

## Risk Diverse Environments: Prioritizing the Priorities

Presented by:  
Sheryl Vacca, CCEP, CHC-F, CHRC  
SVP/Chief Compliance and Audit Officer  
University of California  
sheryl.vacca@ucop.edu

1

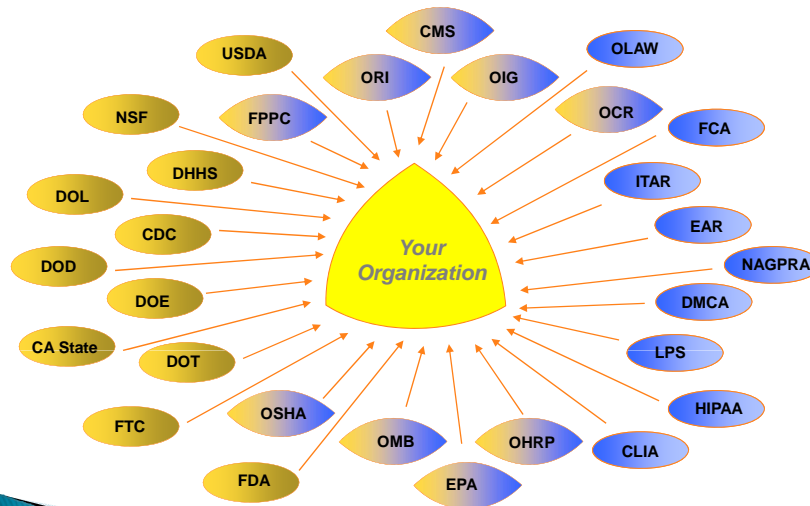
## Risk Diverse Environments: Prioritizing the Priorities

- ▶ Diverse risks, multiple priorities: How to address these through a scalable approach
- ▶ Prioritizing the diverse risks of your organization
- ▶ Addressing diverse risk priorities in a compliance auditing and monitoring plan

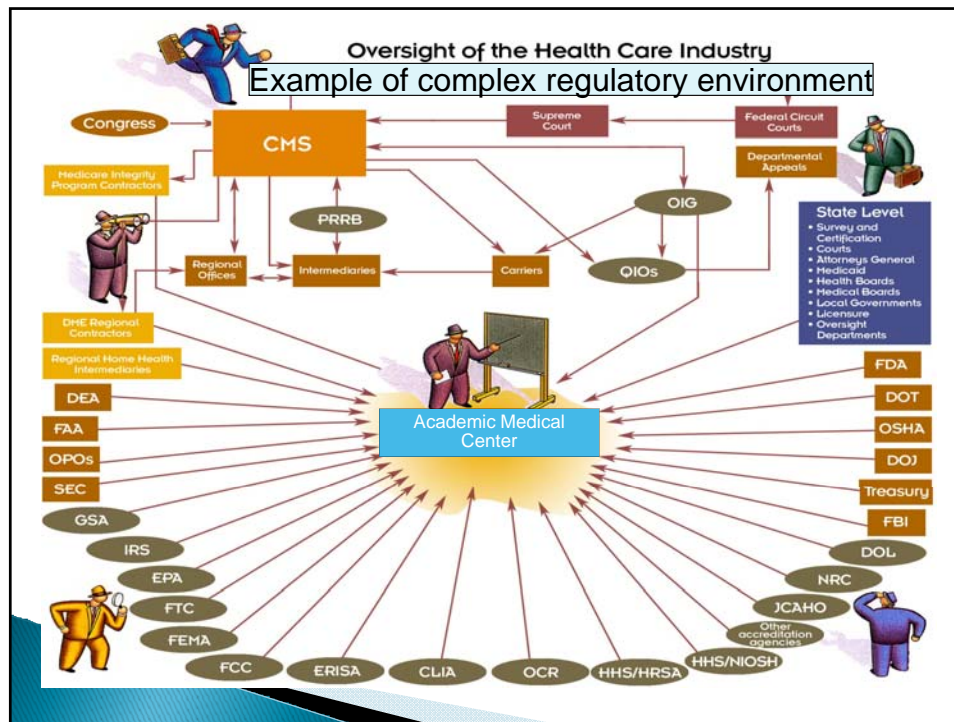
## Environment – Identification of Risks

- ▶ What is the universe?
  - External indicators
    - Regulatory
    - Enforcement activity
    - Public viewpoint
    - Market area activity
  - Internal indicators
    - Culture
    - Enforcement activity
    - Previous audits/monitoring
    - Risk assessments

## Agencies/Regulations Impacting University Compliance\*

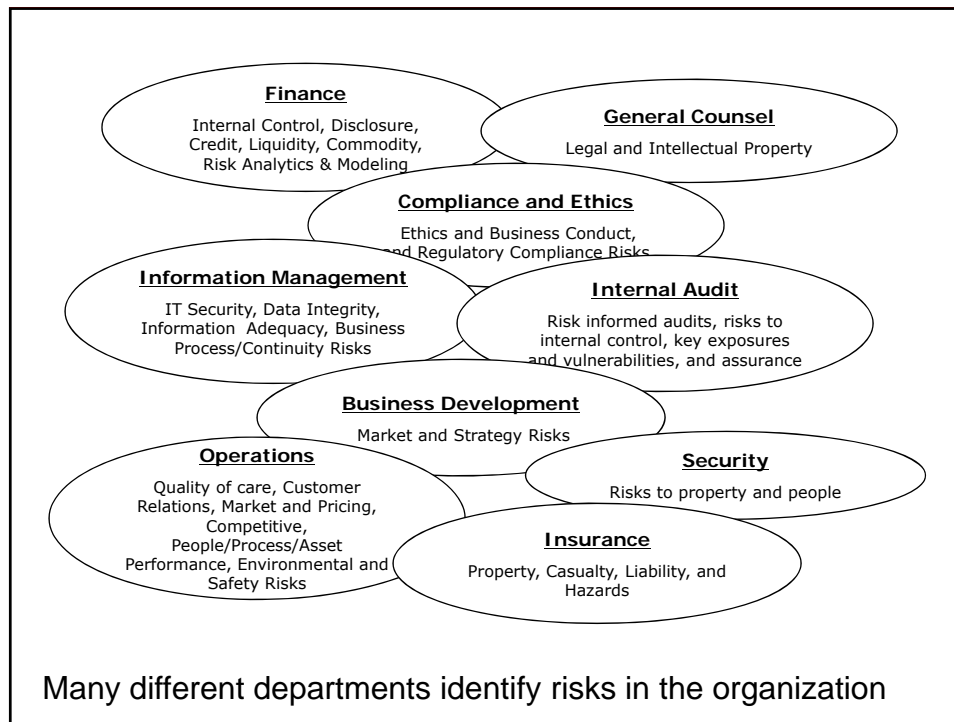


\*Including but not limited to those listed



## Develop Understanding of Environment

- Culture
- Understanding of organization's risk efforts
- Resource/dollar constraints
- Best practices/good works
- Competing initiatives across the organization
- Who else is looking at risks in the organization?



## Collaborate with Key Departments

Gather information about the risks

- Review of documents
  - About business operations
  - Enterprise risk assessments
  - Legal and regulatory docket
  - Compliance case log
  - Industry legal and regulatory trends
  - Employee ethics attitude surveys
- Surveys: validate whether the initial list is correct.
  - Ask for risk priorities and determine which parts of the business face specific risks.
- Interviews of people throughout the organization
  - Provides opportunity to probe and spark insights

## Categorize the Risks

- Code of Conduct risk categories, i.e.: research misconduct, unfair treatment, etc.
- Policies and procedures, i.e.: lack of, aged and not reflecting practice
- Regulatory agency guidance
- Interviews and surveys
- Public perception
- Industry risks and related standards, i.e.: research/time and effort

## Research Areas of Risk – example



## Research Compliance: In the News – example

### **Grants Administration--False Claims Act (FCA) Settlements**

- Yale, Dec 2008—**7.6M**; cost transfers, effort reporting
- St. Louis Univ, July 2008—**1M**; supplemental compensation, effort reporting
- Institute for Cancer Prevention, Jan 2007—**3.2M**; cost allowability, cost allocation

### **Focus on Enforcement**

- NSF Implementation of Program Fraud Civil Remedies Act
- Expansion of FCA under Federal Enforcement and Recovery Act (FERA)
- \$\$ allocated to IG ARRA activities
- NIH activity

### **Conflict of Interest**

- Senator Grassley Inquiries

### **Export Control Violations**

- University of Tennessee professor found guilty of export control violations (Sept 2008; deemed export of “defense articles” to Chinese foreign national)
- FBI investigations

### **IRB**

- GAO Sting Operation

## Research Areas of Potential Risk – example of industry pertinent risk for your organization

- Conflict of Interest Disclosure and Management – Compliance with state, federal, and sponsor rules
- Award terms -- Compliance with UC policies (publication; IP/data rights; nondiscrimination)
- C&G - OMB Circular A-110, A-21 Compliance
- NAGPRA
- ARRA Reporting Requirements
- Research Misconduct
- Stem cell oversight
- Human and animal research protection
- Export control
- Effort Reporting

### How to Quantify Risk (example) – Prioritization

- Likelihood of Occurrence\*
    - 1 = improbable
    - 2 = Remote
    - 3 = Occasional
    - 4 = Frequently
    - 5 = All the time
  - Impact of Occurrence
    - 1 = Minimal/Negligible
    - 2 = Slight
    - 3 = Moderate
    - 4 = Critical/Serious
    - 5 = Catastrophic
- \*vulnerability is replacing likelihood

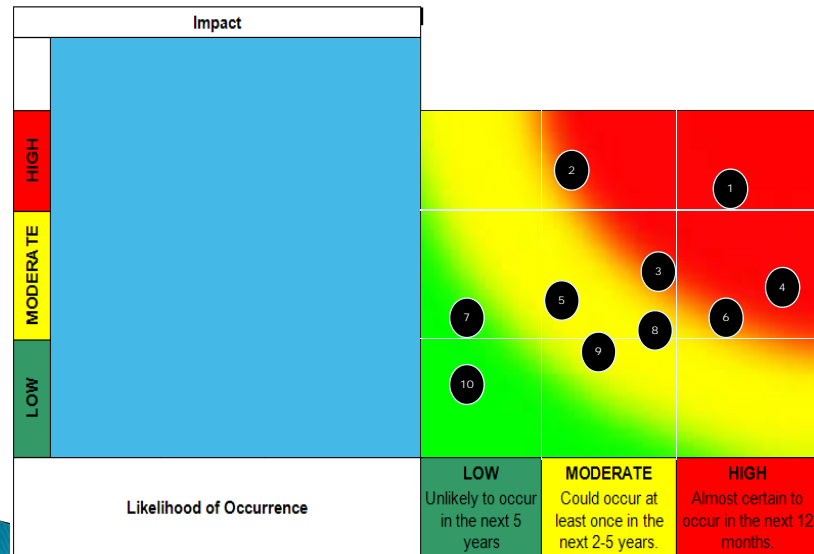
13

### Rank the risks – Prioritization– example

	Reputation	Legal/Regulatory	Financial
High	Systemic loss of public/client confidence resulting in loss of customers; major media coverage – headline news for several days	Major infraction resulting in criminal or civil prosecution and/or significant discipline; loss of ability to operate in one or more countries	Significant financial impact with widespread liability
Moderate	Loss of confidence among large number of customers and a segment of the general public; major media coverage for 1-2 days	Infraction resulting in civil prosecution and/or discipline; loss of ability to operate within local jurisdiction	Considerable financial impact with regional liability
Low	Loss of confidence among a limited number of customers in local market/country; limited local media coverage	Minor infraction that is readily remediated; no loss of ability to operate	Minimal financial impact with localized liability

14

## Prioritize the Risks - Heat Map



15

## Develop Compliance Risk Based Audit and Monitoring Plan

After Prioritization, consider...

- ▶ Risk areas that can be addressed through another department's audit and monitoring
- ▶ What resources are available to address remaining risks?
- ▶ Map out the priority risks by resource availability, i.e.: other departments, your available resources
- ▶ Reprioritize for scalability, where necessary
- ▶ Plan document is dynamic, risks should be re-evaluated

## Summary of Effective Process

- ▶ Identification of risk universe
- ▶ Risk Universe is prioritized to scalable approach considering internal/external indicators
- ▶ Compliance risk based audit/monitor plan is dynamic and reviewed regularly to reflect highest priority risk for the organization
- ▶ Board and Senior Leaders are engaged and feel “ownership” towards risk based plan