Enterprise Risk Management at the University of California

> *Enterprise Risk Management (ERM) confronts the challenge of combining disparate sources of risk to provide senior management and the board with a comprehensive and holistic view of the risks facing the business, so they can achieve the objectives of the business and create value for stakeholders.* - Andrew Waters, Moody's

This paper describes the components of a risk management framework, the University of California's approach, and concludes with a risk maturity index.

Governance Framework

Like most organizations, the University of California has a governance framework that: defines the organizational hierarchy and roles; assures adherence to legal and regulatory requirements; monitors the organization and its environment; develops and assures internal controls; provides for transparency and accountability; and defines, guides, and provides for enforcement of policies and procedures. A risk management framework is an integral part of a governance framework. An ideal risk management framework includes:

- **Risk Oversight** that is well-informed and sets risk tolerances in pursuit of the University's mission and values
- **Risk Infrastructure:** the people, processes, and technology that set the foundation for
- **Risk Management & Control Processes** that support all University activities

---

Risk Oversight - Effective risk oversight provides for delegation, coordination, and facilitation, by clearly laying out procedures and risk escalation processes. A sound organizational culture, set by the Board and leadership, consistently models appropriate risk awareness, behaviors and judgements about risk-taking.

UC's Approach to Risk Oversight

The Board of Regents and University leaders define risk tolerances in pursuit of the University's mission and values, which are codified in Board and leadership decisions, guidance, and University policies and procedures. The Board provides oversight of the accountabilities for managing risks, and for ensuring the effectiveness of internal controls, ethics, and compliance programs. The University's risk management framework supports board members' duty of care obligation: to make decisions on a fully informed basis and with due diligence. Led by UC President Dr. Michael Drake, the Office of the President plays a distinct role in helping to shape the overall vision for the university and in carrying out core activities that allow the campuses, medical centers, ANR and the National Labs to function as a single university. The Academic Senate is empowered by the Board of Regents to exercise direct control over academic matters of central importance to the University.

UC's Approach to Risk Infrastructure

Office of the President Risk Services coordinates with the other systemwide departments to lead and manage the University's systemwide risk infrastructure. Leaders at the University's campuses, health systems, and other locations establish local risk infrastructures by: providing oversight of risk management, assigning roles and accountabilities, allocating resources based on risks, and integrating risk management into organizational activities and decisions. Evidence of University location risk infrastructures include: appropriately resourced organizational support departments such as: Risk Management, Compliance, Controller, Cybersecurity, EH&S; cross-functional risk councils that build a common view of organizational risks; and the adoption of systemwide services, programs, and technology. Below is an outline of the systemwide risk infrastructure provided by UC Risk Services:

People
- Risk & Compliance Committees at Campuses and Health Systems
- UC Risk Partners: collaboration among Risk Management, Compliance, Legal, & Internal Audit
- Centers of Excellence: subject matter risk expertise
- Risk Services supports over thirty systemwide professional workgroups, including:
  - Campus and Health Risk Directors, and Workers Comp Managers
  - Campus and Health EH&S Directors

Programs
- Safety & Loss Prevention
  - Be Smart About Safety - loss prevention and mitigation funding
  - Shoes for Crews – Slip-resistant footwear
  - Ergonomics & Injury Prevention
  - Work Strong – Occupational Wellness
- Insurance programs: including WC, property, student health, construction, liability and claims management
- Travel insurance, trip planning and geographic intelligence resources
- Risk financing via the UC's captive, Fiat Lux Risk and Insurance Company
- Risk Security & Resilience, Emergency Management, and Mission Continuity Planning

Training and Education
- UC Risk Summits
- UC Cyber Security Summits
- UC EH&S Professional Education
- Safety in the Performing Arts
- Risk and Safety Training Center

Technology

- [Risk & Safety Solutions](#)- UC managed business with a suite of innovative risk and safety technology solutions
- Risk Data Management System – platform to analyze events, claims and injury data with benchmarking metrics
- RL Solutions – platform supporting healthcare incident management and reporting
- UC Ready – platform supporting mission continuity and disaster recovery planning
- Certificate of Insurance Issuing platform

Risk Management and Controls – Dynamic, integrated, and proactive risk management and control processes support people to effectively identify, assess, communicate, respond to, and monitor risks to an organization's mission, values, and strategies.

UC's Approach to Risk Management and Controls

UC leadership promotes a proactive risk culture, which bolsters effective risk management and control processes, promotes appropriate risk-taking, and ensures that emerging risks or risk-taking activities beyond the University's risk tolerance are recognized, assessed, and addressed in a timely manner. The slogan, "ERM = Everyone is a Risk Manager", has been widely adopted across the University since it was introduced. It recognizes that those who perform or manage an activity, the *risk owners*, are best suited to manage the risks in their areas of responsibility. UC Risk Services and all UCOP departments provide support centrally to those managing risk locally. Evidence of risk management and control processes can be found across the University system and include: risk assessment techniques and risk management systems and technologies that are widely adopted and integrated into University activities; the use of risk analysis techniques when considering new initiatives; legal, risk and compliance teams that are integrated into decision making across the organization, and risk-based internal auditing that provides assurance on the effectiveness of risk management and control processes. Taken as a whole, the University's risk framework is a vital factor in the successful achievement of the University's mission, strategies and initiatives.

Recognition of Excellence in Risk Management at the University of California

- AVP & Chief Risk Officer Cheryl Lloyd recognized with '2021 Risk Management Honor Roll' by RIMS
- The University of California recognized in 2017 and 2018 as a *RIMS* [Risk Maturity Model Recipient](#)
- 2017 'Outstanding Captive Insurance Company of the Year' awarded by CICA
- In 2013, *APQC* selected the UC in the top 5 global Best-Practice Organizations in ERM
- 2013 Alexander Hamilton Award silver recipient for Enterprise Risk Management by *Treasury & Risk*
- UC was the first non-financial institution to receive a credit rating agency acknowledgement of its enterprise risk management program - *Standard & Poor's*, September 2010

Appendix 1: Risk Maturity Index
(Based on the Aon Risk Maturity Index)

Each component can be scored 1-5 in an organizational assessment, with 5 representing advanced capabilities / best practices, and 1 representing a new or non-existent component.

- ☐ The organization's ability to identify, measure, manage, and monitor risks
- ☐ The degree to which risk management is dynamic and adapts to changing risk environments
- ☐ The level of understanding of the organization's key strategic, internal and external risks, and consistent and timely execution of activities to address them
- ☐ The level of Board's understanding of the organization's key risks and key risk management activities
- ☐ The quality of risk information presented to the Board and its committees
- ☐ Board and management consensus regarding the organization's risk management strategy in relationship to the organization's overall strategy and objectives
- ☐ The organization's approach for gathering and incorporating risk information into strategic planning processes, significant investments, and project decisions
- ☐ The degree that risk and risk management information is explicitly considered in decision processes
- ☐ The level of involvement by the risk management leader during key strategic decisions
- ☐ The manner in which risk information from external sources and strategic partners is used
- ☐ The consistency, frequency and content of risk management communications in the organization
- ☐ The involvement of internal subject matter experts in risk analysis and the execution of risk management processes
- ☐ The organization's approach to understanding and building consensus on risks with cross-functional or cross-divisional impacts
- ☐ The degree of coordination in risk data gathering and analysis conducted by risk-based functions (e.g., Internal Audit, Legal, Compliance, Enterprise Risk Management)
- ☐ The organization's approach and receptivity to communication of negative information or predictions
- ☐ The level of understanding of underlying risk causes, and the manner in which that information is used to support risk management decisions
- ☐ The organization's approach to conducting reviews, scenario analysis, post-mortems, or root-cause analysis, and the degree of learning from them
- ☐ The level of understanding and mitigation of asset and business interruption liability exposures
- ☐ The level of understanding and mitigation of insurable or self-insurable liability exposures
- ☐ The level of understanding of employee engagement and its role as a driver of business performance