management</p>

Description of Risk	Likelihood	Impact	Mitigation and Control Mechanisms	Monitoring Activities	Reporting Mechanism
			<p>completion</p> <ol style="list-style-type: none"> 3. Implement an "at risk" student intervention program to recognize and provide additional support for students who are experiencing personal, family, financial, academic or other challenges 4. Provide student support services designed for online students 	<ol style="list-style-type: none"> 2. Assess the results of "at risk" student intervention program 3. Assess the results of online student support services activities 	
Faculty and staff recruitment, performance, retention	Medium	High	<ol style="list-style-type: none"> 1. Monitor academic master plan 2. implement a professional development plan for faculty, staff, and academic chairs and deans 3. Maintain competitive salaries and benefits 4. Increase diversity of faculty 	<ol style="list-style-type: none"> 1. Assess results of academic plan and faculty development plan activities versus the plans 2. Monitor the number of professional development activities each year 3. Assess faculty hiring and retention statistics 4. Perform comparative analysis of salaries and benefits 5. Assess recruiting tools to target a diversified faculty 6. Monitor turnover rates 	<p>President</p> <p>Human Resources</p> <p>Academic Affairs</p>
Campus security, safety and risk management	Medium	Medium	<ol style="list-style-type: none"> 1. Increase presence, visibility and mobility of armed police officers on campuses. 2. Enhance resources necessary to insure a rapid, adequately-armed, emergency response to violent situations. 	<ol style="list-style-type: none"> 1. Monitor to insure adequate officer visibility and mobility is being provided on campus locations. 2. Test and assess campus emergency preparedness status. 	<p>President</p> <p>VPFA</p> <p>Public Safety</p> <p>Risk Management</p>

Description of Risk	Likelihood	Impact	Mitigation and Control Mechanisms	Monitoring Activities	Reporting Mechanism
			<ol style="list-style-type: none"> 3. Implement and rehearse an emergency management plan 4. Provide periodic emergency preparedness training to campus constituents. 5. Adopt industry best-practices policies regarding field operations, use of force and use of deadly force. 6. Maintain and update risk management programs and plans Provide safety training for students, faculty and staff. 	<ol style="list-style-type: none"> 3. Insure department policies relating to campus safety and security are current. 4. Review and assess written guidelines for safe practices 5. Undergoing TPCA Recognition Program 6. Monitor and assess training and attendance 	
Facilities	High	Medium	<ol style="list-style-type: none"> 1. Pursue gifts and other sources of funding that can be applied to the improvement, expansion and building of adequate facilities 2. Implement a plan to control costs related to campus facilities, especially those associated with the buildings on the new campus 3. Maximize the use of existing facilities in order to accommodate new and expanded programs 4. Request funding from legislature for new facilities 	<ol style="list-style-type: none"> 1. Assess results of the facilities needs analysis 2. Assess result of facilities cost containment activities 3. Assess results of facility utilization activities 	<p>President</p> <p>Finance and Administration</p>
Compliance Institutional (Title IX, Clery Act, Audit) Research (Human Subjects,	Medium	Medium	<ol style="list-style-type: none"> 1. Document and comply with regulatory compliance requirements 2. Monitor a regulatory compliance 	<ol style="list-style-type: none"> 1. Review an assessment of listing of regulatory compliance requirements 2. Assess regulatory 	<p>President</p> <p>Compliance</p>

Description of Risk	Likelihood	Impact	Mitigation and Control Mechanisms	Monitoring Activities	Reporting Mechanism
Biosafety & Chemicals, Animals, Export Controls),			<p>plan that addresses any identified compliance gaps, ensures that rules and procedures are in place</p> <ol style="list-style-type: none"> 3. Develop and maintain rules and procedures to comply with federal and state laws and System policies and regulations 4. Provide training to faculty, staff and students guided by regulatory requirements. 5. Develop and maintain plans to implement all system, state, and federal audit recommendations 	<p>compliance plan and the results of plan activities</p> <ol style="list-style-type: none"> 3. Monitor and assess training and attendance 4. Monitor and assess audit reports 	<p>Research</p> <p>Public Safety</p> <p>Risk Management</p>



1001 Leadership Place
Killeen, Texas 76549