Enterprise Risk Management Process and Procedures

Scope

In accordance with risk management best practices, below describes the standard process for enterprise risk management (ERM), including:

- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment/controls
- Risk monitoring and reporting

The risk management process that UCAR has adopted is based upon the ISO 31000 standard for risk management. A standard approach to risk management allows risks to be appropriately prioritized across all of UCAR’s labs, programs, and departments, which leads to effective controls to ensure that UCAR is able to manage its operations effectively.

These procedures apply to all activities undertaken in the course of UCAR/NCAR/UCP business, whether at UCAR owned and managed facilities or at other locations.

Responsibilities

The UCAR President retains the ultimate responsibility for risk management and for determining the appropriate level of risk that UCAR is willing to accept. The President, or his/her designee, will present to the Audit and Finance Committee upon request an up-to-date risk register and report.

The ERM Steering Committee (ERM-SC) is delegated by the President with responsibility for overseeing the risk management activities at UCAR, and approving appropriate risk management procedures throughout the organization.

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/NCAR/UCP in accordance with the risk management policy and risk management procedures.

ERM Points of Contact (ERM-POC) are 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 will be assigned to each risk. A Risk Owner is responsible for the management of the particular risk. 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 risk assessments performed on new projects.

A Control Owner will be 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 shall diligently identify risks and report them to their supervisor, especially during periods of change to processes or operations.

Risk management 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 essential that the organization is aware of what risks it faces and takes 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 detail (lead by ERM-POC):

Preparation:
ERM-POC notifies the lab/program/department Director/Manager and schedules a risk assessment session with senior management, decision makers and risk owners at least once a year, for completion no later than November 1.

Strategic plan goals and objectives are reviewed with staff.

The risk assessment process and tools are reviewed and communicated to the participants.

ERM-POC and ERM program manager meet to review preparation, process, goals, and tools.

**Step 1: Risk identification**

Risk identification requires documenting reasonably foreseeable risks that have 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, errors be made, or damage/injury occur.

Structured risk identification and review sessions should take place at least once a year in labs/programs/departments and be completed by November 1. As new risks are identified during the normal course of work they should be managed immediately and reported by staff to senior management and the designated ERM-POC for assessment and possible inclusion in the risk register. The intended result of risk identification is a comprehensive list of risks are documented.

**Step 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 added, and date reviewed.

Risks are grouped together using the following categories: strategic, operational, financial, compliance, reputational, technology, or scientific.

**Step 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 certain

When assessing likelihood, it is important to note that the likelihood score for a risk needs to reflect the likelihood of the impact occurring, rather than the likelihood of the risk occurring.

Details and guidance regarding use of the risk criteria evaluation tables can be found on the [Enterprise Risk Management](#) website.

Risk prioritization is determined within the ERM tool by combining the impact ranking and likelihood ranking, resulting in a risk exposure of either: very low, low, medium, high, very high, or highest.

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.

**Step 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. The following options are available for treating risks and may be applied individually or in combination.

- Avoid the risk
- Eliminate the source of the risk
- Change the likelihood
- Change the impact
- Share or transfer the risk (via contract or insurance)
- Retain the risk
Many practical options are possible for mitigating risks, and all should be considered before deciding on an action plan. For assistance, please see the Enterprise Risk Management website or contact your ERM-POC, senior management, or the ERM program manager.

**Step 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 adequately 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 and should expect to be able reduce costs and damage associated with failing to respond. In many cases, the implementation of a robust ERM program contributes to better communication throughout the organization, improved overall compliance, a more agile organization better able to react to change and opportunity, and a perceived enhancement to stakeholder value.

A general ERM process timeline follows:
Role of the ERM Steering Committee risk register monitoring and review

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.

Following the review of Risk Owner’s reports at the ERM-SC annual meeting, the Risk Manager will draft an annual ERM report for presentation at the annual Board of Trustees meeting (usually in February).

The risk monitoring and review process should proceed continuously throughout the year, with Risk Owners supplying updated Risk Owner’s reports at least twice per year to the Risk Manager.

To ensure proper management of risks at a strategic level, the ERM-SC will review the risk register on a regular basis 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 nominated for all new risk controls and new risk controls are being implemented according to the planned schedule.
- Existing risk controls are operating effectively.

**Reporting**

As a guide, the following table shows the reporting and action that is required for each level of risk.

<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 to the ERM-SC and the President 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 the annual or bi-annual ERM-POC meeting.</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 at the annual or bi-annual ERM-POC meeting.</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>
<tr>
<td>Low</td>
<td>Should be reported at the annual or bi-annual ERM-POC meeting.</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.