

# Role of the Audit & Compliance Committee



**AEGIS**  
COMPLIANCE & ETHICS  
4147 N Ravenswood Ave, Ste.200  
Chicago, IL 60613 | 888.739.8194  
www.aegis-compliance.com

**Judy Ringholz**  
VP, Audit and Compliance Services  
Lehigh Valley Health Network  
Allentown, PA

**Steve Ortquist**  
Managing Director  
Aegis Compliance & Ethics Center, LLP  
Chicago, IL



**AEGIS**  
COMPLIANCE & ETHICS  
4147 N Ravenswood Ave, Ste.200  
Chicago, IL 60613 | 888.739.8194  
www.aegis-compliance.com

## History of Audit Committees

- 1939 – NYSE first endorses AC concept
- 1972 – SEC first recommends establishment of AC by publically traded companies
- 1977 – NYSE adopts listing requirement that ACs be composed entirely of independent directors
- 1988 – AICPA issues SAS 61 re: communication with audit committees & management of SEC reporting companies by external auditors
- 1999 – NYSE, NASD, AMEX, SEC and AICPA finalize major rule changes based on Blue Ribbon Committee Work
- 2002 – Sarbanes-Oxley adopted, including financial expert and whistleblower requirements for audit committees



## Audit Committee Responsibilities

- Financial Reporting & Accounting
- Oversight of the External Auditor
- Oversight of Internal Audit Function
- Oversight of Ethics & Compliance Program
- Monitoring Effectiveness of Internal Controls Processes
- Role in Risk Management



## Corporate Governance and Role in Risk Management

- Greater focus since Sarbanes-Oxley
- Requirements for public companies – assurances re: internal controls
- Many opine that same rules should apply to non-profit organizations
  - Fewer charitable funds warrants an emphasis on stronger fiscal responsibility



## Oversight of Risk Management

- Integrity of financial statements
- Fraud and Compliance
- IT / Cybersecurity
- Quality of care



## Financial Expert Required

At least one member should meet the qualifications of a “financial expert”:

- Understand financial statements
- Understand financial risks
- Understand the impact of business decisions on the financial statements
- Understand internal controls related to financial reporting
- Understand audit committee functions



©2013 Aegis Compliance & Ethics Center, LLP

7

## Duty of Care / Fiduciary Duty

- To exercise the level of care “an ordinary prudent person would exercise in a like position under similar circumstances”
- Ensure that the organization has internal controls in place to
  - help prevent/deter fraud
  - discover and investigate timely



©2013 Aegis Compliance & Ethics Center, LLP

8

## Whistleblower Protections

- Sarbanes-Oxley Prohibits Retaliation
  - Non-Retaliation Policy
    - Must be enforced at all levels of org.
    - Must be made known to all through training
  - Employee may not be discharged, demoted, suspended, harassed, or discriminated against in any other way



## Risk Related to IT Functions

- Need for oversight increasing as IT functions are enhanced / expanded
  - Financial reporting-related risks
  - Information security / Vendors
- Committee members not equipped to ask the right questions
- IT expertise should be required
  - Committee member vs. consultant



## Review with Outside Auditors

- Scope of annual audit / Fees
- Independence / Work performed
- Adequacy of organization's controls
- Quality of accounting principles and financial reporting (judgments)
- Expertise of leaders and staff
- Sufficiency of allocated resources
- Cooperation received / Access given
- Material/Serious Recommendations



## Audit Committee Charter

- Composition (3 or more members)
  - Members must be independent
    - Objective and impartial committee
    - No conflicts of interest
    - Definition of a quorum
- Responsibilities / Authority
- Frequency of meetings
  - Executive sessions



## How to Fulfill Responsibilities

- Control and prioritize agendas
- Build relationships with managers and auditors (robust dialogue)
- Ensure that Internal Audit and Compliance develop risk-based workplans each year
- Set “tone at the top” and closely monitor organizational culture



## Resources / Tools for Successful Oversight

### PWC’s Center for Board Governance

- Audit Committee Resources Page
  - Publication:
    - “Key questions for board and audit committee members”

### KPMG’s Audit Committee Institute

- Publications:
  - “Today’s Top To-Do’s for Not-For-Profit Audit Committees”
  - “KPMG’s Audit Committee Priorities for Not-for-Profit Organizations in 2013”

### EY Center for Board Matters

- Publication: (80 Pages)
  - “Staying on course: A guide for audit committees”



## Audit / Compliance Functions – Integrating the Two

- One Department / Committee
- Advantages
  - Comparable Duties
  - Enhanced Efficiencies
  - Cost Effectiveness
- Identifying the Right Leader



©2013 Aegis Compliance & Ethics Center, LLP

15

## Compliance Program Oversight





## Development of the “Duty to Monitor”

Directors’ duty of care includes a duty to attempt in good faith to assure that:

1. A corporate information and reporting system exists, and
2. The reporting system is adequate to assure the board that appropriate compliance-related information will come to its attention in a timely manner, in ordinary course.

*In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. 1996)



**AEGIS**  
COMPLIANCE & ETHICS  
4147 N Ravenswood Ave, Ste.200  
Chicago, IL 60613 | 888.739.8194  
www.aegis-compliance.com

## Development of the “Duty to Monitor”

“In the absence of ‘red flags’ good faith in the context of oversight must be measured by the directors’ actions to assure that a reasonable information and reporting system exists.”

To prevail on a breach of the “duty to monitor” a plaintiff must show either that

- (a) “the directors utterly failed to implement any reporting or information system or controls” or else
- (b) “having implemented such a system or controls, [the directors] consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.”

Scienter Element: “[i]n either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations,” that is, that they were “demonstrating a conscious disregard for their responsibilities.”

*Stone v. Ritter*, 911 A2d 362, 370 (Del. 2006)



**AEGIS**  
COMPLIANCE & ETHICS  
4147 N Ravenswood Ave, Ste.200  
Chicago, IL 60613 | 888.739.8194  
www.aegis-compliance.com

## Importance of External Effectiveness Evaluation

“On February 8, 1993, the Ethics Committee of Caremark’s Board received and reviewed an outside auditors report . . . which concluded that there were no material weaknesses in Caremark’s control structure.”

*In re Caremark*

“The [external firm’s compliance program evaluation] Report reflects that the directors not only discharged their oversight responsibility to establish an information and reporting system, but also proved that the system was designed to permit the directors to periodically monitor AmSouth’s compliance with . . . regulations.”

*Stone v. Ritter*



## Freeh Report (Penn State)

Citing *Stone v. Ritter*, Special Counsel found that the Board failed in its fiduciary duties because:

- In 1998 and 2001 the Board did not have regular *reporting procedures or committee structures* in place to ensure disclosure to the Board of major risks; and
- In 2011 because, after becoming aware of the Grand Jury investigation of Sandusky, Board members did not independently assess the information provided by Spanier (President) and Baldwin (General Counsel) or demand detailed reporting from the same.
- The Board failed to create a “Tone at the Top” environment that Sandusky and other University officials believed they were accountable to.
- The Board’s failure to insist on thorough reporting led to an environment where President Spanier did not feel accountable for keeping the Board immediately informed on serious developments.
- “The Board allowed itself to be marginalized by not demanding ‘thorough and forthright reports on affairs of the University’



## Will the “Duty to Monitor” Expand?

### Classic *Caremark* cases

Theory: Directors should be liable for their failure to monitor employee misconduct or violations of law.

### *Citigroup*

Theory: Directors should be liable for their failure to be informed about and monitor the organization’s business risk.



## Delaware Duty of Care

- Duty to monitor – assure that an adequate/functioning information and reporting system exists
- Pay attention to reports from the reporting system
- “red flags” require increased scrutiny and attention by board members – board members are expected to act when suspicions are aroused or should be aroused.



## Federal Sentencing Guidelines

### Board's leadership obligations:

- Be knowledgeable about the content and operation of the compliance and ethics program;
- Exercise reasonable oversight with respect to the implementation and effectiveness of the compliance & ethics program



## Federal Sentencing Guidelines

Knowledgeable about the content and operation of the program

*"The knowledge about program features and operations that members of a governing authority should gain includes:*

*-practical management information about the major risks of unlawful conduct facing their organization;*

*-the primary compliance program features aimed at counteracting those risks; and*

*-the types of problems with compliance that the organization and other parties with similar operations have encountered in recent activities."*

*(Report of the Ad Hoc Advisory Group leading to the 2004 Sentencing Guidelines amendments, October 7, 2003)*



## Federal Sentencing Guidelines

Exercise reasonable oversight

*“The provisions of this proposal describing the oversight duties of governing authority members recognize that effective management requires that governing authorities be proactive in*

*-seeking information about compliance problems,*

*-evaluating that information when received, and*

*-monitoring the implementation and effectiveness of responses when compliance problems are detected.”*



## Federal Sentencing Guidelines

Other board obligations

- Receive periodic reports from the compliance officer and/or other persons responsible for the compliance program about its implementation and effectiveness
- Compliance personnel must have “reporting obligations” to the board to get credit for the compliance & ethics program (2011 amendments)
- Participate in periodic compliance training
- Accessible to the compliance officer



## Corporate Integrity Agreement Requirements

Tenet, Novartis, Wellcare, AstraZeneca, King's Daughters, etc.

- Quarterly review and oversight by board/committee, including of executive compliance committees and compliance officers
- Annual effectiveness reviews
- Compliance expert to advise board
- Committee resolution/certification (signed by each board committee member)



## CIA Board Resolution

“The Board of Directors has made a reasonable inquiry into the operations of [Organization’s] Compliance Program including the performance of the Compliance Officer and the Compliance Committee. Based on its inquiry and review, the Board has concluded that, to the best of its knowledge, [Organization] has implemented an effective Compliance Program to meet Federal health care program requirements and the obligations of the CIA.”



## DOJ Principles of Federal Prosecution of Business Organizations

### Three central questions:

- Is the ethics & compliance program well designed?
- Reliance on other agencies (e.g., DHHS OIG)
- Is the program being applied earnestly and in good faith?
- Does the ethics & compliance program work?



## Oversight Obligations LEADERSHIP

Should oversight committees include a member(s) with compliance & ethics expertise?

See, e.g., SEC Disclosure Rule re: "Audit Committee Financial Expert"

- Understanding of financial statements and GAAP
- Ability to assess general application of such principles in connection with accounting for estimates, accruals and reserves
- Expertise in preparing, auditing or evaluating financial statements
- An understanding of internal controls
- An understanding of the audit committee functions.



## Oversight Considerations LEADERSHIP

- Does the compliance officer have the right reporting obligations and access to the board/audit & compliance committee?
- Is the compliance officer positioned correctly in the organization?
  - Seniority (*specific individual(s) within High-Level Personnel assigned overall responsibility; High-Level Personnel = substantial control over the organization or a substantial role in policy making. E.g., director, executive officer, in charge of a major business unit or function.*)
- Reporting Relationship
- Is management meeting its obligations and supporting the program?



## Oversight Considerations RISK AREAS

- What are the organization's primary compliance risks/risk areas?
  - Stark and/or Anti-Kickback?
  - Quality of Care?
  - Privacy & Security?
  - Billing/Coding/False Claims?
  - Other?
- Do you have a basic understanding of
  - legal & regulatory requirements in these areas?
  - what other organizations are experiencing?
  - your organization's prior experience?
  - what causes most significant risk for your organization?





## Oversight Considerations STRUCTURE

- Does the compliance program's structure align with the "seven elements?"
- Does the compliance program's structure address what is called for by applicable industry guidance? (E.g., OIG CPGs; DOJ *Principles of Prosecution*)
- Does the compliance & ethics program address organizational risks?
- Does the compliance & ethics program have adequate resources?
- Does the compliance & ethics program work? What is provided by management/compliance officer to illustrate that the program is effective?
- Has there been an external evaluation of the effectiveness of the compliance & ethics program?



## Oversight Considerations STRUCTURE

- Are reporting mechanisms (e.g., hotline) working properly (e.g., confidential, trusted by workforce?)
- Do reporting and response mechanisms assure that appropriate concerns are raised to board's/committee's attention?
- Does the organization take appropriate steps to respond to problems (remediation, prevention, etc.)



## Compliance Resources

United States Sentencing Commission's *Sentencing Guidelines for Organizations* (see particularly § 8B2.1. *Effective Compliance & Ethics Program*)  
[http://www.ussc.gov/Guidelines/Organizational\\_Guidelines/guidelines\\_chapter\\_8.htm](http://www.ussc.gov/Guidelines/Organizational_Guidelines/guidelines_chapter_8.htm)

U.S. DHHS OIG compliance program guidances  
<http://oig.hhs.gov/compliance/compliance-guidance/index.asp>

American Health Lawyers Association/Office of Inspector General Governance Resources  
<http://www.healthlawyers.org/hlresources/PI/InfoSeries/Pages/CorporateResponsibilityCollection.aspx>

Freeh Report (Penn State) <http://progress.psu.edu/the-freeh-report>

U.S. Department of Justice *Principles of Federal Prosecution of Business Organization's*  
[www.justice.gov/opa/documents/corp-charging-guidelines.pdf](http://www.justice.gov/opa/documents/corp-charging-guidelines.pdf)



## QUESTIONS & DISCUSSION



Judy Ringholz  
[judy.ringholz@lvhn.org](mailto:judy.ringholz@lvhn.org)  
484-884-1401

Steve Ortquist  
[sortquist@aegis-compliance.com](mailto:sortquist@aegis-compliance.com)  
312-285-4850



 **AEGIS**  
COMPLIANCE & ETHICS  
4147 N Ravenswood Ave, Ste.200  
Chicago, IL 60613 | 888.739.8194  
[www.aegis-compliance.com](http://www.aegis-compliance.com)