

ERM and GRC Fundamentals

ERM and GRC Roles, Responsibilities
and Risk Ownership

Session 2



Contents

**Importance of Evaluating Risk Roles
and Responsibilities**

**Current GRC Roles &
Responsibilities at CalPERS**

Leading Practices



Importance of Evaluating Risk Roles & Responsibilities: Introduction



Questions to ask of yourself and of others:

“Now that I know what GRC is, who owns it?”

“What is my role in GRC?”

“If I am not focused on GRC, who is?”

“Who should be focused on GRC?”

Importance of Evaluating Risk Roles & Responsibilities

Nothing is more fundamental to business than risk, especially in the context of strategic decision making.

Boards today operate in the most challenging environment any generation of directors has known.

- » **Expectations of boards, complexity of risk, and speed of change are dramatically increasing.**
- » **Boards are coping with ever-fuller agendas, potential liabilities, and often limited time and information to meet challenges of effective risk oversight.**

By clarifying risk roles and responsibilities, board members will be better positioned and equipped to determine how to conduct its oversight.

Current Roles & Responsibilities: CalPERS Risk Intelligent Management Policy

Board of Administration

- » Recognizes that the effective and efficient **management of risk across the enterprise is an integral part of sound governance and management practice**
- » Acknowledges its **responsibility for establishing CalPERS risk policies and tolerance parameters** where appropriate
- » **Holds the Chief Executive Officer and Executive Management accountable** for the establishment and implementation of the organization's risk intelligent enterprise management strategy and architecture
- » The Chair of each standing committee is **responsible for ensuring that all policy items** brought before their committee **contain an appropriate risk assessment.**
- » **Standing committees make recommendations to the full Board** with regard to risk tolerance parameters and, as appropriate, address specific risk issues brought forward by management.
- » **Provides oversight with regard to the overall architecture and structure of CalPERS Risk Intelligent Enterprise Management activities.**

Current Roles & Responsibilities: Risk and Audit Committee GRC Powers Reserved

Board of Administration

- » Approve enterprise risk policies framework and oversee effectiveness of enterprise risk management.
- » Approve risk appetite and strategy (excluding investment risk).
- » Oversee process for investment risk management, investment policy compliance, monitoring , and operating risk management.
- » Oversee enterprise program and policy compliance.
- » Oversee privacy and security compliance.
- » Oversee review of alleged breaches of ethics by board or executives.
- » Oversee service provider compliance (including harmonizing conflict of interest policies).
- » Oversee whistleblower and hotline processes.

Current Roles & Responsibilities: Three Lines of Defense



Leading Practices: The Board's Role in Risk Management

- » **Setting the “tone at the top”**
- » **Reviewing / agreeing with the organization’s risk appetite / tolerance**
- » **Determining board committee expectations (i.e., risk management)**
- » **Reviewing the risk management framework for the organization**
- » **Understanding the top / key business risks**
- » **Regular and active risk management dialogues with management**



Leading Practices: Areas of Board Responsibility for Risk Oversight

Board Focus Areas (per National Association of Corporate Directors)	Risk Oversight (per leading practice)
Board Governance of Risk	Aligning risks and Board committees
Enterprise Risks	Understanding the top risks of the organization
Board-Approved Risks	Approving new strategies or actions (mergers, major investments etc.)
Business Management Risks	Understanding operational risks managed by the executive team
Emerging Risks	Understanding trends and changes in the risk landscape
Stewardship	Promote and support the mission of CalPERS and the culture of risk intelligence



Report of the NACD Blue Ribbon Commission on Risk Governance: "Balancing Risk and Reward" 2009

Leading Practices: Risk Management Roles and Responsibilities

Roles and responsibilities in the risk assessment process are:

Chief Risk Officer (CRO)	Board & Committee Members	Management / Executive Team	Risk Owners and Process Leaders
<ul style="list-style-type: none"> • Guide risk assessment • Monitor completion of risk assessments • Re-perform assessments when changes occur • Monitor risk mitigation efforts and risk reporting • Ensure risk appetites are communicated and align business strategies • Ensure risk practices are supported by corporate culture • Track risk trends over time 	<ul style="list-style-type: none"> • Provide expertise to assigned committees • Review of risk assessment results • Vote on key actions brought for approval • Monitor and report to the committee on new/emerging risks • Oversee and understands risk appetite • Review governance structure 	<ul style="list-style-type: none"> • Based on responsibility <ul style="list-style-type: none"> ✓ Ensure risk assessments are done ✓ Monitor risk mitigation activities ✓ Develop and provide risk reports ✓ Develop risk measures ✓ Monitor emerging risks - Establish risk appetite, tolerance and GRC process - Set governance structure 	<ul style="list-style-type: none"> • Provide owners assessment of risks annually • Report on risks and risk mitigation efforts • Monitor and report key risk indicators • Monitor emerging risks • Apply GRC and risk management process • Monitor governance structures and report • Adhere to set risk tolerances

Summary

- » Roles and responsibilities for GRC are shared – by the Board, Management, OERM, and process and risk owners.
- » The Board provides oversight.
- » Responsibility for managing enterprise risk remains with Executive Management.
- » Managers at all levels are responsible for managing risk in their areas of responsibility.
- » All CalPERS staff are responsible for identify and reporting potential risk to the organization.



Thank You

