



Departmental Risk Assessment Procedures

Objectives of a Risk Assessment

Risk Assessment is the process of identifying the risk level for events based on an assessment, 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. The objectives of performing a Risk Assessment are as follows:

- Identify and control potential risks
- Develop and implement mitigation plans / risk strategies
- Establish continuous monitoring and reporting of risk
- Manage risk in accordance with best practices

What is a Risk Assessment?

A Risk Assessment allows an institution to understand the nature of the risks it faces. Performing a Risk Assessment can help assess the effectiveness of current controls and identify areas where new or more effective controls might be necessary. It is recommended that Risk Assessments be performed annually or as deemed necessary in order to ensure ongoing departmental goals and objectives are achieved.

Why Perform a Risk Assessment?

Performing a Risk Assessment will assist in identifying and mitigating/controlling potential risk. It helps to create awareness of risk and identify measures needed for improvement in attaining departmental objectives that are aligned with the institution's strategies.

Roles

Risk Management

Risk Management will serve as a supporting agent to Risk Owners throughout the college and will assist departments in conducting Risk Assessments including: identifying, assessing, prioritizing, and controlling risks. Risk Management will provide education and training on the Risk Assessment pr

Risk Owner

A Risk Owner is the individual(s) responsible for identifying, assessing, controlling, and reporting risk in their respective areas and ensuring that those risks are controlled. A Risk Owner identifies risk objectives, has budget authority, oversees business/department operations, and has authority to determine risk strategies to control risk. The Risk Owner will provide information to develop and implement risk action plans to control risk and actively work to control risk within their area which has been identified.

The College's Risk Assessment Categories

The College has identified five categories:

- **Strategic** – the risk that your business strategy becomes less effective and your department struggles to reach its goals as a result. It could be due to technological changes, a powerful new competitor entering the market, shifts in customer demand, or spikes in the costs of materials.
- **Compliance** – are you complying with all the necessary laws and regulations that apply to your department, program, or activity? Laws change often and there is always a risk that you will face additional regulations in the future. As your department, program, or activity expands, you might find the need to comply with new rules that did not apply before.
- **Financial** – the risk in terms of extra costs or lost revenue. Risks that may result in loss of physical assets or financial resources. The possibility of a sudden financial loss.
- **Operational** – an unexpected failure in your department's day-to-day operations. It could be a technical failure, such as a server outage, or it could be caused by employees or processes. Operational risk can also stem from a natural disaster, power outage, or a problem with your website host. Anything that interrupts your core operations falls under the category of operational risk.

The Risk Assessment Process

Step 1: Identify the department's objectives

Begin the risk assessment process by considering your objectives. Asking and answering the questions below will help you identify the objectives in your area:

- What are the objectives of the department (comprehensive plan)?
- Are objectives aimed at achieving the College's strategic initiatives and mission?
- What are we trying to accomplish?
- What are the primary functions/activities performed to carry out and realize objectives?

Step 2: Identify risks and causes

Begin identifying and documenting risks. Consider asking and answering the questions below which will help you identify risks.

- What could prevent the department from achieving its objectives?
- What could prevent the department from performing its primary functions?
- What could cause injury, harm, or damage to property?
- Possible risks to consider (e.g., cash handling, safeguarding of assets, appropriate approvals, segregation of duties, overtime, account reconciliations, etc.).
- What keeps you up at night?

Step 3: Identify risk category

Select the category that applies to each documented risk. In some instances, there may be overlap, which is expected. Select the category that you deem best describes the risk.

- **Strategic** – the risk that your business strategy becomes less effective and your department struggles to reach its goals as a result. It could be due to technological changes, a powerful new competitor entering the market, shifts in customer demand, or spikes in the costs of materials.
- **Compliance** – are you complying with all the necessary laws and regulations that apply to your department, program, or activity? Laws change often and there is always a risk that you will face additional regulations in the future. As your department, program, or activity expands, you might find the need to comply with new rules that did not apply before.
- **Financial** – the risk in terms of extra costs or lost revenue. Risks that may result in loss of physical assets or financial resources. The possibility of a sudden financial loss.

- **Operational** – an unexpected failure in your department’s day-to-day operations. It could be a technical failure, such as a server outage, or it could be caused by employees or processes. Operational risk can also stem from a natural disaster, power outage, or a problem with your website host. Anything that interrupts your core operations falls under the category of operational risk.

Step 4: Identify existing controls or risk strategies

- What controls are currently in place?
- Are current controls adequate?
- Are procedures or policy available?
- Are procedures aligned with objectives?

Step 5: Assess (score) inherent risk

- Determine inherent risk level: low, moderate, high, or extremely high.
- Determine whether risk will be accepted, avoided, mitigated, or transferred.
 - If risk is accepted, then the residual risk will not be calculated.

Step 6: Risk response

For each risk, one of the following approaches will be selected:

- Accept
- Avoid
- Mitigate
- Transfer

Step 7: Anticipated action/additional risk strategies or controls

If determined that additional controls are needed or current controls need to be strengthened, develop and implement controls to decrease the likelihood and impact of each risk.

- Provide a brief explanation on how risk will be accepted, avoided, mitigated, or transferred.
- Identify metrics to enable measurement of control or risk strategy performance.

Step 8: Determine the residual risk

- Reassess the risk to determine the remaining risk (only after implementing controls or risk strategies).

Step 9: Review your assessment and update annually or as necessary

Risk may change over time and as a result, a risk assessment should be performed to identify, assess, and control new and emerging risks

Risk Assessment Timeline

Departments will perform – at minimum –a risk assessment in accordance with the timeline below. Risk Assessments may be performed sooner or more frequently as deemed necessary by the Risk Owner. This timeline is subject to change at management’s discretion.


RISK STEP	FUNCTION	DATE
Identify, Assess, and Prioritize Risk	Identify risks impacting department objectives. Once identified, score each risk and determine priority of addressing risks.	September – October
Respond to Risk / Control Risk	Develop risk strategies and action plans needed to control risk. Identify risk metrics to measure residual risk or improvement.	November – June

Monitor Risk	Monitor and report improvement efforts or residual risk. Refine risk strategies as needed.	July - August
--------------	--	---------------

Definitions

- **Inherent Risk** - the risk to the College in the absence of any actions that may be taken to alter the likelihood, vulnerability, or impact related to that risk.
- **Residual Risk** - the risk that remains after the risk mitigation activities occur.
- **Risk** – The possibility that an event will occur and adversely affect the achievement of objectives.
- **Risk Appetite** – The amount of risk, on a broad level, an entity is willing to accept as it tries to achieve its goal and provide value to stakeholders. It reflects the entity’s risk management philosophy and in turn influences the entity’s culture and operating style. Many entities define their risk appetite qualitatively while others take a more quantitative approach.
- **Risk Assessment** –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.
- **Risk Matrix** – a graphic representation of likelihood and impact of one or more risks. It plots quantitative or qualitative estimates of risk likelihood and impact. It is often referred to as a “heat map” since it presents risk levels by color, where black represents extremely high risk, red represents high risk, yellow represents medium risk, and green represents low risk.
- **Risk Owner(s)** – Responsible for the assessed levels of risk and defining and implementing risk response plans to bring risks within tolerance.
- **Risk Tolerance** – The acceptable level of variation relative to achievement of a specific objective. In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Therefore, an entity operating with its risk tolerances is operating within its risk appetite.

Appendix A: Risk Scoring Matrix

RISK SCORING MATRIX						
Impact of risk						
 SOUTH TEXAS COLLEGE	Insignificant	Minor	Moderate	Major	Catastrophic	
	<ul style="list-style-type: none"> No impact on achieving objectives or business interruption. Injuries can be treated on site with no long-term effect. Negligible loss or damage to property. Financial impact \$0 - \$9,999. <p style="text-align: center;">1</p>	<ul style="list-style-type: none"> Minor impact on achieving objectives and business interruption. Minor injuries requiring medical attention off-site with no long-term effect. Minor loss or damage to property. Financial impact \$10,000 - \$99,999. <p style="text-align: center;">2</p>	<ul style="list-style-type: none"> Moderate impact on achieving objectives and business interruption. Several injuries requiring hospitalization with no long-term effects. Moderate loss or damage to property. Financial impact \$100,000 - \$499,999. <p style="text-align: center;">3</p>	<ul style="list-style-type: none"> Major impact on achieving objectives and business interruption. Serious injuries resulting in long-term effects and bodily impairment. Major loss or damage to property. Financial impact \$500,000 - \$999,999 <p style="text-align: center;">4</p>	<ul style="list-style-type: none"> Catastrophic impact on achieving objectives and business interruption. Loss of life. Severe loss or damage to property. Financial impact \$1,000,000 or greater <p style="text-align: center;">5</p>	
Likelihood that risk will occur	Almost Certain Expected to occur immediately (>90% chance of occurring) 5	Medium	Medium	High	Extreme	Extreme
	Likely Likely to occur in time (40% - 89% chance) 4	Low	Medium	High	High	Extreme
	Possibly May occur in time (11% - 39% chance) 3	Low	Medium	Medium	High	High
	Seldom Not likely to occur, but probable (4% - 10% chance) 2	Low	Low	Medium	Medium	Medium
	Unlikely Unlikely to occur (3% or less chance) 1	Low	Low	Low	Low	Medium
Risk Definitions						
Extremely High Risk (17-25)	Activities in this category contain unacceptable levels of risk, including catastrophic and critical injuries or fatalities that are highly likely to occur. Immediate action is essential to eliminate or modify risk strategies to control risk.					
High Risk (11-16)	Activities contain potentially serious risk that are likely to occur. Prompt action is necessary to reduce risk from occurring.					
Medium Risk (5-10)	Activities contain some level of risk and are seldom to occur. It is recommended that organizations consider risk strategies to control risk.					
Low Risk (1-4)	Activities contain negligible risk and are unlikely to occur. Organizations can proceed with current operations.					

Appendix B: Risk Assessment Template

Department Name Risk Assessment												
Objective	Risk	Cause of Risk	Risk Category	Existing Risk Strategies or Controls	Impact (I)	Likelihood (L)	Inherent Risk (I x L)	Risk Response	Anticipated Action/ Additional Risk Strategies or Controls	Impact (I)	Likelihood (L)	Residual Risk (I x L)
							0					0
							0					0
							0					0
							0					0
							0					0
							0					0
							0					0
							0					0
							0					0
							0					0

Appendix C: STC Risk Universe

South Texas College Risk Universe

	Strategic	Compliance	Operational	Financial
Sub-risk Categories	<ul style="list-style-type: none"> ❖ Economic risks ❖ Political risks ❖ Technological risks ❖ Organizational risks ❖ Industry risks 	<ul style="list-style-type: none"> ❖ Legal and regulatory risks ❖ Contract risks ❖ Reporting risks ❖ Intellectual property risks 	<ul style="list-style-type: none"> ❖ Business Continuity risks ❖ Environmental risks ❖ Safety risks ❖ Human Resources risks ❖ Property and assets risks ❖ Marketing risks 	<ul style="list-style-type: none"> ❖ Fraud risks ❖ Financial reporting risks ❖ Credit risks ❖ Budgeting risks ❖ Market risks ❖ Liquidity risks
Potential Risk Areas	<ul style="list-style-type: none"> • Dual Credit partnerships • State and federal legislative changes/rulings • Enrollment • Grant funding • Technological advancements 	<ul style="list-style-type: none"> • Internal controls • Policy and procedure • Data privacy/security • Financial penalties • Funding • Code of Ethics • Conflict of interest • Title IX 	<ul style="list-style-type: none"> • Emergency Preparedness • Safety and security • Process errors • Fraud • Product and service • Adequate staffing • Normal business operations disruption • Staffing • Facility maintenance • Employee retention • Grievance procedures 	<ul style="list-style-type: none"> • Financial aid • Budget • Tuition and fees • Investments • Account and reporting • Taxes • Insurance

Description:

Strategic risk – the risk that your business strategy becomes less effective and your organization or department struggles to reach its goals as a result. It could be due to technological changes, a powerful new competitor entering the market, shifts in customer demand, or spikes in the costs of materials.

Compliance risk - are you complying with all the necessary laws and regulations that apply to your department, program, or activity? Laws change often and there is always a risk that you will face additional regulations in the future. As your department, program, or activity expands, you might find the need to comply with new rules that did not apply before.

Operational risk – an unexpected failure in your department’s day-to-day operations. It could be a technical failure, such as a server outage, or it could be caused by employees, or processes. Operational risk can also stem from a natural disaster, power outage, or a problem with your website host. Anything that interrupts your core operations falls under the category of operational risk.

Financial risk – the risk in terms of extra costs or lost revenue. Risks that may result in loss of physical assets or financial resources. The possibility of a sudden financial loss.

Items found herein are not considered to be an exhaustive list of any or all risk sub-categories or potential risk areas.