University of Colorado Boulder  
Campus Policy

Effective: April 24, 2015

Responsible Office: Senior Vice Chancellor and Chief Financial Officer

Policy Title: Risk Management Policy

Approved

Purpose:
Establish roles and responsibilities for managing risk to university resources.

A. Introduction
University of Colorado Boulder is committed to managing its risks proactively, holistically, and ensuring that risk management is an integral part of all university activities and a core capability. The university’s risk management process is designed to:

- Identify potential events, practices and procedures, trends and opportunities that may significantly affect the university’s ability to achieve its strategic goals and successfully maintain its operations, reputation, and legal obligations.
- Respond to risks based on university’s risk appetite to provide reasonable assurance that the university’s objectives will be achieved.

The university’s objectives for the management of risk include:

- Integrating the practice of risk management into the culture and strategic decision-making process throughout the university.
- Anticipating and responding to changing social, environmental, technological and legislative conditions.
- Managing risk according to best practice and demonstrating due diligence in decision making
- Optimizing value by balancing the cost of managing risk with the anticipated benefits.
- Managing significant risks related to potential financial, reputational, health and safety, and legal negative consequences.

B. Policy
CU-Boulder has established a risk management program to ensure that risks to university resources are proactively identified and managed by the appropriate authority. The management of risk is continuous
and should be applied at both the enterprise level as well as an individual academic and administrative unit level. The university’s principles for managing risk are:

- The Chancellor with the assistance of the Risk Management Steering Committee (RMSC) oversees the management of risk on the campus.
- Campus leadership adopts an open and receptive approach to solving risk problems.
- Campus leadership supports, advises on, and implements policies.
- Campus Organizational unit directors develop and implement effective risk management practices within their units.
- Key risk indicators are identified and monitored on a regular basis.
- Data Owners [provide link] are appropriately included in the evaluation and acceptance of risk to university information.

C. Program Roles and Responsibilities

All employees of the university are responsible for the effective management of risk including the identification of potential risks. Risk management processes will be integrated into existing departmental planning processes and management activities.

**Risk Management Steering Committee (RMSC)**

The RMSC is responsible for the oversight, direction, and support for the risk management efforts and is composed of campus members representing a cross section of the university. RMSC members, including a campus committee Chair, are appointed by the Chancellor or designee. The RMSC is responsible for:

- Determination of priorities of the risk management program.
- Monitoring progress in managing risk.
- Formal identification of strategic risks that have an impact on the university’s goals.
- Development and implementation of strategic risk management plans.
- Reports the status of risks to governance and oversight groups, including campus leadership.

**University Risk Management (URM)**

URM shall:

- In collaboration with the RMSC and the Office of Information Security (OIS), oversee and maintain the risk management framework and associated processes.
- Annually, in collaboration with the Office of Information Security, coordinates the process of identifying, reviewing, and ranking risks. Maintains a consolidated risk register for the campus.
- Assist with facilitating action in those areas where improvements are required.
- Provide guidance to the RMSC as necessary.

**Assistant Vice President and Chief Information Security Officer (CISO)**

Assistant Vice President and Chief Information Security Officer shall:

- Provide guidance to campus Information Security Officers on information risk management processes to ensure that IT security safeguards are applied in a judicious and effective manner.
- Submit reports to the university Security Advisory Committee on risk management decisions pertaining to information and IT resources as appropriate.
- Collaborate with the RMSC, URM, and campus departments to assist with the coordination of risk management planning and reporting efforts.
Organizational Unit (OU) Directors

OU (typically a department with an independent budget represented in the Finance System) Directors and chairs or their designees are responsible for ensuring that all applicable risk management policy requirements are implemented in their respective units. OU Directors shall:

- Assign individuals to complete the service risk assessment, following guidance from URM, for their unit and update it at least annually. OU Directors will ultimately be accountable for the authenticity and completeness of the responses.
- Submit IT services listed on the service risk assessment to the Office of Information Technology for inclusion in the campus IT services catalog.
- Create and implement a risk action plan in response to business risks that they have identified. Risk remediation plans shall be submitted to the RMSC for review and approval.
- Consult with URM, campus information security officer, other campus support departments as necessary to determine appropriate plans for remediating risks.
- Incorporate risk management into their departmental/unit planning processes and management activities.
- Actively participate in the risk assessment process.
- Report on the status of items in the risk register as required when it has an impact on their respective responsibilities as part of the annual planning or review cycle.

C. Processes

University Risk Management, Office of Information Security, and CU-Boulder Office of Information Technology shall collaborate in the maintenance and publication of processes required to support risk management functions at CU-Boulder.

D. Administration and Enforcement

The Senior Vice Chancellor and Chief Financial Officer shall, as determined by the circumstances of a potential policy violation, work with the appropriate University offices such as University Counsel, the AVC for IT and Chief Information Officer, CRO, CISO, deans and directors, and others to enforce this policy.

E. Definitions

F. Selected References to University Policies.

- Information Security Program - http://www.cu.edu/ope/aps/6005
- Standards for Data Classification and System Security Categorization - http://www.cu.edu/sites/default/files/CUdataclassification.docx

G. Contact Information