CalPERS Board Education Program

Risk and Compliance

Bob Yetman
University of California, Davis

CalPERS

UCDAVIS GRADUATE SCHOOL OF MANAGEMENT EXECUTIVE EDUCATION

Outline

- Setting the Stage
  - The Risk Management Process
  - Integrated Model: Three Lines of Defense
  - Board Oversight
- Enterprise Risk Management
  - Strategy and Risk
  - Risk Models
  - Assessment
- Compliance
  - Integrated Culture
  - Compliance Governance
  - Assessment

Setting the Stage: The Risk Management Process

Setting the Stage: Board Oversight of the Risk Management Process

- Boards are responsible for overseeing the processes and controls that reduce residual risk to acceptable levels
- Discussion: What is residual risk?
- Management is responsible for designing, implementing, and testing those systems
- Part of a Board's responsibility is to come to an understanding of whether Management's risk processes and controls are satisfactory and sufficient

Risk Management

- Risk can be thought of as the product of two dimensions:
  - The probability of a loss (likelihood)
  - The cost of a loss
- A loss can be thought of as reductions in assets or increases in liabilities
- Not all losses are financial
- Discussion: Discuss some important risks for CalPERS
  - What is the probability?
  - What is the potential cost (financial and non-financial)?

The Three Lines of Defense

1: Operational
- Day to day management and staff operations
- Everyone plays a role, everyone owns a piece of internal control, not just the auditors

2: Risk Management and Compliance
- Internal risk management structure and efforts (enterprise system)

3: Audit and Assurance
- Internal and external validation of risk management processes

Effective Risk Management Oversight with the Three Lines of Defense

Integrated Assurance Model: The Three Lines of Defense

Board and Management Partners in Risk Mitigation

- Board Governance Policy outlines Board responsibilities
- As well as powers delegated to various committees
- Management structure over risk management guides managerial actions and choices

Board Governance Policy

- The Board approves the risk preferences and tolerances of the fund to prepare the enterprise for high impact risks and to achieve long-term sustainability.
- An effective enterprise risk management framework is used to consistently monitor and report aggregated risk exposures and the effectiveness of mitigation and control. The organization is willing to innovate and take calculated risks considering the long-term best interests of the beneficiaries and participants.

Powers Delegated to Risk and Audit

- Approve and oversee the enterprise risk management framework to effectively manage risks.
- Approve risk appetite and strategy (excluding investment risk).
- Oversee processes for investment risk management, investment policy compliance monitoring, and operating risk management (including audit findings resolutions).
- Oversee enterprise program and policy compliance.
- Oversee service provider compliance (including harmonizing conflict of interest policies).

Management Risk Structure

- Enterprise Risk Management Division
  - Forrest Grimes, Chief Risk Officer
  - The Enterprise Risk Management Division is responsible for creating and maintaining a risk-intelligent culture at CalPERS.
- Enterprise Compliance Division
  - Marlene Timberlake D'Adamo, Chief Compliance Officer
  - Kami Niebank, Deputy Chief Compliance Officer
  - The mission of the Office of Enterprise Compliance is to ensure, promote, and support an organizational culture that builds compliance awareness into the daily business processes

Enterprise Risk Management

- Second Line of Defense
- Provides an independent view of the organization's risk profile
- ERM systems are becoming more common in large complex organizations
  - Otherwise risk identification and mitigation migrates up from the line
  - Resulting in duplication and omission

Strategic Risk

- External to the organization
- If the risk comes to pass, it can change the strategic direction of the organization
- What are some examples of CalPERS strategic risks?
- Changes in pension laws
- Changes in IRS rules regarding retirement or health benefits

Operational Risk

- External or Internal to the Organization
- Impact an organization's ability to achieve the current strategy
- External Operational Risk
  - Stuff happens…
- What are some examples of CalPERS external operational risks?
  - Investment Returns
  - Retiree longevity
  - Inflation rate

Operational Risk

- Internal Operational Risk
  - Preventable and Controllable
- What are some examples of CalPERS internal operational risks?
  - Noncompliance with existing rules
  - Leakage of member data

Risk Mitigation

- Strategic Risk
  - Reduce likelihood (envision possible events, then attempt to reduce/eliminate them)
  - Reduce impact if they occur (be ready for it)
- External Operational Risk
  - Out of your hands, but can anticipate and try to reduce cost of event
- Internal Operational Risk
  - Most control…goal is to eliminate
- Cost – Benefit: Always consider the cost!

ERM Risk Culture

- Whose job is risk identification and mitigation?
  - The Board?
  - ERMD?
  - Office of Enterprise Compliance?
  - Anyone Else?
- Everyone Else!
  - Risk identification and mitigation needs to be owned by every employee in CalPERS
  - Those closest to the issue are in the best position to identify risks and suggest possible mitigation strategies

Concept of Risk Ownership

- Who is responsible for Accounting?
- Who is responsible for Benefits?
- Who is responsible for Investments?
- Who is responsible for risk ID and Mitigation?
- Developing a culture of risk awareness is, in my opinion, the primary goal of both the ERM and Compliance Divisions
  - Strive to embed risk culture within the very fabric of CalPERS

ERM Reporting

- Risk identification and mitigation must be a transparent process
- Frequent reporting by management to Board about ERM activities
  - Board has obligation to be informed
- Board should be forward thinking
  - What new risks are on the horizon?
- “Dashboards” are commonly used communication tools
  - Allows cross-sectional and intertemporal comparisons

CalPERS Enterprise Risk Management Dashboard

	Risk Category	Risk Domain	Risk Ranking						Owner	Oversight
			Oct-13	May-14	Oct-14	May-15	Previous Trend	Projected Trend		
3	Strategic	Pension Funding (Asset Liability Management)	■	■	■	■	→	→	Chief Investment Officer Chief Actuary Chief Financial Officer	Investment Committee Finance and Administration Committee
4	Strategic	Asset Allocation	*	▲	▲	▲	→	↑	Chief Investment Officer Chief Operating Investment Officer	Investment Committee
5	Strategic	Participating Employer Financial Hardship/Insolvency	⬢	■	■	■	→	↓	Chief Financial Officer	Finance and Administration Committee
14	Operational	Business Continuity Management	▲	▲	▲	▲	↓	→	Chief Financial Officer	Risk and Audit Committee
17	Operational	Information Security	▲	▲	▲	▲	→	→	DEO, Operations & Technology	Finance and Administration Committee
6	Strategic	Human Resources Management	▲	▲	▲	▲	→	↑	DEO, Operations & Technology	Performance, Compensation & Talent Management Committee

* Not identified as a risk domain during this reporting period

Residual Risk - Considering risk responses and the remaining risk exposure.	
●	Minimal
▲	Moderate
■	Elevated
⬢	High

Trend - Considering risk management plans and environmental factors, the residual risk trend over the next 6 months.	
↓	Decrease
→	Remain Constant
↑	Increase

Refined Dashboard Coming!

- Expect to see a refined Dashboard in the June Risk and Audit Committee meeting!

Risk Appetite and Tolerance

- What is Risk Appetite?
- What is Risk Tolerance?
- Who establishes Risk Tolerance?
- How is Risk Tolerance set?
- What effects will the Tolerance have?
- Need there be a formal statement of Risk Tolerance?

Risk Appetite and Tolerance

- Appetite
  - General level of risk considered acceptable for a given risk category.
  - Guiding principles that are woven into strategic plans and operational processes.
- Tolerance
  - Tangible and identifiable limits that create boundaries that fence in operations.
  - Measurable, achievable, and monitorable

Setting Risk Appetite

- How is that Appetite set?
- Boards (people?) have trouble talking about acceptable risk…
  - Risk is bad, so why accept it?
    - Because it's far too expensive to mitigate all of it
- Think of automobiles, could we make them safer?
  - Of course, but that costs money, and not everyone can afford that

Setting Risk Appetite

- Results from an informed discussion between management and the Board
- Don’t rush into this
  - Be deliberative
- Produce a meaningful statement on risk appetite
  - Meaningful in that it guides risk tolerances
  - Meaningful in that it is actionable

Setting Risk Tolerance

- How is that Tolerance set?
- Boards (people?) have trouble talking about acceptable risk…
  - Risk is bad, so why accept it?
    - Because its far to expensive to mitigate all of it
- Think of automobiles, could we make them safer?
  - Of course, but that costs money, and not everyone can afford that

Setting Risk Tolerance

- Start simple..
- First identify the risk Category
  - Pension Funding, as an example…
- Then identify their associated rewards
  - Sustainability of the plans' affordability and attractiveness with the goal of low volatility in contributions and appropriate funding levels through the management of assets and liabilities
- Next try to classify how much uncertainty you are willing to live with given the associated rewards
  - What is the appropriate balance between affordability and volatility of the investment portfolio
- Start off with High, Medium, and Low Tolerance

Setting Risk Tolerance

- Produce statement of meaningful and clear tolerances
  - We are willing to accept investment volatility to increase affordability providing funding levels remain within certain limits
  - Otherwise the funds' sustainability becomes overly uncertain
- Tolerances most often have upper and lower bounds!
- Tolerances can help inform strategic choices
- Yes, I know its hard to write these things down in highly visible organizations
  - But how would you make choices that involve tradeoffs?

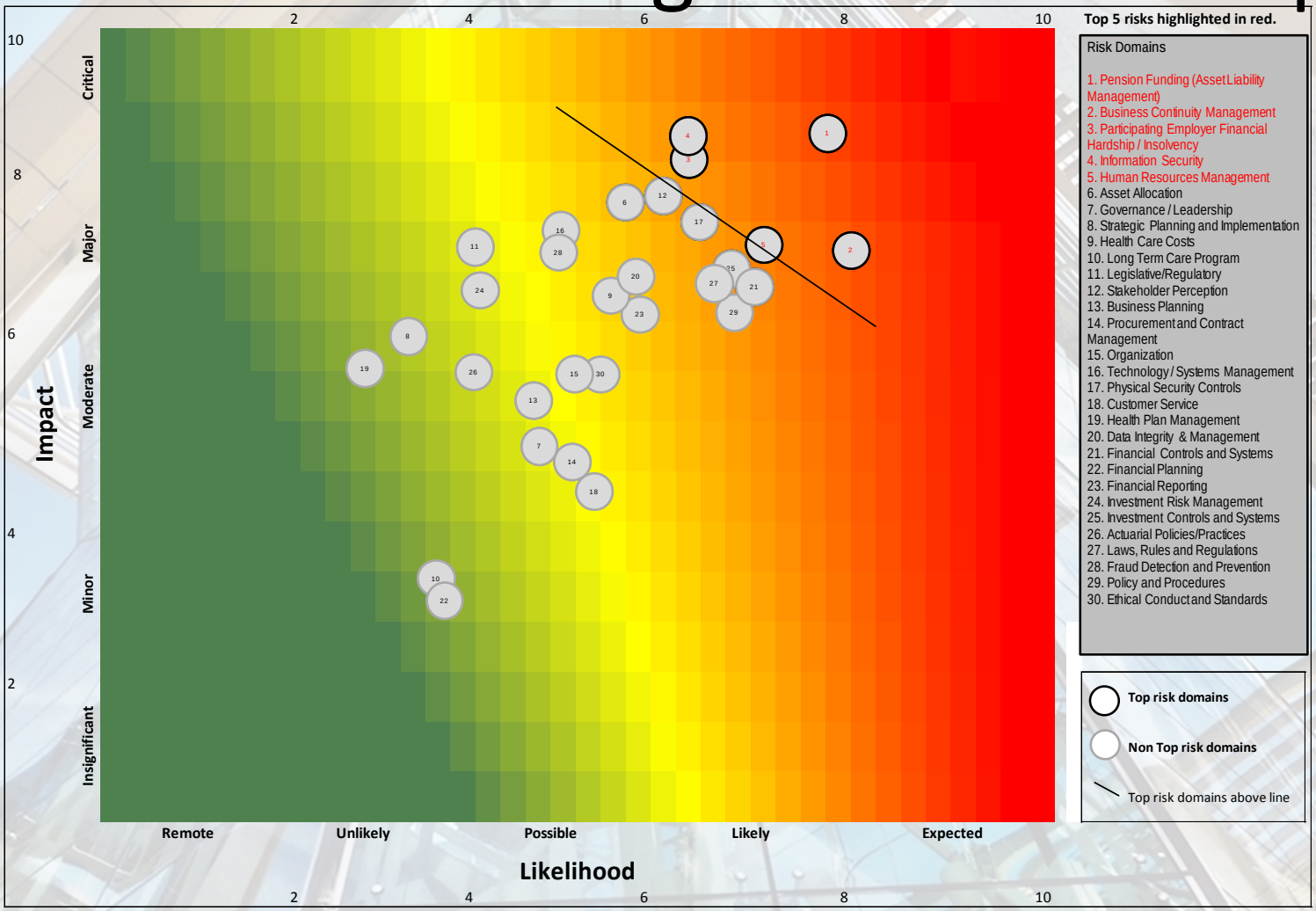
ERM Best Practices

- Establish Policies
- Formalize Risk Tolerance (Appetite) Statement
- Organize Embed Risk Management (First Line Defenses)
- Monitor
- Report upwards
- Communicate across and downwards
- Link ERM and Strategy (current and future)

Current CalPERS Practice
Some Thoughts…

- Lets take a look at current risk categories
- Then discuss how we might be able to apply some of the lessons we have learned

CalPERS Risk Management Heat Map



How Many Risk Categories?

- Tendency of early-stage ERM systems is to consider too many risk categories…
- Result of trying to be careful and not leave anything out
  - Remember how you treated your first child?
    - You would not let anyone hold them
  - The second kid you pass off to anyone you can
- You can always come up with … one … more …risk … and on … and on …

How Many Risk Categories?

- Currently CalPERS considers 30 risk categories
- My professional suggestion would be to reconsider these 30 categories
  - Is there some duplication or overlap?
  - Are they too granular?
  - Are their mitigation strategies coincident?
- Sometimes less is more
  - More focus on higher value risks
- Can Forrest see the Forest for the Trees?

Program vs. Enterprise Risk Category Identification

- One method to identify risk categories is based on programs
  - Example: Investment Risk
- Another method is to have risk categories flow out of a more comprehensive and top down enterprise perspective that cross programmatic silos
  - Example: Human Resources Management

Is There Something Missing?

- Risk categories placed on heat map according to impact and likelihood
- Great first start, but what is missing?
- Risk tolerances around each category should be considered
  - Possible that some high (red) risks have very high tolerances, while some low (green) risks have very low tolerances
- Considering risk tolerances might cause some rearrangement
  - More on that later…

Some Thoughts…

- Consider using an enterprise method for identifying larger risk categories
  - Consider impact of those risks across the entire organization, across silos
- Consider including risk tolerances as a factor when classifying the "heat" of a risk category
- Consider creating fewer risk categories
  - Might focus risk mitigation and reporting

Board Questions for ERM (push the button and ask these)

- Does the right committee have oversight of ERM?
- What are that committee's responsibilities with respect to ERM?
- Does that committee have the necessary skill to oversee ERM?
- What value can that committee bring to ERM?
- How can ERM enhance the relationship between the entire Board and Management?

Compliance

- What is Compliance?
  - Officer on the highway…hope to not get caught?
- A system of controls intended to provide a cost-beneficial level of assurance that the organization complies with all applicable:
  - Laws
  - Regulations
  - Policies
  - Best Practices

But Wait…There's More!

- Can promote a culture with a fair, safe and professional work environment
- Can aid in proactively mitigating compliance risks
- Can enable an organization to build and maintain a positive reputation
- Can help an organization identify what it should not be doing

Where Does Compliance Fit In?

Integrated Assurance Model: The Three Lines of Defense

Changing World…Changing Risks…

- As the world evolves new risks arise, old risks fall away, and existing risks morph.
- A risk compliance system likewise needs to adjust and grow to reflect this unstable reality.
- This makes it particularly difficult to know if you have a sufficient compliance function.
  - You can't simply ask "have we complied" as that is driving through the rear view mirror. The real test is "what level of assurance do we have that we will be compliant in the future?"
- However, as with all things, a cost benefit analysis is imperative. Identify primary strategic objectives, don't lose sight of the Forest for the Trees.

Compliance Ownership

- Goal is not to have a stand-alone compliance program
- Goal is to establish a culture of compliance within and across the organization
  - This starts with the Tone at the Top; the Board, CEO and CFO
- If any employee sees compliance as someone else's job, that would be a failure
- Every employee should identify themselves as a compliance officer!
  - Everyone needs to own their piece of the compliance mosaic
  - And that concept needs to be baked into the organizational DNA

The Compliance Mosaic

- Any complex organization consists of:
  - Employees at various levels of authority
  - Employees within various functional “silos”
- Who is in the best position to identify and mitigate compliance risks?
  - Employees directly involved with the risky task!
- A Compliance Office is not in charge of mitigating every compliance risk
  - Each employee and Board member is in charge of their risk leverage points
  - This establishes Compliance as a cultural value
- A Compliance Office is the central contact point, and oversees Compliance efforts, but is (often) not the source of compliance at the risk leverage points

Compliance in a Post Dodd-Frank World

- Dodd-Frank imposed a variety of new controls over financial transactions
  - i.e., Centrally cleared swaps
- Dodd Frank did not add much in the form of Compliance programs.
  - SOX 2002 contained many compliance requirements. FCPA 1977 did as well.
  - Publicly traded companies must meet exchange listing requirements, which often require compliance programs and reporting.
- Dodd-Frank did create strong incentives for employees to report to the SEC violations of any federal securities laws, including SOX and the FCPA.
- This puts a premium on having a broad, *truly effective* compliance program and a *real* culture of compliance.

What Does a Culture of Compliance Look Like?

- It looks like a culture of dignity and respect for fellow workers … Omnipresent yet Translucent
  - Almost as if you can't see it there, like it belongs there
- 3 C's
- Communication
  - Issues of compliance are discussed upwards and downwards, formal and official channels exist
- Confirmation
  - Compliance is assessed regularly and in a transparent manner
- Correction
  - Lapses in compliance (and there will be lapses) are corrected or mitigated in a cost-effective manner
  - Correction feeds back to Confirmation

Compliance Roadmap | Five-Year Outlook

The organization changes needed to mature compliance capabilities within CalPERS are expected be phased in during a three to five years period.

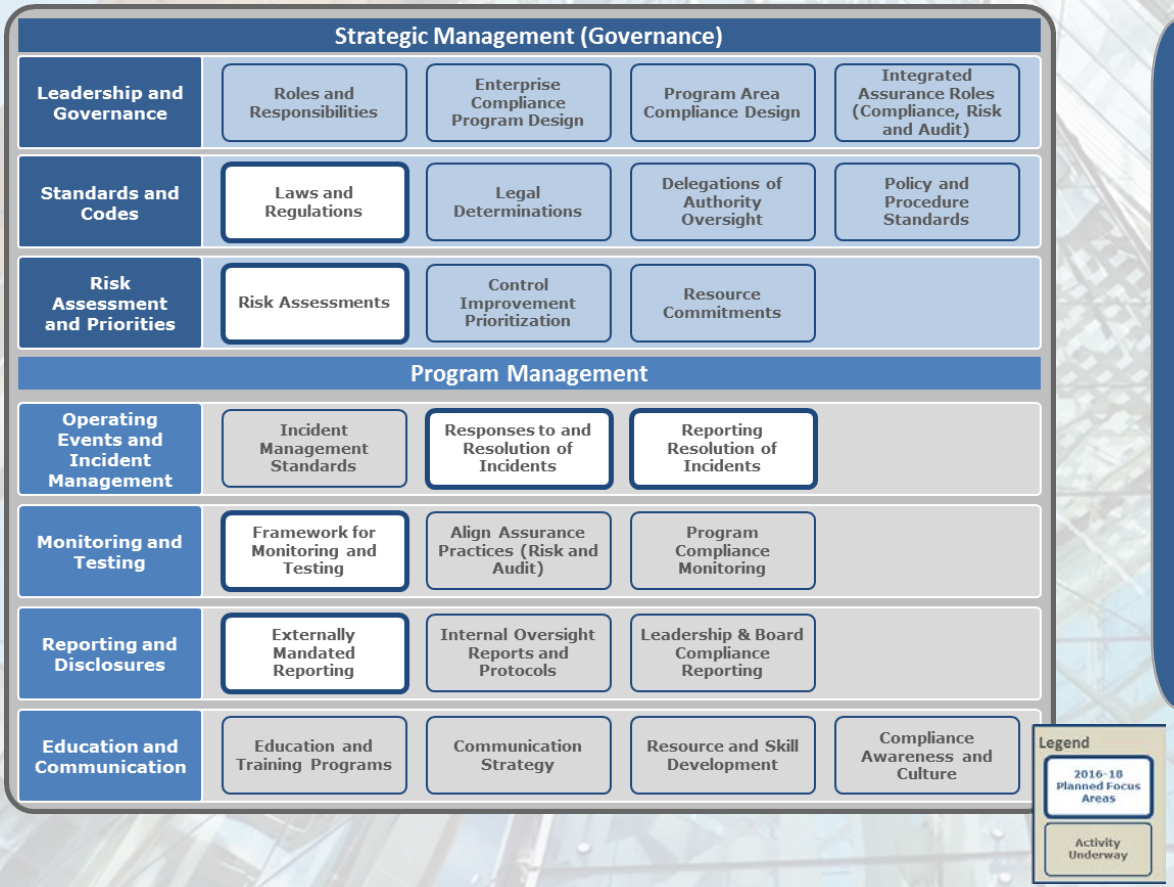
CalPERS Compliance

- There is no regulatory guidance as to what a compliance function looks like, or even to have a compliance function.
  - The only requirement is that you comply. How you get there, no one says!
- Compliance in CalPERS is transitioning towards a fully integrated compliance assurance program.
  - Unlike many initiatives in CalPERS, compliance is an organization-wide effort.
    - Top down and bottom up.

Compliance Mosaic| Focus Areas

Move from inconsistent & foundational frameworks to more focused compliance oversight & monitoring activities

Elements of Compliance Program



Demonstrate Compliance Effectiveness

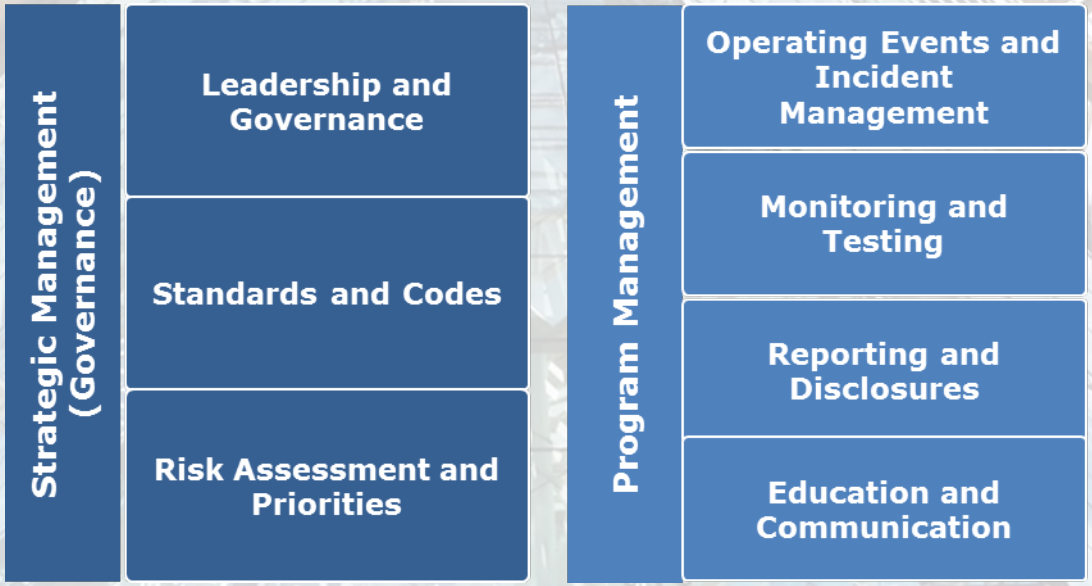
Continue to expand focus areas started in 2015-16

- Roles and Responsibilities
- Policy & Delegation Management
- Embedded Compliance Implementation
- Education and Awareness

Focus Areas for 2016-18

- Laws and Regulations
- Risk Assessment and Priorities
- Resolution and Reporting of Incidents
- Monitoring and Testing (Targeted Reviews)
- External Reporting

Compliance Elements – Alternate View



Specific Example of Best Practice

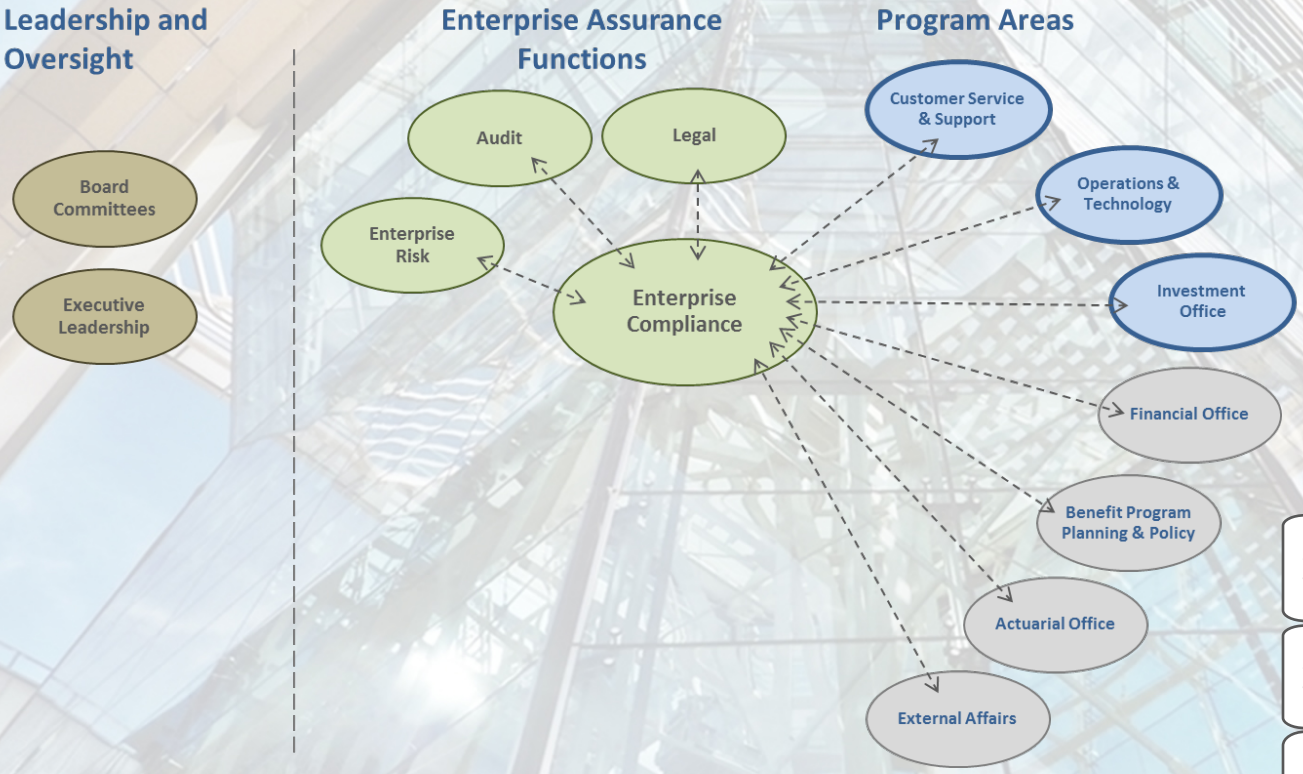
- Best practice is for Compliance to spread across the three lines of defense
  - And have a central compliance function to facilitate enterprise wide compliance efforts
- Consider INVO (Investment Office)
  - Strategically important
  - Complex operations
  - Potential for Compliance issues
- Who is in the best position to identify compliance risks and possible mitigation strategies?
  - INVO or ECOM?

Embedding Compliance

- INVO is in the best position to know its compliance requirements and risks
  - And thus is also probably in the best position to devise mitigation strategies
- But ECOM is a Division, way up in the sky…
- Answer is to embed within INVO a compliance unit
  - Voila: ICOR – Investment Compliance Operational and Risk
- ICOR reports to INVO who reports to CEO

Embedded Compliance | Roles & Responsibilities

Expand upon the partnerships and continue to strengthen compliance roles & responsibilities expected in the integrated assurance model.



Strengthen Foundations

2016-17 Focus Areas

- Strengthen the compliance dialogue with leadership
- Strengthen relationship and capabilities with enterprise assurance functions
- Centralize compliance functions in three (3) programs with major operational complexity

ICOR

- ICOR is the first line of defense
  - With ECOM as its direct second line
  - With Audits as its direct third line
- ICOR is not an appendage to INVO, it is embedded within the fabric of INVO
- Example: Investment Beliefs
  - ICOR helps to manage compliance risk monitoring activities for investment policies, laws and regulations across asset classes
  - ICOR works with INVO Senior Staff to design and implement the operational processes and internal controls to ensure accountability of business objectives, compliance, and risk management
  - Supports the Investment Committee in its oversight capacity with regard to compliance with investment policies

Board Role Over Compliance

- Power delegated to Investment Committee
  - Approve investment policies and oversee compliance with investment policies
- Powers delegated to Risk and Audit Committee
  - Oversee processes for investment risk management, investment policy compliance monitoring, and operating risk management
  - Oversee enterprise program and policy compliance
  - Oversee privacy and security compliance
  - Oversee service provider compliance (including harmonizing conflict of interest policies)
- Power delegated to Board Governance Committee
  - Oversee the process of and compliance with the requirement for board member, Chief Executive Officer, and Chief Investment Officer disclosure statements

But Compliance is Also Personal

- Board is responsible for compliance within the Board
  - Per the Board's Governance Policy
- Are Board members filing required disclosures?
  - Personal Trading, Form 700
- Are Board members following rules related to gifts?

Management Role Over Compliance

- State Leadership Accountable Act (SLAA) (FKA FISMA)
- Starting June 24, 2015 a new focus on assurance that all levels of management are involved in evaluating, strengthening, and monitoring internal controls.
  - Maintain effective systems of internal control; Evaluate and monitor the effectiveness of these controls on an ongoing basis;
  - Biannually report on the adequacy of the agency's systems of internal control.

Compliance Reporting

- Vendors to Programs
  - Vendors should be required to identify compliance issues
    - Staff should act as second check on completeness, but make vendor do the first run through
- Programs to Compliance
  - ECOM should be the central point of contact regarding compliance activities at the program level
- Compliance to Management
  - ECOM should report regularly to senior management
    - Status report, progress report
- Management to Board
  - Board should be given updates of compliance to fulfill their governance responsibilities

Thought Exercise: Ask Yourselves These Questions

- Is responsibility for compliance and ethics universally understood throughout all levels of the organization – from the most junior employees to senior management and the Board – to be an important component of job and company success?

- Is this reflected in performance evaluations?

Thought Exercise #2

- What evidence does the Board have that senior management actively promotes a values-based approach to ethics and compliance that is appropriately synchronized with the corporate culture?
- Is the right tone being set at the top in what behaviors are rewarded and punished?
- Is executive management talking to employees enough about the importance of compliance and internal reporting?

Thought Exercise #3

- Has the organization focused on the key risks in its business and taken adequate steps to ensure compliance with the law?
- The organization should identify its own critical vulnerabilities and ensure that adequate compliance mechanisms are in place
- An Enterprise Risk Management System informs a well functioning Compliance activity
  - Forrest, meet Marlene…Marlene, say hi to Forrest…
- But in all cases … remember …
  - Keep the cost-benefit concept firmly in mind

Thank You

- Robert J. Yetman
- rjyetman@ucdavis.edu