

How to Perform a Risk Assessment



ENTERPRISE
RISK MANAGEMENT

UNIVERSITY OF MINNESOTA
Driven to Discover®



HEALTH, SAFETY,
AND RISK MANAGEMENT

UNIVERSITY OF MINNESOTA

Risk Assessment Steps

What is a risk assessment and why perform one?

- 1. What are our goals?**
- 2. What could keep us from achieving our goals?**
- 3. What are the possible outcomes?**
- 4. What are our assumptions and are there correlations?**
- 5. Is our response enough?**



What is a risk assessment and why perform one?



Risk Assessment: The consideration of the extent to which potential events have an impact on the achievement of objectives. The assessment is done from two perspectives: impact and likelihood. It includes both positive and negative potential events.

Why perform risk assessments?

- Minimize surprise and impact on operations and administration
- Aid in quick, risk-informed, decision making including allocating time and resources
- Allows risks to be prioritized and paired down for action
- All risks map back to strategic goals and priorities

1 What are our goals?

Consider the short and long-term goals and objectives of your group at the University. These may be official statements or implied. What does it mean to be successful?

It's helpful to consider the University's three-part mission and strategic plan. How does your group contribute to the achievement of the system-wide goals?

2

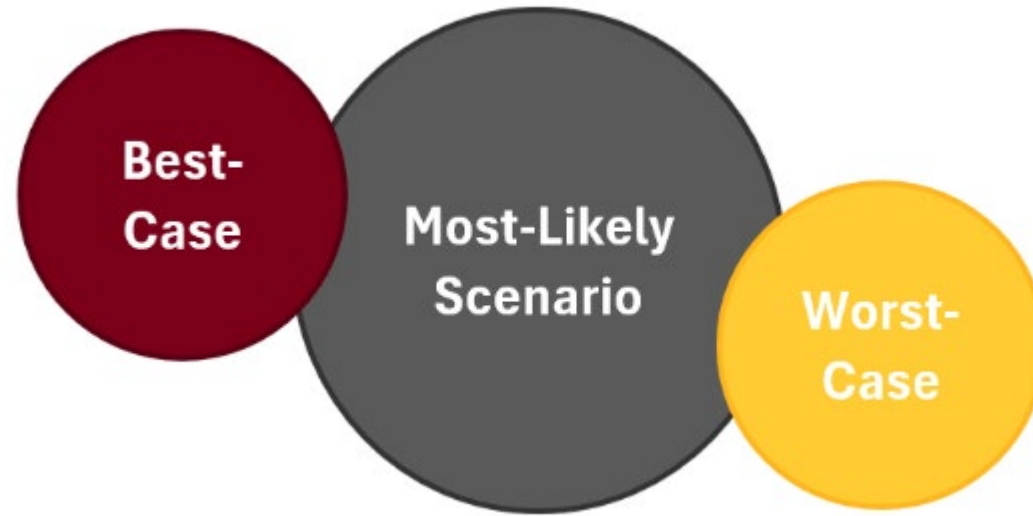
What could keep us from achieving our goals?

- Falling short of a goal can result from many factors or events both internal and external to the University. **These are your risks.**
- Remember, risk represents uncertainty so risk can be negative or positive. An event may occur that provides an opportunity.
- A risk assessment should consider each key risk or risk with the potential to have a significant impact on goals. The Enterprise Risk Management group has created simple and universal tools to help walk through the process.



3

What are the possible outcomes?



After identifying risks to the achievement of your goals or objectives, consider the possible outcomes and scenarios should those risks occur. Look for the worst-case, best-case, most-likely scenarios, and possibilities in-between. The risk assessment template created by the ERM group may be helpful.

Tools & Resources

Risk analysis tools and resources are available for performing risk assessments. The ERM group is also available to assist.

Scoring Grid		Impact				
		Incidental	Minor	Moderate	Major	Extreme
Likelihood	Almost Certain	Medium	Medium	High	Very High	Very High
	Likely	Low	Medium	Medium	High	Very High
	Possible	Low	Low	Medium	Medium	High
	Unlikely	Very Low	Low	Low	Medium	Medium
	Rare	Very Low	Very Low	Low	Low	Medium

Recommendation	
Very High	Immediate action required with detailed planning, allocation of resources and regular monitoring
High	Senior management attention needed, establish plans to mitigate the risk
Medium	Management responsibility should be specified, risk should be monitored or increases in likelihood or impact
Low	Monitor and manage by routine procedures
Very Low	No action required, management may choose to accept the risk

4

What are our assumptions and are there correlations among risk drivers?

- Examine your assumptions when considering risk scenarios. Leaders may rely too heavily on their experience creating “blind spots” in an unpredictable and sudden environment.
- Consider relationships among risk drivers. Risk drivers are the causes or sources of risk such as market conditions, regulatory changes, or climate change. Risks are often interrelated affecting one another.



5 Is our response enough?

Leaders respond to risk in many ways. Approaches include:

- **Mitigation** (controls): Controls generally include any action taken to reduce the impact or likelihood of a risk. Controls may include policies and procedures, preventative computer controls, management reviews, segregation of duties, training, and many others.
- **Transfer** (or Sharing): Unacceptable risk can be transferred from the University to another party such as an insurance company or outside service providers.
- **Acceptance**: There may be cases where a risk is acceptable without taking any action to reduce it.
- **Avoidance**: Leaders may decide the risk cannot be reduced to an appropriate level and therefore avoid the underlying activity entirely.

Effectiveness of my response

It's helpful to consider the potential impact and likelihood of risks both before and after any responses we've already taken. This helps define the "what could go wrong" e.g., if we lost resources or our controls failed, what could happen?



Inherent Risk: The risk to an entity in the absence of any actions the institution might take to alter either the risk's likelihood or impact.

Residual Risk: The remaining risk after management has taken action to alter the risk's likelihood or impact.

Mitigation Plan

If the risk assessment results in the need to further reduce certain risks, a risk mitigation plan is needed. Consider using the Mitigation Plan Template to help identify the various components of your mitigation plan. A proactive and risk-aware response will increase the likelihood we ultimately achieve our goals!

Risk Mitigation Plan

Risk	Risk Trend			Risk Owner			
	Current	Internal/External Factors					
<i>Example:</i> Cybersecurity	Increasing	While ABC group performs yearly cyber reviews and utilizes a software tool to minimize the risk of a cyber event, the risk continues to increase as cybercriminals are constantly developing new and more sophisticated ways to attack organizations. They are also increasingly utilizing artificial intelligence and machine learning to automate their attacks and make them more difficult to detect.		ABC Group Technology Leader			
Current Score Target Score	Impact	Likelihood	Risk Score	Notes			
	Major	Likely	High				
	Moderate	Possible	Medium				
What Could Go Wrong		Current Control/Response	Responsible Position	Control Effectiveness	Response Type	Target Response Description	Target Completion Date
1	<i>Example:</i> Untimely incident response	Policies & Procedures	ABC Group Technology Manager	Generally Effective	Risk Mitigation	In addition to the Cybersecurity Policy, we will create a response playbook that details actionable steps in the event of a cyber attack.	XX/XX/XXXX
2							



UNIVERSITY
OF MINNESOTA
Driven to Discover®

Thank you!

Please feel free to reach out with additional questions.



Katharine Bonneson

Assistant Vice President
(612) 625-0518
kbonneso@umn.edu



Nate Weidner, MBA, CPA

Enterprise Risk Manager
612-624-6212
weid0077@umn.edu

