

South Texas College

Risk Assessment Instructions & Scoring Matrix

Introduction

What is risk management?

Risk management foresees the challenges to achieving objectives and attempts to lower the probabilities of negative outcomes occurring and/or their impacts should they occur. The effectiveness of risk management depends in large part on decisions made by managers responsible for risk governance.

What is a risk assessment?

A risk assessment is a tool that allows an institution to understand the nature of the risks it is currently facing or could face when engaging in an activity. Performing a risk assessment can help determine the probability and impact of an event that may affect the achievement of an objective. It can also validate the effectiveness of current controls and identify areas where new or enhanced controls might be necessary to maintain risk within acceptable levels.

It is recommended that risk assessments be performed annually, when there is a significant change in activity, or as deemed necessary in order to ensure ongoing departmental goals and objectives are achieved. This tool will not make decisions for you, but it will help you organize your thinking as you consider your department's objectives.

Why perform a risk assessment?

It will assist the department in identifying and mitigating/controlling risk. It helps to create awareness of risk and identify measures needed for improvement in attaining departmental objectives, which are aligned with the institution's strategies.

Definitions

- Accept risk – continue with current business operations. Risk level is acceptable.
- Avoid risk – eliminate the risk by eliminating the cause or objective.
- Control/Risk Strategy – Internal controls or strategies developed and implemented with the goal of mitigating and/or preventing risk(s) from occurring.
- Inherent Risk – level of risk considering the impact and likelihood of current controls or risk strategies.
- Mitigate Risk – identify ways to reduce the impact and likelihood of risk.
- Objectives – activities the department aims to achieve which are aligned with the institution's core strategies.
- Risk – an event, which may occur and adversely affect the achievement of objectives.
- Residual Risk – level of estimated risk after controls have been implemented.
- Transfer risk – transfer risk to another party (e.g. outsourcing, insurance, subcontracting, etc.).

How to Perform a Risk Assessment

There are no fixed rules on how a risk assessment should be carried out; however, there are a few general principles that should be followed. Focus improvement efforts based on risk priority levels (e.g. extremely high-risk items should take priority over low risk items identified).

The following nine steps will ensure that your risk assessment is carried out appropriately:

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, or 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.

Using the Risk Assessment Template and Risk Matrix

1. Enter the objective in the "Objective" column of the Risk Assessment template.
2. Enter risks in the "Risk" column.
3. Enter causes of those risks in the "Cause of Risk" column.
4. Determine the risk category (select from the drop-down menu).
5. Enter current controls or risk strategies in the "Existing Risk Strategies or Controls" column.
6. Refer to the "Risk Scoring Matrix." This will assist you with the following steps.
7. Using the criteria found on the Risk Scoring Matrix, fill in the "Impact" and "Likelihood" columns considering existing controls and risk strategies.
8. The value in the "Inherent Risk" column will be calculated for by multiplying values entered in the "Impact" and "Likelihood" columns. (Example: Impact 3 x Likelihood 5 = 15.)
9. Risk response: accept, mitigate, avoid, or transfer (select from the drop-down menu). *If risk is "accepted" then additional controls or risk strategies are not required, and residual risk will not be calculated.*
10. Provide brief explanation of risk response in the "Anticipated Action/ Additional Controls and Risk Strategies" column.
11. Only after implementing additional controls or risk strategies, if determined by management or department, reassess the risk likelihood and impact to determine "Residual Risk" column.

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) <p style="text-align: center;">5</p>	Medium	Medium	High	Extreme	Extreme
	Likely Likely to occur in time (40% - 89% chance) <p style="text-align: center;">4</p>	Low	Medium	High	High	Extreme
	Possibly May occur in time (11% - 39% chance) <p style="text-align: center;">3</p>	Low	Medium	Medium	High	High
	Seldom Not likely to occur, but probable (4% - 10% chance) <p style="text-align: center;">2</p>	Low	Low	Medium	Medium	Medium
	Unlikely Unlikely to occur (3% or less chance) <p style="text-align: center;">1</p>	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.