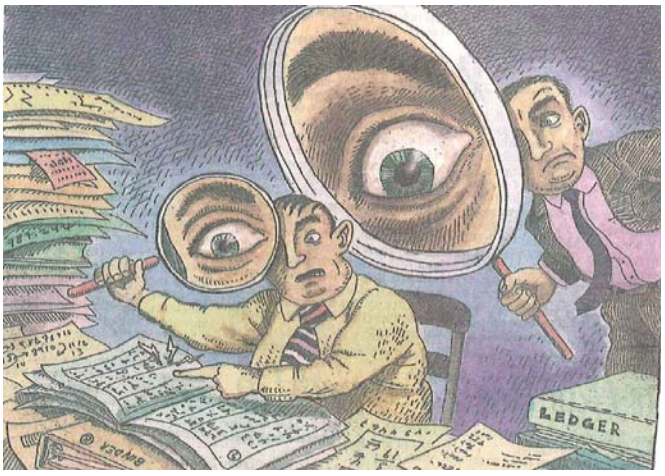
COMPLIANCE AT LARGER INSTITUTIONS

November 11 – 13, 2009

Robert F. Roach
Chief Compliance Officer
New York University

I. Introduction - What is Compliance?



We're Watching You!

In a University setting, the process of compliance starts with a handicap – the name. For example, look in Black's Law Dictionary and you will see the definition of compliance as, *"Submission, obedience, conformance."* Clearly, a program based primarily on mandated submission and obedience would not be well received on most American campuses.

Nowadays, instead of submission and obedience we need to think of compliance programs as a reflection of an organizational culture that encourages a commitment to compliance with the law. This organizational culture should be defined as the shared sets of norms or beliefs that are shaped by the organization's leadership, often expressed as shared values or guiding principles, and are **reinforced by systems and procedures throughout the organization.** *See Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines* (October 2003).

This "shared values" concept of compliance, driven by organizational leadership, was described by Lynn Sharpe Paine, in *Managing for Organizational Integrity*, Harvard Business Review (March-April 1994). According to Paine, it is the responsibility of an organization's leadership to:

> Define and give life to an organization's guiding values, to create an environment that supports ethically sound behavior, and to instill a sense of shared accountability among employees . . . The need to obey the law is viewed as a

positive aspect of organizational life, rather than an unwelcomed constraint imposed by external authorities.

Thus, a university compliance program should ideally reflect the university community's shared values - a commitment to integrity, and a desire to fulfill its academic mission consistent with the university's legal, regulatory and ethical responsibilities.

In the sections below, we provide: II. a brief history of organizational compliance practices and laws; III. the elements of an effective compliance program, including directions for large organizations;

In the program materials for the session entitled, "*Developing and Implementing a Compliance Calendar and Other Tools",* we set out reference materials and compliance tools for each of the "elements of an effective compliance program" set forth in section III below. Materials for these two sessions, as well as the reference citations and compliance tools, are included in a toolkit cd-rom.

II. History of Compliance

1986 - Defense Industry Initiative on Ethics and Conduct

The Defense Industry Initiative (DII) is general considered the beginning of formal organizational ethics and compliance programs. During the 1980s, allegations of fraud and government mismanagement resulted in a Presidential Blue Ribbon Commission on Defense Management (called referred to as the "Packard Commission"). The Commission found that public confidence in the defense industry had been eroded by reports of waste, fraud and abuse within both the industry and the Defense Department. The Commission concluded that the defense acquisition process, the defense business environment, and confidence in the defense industry could be improved by placing greater emphasis on corporate self-governance. Subsequently, several leading defense contractors voluntarily joined together to establish the DII, which has three main purposes:

- to nurture and promote a culture of ethical conduct within every company in the defense industry;
- to promote self-governance as a means of confirming management's commitment to abide by ethical standards – even when they exceed legal requirements – and of discovering and correcting instances when conduct falls below these standards; and
- that companies share best practices in dealing with ethics and business conduct issues, which included the development of formal Codes of Ethics and mandatory ethics training for employees, internal "hotlines" and other reporting mechanisms, with a promise of no retaliation

However, the 1980's were rife with corporate corruption scandals that extended well beyond the defense industry. (Anyone remember Ivan Bosky, Michael Milken and "Junk Bonds"?) These scandals lead to additional programs designed to encourage greater corporate self government.

1991 – The U.S. Federal Sentencing Guidelines

In response to a variety of corporate corruption scandals, the federal government amended the U.S. Federal Sentencing Guidelines to provide credit to organizations with "an effective program to prevent and detect violations of law." *See* U.S. Federal Sentencing Guidelines § 8B2.1. These amendments were designed to encourage greater self governance efforts. Under these Guidelines, the hallmark of an effective ethics and compliance is "due diligence in seeking to prevent and detect criminal conduct." (There are seven – plus one -basic elements to an effective ethics and compliance program, which are discussed below).

1992 -The COSO Report, *Internal Control – Integrated Framework*

While the new Sentencing Guidelines for Organizations were being developed, a group of leading public accounting organizations called the Committee of Sponsoring Organizations (COSO) joined together to address perceived deficiencies in financial accounting practices. COSO's report *Internal Control – Integrated Framework* sets forth a methodology for helping assure ethical and legally compliant accounting and financial reporting practices. The COSO report sets forth a comprehensive risk assessment methodology and a process for establishing a system of internal controls designed to achieve:

- Effectiveness and efficiency of operations;
- Reliability of financial reporting, and
- Compliance with applicable Laws and regulations.

The COSO Framework is discussed in more detail below in the section on "risk assessment" below.

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

In *Caremark*, the Delaware Chancery Court was asked to review a proposed settlement of litigation against the company's directors. The company engaged in illegal payments in violation of the federal anti-referral payments law. The suit alleged that the company's directors' breached their fiduciary responsibility to the shareholders through a lack of proper oversight.

The Caremark court stated, in effect, that a board of directors has a fiduciary responsibility to assure that the company has an effective compliance program following the Federal Sentencing Guidelines. According to the court, "Any rational person attempting in good faith to meet an organizational governance responsibility would be bound to take into account [the Federal Sentencing Guidelines] … and the opportunity for reduced sanctions…."

2002 – 2004 SOX and Amendments to Federal Sentencing Guidelines

Despite these efforts to encourage good self governance, corporate corruption scandals continued to unfold, including the Enron and WorldCom corporate scandals. As a result of these scandals, the Sarbanes Oxley Act of 2002, Public Law 107–204 (SOX) was passed and the Federal Sentencing Guidelines were further amended.

SOX requires that as part of "internal controls" public companies must adopt and publish a Code of Ethics which promotes:

- Honest and ethical conduct;
- Avoiding conflicts of interest;
- Full, fair, accurate, timely and understandable disclosures;
- Compliance with government laws, rules and regulations;
- Internal reporting of violations of the code, and
- Accountability for adherence to the code.

Section 805(a)(2)(5) of the Sarbanes-Oxley Act directed the Federal Sentencing Commission to review and amend, as appropriate, the Federal Sentencing Guidelines and related policy statements to ensure that the guidelines that apply to organizations "are sufficient to deter and punish organizational criminal misconduct." Accordingly, the Guidelines were amended to:

- Require corporations to "promote an organizational culture that ***encourages ethical conduct*** and a commitment to compliance with the law."

- Add "eighth" element of an effective compliance program. The new Guidelines provided that, "In implementing [an effective compliance program], the organization shall ***periodically assess the risk of criminal conduct*** and shall take appropriate steps to design, implement, or modify each requirement [for an effective compliance program] ***to reduce the risk of criminal conduct identified through this process."***

Up to Present - Other Regulatory Requirements:

In recent years, other federal laws and guidelines have been amended or promulgated to require ethics and compliance programs, including the Federal Acquisition Contracting (FAR) Regulations; the Deficit Reduction Act (Medicare/Medicaid); and the Health and Human Services Office of Inspector General (HHS OIG) Guidelines.

III. Elements of an Effective Compliance Program

To have an effective compliance program, an organization must establish and maintain an organizational culture that *"encourages ethical conduct and a commitment to compliance with the law."* U.S. Sentencing Guidelines §8B2.1(a)(2)

There are seven (plus one) elements of an effective ethics and compliance program:

1. High level company personnel who exercise effective oversight;
2. Written policies and procedures;
3. Training and education;
4. Lines of communication;
5. Standards enforced through well-publicized disciplinary guidelines;

6. Internal compliance monitoring; and,
7. Response to detected offenses and corrective action plans.
8. Periodic "risk assessments" (added by amendment to the original seven Guideline elements).

The commentary to the Federal Sentencing Guidelines provides:

> (A) In General. Each of the requirements set forth in this guideline shall be met by an organization; however, in determining what specific actions are necessary to meet those requirements, factors that shall be considered include: (i) applicable industry practice or the standards called for by any applicable governmental regulation; (ii) the size of the organization; and (iii) similar misconduct.
> (B) Applicable Governmental Regulation and Industry Practice.—An organization's failure to incorporate and follow applicable industry practice or the standards called for by any applicable governmental regulation weighs against a finding of an effective compliance and ethics program.

Large Colleges and Universities should also consider the additional following commentary guidance:

> (C) The Size of the Organization.—
> (i) In General.—The formality and scope of actions that an organization shall take to meet the requirements of this guideline, including the necessary features of the organization's standards and procedures, depend on the size of the organization.
>
> (ii) Large Organizations.—A large organization generally shall devote more formal operations and greater resources in meeting the requirements of this guideline than shall a small organization. As appropriate, a large organization should encourage small organizations (especially those that have, or seek to have, a business relationship with the large organization) to implement effective compliance and ethics programs.

Each of these elements is addressed in greater detail below:

Element One
High Level Company Personnel Who Exercise Effective Oversight

A. The Governing Authority

Under the Federal Sentencing Guidelines, an organization's governing authority should:

- **Be knowledgeable about the program;**
- **Exercise effective oversight.**

When the Guidelines were amended in 2002, the Advisory Committee noted that almost all of the corporate scandals that motivated the passage of SOX and the amendments to the Guidelines were caused by either high level manages or members of the organizations' governing body. These misdeeds lead to "the public's lack of confidence in public markets." *Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines* (October 2003). These concerns resulted in Guidelines provisions which established clear compliance responsibilities for the organization's "governing authority."

Under the Guidelines, "Governing authority" means the "(A) the Board of Directors; or (B) if the organization does not have a Board of Directors, the highest-level governing body of the organization." *See* Commentary to §8.B.2.1., Application Notes, 1. Definitions.
According to the Ad Hoc Committee, the governing authority is ultimately responsible for the activities of the organization and that it could only fulfill this responsibility if its members are knowledgeable about management's ethical and legal compliance performance and exercise reasonable oversight with respect to the effectiveness and implementation of the program. (Citing the decision in *Caremark, supra*).

The type of knowledge that the governing authority should have includes: practical management information about compliance risks faced by the organization and others with similar operations, and the primary program features aimed at counteracting those risks. The governing body will typically obtain this information through reports from senior organization managers. Governing authorities are expected to be proactive in seeking and evaluating information about their organization's compliance programs, evaluating that information when received, and monitoring the implementation and effectiveness of responses when compliance problems are detected.

B. High Level Personnel

Under the Federal Sentencing Guidelines, an organization's "high level" and substantial authority personnel should:

- **Have overall responsibility for the compliance program;**
- **Ensure that the program is effective.**

Under the Guidelines, one or more specific individuals within the "high-level personnel" of an organization should be designated as the organizational official or officials with primary responsibility for the operation of the compliance program. This requirement helps to ensure that the official charged with implementing an organization's compliance program has the formal authority, access to senior management, and the respect needed to manage and oversee the implementation of a program

High-level personnel and other "substantial authority personnel" of the organization must also be knowledgeable about the compliance program and must promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Under the Guidelines, the term "high-level personnel of the organization" means individuals who have substantial control over the organization or who have a substantial role in the making of policy within the organization. The term includes: a director; an executive officer; or an individual in charge of a major business or functional unit of the organization, such as sales, administration, or finance. The term "substantial authority personnel" means individuals who within the scope of their authority exercise a substantial measure of discretion in acting on behalf of an organization. *See* Commentary to §8.A.1.2, Application Notes, 3.

C. Day to Day Responsibility

Specific individuals, often a compliance and ethics officer (CECO), are assigned overall responsibility for the day to day operations of the compliance program. The CECO must

- **Periodically report status to high level personnel and/or the governing body, and**
- **Must have adequate resources, appropriate authority and direct access to governing body.**

The Guidelines reflect the position that the head of an organization's compliance program will have key information necessary for the governing authority to exercise effective oversight, so periodic reports to the governing authority are expected (at least on an annual basis).

Element Two and Three
Written Policies and Procedures and Training

Under the Guidelines an organization must take reasonable steps to communicate to its employees compliance standards and procedures, and other aspects of the compliance and ethics program by:

- **Conducting effective training programs, and**
- **Disseminating information to employees consistent with their respective responsibilities.**

For University's, this will typically involve developing policies that **e**xplain relevant legal requirements to employees, consistent with their job functions, as well as related training programs and/or materials so that employees understand their obligations. Training need not be formal or expensive to be effective and organizations have great leeway in formulating programs that suit their organizational needs and resources. To be effective though, training must do more than impart information; it should be designed to motivate employees to comply with the law. Also, it should be noted that the *Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines* (October 2003) states:

> **The larger the organization, the more appropriate it maybe to have a more formal training program with appropriate documentation and dedicated resources and tools to measure the training program's impact. The burden would thereby remain on the organization to explain what training occurred and why the organization considered it effective. *Id* at 73. (Citations omitted).**

Training should be provided to the governing body and high level executives as well as employees, and where appropriate, to the organization's agents and vendors.

A "Code of Ethical Conduct:" is typically the centerpiece of an effective ethics and compliance program. A good code will include a statement of values and the commitment of the organization's leadership to ethics and compliance. The Code will also cover the organizations key legal and ethical obligations, the employees' obligation to comply with these legal obligations and possible disciplinary sanctions for non-compliance. The Code should also provide a mechanism for reporting compliance concerns and a clear policy of non-retaliation for good faith reports.

Element Four
Lines of Communication

Information about the compliance program must be widely communicated at all levels of an organization. To enhance the effectiveness of the compliance program, the program must establish lines of communication whereby:

- **Employees and agents may seek guidance and report concerns, including the opportunity to report *anonymously* (such as a compliance hot line);**
- **There are assurances that there will be *no retaliation* for good faith reporting**

Employees should be encouraged to use internal reporting mechanism to seek advice if they are not sure whether the conduct of concern would be a violation of the law. Reports regarding contacts and activities related to the hotline should be made periodically to the organization's governing authority.

Element Five
Standards Enforced Through Well-Publicized Disciplinary Guidelines

The organization's compliance and ethics program should be promoted and enforced consistently through well-publicized guidelines that provide:

- **Incentives to support the compliance and ethics program;**
- **Disciplinary measures for disobeying the law, the organization's policies, or the requirements of the compliance and ethics program.**

Element Six and Seven
Internal Compliance Monitoring
Response to Detected Offenses and Corrective Action Plans

The organization shall take reasonable steps, including monitoring and auditing, to:

- **Ensure that the organization's compliance and ethics program is followed;**
- **Periodically evaluate the effectiveness of the organization's compliance program.**

After monitoring and auditing of the compliance program, the organization shall take reasonable steps to:

- **Respond appropriately to any violations of the law or policies to prevent future misconduct;**
- **Modify and improve the organization's compliance and ethics program.**

The *Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines* (October 2003) described monitoring and auditing as "essential" to effective compliance programs for the following reasons:

> [A]n increased emphasis on monitoring, auditing, and evaluation practices is justified on three independently sufficient grounds:(1) the recognition of the importance of compliance monitoring, auditing, and evaluation in recent legal standards; (2) practical evidence of the importance of these practices in revealing recent incidents of major corporate misconduct; and (3) privately developed standards and expert opinions identifying monitoring, auditing, and evaluation efforts as important components of effective compliance programs. *Id.* at 78.

The report further advises:

> Determinations of the sorts of periodic compliance assessments that will compose sufficient monitoring, auditing, and evaluation practices will depend on the characteristics and activities of specific organizations. In small organizations, periodic evaluations of compliance in the course of day-to-day business operating practices will often be adequate monitoring steps so that further auditing or evaluations will not be needed. ***In larger organizations, however, separate audits of compliance performance will usually be warranted, with such audits being conducted by internal or external parties who are independent of the managers overseeing the performance under scrutiny.*** *Id.* (Emphasis added).

Element Eight
Periodic Risk Assessments

For a compliance and ethics program to be truly effective, an organization must periodically access the risk of non-compliance or misconduct and take appropriate steps to design, implement, or modify the program to reduce the risk of non-compliance or misconduct identified through this process.

An organizations activities and related legal obligations may change over time. Periodic compliance risks assessments help to ensure that compliance efforts are designed to mitigate compliance risks in the context of the organizations a company's present legal and operational environment. Thus, a regular, periodic risk assessment should be used to design and implement a range compliance activity, such developing appropriate compliance program standards and

procedures; determining the specific actions that should be taken to ensure compliance with legal requirements; and helping compliance program evaluators target the frequency and content of program monitoring activities.

A Sample Risk Assessment Process

The COSO *Internal Controls Integrated Framework* was established in 1992 by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, which consisted of all of the major U.S. professional accounting organizations. COSO's mission was to establish a methodology to minimize the opportunity for fraud in companies, and to help assure that companies complied with all applicable laws.

The American Institute of Certified Public Accounts (AICPA) Auditing Standards (SAS 78 – AU 319) made the COSO Framework applicable to all U.S. research universities. *See also* SAS 112 and OMB Circulars A-110 and A-133.

The COSO *Internal Controls Integrated Framework* provides organizations with a methodology to conduct annual compliance risk assessment including:

- Identifying possible risk events;
- Assessing the likelihood or frequency of the risk occurring;
- Estimating the significance or impact of the risk (including operational, regulatory, legal, reputational impacts)
- Determining how the risk should be managed, and
- Assessing what actions should be taken.

(Note: *See* program materials and tools in session on "*Developing And Implementing A Compliance Calendar And Other Tools"* for a COSO- based compliance risk assessment tool.