

**SOCIETY OF CORPORATE
COMPLIANCE AND ETHICS**


Conference for Effective Compliance Systems in
Higher Education
April 21-24, 2010 | Dallas, Texas

Internal Audit's Role in Promoting and Evaluating Institutional Compliance

Urton Anderson – Moderator
Gail Klatt – U of Minnesota
Daniel Roach – Catholic HealthCare West
Sheryl Vacca – U of California
Kathie Schwerdtfeger – Deloitte & Touche

Panel Gail Klatt

- Associate VP of Internal Audit for the University of Minnesota
- Audit Committee Member
 - Fairview Health Services
 - University of Minnesota Foundation



www.corporatecompliance.org 2

Panel
Daniel Roach

- Vice President,
Compliance & Audit
for Catholic
Healthcare West
- Past President of the
Health Care
Compliance Association
- Co-chair of the Society
of Corporate
Compliance & Ethics



www.corporatecompliance.org 3

Panel
Sheryl Vacca

- SVP/Chief Compliance
and Audit Officer at the
University of California
- Past President of the
Health Care
Compliance Association
- Advisory Board Member
of SCCE



www.corporatecompliance.org 4

Panel
Kathie Schwerdtfeger

- Partner, Deloitte & Touche
- National Public Sector Internal Audit Leader
- Former Special Assistant to the State Auditor and Federal Single Audit Coordinator, Texas State Auditor's Office .



www.corporatecompliance.org 5

Agenda

- IA's Role in the organization's ethics and compliance program
- How can IA
 - successfully provide assurance on institutional-wide compliance through auditing and evaluation of the ethics and compliance program
 - be an active participant in promoting ethics and values and improving the organization's ethical culture beyond simply auditing

www.corporatecompliance.org 6

The Internal Audit Value Proposition

The fundamental value proposition for internal auditing is the role it plays in maintaining a system of effective organizational governance.

www.corporatecompliance.org 7

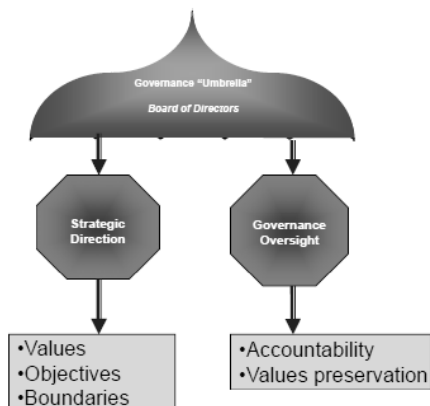
What is organizational governance?

The process through which

- (1) values and goals are established and communicated,
- (2) the accomplishment of goals is monitored,
- (3) accountability is ensured, and
- (4) values are preserved.

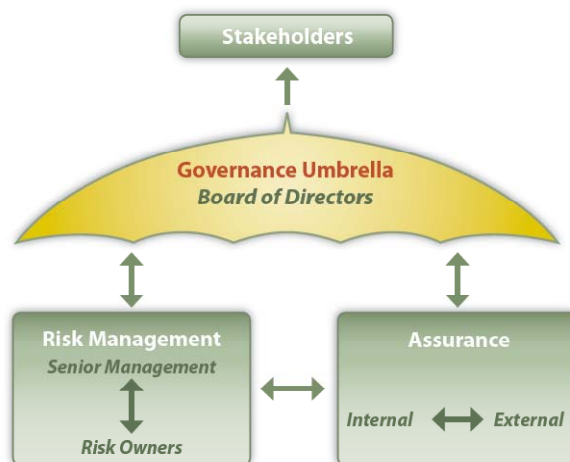
www.corporatecompliance.org 8

The Two Basic Responsibilities of the Governance Body of an Organization



www.corporatecompliance.org 9

Key Components of Governance Oversight



www.corporatecompliance.org 10

IIA Standards 2110 - Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization; and
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management

www.corporatecompliance.org 11

Standard 2110.A1

The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities

www.corporatecompliance.org 12

Federal Sentencing Criteria for Effective Compliance program – 7 elements

#5. The organization shall take reasonable steps—

- (A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;
- (B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and

www.corporatecompliance.org 13

Auditing Compliance System Effectiveness

Part 1 - The assessment of the entity level controls over the compliance program which at a minimum would include evaluating the organization's process for assessing risk of noncompliance and ethical misconduct and the design and implementation of seven elements of the Guidelines.

Part 2 – Evaluating the effectiveness of controls specifically designed to reduce the risk of noncompliance in the high risk areas identified by the organization's risk assessment process.

www.corporatecompliance.org 14

Panel
Gail Klatt

- Associate VP of Internal Audit for the University of Minnesota
- Audit Committee Member
 - Fairview Health Services
 - University of Minnesota Foundation



www.corporatecompliance.org 15

University of Minnesota



- Reporting Relationships
 - Internal Audit reports to the Board of Regents
 - Institutional Compliance reports to the President
- The University adopted the COSO internal control framework in the early 1990s.
- The Compliance Officer reports to the Board of Regents Audit Committee at least twice a year.
- A separate “ad hoc” group of Board members meets as needed to be informed of specific compliance issues.

www.corporatecompliance.org 16

University of Minnesota

Office Of Internal
AUDIT

- How do we fulfill our professional responsibilities regarding the *assessment* of our compliance program and activities?
 - Carry out specific risk based audit work from a very granular level (reviewing individual grants) to system-wide reviews (the entire effort reporting process).
 - Participate in policy formulation and maintenance efforts to ensure that policies incorporate sufficient compliance direction, are understandable, and are auditable.
 - Participate in the President's Executive Compliance Oversight Committee which provides direction and support for our Institutional Compliance Officer.
 - Triage reports received on our confidential reporting hotline, along with the Compliance Office.

www.corporatecompliance.org 17

University of Minnesota

Office Of Internal
AUDIT

- Fulfilling our professional responsibilities:
 - Perform trending analyses of audit findings to identify potential systemic weaknesses.
 - Include questions regarding ethical conduct and compliance in employee surveys conducted as part of every audit. The results of these surveys are shared with the Compliance Officer.
 - Along with the Compliance Officer and the General Counsel, review semi-annual compliance reports submitted by functional compliance personnel.

www.corporatecompliance.org 18

University of Minnesota

Office Of Internal
AUDIT

- How do we fulfill our professional responsibilities to *promote* institutional compliance?
 - Emphasize the importance of monitoring compliance activity
 - Help delineate the “must dos” from the “nice to haves”
 - Focus attention on risk assessment and the need to balance institutional requirements against the risks being mitigated
 - Help promote accountability for compliance
 - Help coordinate resources in addressing compliance issues
 - Serve as liaison between the compliance officer and the Audit Committee

www.corporatecompliance.org 19

University of Minnesota Executive Compliance Oversight Committee

- Institutional Compliance Officer
- General Counsel
- Chief Audit Executive
- VP Research
- SVP Health Sciences
- VP for Multicultural Affairs and Diversity
- VP Human Resources
- VP University Services (Operations)



www.corporatecompliance.org 20

University of Minnesota Compliance Partner Program



- Access/ Disability Issues
- EOAA
- Athletics
- Privacy
- Occupational Health & Safety
- Environmental Health & Safety
- Animal Research
- Human Subjects Research
- Conflict of Interest
- Human Resources
- Immigration (Taxes & SEVIS)
- Study /Research /Teaching Abroad

- Biosafety & Biosecurity
- Public Safety
- Workplace Safety
- Housing & Dining
- Information Technology
- Grant Administration
- Technology Transfer
- Student Finance
- HIPAA
- Clinical Services
- Fiscal (purchasing, disbursements, etc)
- Tax

www.corporatecompliance.org 21

University of Minnesota Silos – Are they really bad?



They can be, IF:

- They perceive, evaluate, and report on risk differently
- They result in fragmented institutional response
- Reporting and escalation occurs in different ways

www.corporatecompliance.org 22

University of Minnesota Silos – Are they really bad?



They can be, IF:

- They perceive, evaluate, and report on risk differently
- They result in fragmented institutional response
- Reporting and escalation occurs in different ways

We pull them together through
our compliance partner
reporting program

www.corporatecompliance.org 23

University of Minnesota Compliance Reporting



- Compliance Partners/Risk Owners report 2X/yr.
 - Report major and significant risks in their subject matter area. “Major” and “significant” are specifically defined.
 - Identify any risks they feel are not being appropriately mitigated and what else needs to be done.
 - Identify trends – both positive and negative
 - Reports are reviewed, and followed up on, by the Institutional Compliance Officer
 - Significant risks are codified and reported to the CAE and the General Counsel
 - Overall trends are reported to the Audit Committee
 - Information on specific concerns are reported to the Board Chair and Vice Chair and the Chair of the Audit Committee

www.corporatecompliance.org 24

Panel Sheryl Vacca

- SVP/Chief Compliance and Audit Officer at the University of California
- Past President of the Health Care Compliance Association
- Advisory Board Member of SCCE



www.corporatecompliance.org 25

University of California

- 10 campuses across California
- 20 billion revenue
 - 5 billion research
 - 5 billion medical centers
- 5 Medical Centers
- 3 National Labs (1 subsidiary, 2 JV)
- Agriculture and Research – across California/ 4H and other community programs
- 140,000+ employees
- 200,000+ students

www.corporatecompliance.org 26

26

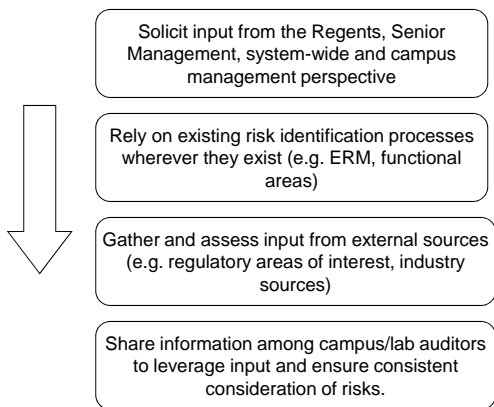
INTERNAL AUDIT PLAN OBJECTIVES

- Address the University’s significant financial, operational and compliance risks;
- Leverage existing efforts by others to identify, evaluate and mitigate risks;
- Support management’s restructuring and budget coping strategies;
- Serve the needs of campus/lab leadership while addressing broader issues from a systemwide perspective;
- Support the Systemwide Compliance Program; and
- Meet the challenge to enhance the value of the Internal Audit Program.

www.corporatecompliance.org 27

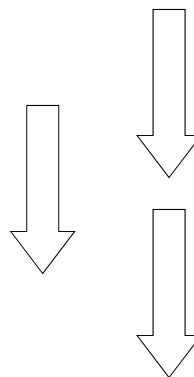
AUDIT PLAN DEVELOPMENT

Risk Assessment Process



COMPLIANCE PLAN DEVELOPMENT

Risk Assessment Process



The result of the risk assessment is an informed perspective on the current risk environment – including a prioritization of risks that are scalable to available resources.

www.corporatecompliance.org 28

HIGH LEVEL VIEW OF KEY RISK AREAS

Financial

- Compensation
- Construction
- Account Reconciliations
- Extramural Funds Accounting
- Charge Capture (hospital)
- Billing and Coding (hospital)
- Physician Billings
- Investments
- Segregation of Duties
- Cash Handling

Operational

- IT Security
- Business Continuity
- Data Center Operations
- Business Contracts
- Third Party Relationships
- Disaster Recovery Plans
- Contracts & Grant Administration
- International Activities
- Facilities Administration

Compliance

- Research – Effort Reporting
- Conflicts of Interest/commitment
- Compensation
- Health Sciences
- HIPAA/Privacy
- EH&S/Lab Safety
- ARRA – Stimulus monies and related compliance
- Development areas/commitment of monies

Note: Issues are inter-related across these risk types. The above categorization is not meant to be exclusive.

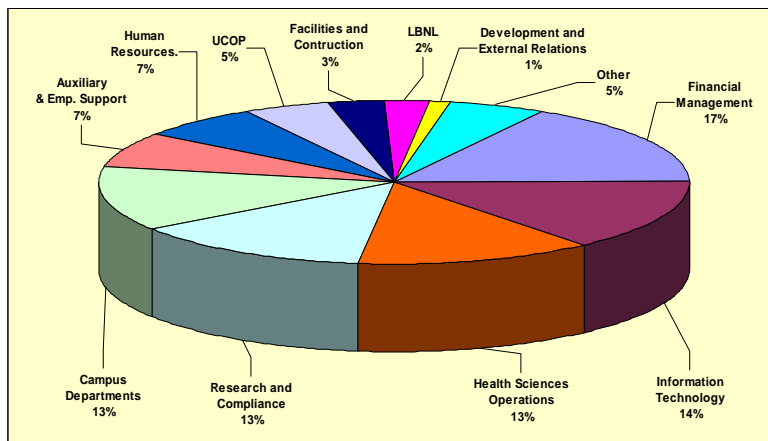
29

SYSTEMWIDE AUDIT AREAS – Assist Compliance Efforts

| Example AREA | Example SCOPE | PROJECTED TIMING |
|-------------------------------------|--|-------------------------|
| Health Science Vendor Policy | Assessment of the campus implementation of and compliance with the Healthcare Vendor Relations Policy. | 1 st Quarter |
| Billing and Coding* | Review of coding area in AMC's and associated billing | 4 th Quarter |
| Effort Reporting* | Identify appropriate processes for reconciling time and effort are in place | 2 nd Quarter |
| HIPAA Compliance* | Review appropriate processes are in place at 2 AMC's to assure protection of PHI | 4 th Quarter |
| ARRA- Stimulus Package* | Monitor compliance requirements | 3 rd Quarter |

*Represent systemwide compliance reviews that will be coordinated by **302** ECAS www.ecas.com/corporate/compliance.org 30 and may be outsourced.

The chart below depicts audit coverage across the University organizationally. It demonstrates breadth of coverage while indicating that major business processes, Research & Compliance activities, Health Sciences operations, campus academic departments and information technology collectively command nearly 75% of our effort.



Distribution of Projects

www.corporatecompliance.org 31

Key Systemwide Compliance Risk Grid (examples)

| | | |
|---|--|---|
| 1 | Government Reporting Accuracy, (e.g., time and effort reporting, ARRA monies, health sciences billing and coding accuracy) | Monitor for presence of adequate location protocols and processes to ensure accurate and timely submission of reports to government to support expenditures of funds and/or reimbursement of claims |
| 2 | Campus Safety, e.g., diversity awareness/sensitivity and pre-meditated acts of violence | In collaboration with risk management, ensure that comprehensive safety preparedness plans are in place at all locations |
| 3 | Data Privacy and Security | Data privacy and security efforts meet regulatory requirements and staff compliance to established protocols is enhanced through education and enforcement activities |
| 4 | Research-related compliance risks, including conflicts of interest, industry relations, export controls and intellectual property. | Research-related compliance policies, procedures and implementation steps are in place to ensure compliance with applicable regulatory requirement. |
| 5 | Culture of Ethics and Compliance | Establishment of appropriate controls surrounding administrative and faculty compliance-related training and enforcement guidelines for non-compliance |
| 6 | Investigation Practices | Enhance current investigation protocols to establish more consistent approach to investigations and reporting of observations/findings Provide systemwide training by external experts on investigation techniques |
| 7 | Health Care Reform | In collaboration with External Affairs and Health Sciences, monitor government/legislative reports on implementation strategies to determine impact on UC |

Compliance and Internal Audit

- Partners in identifying risks
- Assurance as to systems and controls provided
- Risk resolution is key importance, ie: control level (IA) and overall risk level (compliance)
- Both independent functions with reporting chain to the Board
- Compliance goal of prevention, detection and deterrence of risks is assisted by IA efforts and focus

www.corporatecompliance.org 33

Panel Kathie Schwerdtfeger

- Partner, Deloitte & Touche
- National Public Sector Internal Audit Leader
- Former Special Assistant to the State Auditor and Federal Single Audit Coordinator, Texas State Auditor's Office .



www.corporatecompliance.org 34

Risk and Compliance Management Medium Private University

- Individual risk management and compliance monitoring efforts happening across the University to include:
 - General Counsel
 - Internal Audit
 - Risk Management
 - Sponsored Projects
 - Finance
 - Tax
- Began networking informally to discuss what everyone was doing
- Determined there was real need for a more formal process

www.corporatecompliance.org 35

Risk and Compliance Management Medium Private University

- Established a Risk and Compliance Steering Committee
- Brought in a consultant to do risk and compliance training
- Initiated a formal study of their current practices which is currently ongoing
- Expected next steps:
 - Develop recommendations for a more formal and sustainable program
 - Establish a formal Risk Management Framework
 - Establish policies and procedures to communicate and implement that framework across the organization
 - Tie program activities into routine operations and overall organizational strategy

www.corporatecompliance.org 36

Role of Internal Audit Medium Private University

- One of the original parties that initiated informal sharing of risk management practices with other Departments
- Performs entity wide risk assessment as part of the process to develop the annual internal audit plan
- Collaborates with management to identify and prioritize risks for the annual internal audit plan and individual audit level
- Routine communication with the Audit Committee and Board on risk matters and internal audit's current role in addressing those matters
- Supporter of formal program for risk and compliance management
- Participant in steering committee but careful to maintain independence.

www.corporatecompliance.org 37

Risk and Compliance Management Large For Profit University

- Entity wide risk and compliance department
- Reports to Audit and Compliance Committee of the Board
- Collaborates across the entity to manage compliance and ethics risks
- Main focus is to preserve and enhance their reputation and ensure regulatory and policy compliance
- Utilizes a formal risk and compliance framework
- The risk and compliance framework includes specific elements each tied to organizational strategies and initiatives

www.corporatecompliance.org 38

Risk and Compliance Management Large For Profit University

- Elements of the program include:
 - Official code of conduct ,ethics policy, conflicts of interest policy
 - Anti-fraud program
 - Linked to diversity programs
 - Ongoing risk assessment
 - Robust training and communication
 - Programs to reward compliance
 - Processes to prevent, detect, and manage risks
 - Investigative function
 - Support with remediation efforts
 - Continuous improvement activities
 - Linkage to internal control management program and corporate governance activities
 - Routine reporting to executive management and the Board

www.corporatecompliance.org 39

Role of Internal Audit Large For Profit University

- Coordination of the annual internal audit risk assessment activities with the risk and compliance division risk assessment activities
- Periodic audits of risk and compliance program activities
- Consultative services aimed at enhancing the overall risk and compliance program
- Serves as a subject matter expert on risk, control, and technology matters
- Leads various training programs

www.corporatecompliance.org 40

Risk and Compliance Management Large Community College District

- Risk management activities informal and decentralized across the Campuses
- For the most part, the current risk manager is focused on workers compensation claims and employee disputes
- General Counsel is focused on litigation risks
- The CFO is worried about financial risks
- Technology risks are greatly misunderstood
- Campus police is worried about staff and student safety
- The District is in a reactive mode with a few too many surprises over the past few years
- Unclear lines of responsibility for risk and compliance matters between the Board and executive management
- No formal risk and compliance program or enterprise risk management activity

www.corporatecompliance.org 41

Role of Internal Audit Large Community College District

- Historically underutilized internal audit function
- Prior function focused primarily on compliance with policy
- New Chief Audit Executive focused on rebuilding the internal audit function and educating management and the Board on the importance of risk and controls as well as compliance matters
- Not enough resources to address “known” risks much less those that have yet to be identified
- Would like to serve as facilitator for ERM initiative and evaluator once implemented by management

www.corporatecompliance.org 42

Overall Observations and Comments

- More Board level awareness of and expectation for robust risk and compliance management
- Not every organization desires the same level of capability or sophistication when it comes to managing risk and compliance
- The “appropriate level” for any organization is a level that is commensurate with the nature and complexity of the organization and takes into consideration the risks the organization faces
- The Board and Executive Management sets the desired level of capability and determines the policies necessary to promote the desired outcomes
- The risk and compliance function(s) is then responsible for building and executing the individual processes necessary to achieve the desired level of capability

www.corporatecompliance.org 43

Overall Observations and Comments

- Risk and compliance management can be centralized or decentralized—what’s important is that it be coordinated in a standard fashion across the organization such that results can be easily accumulated, assessed, and acted upon in a timely manner
- A formal risk and compliance framework should be established and communicated to create a common “language” and common set of expectations across the organization
- The elements of that framework must be clearly defined and accountabilities assigned
- Risk and compliance management is an ongoing sustainable process—not a one time program or initiative
- Risk and compliance management adds true value when its heavily linked to the achievement of organizational strategies

www.corporatecompliance.org 44

Overall Observations and Comments

- Risk and compliance management should ideally include periodic self or external assessment and should be tailored as needed to meet changing risks and needs of the organization
- Risk and compliance within the University environment can be very complex and the list of stakeholders very broadly. Get representatives from all stakeholder groups involved
- Key participants would normally include Risk Management, General Council, Internal Audit, Sponsored Projects, Finance, Technology, Student Affairs, and Campus Police
- Faculty and student representation is important and should occur at select points in the process
- Executive management and the Board should be involved throughout the process

www.corporatecompliance.org 45