ERM and GRC Fundamentals

Risk Management Definitions & Guiding Principles

Module 1

Agenda

Introduction:

Purpose and Goal of the Training (5 min.)

Section 1:

ERM / GRC Terms & Concepts (15 min.)

Section 2:

GRC Guiding Principles

(30 min., including 20 min. exercise)

Section 3:

Summary of Module 1 (5 min.)

Section 4:

Preview of Modules 2 and 3 (5 min.)

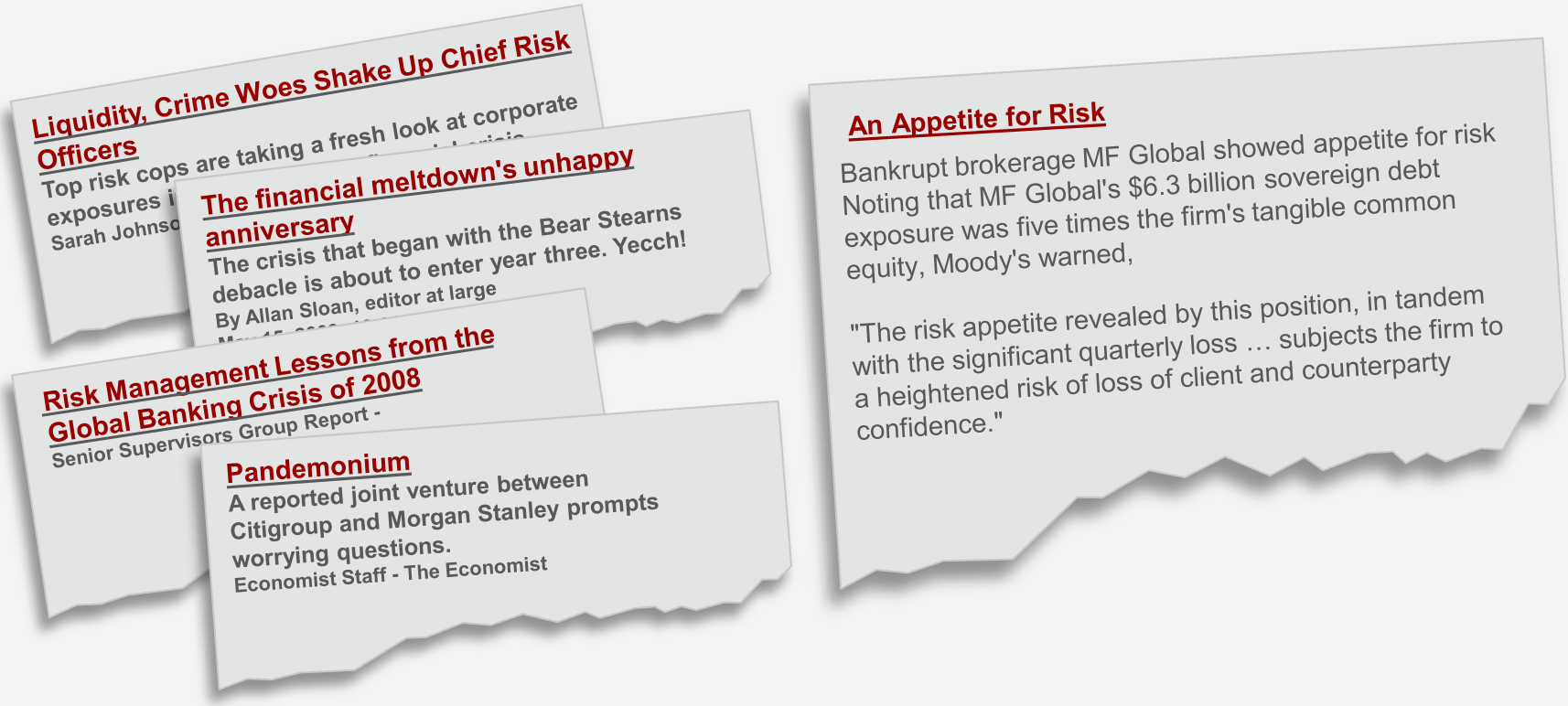
Section 5:

Internal Assurance & Audit Services (30 min.)

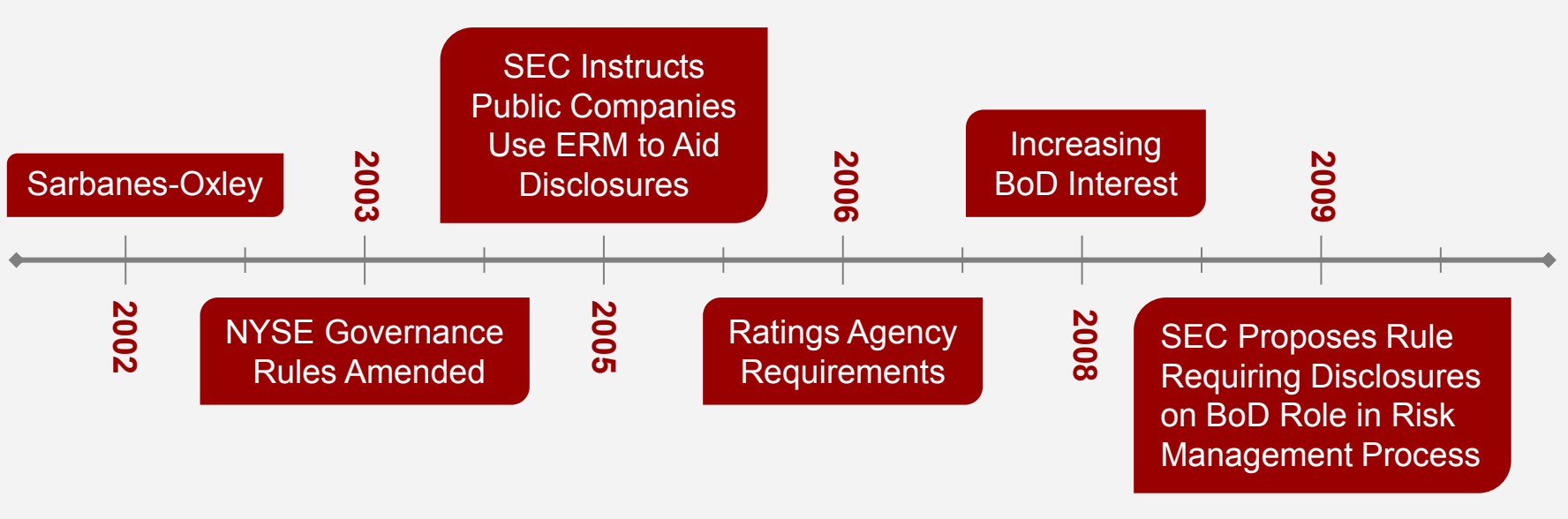
Background

- **The Risk Management landscape in 2012 and beyond is changing.**
- **The Board's responsibility to understand the organization's risk framework has increased.**

Risk Management In the News



Background (continued)



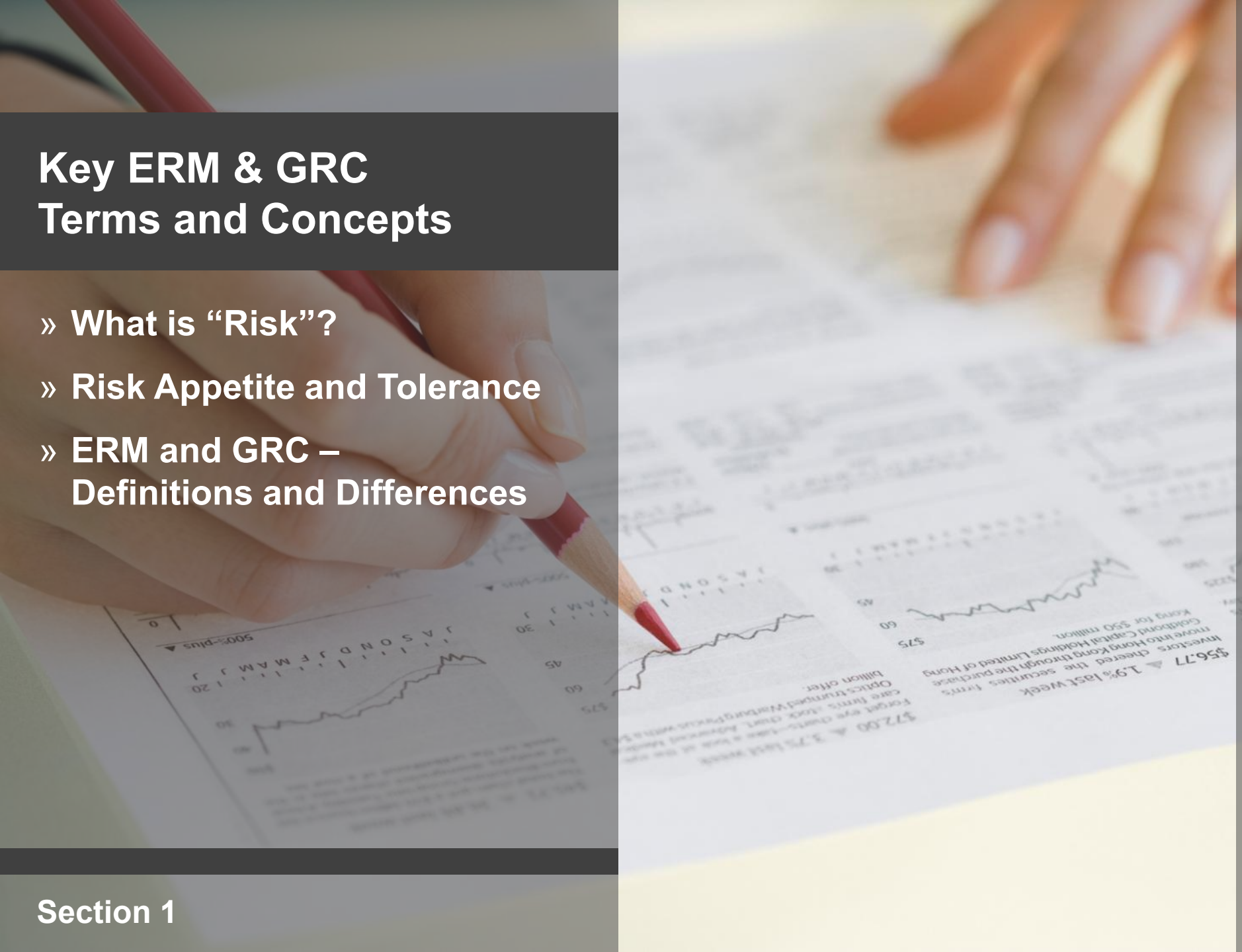
- NYSE
- SEC
- Standard and Poor's
- Boards of Directors request more information

Introduction

- In 2009, Governance Risk Management Initiative
- In 2010, established Office of Enterprise Risk Management
- In 2012, created Risk & Audit Committee
- Currently, CalPERS leads the way in GRC among public pension systems
- The journey continues…

Key ERM & GRC Terms and Concepts

- What is “Risk”?
- Risk Appetite and Tolerance
- ERM and GRC – Definitions and Differences



Section 1

What is Risk?

Risk: **The threat of an event, action (or inaction), or loss of opportunity that could adversely impact CalPERS' ability to achieve its strategic and business goals and initiatives.**

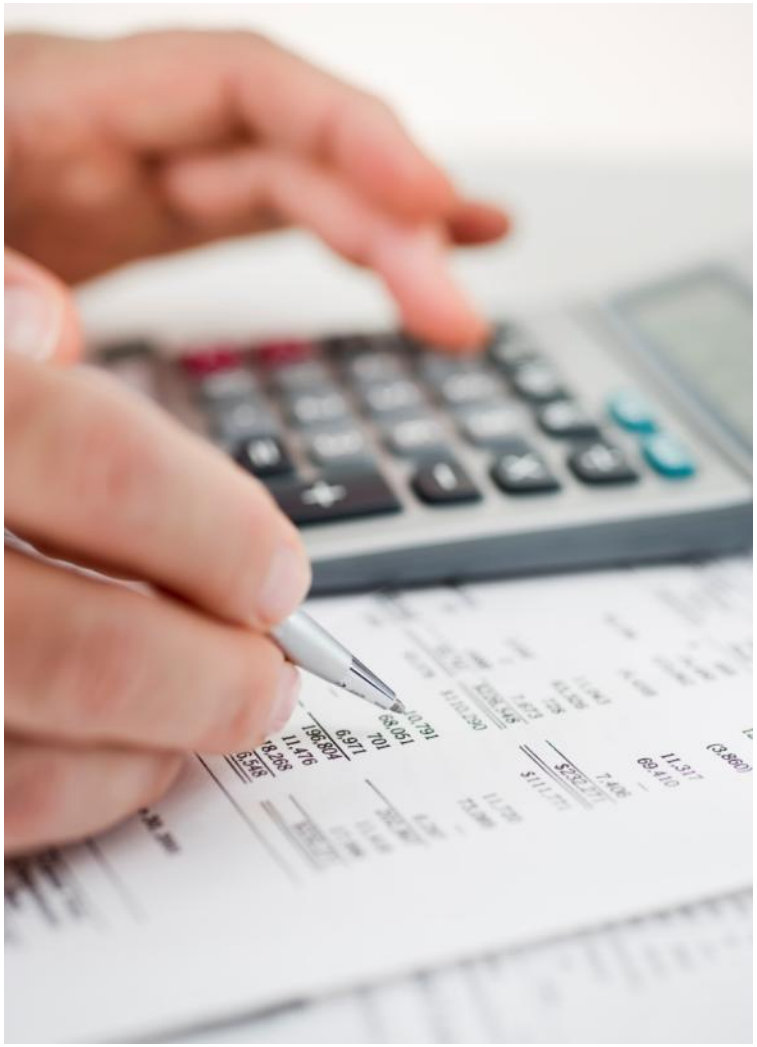
Risk Assessment: **A systematic approach to the identification and assessment of the organization's strategic business risks that threaten business objectives.**

Enterprise Risk Management

Enterprise risk management is:

- A process across the enterprise
- Overseen by Board of directors
- Applied in strategy setting
- Identify potential events
- Management of risks within risk appetite
- Reasonable assurance

> **Risk Management is everyone's responsibility**



Risk Appetite vs. Risk Tolerance

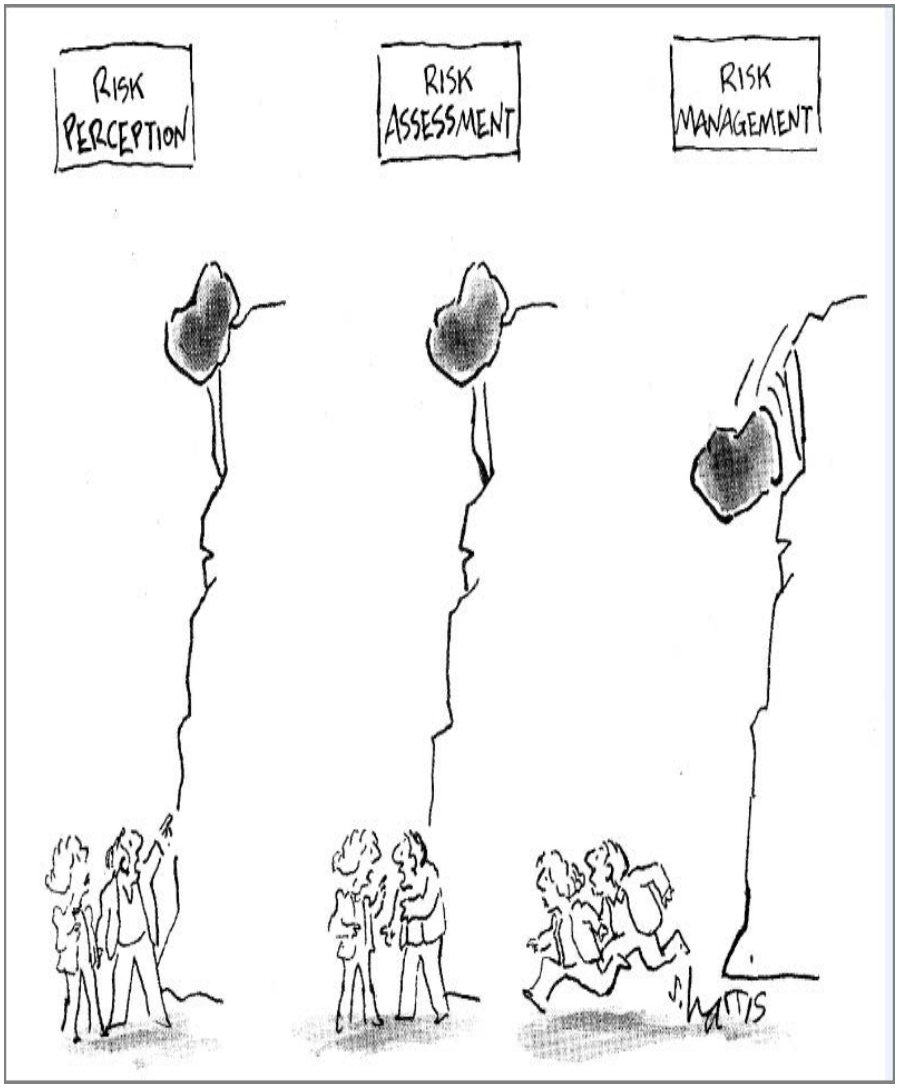
Risk Appetite:	Amount of risk the organization is willing to accept in pursuit of value.
Risk Tolerance:	Acceptable levels of variation relative to the achievement of objectives.

There should be a clear link:

What ERM is Not – Common Misconceptions

What ERM is NOT

- A program
- A method to eliminate all risks
- A guarantee there will be no losses
- A collection of longstanding and disparate practices
- A rigid set of rules
- Limited to compliance and disclosure
- A replacement for internal controls
- Exactly the same for one organization to the next
- A passing fad



How ERM is Different Than GRC

Evolution of Risk Management

Risk Assessment

- Enabled by People
- Internal Audit and Audit Committee
- Performed in silos

Enterprise Risk Management

- Enabled by Process
- Executive Management
- Alignment to Strategy and Operations
- Enterprise-wide
  - Discipline
  - Assessment

Governance, Risk and Compliance

- Enabled by Technology
- All Levels of the Organization
- Convergence Effort , Includes Compliance and Internal Audit
- Single Source of Understanding and Truth

What is GRC?

An approach to align the organization's governance, risk and compliance processes to its strategy, allowing for:

- **convergence**
- **transparency of information**
- **improved performance**
- **resilience in a dynamic business environment**

What GRC Is and What It Is Not

What GRC is

- Starts with understanding strategic objectives, mission and business model
- Comprehensive view of the oversight functions
- Converging risk related information from various oversight functions
- Encompasses people, processes and technology considerations

What GRC is not

- Not just a technology solution, but frequently involves technology enablement
- Not just another name for Enterprise Risk Management
- Does not eliminate the need for existing functions (e.g., Compliance)
- Not just conceptual – must be practical

GRC
Guiding Principles

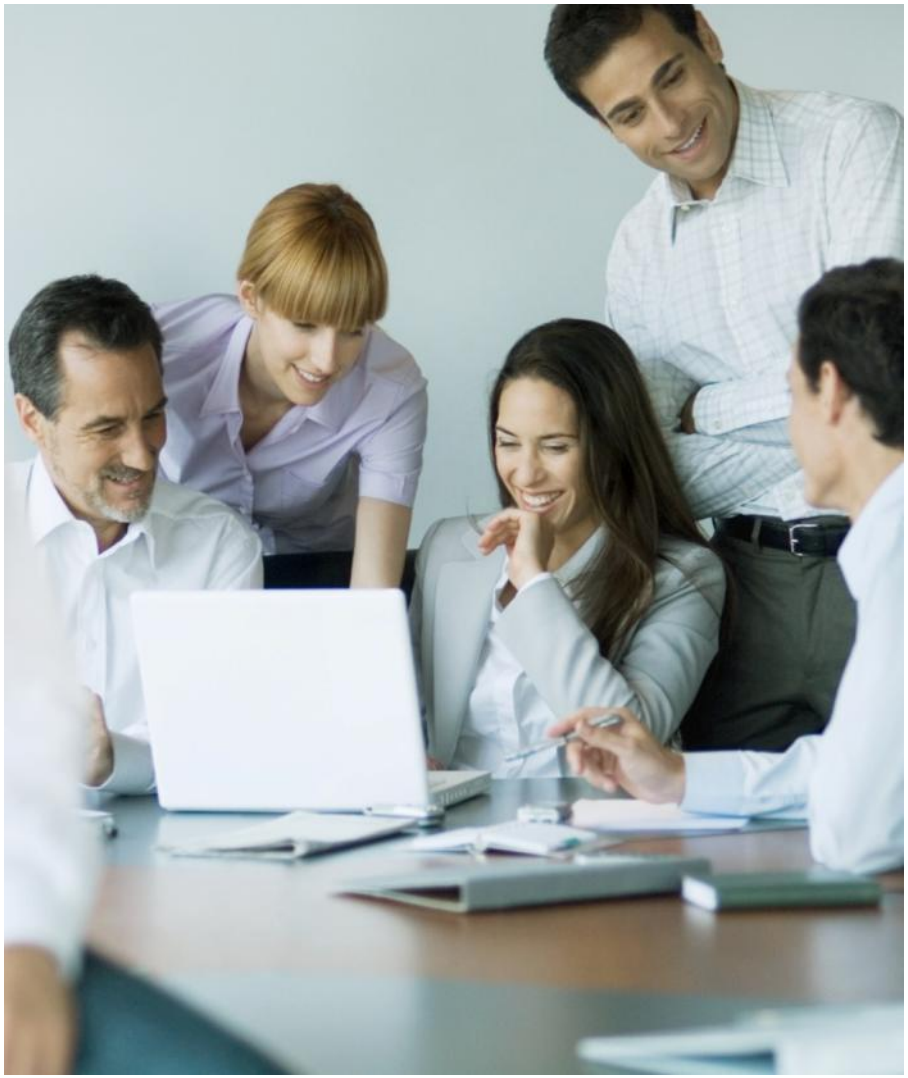
- GRC FAQs
- GRC Themes
- Sample Principles
- CalPERS Guiding Risk – Intelligent Principles
- GRC Guiding Principles Exercise

Section 2

GRC Guiding Principles FAQs

1. Why does a GRC program need guiding principles?

- Establishes ground rules
- Past approaches merely regarded as business processes
- To consistently apply principles of:
  - governance, integrity, discipline, transparency, accountability, independence, and communication



GRC Guiding Principles FAQs *(continued)*

2. How does an organization practically use these GRC guiding principles?

- Design GRC processes, structures and techniques
- Reflected in policies and implementation plans.
- The principles need to be tailor-made for every organization.

GRC Guiding Principles FAQs *(continued)*

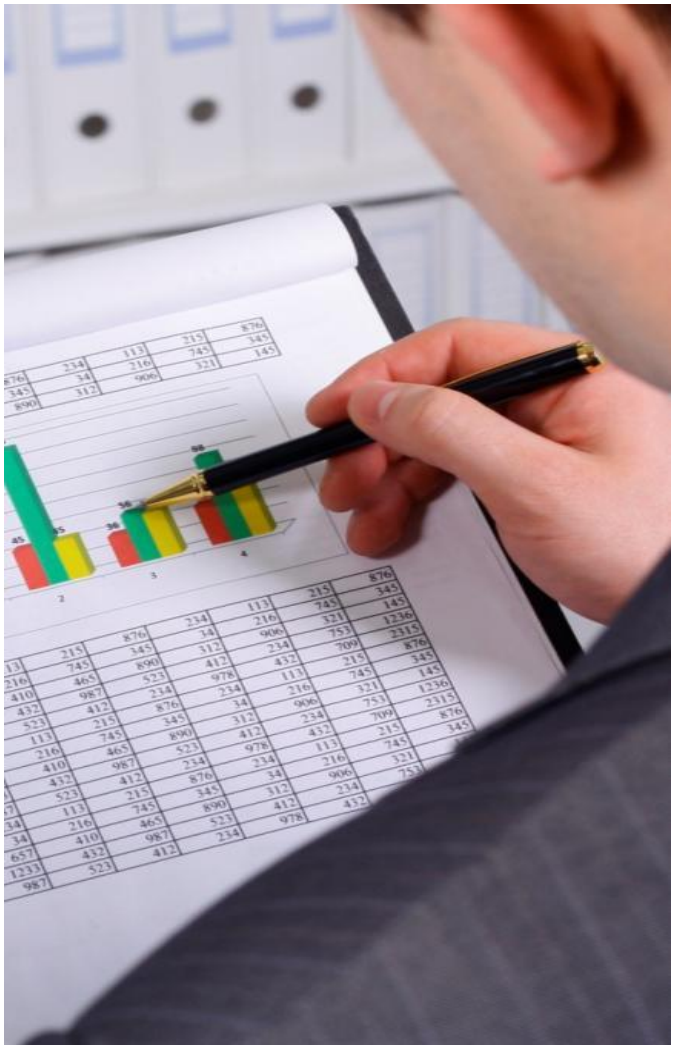
3. How are the GRC guiding principles entrenched?

- Change management
- Key decision processes
- GRC implementation

Guiding Principles Themes

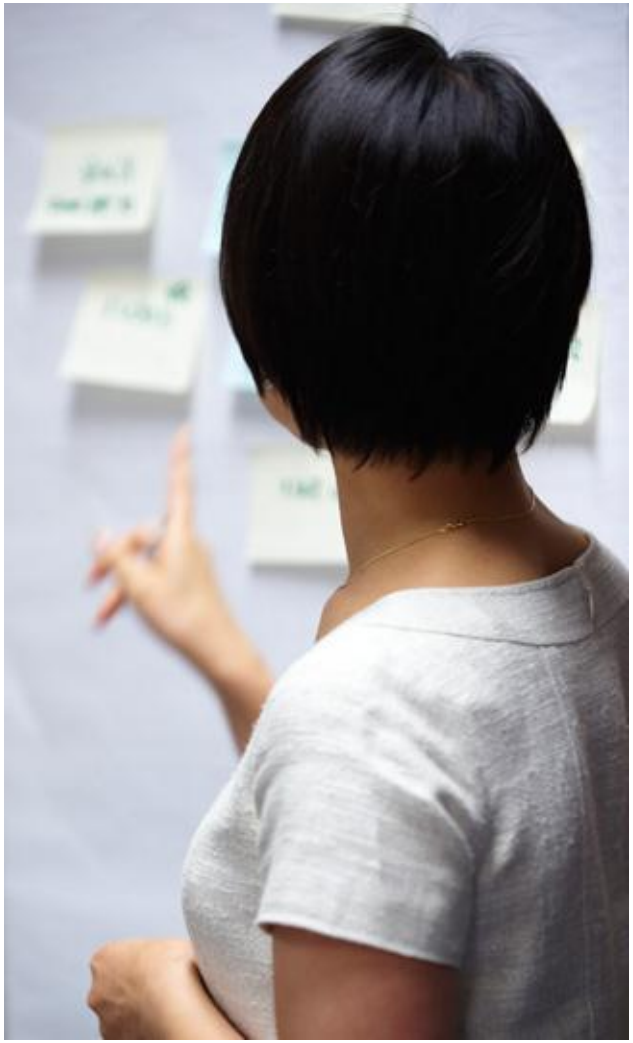
Guiding Principles – 1. Accountability

1. Board leadership
2. Executive leadership
3. Risk management and performance management
4. Compliance system is robust and effective



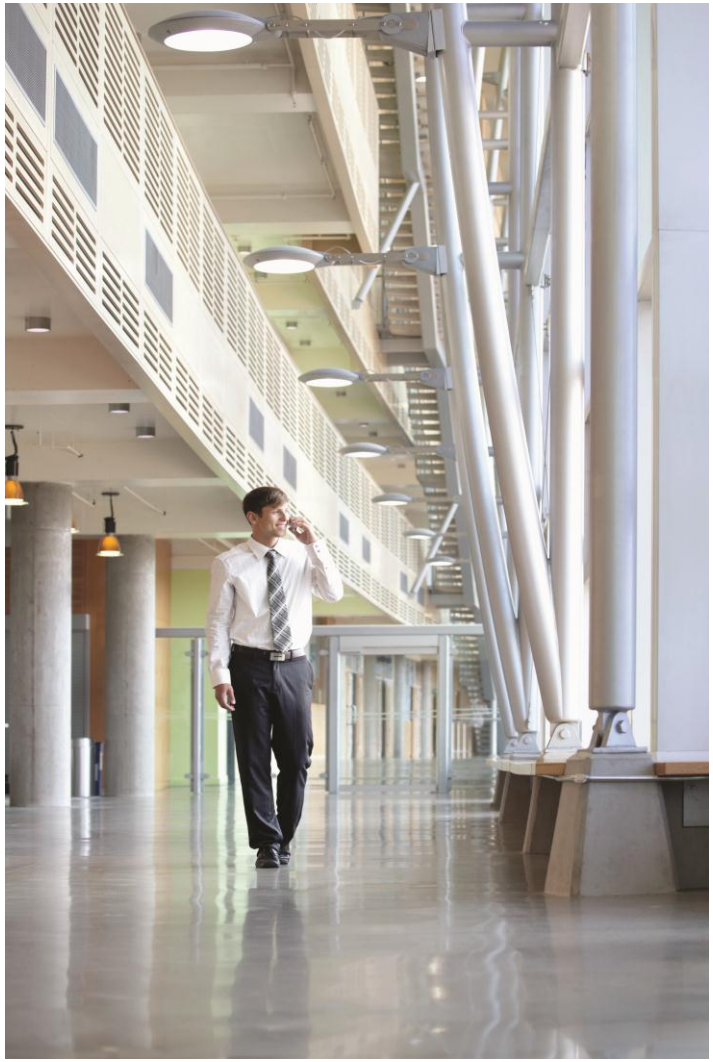
Guiding Principles – 2. Responsibility & Governance

1. Operating performance targets
2. Effective compliance framework and compliance controls
3. Formalized roles and responsibilities for GRC
4. Enterprise-wide consistency
5. Management emphasizes solutions to GRC challenges



Guiding Principles – 3. Discipline

1. Defined risk appetites
2. Applied to top mission-critical processes
3. Part of operating policies and procedures
4. Cost of non-conformance understood and managed
5. Issues are tracked



Guiding Principles – 4. Transparency

1. An enterprise-wide view of GRC
2. Risks are understood and made known
3. No surprises
4. Staff are properly trained
5. GRC Scorecard

Guiding Principles – 5. Independence

1. Key controls and corrective actions
2. The Audit Committee approves an internal audit plan
3. Financial reporting independently validated by external auditors
4. Challenge management assertions and assumptions
5. Established structure for internal assurance

Guiding Principles – 6. Integrity

1. Risk management reports are honest and transparent
2. Management committees are credible and effective
3. Enforcement of GRC policies is evident
4. Executive team provides ethical leadership
5. Ethics are enforced and monitored

Guiding Principles – 7. Communication

1. A common well documented vocabulary
2. An early-warning system
3. Transparent and timely disclosure of material matters
4. Reporting is relevant, understandable and consistent
5. Roles and responsibilities communicated effectively

Risk Intelligent Enterprise Management Policy *(adopted Q1 2011)*

The Board sets forth the following guiding risk-intelligent principles:

Value and risk governance

- Common definitions of “risk”
- Part of decision-making culture
- Common framework
- Key roles, responsibilities, and authority defined and delineated
- The Board has appropriate transparency and visibility

Risk infrastructure and management

- Executive management responsible for designing, implementing, and maintaining program
- A common risk management infrastructure

Risk Ownership

- Business units responsible for the risks they take
- All staff, managers, and the Board have an affirmative responsibility to exercise judgment regarding the awareness, identification, and management of risk

Exercise: Guiding Principles for CalPERS *(30 mins.)*

1) Each group to review and discuss two of the Guiding Principles themes
   - » *Table 1: Accountability & Discipline*
   - » *Table 2: Responsibility & Governance*
   - » *Table 3: Transparency & Independence*
   - » *Table 4: Integrity & Communication*
2) Review the CalPERS Guiding Principles and the Example GRC Guiding Principles
3) Discuss these questions:
   - » Which of CalPERS' Guiding Principles are the most meaningful for the group?
   - » Which of the sample GRC Guiding Principles should CalPERS consider adopting?
4) Share table results

Summary of Module 1

Section 3

Summary of Module 1

- **Risk Appetite and Tolerance**
- **ERM is a an organization-wide approach**
- **GRC is an approach to align the organization's governance, risk and compliance processes**
- **Guiding principles are the ground rules**.

Module 2:
GRC Roles, Responsibilities & Risk Ownership

Module 3:
Risk Appetite – Knowing the Boundaries

» Preview for Training Modules 2 & 3

Section 4

Module 2: GRC Roles, Responsibilities and Risk Ownership

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?"

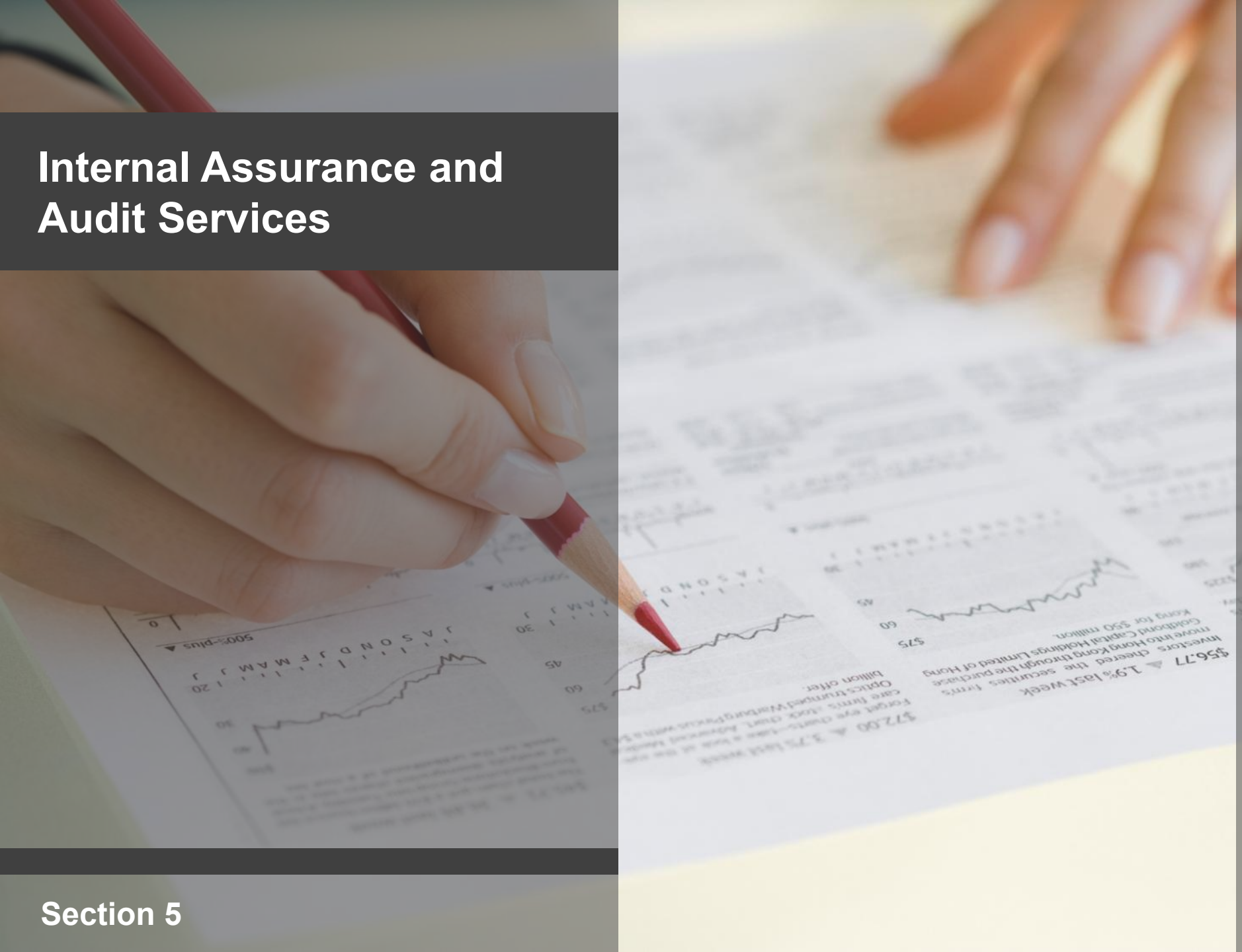
Module 3: Risk Appetite – Knowing the Boundaries

This Module will explore:

- The culture of risk appetite at CalPERS
- A sample of risk appetite statements
- Lessons learned and leading practices from other organizations
- Answer tactical questions:

"How can CalPERS GRC program support risk-based decision making?"

Internal Assurance and Audit Services



Section 5

How do Internal Assurance and Audit Services Relate to GRC?

- Critical Oversight Function
- Financial Integrity, Accountability, Disclosure, Independence, Internal Controls

Illustrative List of Audit Committee Responsibilities

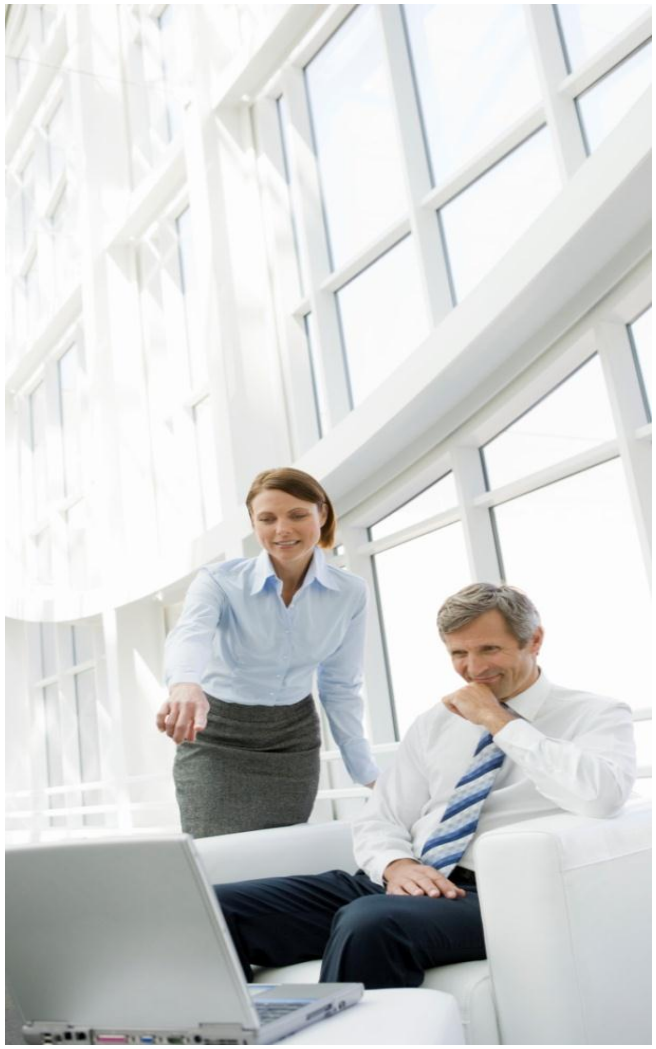
- Review plan and scope for financial statement audit
- Review financial statements, independent auditor's reports and communications
- Review critical accounting policies, practices, estimates, significant issues, significant transactions, unusual items
- Review Management Representation Letter to ensure informed about any sensitive issues
- Oversee adequacy of the system of internal controls
- Review Management Letter comments and management's responses. Ensure follow-up and implementation of recommendations.
- Approve External Auditor
- Oversee and provide forum for internal audits to report results of work

Main Areas Related to CalPERS Audit Functions

- **Internal Audits**
- Operates under the Board-Approved Office of Audit Services Charter
- Conducts activities in accordance with International *Standards for the Professional Practice of Internal Auditing* (Red Book)
- Internal Audits and Consulting
- Contracting Public Agency Payroll and Membership Reviews
- Liaison and Contract Manager for External Audits including Financial Statement Audit and Agreed-Upon Procedures engagements with external audit firms

Financial Statement Audit

- **Financial Statement Audit Timeline**
- Audited financial statements will be presented at the December 2012 Risk and Audit Committee Meeting
- Management Letter comments will be presented at the March 2013 Risk and Audit Committee Meeting

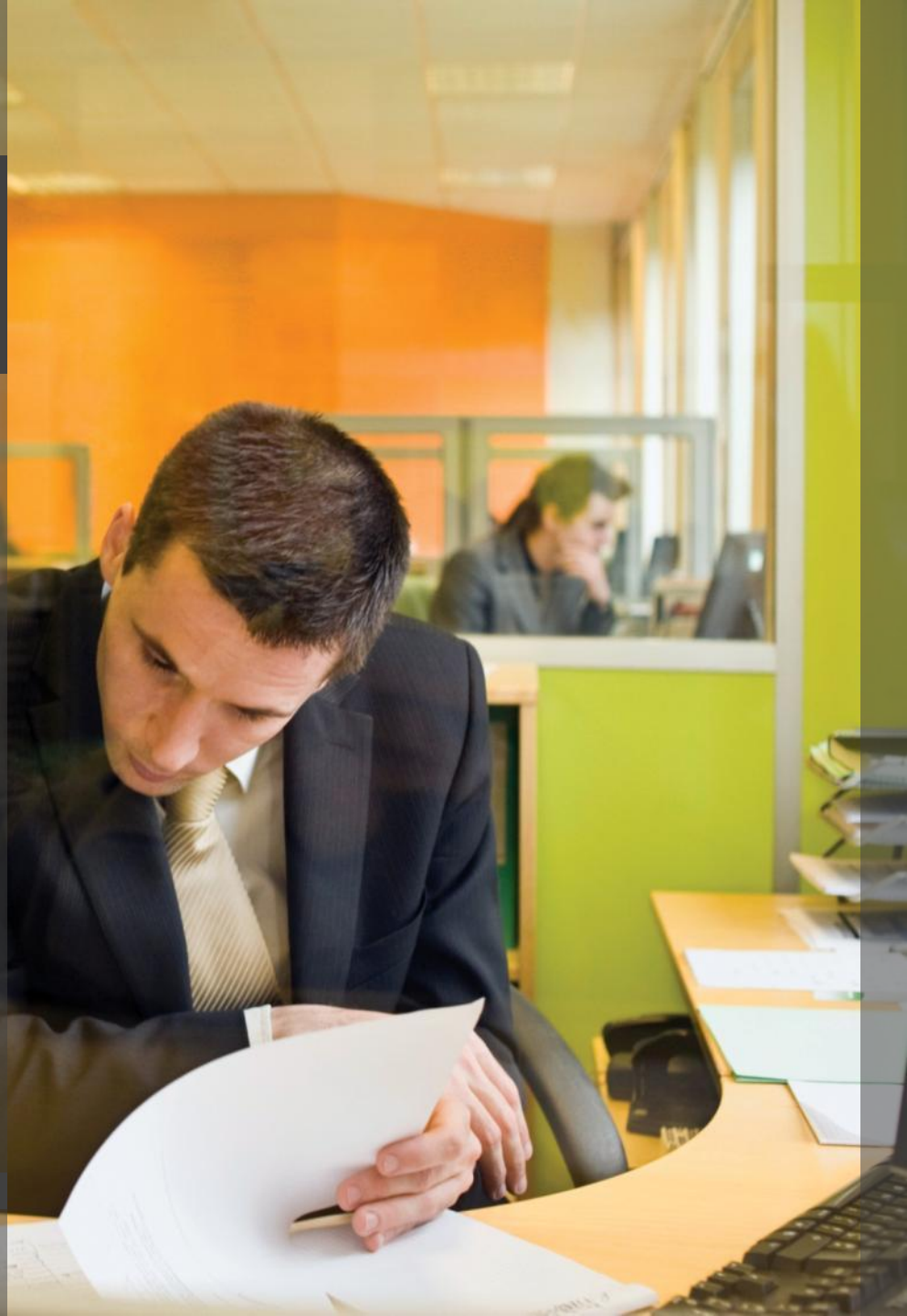


Management's Responsibility Related to Financial Statement Audit

Prepare financial statements in accordance with GAAP

Establish and maintain internal controls over financial reporting

Provide Management Representation Letter



Financial Statement Auditor's Responsibility

Plan and perform audit to obtain reasonable assurance that financial statements are fairly stated in all material respects

Review internal controls over financial reporting for the purpose of designing audit procedures

Does not provide assurance on internal controls

Financial Statement Auditor's Reporting

Auditor's Opinion

Explanatory Paragraphs

Required Communications With Those Charged with Governance

Management Letter Comments

Required Communications with Those Charged with Governance

- Qualitative aspects of accounting practices
- Difficulties encountered in performing the audit
- Corrected and Uncorrected Misstatements
- Disagreements with Management
- Management Representation Letter
- Management Consultations with Other Independent Accountants
- Other Audit Findings or Issues
- Other Information in Documents Containing Audited Financial Statements

Risk and Audit Committee Powers Reserved Related to Audits

- Approve, as required, and oversee actuarial, external, financial, internal and real estate audit and reassurance
- Select and approve the external auditor

Other Criteria Governing CalPERS Audit Activity

Government Code Section 13886

Government Code Section 20228

American Institute of Certified Public Accountants (AICPA) Toolkit

International Standards for the Professional Practice of Internal Auditing

Thank You