Enterprise Risk Management Framework

V 1.0 June 2019

Table of Contents

Terms and Definitions[1]

risk

effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Risk is usually expressed in terms of **risk sources**, potential **events**, their **consequences,** and their **likelihood**.

risk management

coordinated activities to direct and control an organization with regard to **risk**

stakeholder

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

risk source

element which alone or in combination has the potential to give rise to **risk**

event

occurrence or change of a particular set of circumstances

An event can have one or more occurrences, and can have several causes and several **consequences**.

An event can also be something that is expected which does not happen, or something that is not expected which does happen.

An event can be a risk source.

consequence

outcome of an **event** affecting objectives

A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Consequences can be expressed qualitatively or quantitatively.

Any consequence can escalate through cascading and cumulative effects.

likelihood

[1] ISO 31000:2018

chance of something happening

In **risk management** terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

control

measure that maintains and/or modifies **risk**

Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Controls may not always exert the intended or assumed modifying effect.

Introduction

What are the goals of an ERM framework?

- Appropriate risk governance
- Well-informed, risk-aware culture
- Defined organizational risk appetite
- Consistently-applied risk management techniques
- Integration with business decision making

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 parties

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

Risk Appetite	Risk Tolerance	Risk Management Approach	Management Action
No appetite	Zero tolerance	Highly cautious	Crisis mode; Board informed
Low appetite	Low tolerance	Cautious	PC informed
Moderate appetite	Moderate tolerance	Conservative	Lab/program/dept director approval
High appetite	High tolerance	Confident	Business case

Risk Appetite: Amount and type of risk that UCAR/NCAR/UCP is willing to pursue or retain.

UCAR's approach to its risk appetite is to minimize its exposure to reputational, compliance, financial, operational, compliance, technology and strategic risks, while also accepting and encouraging risk in pursuit of its mission and objectives. UCAR understands that its appetite for risk varies according to activities undertaken, and that acceptance of risk always takes into consideration potential benefits of a risk as well as a thorough understanding of risk, with reasonable mitigation action plans in place before approving and undertaking activities.

Reputation: UCAR has an established and enviable track record for world-class atmospheric research. As such, UCAR has:

- **no appetite** for any risks which would negatively impact its reputation, brand, ethical standing, or legacy in its field which could lead to adverse publicity or cause a loss of confidence of its community, members, collaborators, or sponsors.

Compliance: UCAR is committed to maintaining the highest standards of integrity, compliance and ethics. As such, UCAR has:

- **no appetite** for any breaches in statute, regulation, professional standards, research ethics, bribery, or fraud. This applies to UCAR internal systems, policy and processes, as well.

Financial: UCAR has a long-standing history of sound financial management based in prudent stewardship over its financial resources in fulfillment of its mission. UCAR has:

- **low appetite** for weaknesses in financial stewardship, internal controls, reporting, and resource utilization and expenditures that impair completion of mission-critical functions,
- **moderate appetite** for short-term financial risk that occurs in response to external factors.

Operational: Major change and modernization activities are periodically required to maintain UCAR's high standards of operational excellence. UCAR manages such projects according to best practices in project and change management and has:

- **no appetite** for physical security lapses, employee health/safety/misconduct issues,
- **low appetite** for unsatisfactory employee conduct, business continuity planning lapses, governance process issues, and internal controls and communications failures,
- **moderate appetite** for undertaking innovation and creativity in pursuit of more efficient operations that improve integration between people, processes, and systems.

Technology: Information systems are relied upon to support UCAR/NCAR/UCP core functions with sufficient capability, capacity, resiliency, and security from internal and external threats. UCAR relies on an increasingly mobile and technologically dependent workforce to carry out its mission and objectives. Therefore UCAR has:

- **low appetite** for unreliable technology,
- **no appetite** for unauthorized access to systems and confidential data,
- **low appetite** for losing continuity of business operations; and,
- **moderate appetite** for innovative technology solutions to meet user demands in a rapidly changing environment.

Strategic: UCAR's mission is to provide leadership in the earth system science community through research, computing, observational facilities, and educational outreach. Its strategic objectives closely align with the mission, vision, and core values in support of the mission, and are effectively prioritized, communicated, and executed. UCAR has:

- **low appetite** for activities that do not align with mission-critical goals,
- **moderate appetite** for responsible innovation in responsiveness to internal and external change to remain competitive and supportive to the community.

Risk Tolerance

Risk Tolerance: UCAR/NCAR/UCP or stakeholder's readiness, in pursuit of its objectives, to bear a risk after risk mitigation action plans have been applied. The enterprise risk tolerance is assessed by the UCAR President, in consultation with the Board of Trustees, Senior Vice President/Chief Operating Office and the ERM Manager. Risk tolerance assessments are dependent on the risk, during the quarterly reviews and the BoT sessions.

Roles and Responsibilities

- Board of Trustees

  Oversees ERM activities

Reviews and approves ERM policy and framework at least every two years

Reviews and approves risk appetite and tolerance statements at least every two years

Delegates to the Audit and Finance Committee, responsibility for implementing risk management process and framework

Periodic reviews of enterprise risks in context of UCAR's strategic plan

- Audit and Finance Committee

  Oversees the effective implementation of ERM at all levels of the organization

  Regularly reviews enterprise risks and actively engages in the risk assessment process

  Reviews policy, framework, risk appetite and tolerances and recommend them for Board approval

- Other Board Committees

  Regularly review risks as they relate to the function of their committee

- SVP & COO, Senior Management Team

  Implements ERM framework

  Regularly reviews enterprise risks, appetite and tolerance and engages with the Audit and Finance Committee.

- Risk Manager

  Executes, supports and coordinates activities related to the ERM process

  Promotes ERM awareness

- Internal Audit

  Provides independent assurances on the state of risk management

  Utilizes the ERM risk register when developing annual risk-based internal audit plan

- Labs/Programs/Departments

  Accountable for assigning ownership for all risks facing their areas of responsibility and for managing them in line with the framework, including maintaining a risk register

- Risk Owners

Responsible for managing specific risks, monitoring and reporting on progress and effectiveness of risk controls

- Risk Controls Owners

  Responsible for developing, executing, and reporting to risk owner on progress of action plans to mitigate particular risks

- All Staff

  Responsible for reporting to lab/program/department manager all actual or potential incidents which present risk to the organization

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 and its ability to achieve its goals. 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.

Access to Risk Registers is restricted to senior management stakeholders. Risks should be clearly stated without being overly wordy using the following format: The risk that *'an event'* may occur resulting in *'consequences'*. Example: The risk that icy and snowy surfaces could cause a slip and fall resulting in physical injury. Focus on risks that affect your lab/prog/department.

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 type, triggers, and risk owner. During the risk analysis consideration should be given to the causes and consequences of risks.

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 – 1-insignificant, 2-minor, 3-moderate, 4-major, and 5-critical

Likelihood – 1-rare,2- unlikely, 3-possible,4- likely, and 5-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

	Description	%	Rate of Occurrence
5 Almost Certain	HIGH, almost certain, expected in most circumstances	> 75%	Daily - Weekly
4 Likely	MEDIUM-HIGH, likely, will probably occur	Up to 75%	Monthly
3 Possible	MEDIUM, possible, could occur at some time	Up to 50%	Once or twice a year
2 Unlikely	MEDIUM-LOW, unlikely, not expected to occur	Up to 30%	Every 2 – 5 years
1 Rare	LOW, rare, exceptional circumstances only	< 10%	10+ years

Risk Evaluation Criteria - Impact

	Service Disruption, Affect Upon Funds or Process	Reputation	Failure to Comply or Meet Obligations	People
5 Critical	Total failure of service, extremely expensive, >$1M, $$$$	National publicity >3 days, resignations	Claim, fine, or impact above $5M	Fatality of 1+ employees or citizens
4 Major	Serious disruption to service, $1M, $$$	National public or press interest	Claim, fine, or impact above $500K	Serious injury or disability of 1 + people
3 Moderate	Disruption to service, $500K, $$	Local public and press interest	Claim, fine, or impact above $100K	Major injury to people
2 Minor	Some minor impact on service, $100K, $	Contained within the dept but known by entity	Claim, fine, or impact above $10K	Minor injuries to people
1 nsignificant	Annoyance, small or no $ impact, $5K	Contained within the dept	Claim, fine, or impact <$10K	Minor injury to individual

Risk prioritization is determined by combining the impact ranking and likelihood ranking, resulting in a risk exposure of either low, medium, high, or extreme 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.

RISK ASSESSMENT MATRIX KEY

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, including costs, 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.

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 will be able to make more informed decisions. 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.

Risk stakeholders throughout UCAR/NCAR/UCP have access to the enterprise level risk register in a shared Google Team drive. Labs/programs/departments regularly update their group's risks in separate tabs of the risk register. Monthly, the aggregated risk register is reviewed by the Risk Manager, the SVP-COO, and the UCAR President.

To ensure proper management of risks at an enterprise level, President's Council and the Audit and Finance committee of the Board of Trustees 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.

As a guide, the following table shows the reporting and action that is required for each level of risk as emerging risks are identified:

Level of risk	Reporting requirements	Action required	Accountability
Extreme	Must be immediately reported to Risk Manager who will consult with SVP/COO and President's Council for possible reporting to the Audit and Finance Committee.	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 and the Board via the Risk Manager.	Assign ownership to the appropriate individual.
High	Should be listed on the risk register when identified and reported at least monthly to the Risk Manager	Action should be considered to manage the risk. PC may be informed.	Assign ownership to the appropriate individual.
Medium	Should be listed on the risk register when identified and reported at least monthly to the Risk Manager.	It may be appropriate that medium risks require no extraordinary action to reduce the risk further. Lab/prog/dept director should be notified.	Assign ownership to the appropriate individual.

Low		Should be listed on the risk register at least monthly.		It may be appropriate that low and very low risks require no specific action to reduce the risk further.		Assign ownership to the appropriate individual.

Mitigation Expenses

Risk and control owners are responsible for covering all costs related to action plans that are put in place to mitigate their risks. UCAR/NCAR/UCP budget offices have procedures in place to handle pre-spending, overspending, and ongoing budget planning. Please note, all persons responsible for managing accounts, including expenditures and encumbrances in those accounts, are responsible for monitoring, preventing, and resolving overspending as they pertain to risk mitigation affecting their areas of operation. These procedures are also intended to provide management with an early warning of potential funding problems so action can be taken as needed.

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.

Risk Contacts

For more information contact:

- David Sundvall, ERM program manager, risk@ucar.edu, 303-497-8898
- Lory Wingate, SVP/COO, wingate@ucar.edu, 303-497-1719
- Members of President's Council
- Lab/Program/Department Director