Texas State University-San Marcos
LBJ Student Center

Enterprise Risk Self-Assessment
May 29, 2009

Purpose

THE PURPOSE OF THIS RISK ASSESSMENT EXERCISE:

- This tool is provided to help organizations annually evaluate risk management and control activities. Recent events have reconfirmed the importance of focusing on risk management to assure the organization is attending to all risks.
- A written risk assessment by management and their team along with a strong internal control environment can better position business units to achieve their compliance, financial and operational objectives.
- Sharing individual observations, potential risks and concerns of multiple employees within each organization is often helpful to understanding the magnitude of risks and the effectiveness of controls.
- The goal of Enterprise Risk Management is to provide reasonable assurance regarding the achievement of organizational objectives by identifying events that may effect the organization and managing risk to be within the organization's risk appetite.

HOW TO COMPLETE THIS ASSESSMENT:

- The <u>first</u> section on page 3 below focuses on a review of Risk Management issues and an organization's risk identification process.
- The <u>second</u> section beginning on page 4 below includes examples of questions that may help identify potential risk areas in an organization. The questions have been designed so that each "no" answer indicates an area of opportunity. This may indicate a risk area that should be explored in more detail. Please do not limit your analysis to only these questions. A questionnaire approach might overemphasize controls of historical risks and underemphasize forward-looking analysis of risks that have not yet occurred.
- The <u>third</u> section on page 6 is an example of a Risk Register that each organization should complete annually. This allows you to evaluate and rank your major risks, and to assess your organization's controls over specific business processes. It could also help provide evidence that an effective Enterprise Risk Management process is in place.

By thoroughly considering the potential risk areas in your organization, you will be evaluating your major risks and the existing control environment against sound businesses practices. It is often beneficial to engage your team in the exercise to brainstorm actions for those areas of opportunity and to share lessons learned.

- For additional help in understanding specific questions, please contact Audit and Compliance. You can call 5-2533 to speak to an auditor about the risk management process.

Enterprise Risk Self-Assessment

Part 1:

Risk Management

Identification of risks and effective risk management actions are essential for successful management in all areas of higher education institutions. Risks, and therefore risk management activities, must continually be assessed to provide reasonable assurance that controls are adequate and working effectively.

A *risk* is defined as anything that can prevent the achievement of goals and objectives. To manage or *control* risk is to do something that will reduce the probability or likelihood of occurrence to an acceptable level. Risk exposure is the *residual or net risk* that remains after all controls to mitigate a risk have been taken into account. Risk assessment includes evaluating the potential "*Impact*" or effect of the risk on the achievement of goals, and also considering the probability or "*Likelihood*" of occurrence of each risk. Business Leaders have always managed the risk and control trade-off.

A sample of potential risk categories in higher education could include:
- New policies or regulations from political or regulatory bodies
- Financial and economic issues, conditions, waste or abuse
- Technology availability, integrity, security, or privacy
- Environment, health, safety, or research
- Governance, compliance, image, or conflict of interest
- Resource allocation, reliability, or misuse
- Personnel capability, delegation of duties, training, or misconduct

Potential benefits of a well planned risk management process include:
- Fulfill a fundamental responsibility of senior management
- Assure the organization is attending to all major risks
- Communicates the organizations efforts to maintain a manageable risk profile
- Promote continual improvement and accountability
- Reduce operational surprises and losses
- Provide greater awareness of activities and initiatives

Risk management practices (such as annually completing a *Risk Register* as shown in Part 3 below) provide management an opportunity to effectively deal with operational uncertainties and the associated risks and opportunities. Risk management also helps employees to understand risks in the context of the institution's objectives.

The need and focus for risk management will likely change from year to year due to changes in systems, regulations, policies, procedures and personnel. An annual risk assessment review is a good opportunity to reflect on the success of risk management in the previous year, and to recommend improvements for the forthcoming year. It will help to ensure the process continually improves and delivers the expected benefits.

Enterprise Risk Self-Assessment

Part 2:

   The following two pages contain various examples of risk management questions your organization could consider about the risks and controls in your area:

<div align="center">

Self-Assessment Questions

</div>

	Yes/No	Describe Key Controls
Do employees know what to do if they encounter unethical behavior?	Y	Employee handbook, staff training, accessible senior management team
Does the organization's structure promote effective management oversight and efficient outputs? Are there clear organization charts, defined roles and responsibilities and monitoring?	Y	The organizational chart is updated when changes are made. Staff reviews their GOJA annually which is paramount to a review of job task and responsibilities. There are good checks and balances associated with our policies and procedures which assure effective management oversight.
Are financial reports regularly provided to managers to support decision making and accountability?	Y	Monthly reports provided for reconciliation, up to date information supplied upon request.
Are there controls in place to ensure that University and department policies are adhered to, e.g., training, segregation of duties, supervisor review?	Y	Financial policies specifically dictate and provide controls. Monthly reconciliation done on all budgets with built in checks and balances approved through audit review. P-cards are reviewed by non-card holders and signed off on by reviewers each month. All university policies and procedures are reviewed by the management staff and they are responsible for oversight to be sure of adherence of all university policies.
Are there significant risks in your processes because you depend heavily on assets for goal achievement? [Assets include: physical assets such as plant and equipment, financial assets such as cash and investments, human assets (including knowledge and experience of staff), and intangible assets such as information and reputation.]	Y	Being a fee based entitiy; we depend nearly entirely on our personnel and facility. Monitor assets. We have a strong financial monthly reconciliation system in place. We have a strong cash handling system in place. We have a strong

		inventory control system in place.
Does your organization understand and follow all University and TSUS policies and procedures for the development, approval and administration of all contracts?	Y	Division policies followed. All policies available online, The Vice President of Student Affairs has established policies regarding proper approval of contracts.
Are contracts reviewed and signed by authorized employees?	Y	The Vice President of Student Affairs has established policies regarding proper approval of contracts. Policies are followed.
Are business travelers and approvers knowledgeable of University travel and reimbursement policies?	Y	Training is provided and policies are readily available on-line. There is a full time staff member in the LBJ Student Center business office assigned the responsibility of making sure that all rules and policies are followed.
Is scenario planning used to answer questions such as: "What could disrupt our plans? And how vulnerable are we to it?	Y	Part of training. This is a normal technique used in our planning process.

	Yes/No	Describe Key Controls
Are cardholders and account managers conversant with P-Card policies (e.g., account manager review & approval, dollar limits, University business use only, restricted commodities, no sales tax, collect cards from departing employees, etc)?	Y	Annual training is provided in the Student Center. We contact Finance and Administration when there are questions. P-cards are reconciled each month by non-P-card holders. P-cards are cancelled for any staff member who does not follow the rules.
For sponsored research, are relevant committees included in the proposal review and approval process for issues such as human subjects, animal use, stem cells, biohazards, select agents or other requirements specific to the unit?	NA	
Are fixed asset records maintained and updated on a regular schedule (e.g., purchases, donations, transfers, disposals)	Y	Records are made of any asset received and the monitoring of those assets and records are assigned to either the operations staff if it is an item on our inventory system or if it is financial in nature then the records are maintained and monitored by the LBJ Student Center Business office. Each year there is an annual inventory check and each month there is a reconciliation of all financial assets recorded.
Are unexplained entries to the inventory records examined for source documentation?	Y	Inventory control is assigned to the operations unit of the Student Center. Any unexplained entries would be immediately addressed by staff assigned the responsibility for monitoring the inventory records of the LBJ Student Center. Source documentation review would be a part of what would be done to determine any unexplained entries.
Are there environmental health or safety risks in your area that have not been appropriately evaluated and controlled?	N	Training, monitoring, and Risk Management Office reviews are done on regular bases. This responsibility is assigned to the operations area. All known risk are assessed and controlled with consultation of the university safety officer.
Are your organization's confidential documents and sensitive	Y	Confidentiality statements are signed by all student

high-risk information secured and is access restricted?		workers. All records are kept secure. Office security is strictly enforced. Documents that require confidential treatment are well defined and staffs responsible are instructed regarding safe keeping of these documents. The LBJ Student Center has a strong key control and security system in place. Keys are assigned by the operations area of the LBJ Student Center. After hours all doors are checked every day to assure that the doors have been properly secured. If doors are found unlocked they are reported daily to those responsible. We have a contractor in the building at night from our closing until 6 a.m. and our morning staff starts their work day at 6 a.m. These staffs actually pass each other in the changing of the guard. On holidays the staff comes to the LBJ Student Center to make general checks of the building. Often special projects are preformed during holiday periods which give a measure of security by having workmen the building. The LBJ Student Center has someone in the building almost 24 hours each day during normal operations.
Are adequate controls in place in your organization to address potential threats such as Errors, Delays, Omissions or Fraud?	Y	The LBJ Student Center has established complete policies and procedures on cash handling, travel, accounting, p-cards, etc. Our policies and systems have been reviewed by auditors from time to time to assure that all safe guards are adequate and in place to guard against these concerns. Monthly reconciliations are done with the financial records. Those reports have built in "checks and balance" systems to assure that no individual could generate funds or spend funds without going through multiple levels and individuals in accounting for those transactions. The business manager is assigned responsibility for administering periodic

		surprise cash audits within all of our operations. Systems exist in various offices for logging in/out documents. This tracking system helps with know where paper work is in the process and helps with delays resulting in lost files. Our marketing area has a review process for all documents to be printed.
To increase the opportunity for a successful recovery of valuable records and key business operations, is there a documented, well-established and thoroughly tested disaster recovery and business continuity plan in place for your organization's essential operations?	Y	All data is backed up daily. The LBJ Student Center backs up the data to university maintained servers that are protected by agreements with other universities in case of disasters. The LBJ Student Center has not tested recovery of data. This testing of data recovery systems would be done by a different department of the university.
Is there an effective and reliable Emergency Response Plan in place for your organization that is fully documented and tested to help people respond appropriately to potentially damaging or threatening events that could occur on or near the campus?	Y	The university has this plan in place and the LBJ Student Center has a part as needed relative to major disasters. The emergency plan for response to such events as fire alarms, bombs in the building, active shooters have been reviewed at our annual kickoff program and staffs are aware of what they should do in those instances. Due to the number of false alarms that occur in the student center these procedures related to fire are tested often.
Does your organization use Identity and Access Management techniques to ensure the implementation of physical, technical, and administrative controls that limit access to University resources to authorized persons?	Y	This is a function of our operations area of the student center. We have a comprehensive system of key control and nightly checking for unlocked doors, etc. During normal operations the Student Center has someone in the building 24 hours each day.

Part 3:

Risk Register
Division: Student Affairs-
Department: LBJSC

Enterprise Risk Self-Assessment

Prepared By: Andy Rhoades
Date Prepared: 5-29-2009

Developing a list of the top 10 major risks for each business unit provides management and their staff an opportunity to evaluate and rank the risks based on their in-depth Knowledge of the business area. Management and their staff may wish to identify more than the top 10 risks and controls to ensure they have a thorough understanding of risks and controls in their area. Completing a document such as the one below is one way to identify, evaluate and present risks based on their significance in the organization. Completing this document could also help provide evidence than an effective Enterprise Risk Management process is in place in an organization.

Item #	Goals & Objectives	Major Risks	Risk Impact(H,M,L)	Likelihood(H,M,L)	Actions to Manage & Control Risks
1	Goal II: Create the center of campus life for Texas State through student-planned cultural, educational, social, and recreational programs	Student – Planned Program failure	H	M	Budgeting, programming planning training, staff training, review contracts, program evaluation and review.
2	Goal II: Create the center of campus life for Texas State through student-planned cultural, educational, social, and recreational programs; and Goal V: Develop students holistically (intellectually, spiritually, physically, emotionally and ethically by participation in programs and organizations in an environment that models civic responsibility, promotes social responsibility and	Student Event/Travel	H	L	Travel policies, risk management training, program review, advisor training

	develops leadership.				
3	Goal III: Develop and manage financial resources effectively, efficiently, and responsibly.	Mishandling of funds	H	L	The Business office is involved in all transactions, p-card training is done annually. Cash handling procedures are well defined and adherences to these procedures are monitored by the business manager. Monthly review of financial statements by functional areas and business office.
4	Goal V: Develop students holistically (intellectually, spiritually, physically, emotionally and ethically by participation in programs and organizations in an environment that models civic responsibility, promotes social responsibility and develops leadership	Hazing	H	M	Follow appropriate Risk Management procedures for program planning, including staff supervision, when necessary. Providing annual training involving high risk groups (Greeks, etc.) associated with hazing activity. Provide ongoing system (Disciplinary Review Team) to monitor possible violations and provide follow up training on an individual bases as needed.
5	Goal 1: Provide quality services and facilities for the university and greater community. Goal II: Create the center of campus life for Texas State through student-planned cultural, educational, social, and recreational programs Goal IV: Maintain and manage physical facilities to achieve optimal use. Goal V: Develop students holistically (intellectually, spiritually, physically, emotionally and ethically by participation in programs and	Serious Injury at programs or events or in the building.	H	M	Students and staff are trained to follow university policies and procedures regarding program planning and risk management issues. Full time professional staffs are present at events.

	organizations in an environment that models civic responsibility, promotes social responsibility and develops leadership				
6	Goal I: Provide quality services and facilities for the university and greater community Goal IV: Maintain and manage physical facilities to achieve optimal use.	After hours access to the building and doors being propped open and left unsecured (students and employees). Risk ranges from opening the building to damage as a result of vandalism, graffiti, stolen furniture, intruders, personal safety of staff and students, etc. Risk also includes on site Band and other financial transaction sites including Bookstore, Business office and Market.	H	M	I-Buttons used for access and all staffs are instructed to secure doors behind them upon entering or leaving the building. Staffs are instructed to give notification to building operations if people working late or coming into the building during hours that we are normally closed.
7	Goal 1: Provide quality services and facilities for the university and greater community. Goal II: Create the center of campus life for Texas State through student-planned cultural, educational, social, and recreational programs Goal IV: Maintain and manage physical facilities to achieve optimal use. Goal V: Develop students holistically (intellectually, spiritually, physically, emotionally and ethically by participation in programs and	Slips resulting in falls which could result in serious injury.	H	M	On rainy days when floor is likely to get wet, carpet is provided at all entrances as a walk-off to prevent tiles on floor and steps from becoming slippery. Adhesive sand paper strips have been added to tile steps to help prevent those using the steps from slipping. All floors are monitored by staff and spills which could result in slips and falls are cleaned up as soon as they are noticed. Warning signs are used when wet spots occur. Problem areas are closed when necessary with warning tape clearly marking the area of concern. All floors are monitored and maintained. Repairs are made to uneven surfaces and cracks. Handrails are maintained in good repair.

	organizations in an environment that models civic responsibility, promotes social responsibility and develops leadership			
8	Goal IV: Maintain and manage physical facilities to achieve optimal use.	Fire in the building that could result in a range of problems from damage to the building to injury and death to users of the facility	H	L	Follow risk management procedures which include annual staff training, fire drills, periodic review of safety procedures by University Safety staff, maintenance of fire alarm system, etc. Monitoring and restriction on such things as using candles in the building, safe storage of any combustibles that might be in the building, etc.

Goals & Objectives: Goals and objectives should be clearly defined, measureable and attainable.
Major Risks: List major risks to the achievement of each goal and objective. Consider both internal and external risk factors.
Risk Impact: For each risk, estimate the potential impact on operations, financial reporting or compliance with laws and regulations.
Likelihood: For each risk, assess the likelihood of the risk occurring. Use High, Medium or Low or probable, reasonably possible, or remote.
Actions: List both the actions to mitigate the risk and the control activities to ensure that those actions are carried out properly and timely.