# Table of Contents

Introduction .................................................................................................................... 2  
Approach ........................................................................................................................ 2  
Risk Appetite ................................................................................................................... 3  
Roles and Responsibilities ................................................................................................. 3  
Process ........................................................................................................................... 4  
Risk Evaluation Criteria - Likelihood.................................................................................... 7  
Risk Evaluation Criteria - Impact........................................................................................ 8  
Integrating Risk Management into UCAR Culture ................................................................. 11  
Glossary of Terms .......................................................................................................... 12  
Risk Contacts................................................................................................................. 12
Introduction

Enterprise Risk Management (ERM) is UCAR’s comprehensive program to proactively and continuously identify and manage risks that could affect the organization’s ability to achieve its goals and objectives.

As with universities or organizations within the private sector, UCAR operates in an inherently risky environment. Risks can be categorized in many different ways including:

Root cause
- External risks – risks caused by outside people, entities and environments
- People risks – risks involving people who work for the organization
- Process risks – risks arising from the execution of business operations
- Relationship risks – risks caused by connections with third parities
- Systems risks – risks due to data or information assets

Functional
- Strategic risks – risks aligned with strategic goals and objectives
- Operational risks – risks from day to day operations
- Financial risks – risks related to funding and spending
- Compliance risks – risks associated with laws, regulations and contractual obligations
- Technology risks – risks arising from software, technical data, hardware, and networks

Managing this portfolio of risks is especially important to help ensure that UCAR can continue to work toward its mission of empowering its member institutions, NCAR, and community programs. By strategically managing risk, we can reduce the chance of loss, create greater financial stability, and protect our resources.

Approach

UCAR’s approach to risk management has been developed to support the key requirements of responsible corporate governance. It is an important management discipline that helps to ensure that UCAR achieves the goals and objectives that are set by both NCAR and UCAR. This approach ensures that:

- Risk management supports strategic planning and decision making.
- Managing risk is a transparent process that provides management, auditors, and board members with access to information on current risks and how they are being managed.
• There is consistency in the process for regular risk review, documentation and reporting as circumstances change and are acted upon.
• There is clear accountability for risks. Each risk is assigned an individual owner who is responsible for assessing, evaluating, reviewing, reporting and managing controls.
• Appropriate innovation and progress is encouraged.
• Risks are managed in a balanced way to avoid surprises without becoming bogged down in details.
• Adequate resources are assigned to risks and controls to ensure satisfactory results.

Successful risk management helps UCAR to manage challenges, organizational changes and regulatory changes to better deliver on its mission. The Board of Trustees, President’s Council and Senior Management are advocates of the risk management process and provide the framework for risk management process to work. UCAR’s approach to risk management ensures that there are controls and actions in place to mitigate risks, along with resources needed to succeed in managing risks.

Risk Appetite

It is important that UCAR management focus on risk awareness rather risk avoidance. Management should carefully consider risks it is willing to retain without any additional mitigating actions, thereby setting an invisible line between acceptable risks and risks that require active controls to manage the risk exposure. A higher exposure equates to a higher priority for actions. An acceptable level of risk is the point where the cost and effort of additional mitigation to reduce the level of risk is greater than the loss that would be experienced if the risk were to occur.

Roles and Responsibilities

The UCAR President retains ultimate responsibility for risk management.

• Determines the appropriate level of risk that UCAR is willing to accept.
• Presents current risk register and detailed reports to the Audit and Finance Committee or the Board of Trustees upon request.

The ERM Steering Committee (ERM-SC) roles and responsibilities are currently being handled by President’s Council (PC) who have been delegated by the President with responsibility for overseeing risk management activities at UCAR.

• Approves appropriate risk management procedures throughout the organization.
• Owns and manages enterprise level risks for the organization.
• Reviews the risk register regularly and delegates appropriate actions as needed.
• Considers adding or dropping risks from the risk register.
• Acts as risk champions throughout UCAR/NCAR/UCP.
• Ensures that managing risks is integrated with other UCAR processes.
The Audit and Finance Committee of UCAR’s Board of Trustees collaborate with UCAR management in monitoring key risks and report to the Board of Trustees on assurances concerning the management of risks within UCAR.

The Enterprise Risk Manager is responsible for ensuring that risk management activities are carried out effectively throughout UCAR in accordance with the risk management policy and procedures.

- Maintains risk register and risk data in JCAD CORE system.
- Advises President’s Council on ERM best practices.
- Supports the regular review of risk management policy and procedures and makes recommendations.
- Produces regular reports for the Board of Trustees, President’s Council, and risk and control owners.

ERM Points of Contact (ERM-POC) will be appointed by lab/program/department Directors to serve as local go-to contacts for all ERM matters in their lab/program/department, and to guide the development of localized risk registers and risk control plans. Localized risk registers are updated at least twice a year and provided to the Enterprise Risk Manager for review, consolidation, and reporting to the ERM Steering Committee.

A Risk Owner is assigned to each risk. A Risk Owner is responsible for the management of the particular risk and ensuring that appropriate and effective controls are in place and operating as intended. It is the Risk Owner’s responsibility to provide the President and the Risk Manager with information to report to the Audit and Finance Committee on progress toward mitigation control plans and the results of any new risk assessments.

A Control Owner is assigned to each mitigation control plan or activity. It is the Control Owner’s responsibility to provide the Risk Owner with regular updates on the progress and effectiveness of mitigation activities. The Control Owner also reports on control failures and incidents that affect risks to goal achievement.

All Staff are expected to maintain an awareness of the need to manage risks when making decisions and in day to day operations. Staff share responsibility for identify risks and reporting them to their supervisor, especially during periods of change to processes or operations.

**Process**

A risk to the organization is any event or action that could have a negative impact. This includes events that could lead to:

- Death or injury.
- Financial loss.
- Damage to the UCAR/NCAR/UCP’s reputation or adverse media coverage.
- Damage to facilities, including land, water or air quality.
- Failure to meet regulatory or contractual requirements.

The failure to identify and capitalize on opportunities can also be considered a risk.

It is good management practice to be aware of risks and take precautions to avoid significant damage as a result of those risks. Therefore, UCAR has developed a risk management program to ensure that management of risks is undertaken in a systematic and standard approach across all of its operations.
Risk assessment process:

1: Risk identification

Risk identification requires documenting reasonably foreseeable risks that have or may have a significant impact on the organization. Risks may arise from the possibility that opportunities will not be realized, or from the possibility that threats will materialize, mistakes made, or damage/injury occur.

Structured risk identification and review sessions should take place at least once a year in labs/programs/departments. As new risks are identified during the normal course of work they should be managed immediately and reported by staff to senior management for assessment and possible inclusion in the risk register. The result of the risk identification process is a comprehensive list of risks known as a risk register.

2: Risk analysis

A thorough analysis needs to be documented for each identified risk, and should include the following information: summary of the risk, detailed description of the risk, impact, likelihood, risk exposure, risk category, goals that are affected, risk source, triggers, consequences, current controls, effectiveness of controls, new controls, risk owner, date risk was added, date risk was reviewed, and a time interval for reviews.

Risks are identified using the following root-cause categories: external, people, process, relationships, or systems.

3: Risk evaluation
Risk evaluation prioritizes risks resulting in identification of risks that require the most attention or additional attention. The level of risk determined in the analysis process is compared to risk criteria using the following options:

- Impact – insignificant, minor, moderate, major, and critical
- Likelihood – rare, unlikely, possible, likely, and almost certain

When assessing likelihood, note that the likelihood score for a risk needs to reflect the likelihood that the impact may occur, rather than the likelihood of the risk occurring.
## Risk Evaluation Criteria - Likelihood

<table>
<thead>
<tr>
<th>Description</th>
<th>%</th>
<th>Rate of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5</strong> Almost Certain</td>
<td>HIGH, almost certain, expected in most circumstances</td>
<td>&gt; 75%</td>
</tr>
<tr>
<td><strong>4</strong> Likely</td>
<td>MEDIUM-HIGH, likely, will probably occur</td>
<td>Up to 75%</td>
</tr>
<tr>
<td><strong>3</strong> Possible</td>
<td>MEDIUM, possible, could occur at some time</td>
<td>Up to 50%</td>
</tr>
<tr>
<td><strong>2</strong> Unlikely</td>
<td>MEDIUM-LOW, unlikely, not expected to occur</td>
<td>Up to 30%</td>
</tr>
<tr>
<td><strong>1</strong> Rare</td>
<td>LOW, rare, exceptional circumstances only</td>
<td>&lt; 10%</td>
</tr>
</tbody>
</table>
## Risk Evaluation Criteria - Impact

<table>
<thead>
<tr>
<th>Level</th>
<th>Criteria</th>
<th>Service Disruption, Affect Upon Funds or Process</th>
<th>Reputation</th>
<th>Failure to Comply or Meet Obligations</th>
<th>People</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Critical</td>
<td>Total failure of service, extremely expensive, &gt;$1M, $$$$$</td>
<td>National publicity &gt;3 days, resignations</td>
<td>Claim, fine, or impact above $5M</td>
<td>Fatality of 1+ employees or citizens</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>Serious disruption to service, $1M, $$</td>
<td>National public or press interest</td>
<td>Claim, fine, or impact above $500K</td>
<td>Serious injury or disability of 1+ people</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Disruption to service, $500K, $$</td>
<td>Local public and press interest</td>
<td>Claim, fine, or impact above $100K</td>
<td>Major injury to people</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td>Some minor impact on service, $100K, $</td>
<td>Contained within the dept but known by entity</td>
<td>Claim, fine, or impact above $10K</td>
<td>Minor injuries to people</td>
</tr>
<tr>
<td>1</td>
<td>Insignificant</td>
<td>Annoyance, small or no $ impact, $5K</td>
<td>Contained within the dept</td>
<td>Claim, fine, or impact &lt;$10K</td>
<td>Minor injury to individual</td>
</tr>
</tbody>
</table>
Risk prioritization is determined within the JCAD CORE tool by combining the impact ranking and likelihood ranking, resulting in a risk exposure of either very low, low, medium, significant, or high, that can be plotted on a heat map matrix as shown below.

The exposure ranking of a risk determines:

- The nature of further action that is required, and the urgency with which mitigation action should be undertaken.
- The reporting requirements for the risk, including who the risk is reported to.
- How often the risk is monitored.

4: Risk controls

Controlling risks involves identifying the options for treating each risk, evaluating those options, assigning accountability for oversight, preparing risk treatment plans and implementing them.

Many practical options are possible for mitigating risks, and all should be considered before deciding on an action plan.
5: Risk monitoring and reporting

Regular monitoring of risks and risk control action plans is an essential part of the risk assessment process. On a regular basis, risk owners need to ensure that new risks are identified and considered as they arise, and that existing risks are being monitored for changes that may need additional mitigation. Risk control owners need to monitor existing controls to ensure that they are in place and performing as planned. There needs to be ongoing conversation between risk owners and control owners to ensure that the complete risk environment is being managed to expectations. Risk information needs to be communicated through the President or his/her designee to the Audit and Finance Committee, who then will bring significant risk issues to the attention of the Board of Trustees.

By adhering to this risk management assessment process, UCAR will be better able to anticipate and respond to events that might otherwise cause damage. In many cases, the implementation of a robust ERM program contributes to better communication throughout the organization, improved overall compliance, and a more agile organization better able to react to change and opportunity.

The role of the ERM-SC in their review of risk owner’s reports is to advise the President on acceptability and relevance of the controls detailed in the reports.

The role of the Risk Manager is to draft an regular ERM report for presentation at the Board of Trustees meetings.

The risk monitoring and review process should proceed continuously throughout the year according to an established schedule, with risk owners supplying risk and control reviews and updates to the Risk Manager.

To ensure proper management of risks at a strategic level, President’s Council will regularly review the risk register to ensure:

- New risks to UCAR are identified and considered.
- Existing risks are monitored to identify any changes which may have an impact.
- Risks have been properly assessed and recorded in the risk register together with relevant information such as existing risk controls.
- An appropriate person has been identified for all new risk controls and new risk controls are being implemented according to the planned schedule.
- Existing risk controls are operating effectively.
Integrating Risk Management into UCAR Culture

To successfully integrate risk management into UCAR culture staff must be aware the importance of risk management and be engaged in the process. UCAR’s Board of Trustees and President's Council are aware of the value of ERM and are strong proponents of the practice. Staff can find out more about ERM on the Office of the President website: [http://president.ucar.edu/](http://president.ucar.edu/). Periodically, ERM updates will be a part of UMF (UCAR Management Forum) and other all-staff trainings and meetings.

<table>
<thead>
<tr>
<th>Level of risk</th>
<th>Reporting requirements</th>
<th>Action required</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Must be reported to Risk Manager who will report President’s Council for possible reporting to the Audit and Finance Committee.</td>
<td>Immediate action must be taken to reduce the risk. If it is not possible to reduce the risk immediately, it must be referred to the President via the Risk Manager.</td>
<td>Assign ownership to the appropriate individual.</td>
</tr>
<tr>
<td>Significant</td>
<td>Should be reported at least quarterly to the Risk Manager</td>
<td>Action should be considered to manage the risk.</td>
<td>Assign ownership to the appropriate individual.</td>
</tr>
<tr>
<td>Medium</td>
<td>Should be reported within 6 months to the Risk Manager</td>
<td>It may be appropriate that medium risks require no extraordinary action to reduce the risk further.</td>
<td>Assign ownership to the appropriate individual.</td>
</tr>
<tr>
<td>Low, Very Low</td>
<td>Should be reported annually to the Risk Manager</td>
<td>It may be appropriate that low and very low risks require no specific action to reduce the risk further.</td>
<td>Assign ownership to the appropriate individual.</td>
</tr>
</tbody>
</table>
Glossary of Terms

A glossary of commonly used terms can be found on the Enterprise Risk Management website.

Risk Contacts

For more information contact:

- David Sundvall, ERM program manager, risk@ucar.edu, 303-497-8898;
- Members of President’s Council