

RISK ASSESSMENT OVERVIEW



PRESENTED BY
Ken Lyons, MBA
Risk Manager



**SOUTH TEXAS
COLLEGE**

WHAT IS RISK?

- Risk is inherent in everything we do
- We experience risk every day
- Risk is defined as: *The possibility that events will occur and affect the achievement of strategy and business objectives.*
- Not all risk is bad. Some risks must be taken in order to progress and manage change.

WHAT IS RISK ASSESSMENT?

- 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
- It is a living tool/resource that should be continually monitored and adjusted according to current and new risks

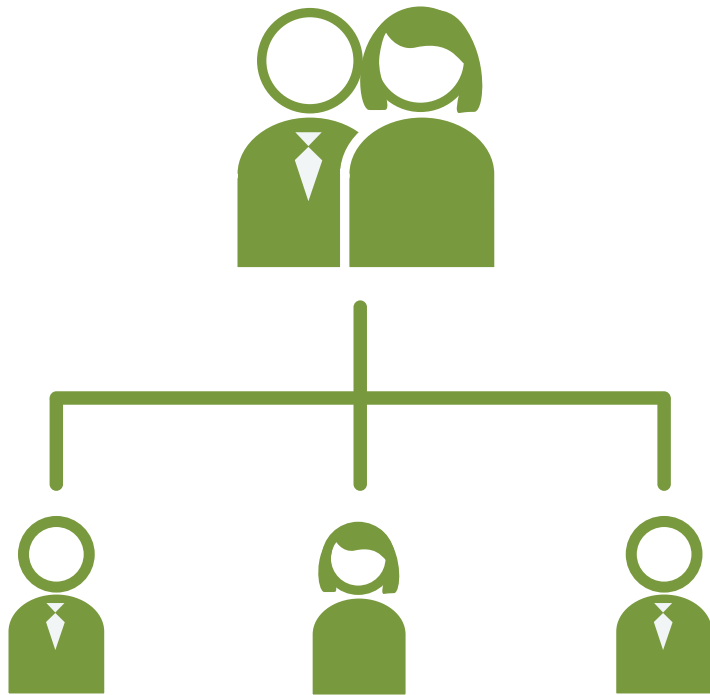
WHY PERFORM A RISK ASSESSMENT?

- It can assist a department in identifying and mitigating/controlling risk
- It helps to create awareness of risk and identify measures needed for improvement in attaining departmental objectives.
- It can validate the effectiveness of current controls and identify areas where new or enhanced controls might be necessary to maintain risk within acceptable levels
- Reduce incidents in the workplace
- Save costs by being proactive rather than reactive
- It's a good business practice

WHEN TO PERFORM A RISK ASSESSMENT?

- When there is a significant change in activity, objective, or operation
- Requirement of a regulatory agency or statute governing your area
- Acquisition of a new product or service
- An activity that may present a risk of property damage or injury
- As deemed necessary by department supervisors

WHO SHOULD PERFORM A RISK ASSESSMENT?



- Department supervisors
 - Include staff who have direct knowledge of work functions and operations
- Management

STEP 1: Identify objectives

- What are the objectives of the department (Comprehensive Plan / IE Plan)?
- What are you trying to accomplish?
- What are the primary functions/activities performed to carry out and realize objectives?

STEP 2: Identify risks and causes

- 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?
- What keeps you up at night?
- Possible risks to consider
 - safety and health of individuals
 - cash handling
 - safeguarding of assets
 - appropriate approvals
 - overtime
 - reconciliations
 - network vulnerabilities

STEP 3: Identify risk category

- Strategic (ex: technological changes)
- Compliance (ex: laws, rules, regulations)
- Financial (ex: lost revenue due to decrease in enrollment)
- Operational (ex: server outage)


STEP 4: Identify existing controls or risk strategies

- What controls are currently in place?
- Are current controls adequate?
- Are administrative controls available (procedures or policies available)?

STEP 5: Assess (score) inherent risk

- 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.

RISK SCORING MATRIX

RISK SCORING MATRIX						
Impact of risk						
 <p>SOUTH TEXAS COLLEGE</p>		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>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>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>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>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>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.					

STEP 6: Risk Response (Control Risk)

- For each risk, determine whether risk will be accepted, avoided, mitigated, or transferred. One of the following approaches will be selected:



ACCEPT

Continue with current business operations. Risk level is acceptable. If “accepted”, then the residual risk will not be calculated. Risk that has been “accepted” does not require further controls.



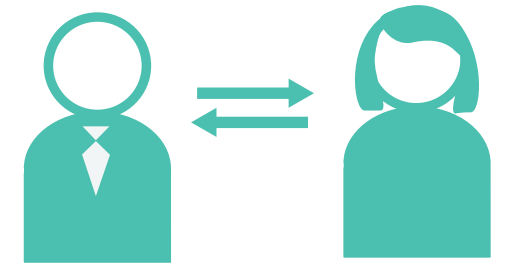
AVOID

Eliminate the risk by eliminating the cause or objective.



MITIGATE

Action is taken to reduce risk likelihood or impact, or both.



TRANSFER

Transfer risk to another party

STEP 7: Additional risk strategies or controls

- If determined that additional controls are needed or current controls need to be strengthened, develop and adjust controls to decrease the likelihood and impact of each risk
 - Identify metrics to enable measurement of control or risk strategy performance

STEP 8: Determine the residual risk

- Residual Risk – the risk that remains after the risk mitigation activities occur
- 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.
- Monitoring Risk - Department supervisors are responsible for monitoring their risks and executing risk responses when appropriate.

TIMELINE

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 – November
Respond to risk/ Control risk	Develop risk strategies and action plans needed to control risk. Identify risk metrics to measure residual risk or improvement.	December - June
Monitor risk	Monitor and report improvement efforts or residual risk. Refine risk strategies, as needed.	July - August