AUDIT COMMITTEE INTERACTION WITH INTERNAL AUDIT AND CORPORATE COMPLIANCE AND ETHICS, AND RELATED TOPICS

(These materials are updated periodically–this version is dated 11.01.08)

Dave Tate, CPA, Esq.
San Francisco, CA
http://davidtate.us
tateatty@yahoo.com

CONTENTS:

I. INTRODUCTION
II. INTERNAL AUDIT
III. CORPORATE COMPLIANCE AND ETHICS; FEDERAL SENTENCING GUIDELINES
IV. ENTERPRISE RISK MANAGEMENT
V. THE FOREIGN CORRUPT PRACTICES ACT
VI. INTERNAL INVESTIGATIONS AND REVIEWS

I. INTRODUCTION

This paper is part of a series of papers that cover essential public and private company audit committee functions and responsibilities in a quick-read summary format. This paper primarily covers internal audit, corporate compliance and ethics, federal sentencing guidelines, enterprise risk management and The Foreign Corrupt Practices Act. Audit committees are regulated or impacted by numerous statutes, cases, rules, regulations and pronouncements. While some audit committee responsibilities are mandatory, other committee functions and responsibilities are discretionary depending on the circumstances. Although an increasing number of the functions and responsibilities are specified by statute, rule or regulation, an audit committee's standard of care remains significantly dependent on due diligence and prudent judgment. Additional materials can be found at http://davidtate.us.

Contact me if you are looking for a speaker on these or other audit committee topics, or if you are looking for help with audit committee activities including help with an audit committee evaluation process.

The materials in this paper do not provide legal, accounting or other professional advice. These materials are not a solicitation for work. The materials do not apply to any particular person, entity, event, transaction or situation. These materials are only a summary. It should be clear that if you have questions or issues about a particular specific situation, you need to seek your own legal, accounting or other professional assistance, and you absolutely should not rely on the summary materials in this paper. The materials in this paper are update and changed periodically, and cannot be relied upon for that additional reason.

II. INTERNAL AUDIT

The Institute of Internal Auditors (http://www.theiia.org) provides that "internal audit is an independent, objective assurance and consulting activity designed to add value and improve an organization's

operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. Performed by professionals with an in-depth understanding of the business culture, systems, and processes, the internal audit activity provides assurance that internal controls in place are adequate to mitigate the risks, governance processes are effective and efficient, and organizational goals and objectives are met.

The internal audit activity evaluates risk exposures relating to the organization's governance, operations and information systems, in relation to:

-Effectiveness and efficiency of operations.

-Reliability and integrity of financial and operational information.

-Safeguarding of assets.

-Compliance with laws, regulations, and contracts.

Based on the results of the risk assessment, the internal auditors evaluate the adequacy and effectiveness of how risks are identified and managed in the above areas. They also assess other aspects such as ethics and values within the organization, performance management, communication of risk and control information within the organization in order to facilitate a good governance process.

The internal auditors are expected to provide recommendations for improvement in those areas where opportunities or deficiencies are identified. While management is responsible for internal controls, the internal audit activity provides assurance to management and the audit committee that internal controls are effective and working as intended. The internal audit activity is led by the chief audit executive ("CAE"). The CAE delineates the scope of activities, authority, and independence for internal auditing in a written charter that is approved by the audit committee."

The fact is that the audit committee significantly relies on other people to help it perform its duties. An internal audit function can be one of the best resources available to help the audit committee perform its function. Pursuant to NYSE Listed Company Manual §303A.07, each listed company must have an internal audit function; however, it is not just NYSE listed companies that have or should consider having an internal audit function or department. Throughout this paper references are made to the audit committee's governace over and interactin with the internal audit function. Certainly the audit committee members of each public company should consider the value of having an internal audit function to assist the committee members in satisfying their functions and responsibilities.

The nature of the audit committee function is evolving. It is now standard that the person serving in the position of the chief audit executive functionally reports directly to the audit committee, and administratively, or by dotted line to the CEO, CFO or other compliance officer.

NYSE Listed Company Manual §303A.07 provides that the audit committee must have an audit committee charter that addresses the committee’s purpose which in part must be to oversee the performance of the company’s internal audit function; that the audit committee shall meet separately

and periodically with management, with the internal auditors; and that the audit committee shall report regularly to the board of directors, and review with the full board any issues that arise with respect to the quality or integrity of the company's financial statements, the company's compliance with legal or regulatory requirements, the performance and independence of the company's outside auditor, and the performance of the internal audit function.

Commentary to §303A.07 states that the audit committee should evaluate the outside auditor's qualifications, performance and independence, and that in doing so the audit committee also should take into consideration the opinions of management and the company's internal auditors, and further provides in part that the audit committee may want to review with the auditor are the responsibilities, budget and staffing of the company's internal audit function.

Pursuant to SAS 112, an ineffective internal audit function or risk assessment function for a company for which those functions are important to the monitoring or risk assessment component of internal control should be regarded as at least a significant deficiency and a strong indicator of a material weakness in internal control.

PCAOB Auditing Standard No. 5 directs that the outside auditor should use a top-down approach to the audit of internal control over financial reporting, beginning at the financial statement level and company-level controls, and that company-level controls in part include controls to monitor other controls, including activities of the internal audit function, the audit committee, and self-assessment programs.

Internal audit has no direct operational responsibility or authority over any of the activites that it reviews. Internal audit does not develop or install systems or procedures, prepare records, or engage in any activity which would normally be audited. In that sense, internal audit is independent, although still an internal function of the company.

Internal audit carries out assigned responsibilities to examine and evaluate the adequacy and effectiveness of the organization's governance, risk managment processes (enterprise risk management is discused in other materials written by the author), system of internal control, monitoring processes, and quality of performance to achieve the organization's stated goals and objectives. Internal audit also can act as an advisor and provide critical services that are integrated into the audit committee's activities and processes. Internal audit should have direct reporting authority and access to the audit committee and/or the committee's chair.

The chief audit executive usually submits to the audit committee and senior management a report of planned audit work, staffing, and a budget for the fiscal year, or more often. The audit work planned is developed using a priority, risk-based methodology. Internal audit should regularly report to the audit committee significant risk exposures and control issues, corporate governance issues, and other requested information.

Pursuant to the Institute of Internal Auditors, to establish an effective relationship between the audit committee and internal audit, the chief audit executive should,

-Communicate with the audit committee and management regularly on risks faced by the organization;

-Help the audit committee ensure that the committee's charter, activities and processes are appropriate;

-Ensure that internal audit's charter, role and activities are clearly understood and responsive to the needs of the audit committee and the board;

-Maintain open and effective communications with the audit committee and the committee's chair; and

-Provide training, when appropriate, to the members of the audit committee on topics of risk and internal control.

There needs to be a direct channel of communication between the chief audit executive and the audit committee. Typically the chief audit executive may attend portions of audit committee meetings to report on the results of major audits and key audit findings, and discuss internal audit's observations on risk and internal controls. The relationship can be strengthened by out-of-session communications between the chief audit executive and the audit committee chair and/or audit committee about critical circumstances or events. The chief audit executive and the audit committee should meet periodically without management or the outside auditor present.

The scope of internal audit may include:

-Reviewing the reliability and integrity of financial and operating information and the means used to identify, measure, classify, and report that information;

-Reviewing the systems established to ensure compliance with policies, plans, operations, and reports and whether the organization is in compliance;

-Reviewing the means of safeguarding assets and verifying the existence of assets;

-Reviewing operations and programs to ascertain whether results are consistent with objectives and goals, and whether operations and programs are being carried out as planned;

-Reviewing specific operations at the request of the audit committee or management as appropriate;

-Monitoring and evaluating the effectiveness of the organization's risk management and internal control systems;

-Reviewing the quality of the performance of the outside auditor and the degree of coordination between the outside auditor and internal audit; and

-Helping the audit committee to satisfy the committee' functions and responsibilities.

Following the conclusion of each audit assignment a report should be prepared and issued by the chief audit executive to the audit committee, and distributed as appropriate. As appropriate, the report may include management's responses and corrective actions to be taken in regarding to the specific findings and recommendations. If management's responses and corrective actions are not included in the report,

as appropriate management should be provided time to provide written responses to internal audit, the audit committee, and other people on the distribution list. If the audit committee desires, internal audit should be responsible for appropriate follow up until the open issues are cleared.

Each member of the audit committee has unique experiences and knowledge. Thus, to a certain extent, internal audit can provide benefit and help to the individual audit committee members in similar, but also different individual ways. An audit committee member should be looking to internal audit for assistance in helping both the overall committee and the individual member satisfy the audit commitee's functions and responsibilities. By understanding the audit committee's functions and responsibilities, and the experiences, knowledge, strengths and weaknesses of the individual committee members, internal audit can best work to develop a plan of action that helps the audit committee to fulfill its functions and responsibilities, and help achieve the organizational objectives. Developing the plan of action is an interactive process involving the audit committee, internal audit, and management.

At the end of the day, in addition to satisfying his or her functions and responsibilities, an audit committee member should want to ensure that no significant, arguably avoidable, unfavorable ("bad") events occur for which it can be said that he or she might have had oversight responsibilities, and that if such an unfavorable event does unfortunately occur, he or she can establish that it occured despite his or her verifyable, diligent, best practice efforts and activities as an audit committee member. Internal audit can be instrumental in helping the audit committee members achieve that level of comfort.

III. CORPORATE COMPLIANCE AND ETHICS; FEDERAL SENTENCING GUIDELINES

Organizations, such as corporations, can be guilty of criminal conduct, just like individuals. The measure of an organization's punishment for felonies and certain misdemeanors is governed by Chapter Eight of the U.S. Federal Sentencing Guidelines. Organizations cannot be imprisoned like people, but organizations can be fined, sentenced to probation, ordered to make restitution and issue public notices of conviction, and exposed to forfeiture statutes.

Some of the common offenses committee by organizations are fraud, environmental waste, tax offenses, antitrust offenses, and food and drug violations.

An organization can be found criminally liable whenever an employee of the organization commits an act within the apparent scope of his or her employment, even if the employee acted contrary to company policy or instructions. An organization also can be held criminally liable for any of its employees' illegal actions even if it made reasonable efforts to prevent the wrongdoing. Recognizing this fact, in enacting the sentencing guidelines, the U.S. Sentencing Commission has attempted to lessen some of the harshest aspects of potential liability for organizations that can demonstrate that they have enacted appropriate and effective preventative, deterrent and reporting compliance programs.

The Federal Sentencing Guideline Manual at Chapter 8, Part B, §8B2.1, Effective Compliance and Ethics Program, specifies that to have an effective compliance and ethics program, an organization shall:

-Exercise due diligence to prevent and detect criminal conduct;

-Promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law; and

-Design, implement, and enforce its compliance and ethics program so that it is generally effective in preventing and detecting criminal conduct. USSG §8B2.1(a).

Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law minimally require that:

-The organization establishes standards and procedures to prevent and detect criminal conduct.

-The organization effectively communicates and promotes its standards, expected manner of conduct, procedures and other aspects of its compliance and ethics program throughout the organization including, but not necessarily limited to, all levels of employees, officers, managers, supervisors and directors.

-The organization's governing authority is knowledgeable about the content and operation of the compliance and ethics program and exercises reasonable oversight with respect to the implementation and effectiveness of the program.

-High-level personnel of the organization ensure that the organization has an effective compliance and ethics program, and are assigned overall responsibility for the program.

-Within the organization a specific person is, or specific people are, delegated day-to day operational responsibility for the compliance and ethics program, with adequate resources, appropriate authority and direct access to the governing authority, and shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. USSG §§8B2.1(b)(1)-(2).

-The organization takes reasonable steps:

-To ensure that the compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

-To evaluate periodically the effectiveness of the compliance and ethics program; and

-To have and publicize a system, which may include mechanisms that allow for anonymity and confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

-The organization's compliance and ethics program is promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

-After criminal conduct has been detected, the organization takes reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

-In implementing the program, the organization periodically assesses the risk of criminal conduct and takes appropriate steps to design, implement, or modify each requirement to reduce the risk of criminal conduct identified through the process. USSG §§8B2.1(b)(5)-(7); USSG §8B2.1(c).

The term "governing authority" means the (1) the board of directors; or (2) if the organization does not have a board of directors, the highest-level governing body of the organization. USSG §8B2.1, Commentary Definitions.

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; an individual in charge of a major business or functional unit of the organization, such as sales, administration, or finance; and an individual with a substantial ownership interest. USSG §8B2.1, Commentary Definitions, and §8A1.2, Commentary.

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. The term includes high-level personnel of the organization, individuals who exercise substantial supervisory authority (e.g., a plant manager, a sales manager), and any other individuals who, although not a part of an organization's management, nevertheless exercise substantial discretion when acting within the scope of their authority (e.g., an individual with authority in an organization to negotiate or set price levels or an individual authorized to negotiate or approve significant contracts). Whether an individual falls within this category is determined on a case-by-case basis. USSG §8B2.1, Commentary Definitions.

In the landmark case *In re Caremark International, Inc. Derivative Litigation* (Del. Ch. 1996) 698 A.2d 959-968-69, the court held that to satisfy a director's duty to monitor and of oversight, the director's obligation includes a duty to attempt in good faith to assure that the corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards. Thus, under some circumstances a board may not escape liability under the business judgment rule unless it takes some actions to implement a program to detect potential violations of law or corporate policy and exercises a duty of oversight. A small but growing number of cases have reaffirmed the same or similar principle that was recognized in *Caremark*. See, *McCall v. Scott* (6th Cir. 2001) 239 F. 3d 871; *In re Abbot Laboratories Derivative Shareholder Litigation* (7th Cir. 2003) 325 F. 3d 795; *Miller v. Foodservice, Inc.* (D. Md. 2005) 361 F.Supp.2d 470; and *Stone v. Ritter* (Del. 2006) 911 A. 2d 362.

As stated above, for a compliance and ethics program to be effective, the Federal Sentencing Guidelines require that within the organization a specific person is, or specific people are, delegated day-to day operational responsibility for the program, with adequate resources, appropriate authority and direct access to the governing authority. In many organizations that person may hold the title chief

compliance or chief compliance and ethics officer. The compliance and ethics function may also be some manner interconnected with the internal audit function. For an additional discussion about the compliance and ethics function, and resource materials, you can refer to the Society of Corporate Compliance and Ethics at http://www.corporatecompliance.org. A properly structured and functioning compliance and ethics function is another valuable resource to assist the audit committee members in satisfying their due diligence and oversight obligations.

IV. ENTERPRISE RISK MANAGEMENT

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines enterprise risk management as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The definition reflects certain fundamental concepts. Enterprise risk management is:

-A process, ongoing and flowing through an entity;

-Effected by people at every level of an organization;

-Applied in strategy setting;

-Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk;

-Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite;

-Able to provide reasonable assurance to an entity's management and board of directors; and

-Geared to achievement of objectives in one or more separate but overlapping categories." See also, http://www.coso.org.

Enterprise risk management focuses on the achievement of objectives established by the business entity such as performance and profitability targets--to help the business get to where it wants to go--and avoid loss of resources, pitfalls and surprises along the way. Internal control is a component of enterprise risk management.

Various authorities require that the audit committee oversee financial internal controls, the outside auditor, and internal audit. Although no authority expressly requires the audit committee to exercise oversight over enterprise risk management as that term is broadly defined by COSO, in pertinent part, NYSE Listed Company Manual §303A.07 requires the audit committee's charter to address the committee's duties and responsibilities including the responsibility to discuss policies with respect to risk assessment and risk management. Commentary to §303A.07 states that the CEO and senior

management should assess and manage the company's exposure to risk, but that the audit committee must discuss guidelines and policies to govern the process by which this is done. The audit committee should discuss the company's major financial risk exposures and the steps management has taken to monitor and control exposures. If a company manages and assesses its risk through mechanisms other than the audit committee, the processes that the company has in place should be reviewed in a general manner by the audit committee, but those mechanisms need not be replaced by the audit committee. Various audit committees have also included elements of risk management oversight responsibilities in their respective charters.

In pertinent part, copies of the NASDAQ and NYSE audit committee charters for April 16, 2008 and January 31, 2008, respectively, are reproduced at the end of these materials—both charters include aspects of risk management oversight. With respect to risk oversight the NASDAQ charter states:

"The Committee should take the appropriate actions to set the overall corporate policy for quality financial reporting, sound business risk management practices, and ethical behavior"; and

"Also, the Committee shall discuss with management, the internal auditors, and the independent auditors the adequacy and effectiveness of the NASDAQ OMX Group's internal controls, including systems to monitor and manage business risk, and legal and ethical compliance programs and financial reporting."

With respect to risk oversight the NYSE charter states:

"The Audit Committee ("Committee") is appointed by the Board of Directors ("Board") of NYSE Euronext ("Company") and charged with assisting the Board in its oversight of: (a) the integrity of the Company's financial statements and internal controls, (b) compliance with legal and regulatory requirements, including the Company's ethical standards and policies, (c) the qualifications, independence and performance of the Company's independent auditor, (d) the process relating to internal risk management and control systems, (e) the performance of the Company's internal audit function and its independent auditors, and (f) the Company's tax policy; and preparing the Audit Committee report to shareholders for inclusion in the Company's annual proxy statement";

"[The committee shall] discuss the Company's major financial and other significant risk exposures or deficiencies, and the steps management has taken to monitor and control or mitigate such exposures and deficiencies. Discuss the Company's risk assessment and risk management policies"; and

"[The committee shall] periodically assess whether the Company has implemented the appropriate internal risk management and internal control culture."

COSO further details enterprise risk management as:

1. Enterprise risk management encompasses:

-*Aligning risk appetite and strategy* – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.

-*Enhancing risk response decisions* – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.

-*Reducing operational surprises and losses* – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.

-*Identifying and managing multiple and cross-enterprise risks* – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.

-*Seizing opportunities* – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.

-*Improving deployment of capital* – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

2. Within the context of an entity's established mission or vision, management establishes strategic objectives, selects strategy, and sets aligned objectives cascading through the enterprise. This enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:

-*Strategic* – high-level goals, aligned with and supporting its mission.

-*Operations* – effective and efficient use of its resources.

-*Reporting* – reliability of reporting.

-*Compliance* – compliance with applicable laws and regulations.

3. Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. These components are:

1. Internal Environment – management sets a risk philosophy and establishes the entity's risk culture and risk appetite.

2. Objective Setting – management considers its risk appetite in the setting of objectives.

3. Event Identification – management identifies the events, both internal and external, that present risk or opportunity to the organization. Opportunities are channeled back to strategy and objective-setting processes.

4. Risk Assessment – the likelihood and impact of risks are assessed to clarify the extent to which they might impact objectives. This employs a combination of qualitative and quantitative methodologies and forms a basis for the management of those risks.

5. Risk Response – management makes the decision as to whether the risk should be avoided, accepted,

reduced, or shared; and then develops a set of actions to align the risks with the organization's risk tolerance.

6. Control Activities – policies are established to ensure management's risk responses are carried out effectively.

7. Information and Communication – thorough and timely communication takes place to ensure roles and responsibilities can be performed effectively in the process of identifying, assessing, and responding to risk.

8. Monitoring – ongoing ERM monitoring occurs, and modifications are made as warranted.

When designing and implementing a program of enterprise risk management the company begins by taking an inventory of risk factors pertaining to each driver of success, which may, for example, include financial (including market, credit, and liquidity risks and fraud), operational (including product risks, distribution channels, information security, and business continuity), business (including technological disruption, disintermediation, and competition changes), governance (CEO succession and compliance with laws and regulations), and human resource (employee relations and business conduct and ethics) risks.

Pursuant to the Institute of Internal Auditors (http://www.theiia.org), "[a]lthough the internal auditors do not have primary responsibility for ERM implementation or maintenance, they play an important role in monitoring, examining, evaluating, and reporting on ERM. They also assist management and the board or audit committee by recommending improvements to ERM processes. Internal audit activities may include:

• Reviewing the adequacy and effectiveness of the entity-wide ERM processes (including the processes to identify, analyze, manage, and report on risks) and providing recommendations for improvement.

• Reviewing critical control systems and risk management processes and responses for adequacy and effectiveness.

• Providing advice in the design and improvement of control systems and risk mitigation strategies.

• Implementing a risk-based approach to planning and executing the internal audit process.

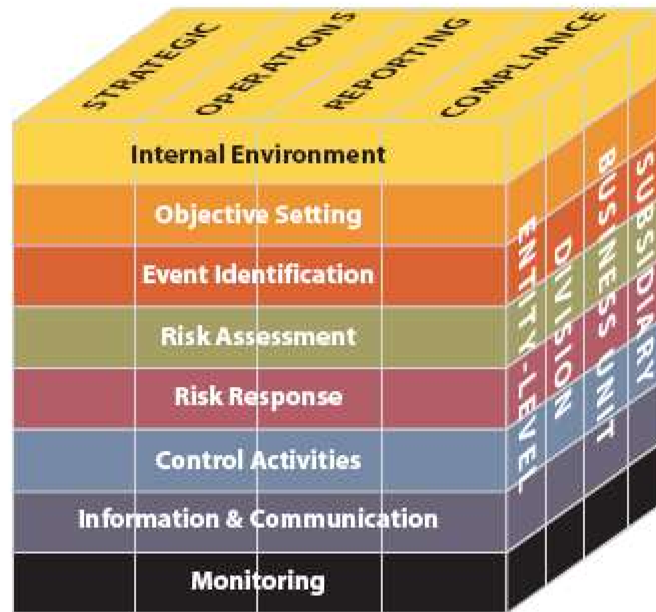
• Ensuring that internal audit resources are directed at those areas most important to the organization.

• Challenging the basis of management's risk assessments and evaluating the adequacy and effectiveness of risk-treatment strategies and the reliability of management's assurances.

• Providing assurances on the completeness, accuracy, and appropriateness of management's classification and reporting of risks.
• Facilitating ERM workshops."

The relationship between objectives, which are what an entity strives to achieve, and enterprise risk

management components, which represent what is needed to achieve them, has been depicted in a three-dimensional matrix, in the form of a cube. The four objectives categories – strategic, operations, reporting, and compliance – are represented by the vertical columns, the eight components by horizontal rows, and an entity's units by the third dimension. This depiction portrays the ability to focus on the entirety of an entity's enterprise risk management, or by objectives category, component, entity unit, or any subset thereof. The eight components will not function identically in every entity. Application in small and mid-size entities, for example, may be less formal and less structured.



V. <u>THE FOREIGN CORRUPT PRACTICES ACT</u>

The Foreign Corrupt Practices Act (15 U.S.C. §§ 78dd-1, et seq.) is a U.S. federal law that is comprised of two primary provisions: (1) the accounting record keeping and internal control provision, and (2) the antibribery provision.

The accounting record keeping and internal control provision (15 U.S.C. § 78m) was intended to compliment or work in tandem with the antibribery provision, but in fact is perhaps more broad in application because it applies to all companies whose securities are listed on a U.S. stock exchange, and is enforced by the Securities and Exchange Commission. Generally, the accounting provision was intended to require covered companies to keep accounting records that accurately reflect the transactions of the company, and to devise and maintain an adequate system of internal accounting control. The accounting provision is intended to address three areas of concern: (1) situations where transactions are not recorded; (2) situations where transactions are falsely recorded; and (3) situations where transactions are recorded correctly but are also misrepresented in substance (e.g., where a payment is correctly recorded is being made to the appropriate person but with substantial certainty that

person then will transfer the payment to another person for an unlawful purpose.

The FCPA does not mandate the specific elements or form of internal control system. The Act requires reasonable detail and assurances. "Materiality" is not a minimum threshold safe harbor, not is lack of knowledge or substantial certainty.

The accounting and internal control provision requires covered companies to:

> -Keep books, records and accounts that, in reasonable detail, accurately and fairly reflect the company's transactions; and
>
> -Devise and maintain a system of internal control sufficient to provide reasonable assurance that:
>
> > -Transactions are authorized by management;
> >
> > -Transactions are recorded to permit preparation of financial statements in conformity with Generally Accepted Accounting Principles and other applicable standards, and to maintain accountability over assets;
> >
> > -Access to assets is permitted only with management authorization; and
> >
> > -Recorded accountability for assets is periodically reconciled with existing assets.

The Act also requires that a covered company that holds sufficient voting power over another company, including a foreign corporation, comply with the Act's provisions with respect to the other company. Sufficient voting power is present when a covered company controls 50 percent or more of the voting securities of a subsidiary. However, depending on the facts and circumstances, sufficient voting power also can be present when a covered company controls between 20 and 50 percent of a subsidiary–subject to contrary proof by the covered company that its ownership does not constitute control.

Generally, the antibribery provision makes it unlawful for (1) U.S. firms and persons, and certain foreign issuers of securities, to make a corrupt payment (e.g., a bribe) to a foreign official for the purpose of obtaining or retaining business, and (2) foreign firms and persons to act in furtherance of a corrupt payment while in the United States.

The Department of Justice is responsible for criminal and civil enforcement with respect to domestic concerns, foreign companies and nationals. The SEC is responsible for civil enforcement of the antibribery provisions with respect to issuers.

Establishing a violation of the antibribery provision involves five basic elements.

<u>To whom the Act applies</u>. The Act applies to any individual, firm, officer, director, employee, or agent of a firm and any stockholder acting on behalf of a firm. Individuals and firms may also be penalized if they order, authorize, or assist someone else to violate the antibribery provisions, or if they conspire to

violate those provisions.

United States jurisdiction over improper payments to foreign officials depends on whether the violator is an "issuer," a "domestic concern," or a foreign national or business.

An "issuer" is a corporation that has issued securities that have been registered on a U.S. exchange, or that is required to file periodic reports with the SEC.

A "domestic concern" is any person who is a citizen, national, or resident of the United States, or any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship which has its principal place of business in the United States, or which is organized under the laws of a State, territory, possession or commonwealth of the United States.

For acts that occur within the territory of the United States, issuers and domestic concerns are liable if they perform an act in furtherance of a corrupt payment to a foreign official using the U.S. mails or other means of interstate commerce, including, for example, telephone calls, faxes, wire transfers, and interstate or international travel.

Issuers and domestic concerns may also be liable for acts performed in furtherance of a corrupt payment made outside the United States. Thus, a U.S. company or national may be held liable for a payment authorized by employees or agents operating outside the United States, using money from foreign bank accounts, and without any involvement by a person located in the United States.

The FCPA was expanded in 1998 to include jurisdiction over foreign companies and people who cause, directly or through agents, an act in furtherance of the corrupt payment to take place in the territory of the United States, whether or not the act makes use of the U.S. mails for other means of interstate commerce.

U.S. parent companies also may be held liable for the acts of foreign subsidiaries, the activities of which they authorize, direct, or control, as can U.S. citizens or residents ("domestic concerns) who were employed by or acting on behalf of the foreign subsidiary.

Wrongful intent or purpose. The person making or authorizing the payment, offer, promise or inducement must have a wrongful or corrupt intent or purpose, and the payment must be intended to induce or influence the foreign official who is receiving the payment to misuse his or her official position, to breach his or her lawful duty, to make a decision, or to otherwise act to direct business wrongfully to the payer or to any other person, or to obtain any improper advantage, or to induce the foreign official to use his or her influence improperly to affect or influence any act, event or decision. However, the intended corrupt act does not have to actually succeed in purpose for a violation to occur. Thus, an offer or promise alone can be a violation.

Payment. The Act prohibits paying, offering, promising to pay (or authorizing to pay or offer) money, or anything of value.

The Act also prohibits corrupt payments made through an “intermediary,” also referred to as third party payments. The “intermediary” is the recipient who is making the payment to the foreign official. It is

unlawful to make a payment to a third party, while "knowing" that all or a portion of the payment will go directly or indirectly to a foreign official. The term "knowing" includes conscious disregard and deliberate ignorance. In other words, it is not necessary to show actual knowledge for there to be a violation. Thus, U.S. companies should exercise due diligence, investigate other entities and persons with whom they interact, react to and investigate "red flags," and establish proper and prudent compliance staffing, procedures and processes. See also the overview of the FCPA accounting record keeping and internal control provision.

The recipient. The Act applies only with respect to corrupt payments to a foreign official, a foreign political party or party official, or any candidate for foreign political office.

A "foreign official" means any officer or employee of a foreign government, a public international organization, or any department or agency thereof, or any person acting in an official capacity, regardless of rank or position. The Act focuses on the purpose of the payment, not the duties of the recipient (see however, the "facilitating" payment exception discussed below). Whether or not a person is a "foreign official" can be difficult to determine. Consider, for example, royal family members, an official of a state-owned business, or members of a legislative body.

The business purpose test. The Act prohibits payments made in order to assist the firm in obtaining or retaining business for or with, or directing business to, any person. You should be aware that the term "obtaining or retaining business" is broadly interpreted for enforcement purposes. Additionally, the business to be obtained or retained does not need to be with a foreign government or foreign government instrumentality.

The exception for facilitation payments for routine governmental actions. The Act provides that there is no violation of the antibribery provision for payments made to facilitate or expedite performance of a "routine governmental action." The Act lists the following examples: obtaining permits, licenses, or other official documents; processing governmental papers, such as visas and work orders; providing police protection, mail pick-up and delivery; providing phone service, power and water supply, loading and unloading cargo, or protecting perishable products; and scheduling inspections associated with contract performance or transit of goods across country. Other similar actions might also be excluded. However, the "routine governmental action" exclusion does not include or apply to any decision made by a foreign official to award new business or to continue business with a particular party.

Possible affirmative defenses available to a person charged with a violation:

In addition to being able to prevail on one or more of the five basic elements discussed above, there are a couple of affirmative defenses that an accused defendant may be able to argue and establish for the payment or action:

-The payment was lawful under the written laws of the foreign country. Obviously, prior to making a potentially improper payment you should seek the advice of counsel regarding the "legality" of the payment under the laws of the foreign country; and

-The money was spent as part of demonstrating a product or performing a contractual obligation.

Criminal sanctions, penalties and jail time. Criminal punishment for violation of the FCPA antibribery provisions are as follows: corporations and other business entities may be fined up to $2,000,000; and officers, directors, stockholders, employees, and agents may be fined up to $100,000 and imprisonment for up to five years. Additionally, under the Alternative Fines Act the fine may increased up to twice the benefit that the defendant sought to obtain by making the corrupt payment. Fines imposed on individuals cannot be paid by the individual's employer or principal.

Civil fines and injunctive remedies:

The Attorney General or the SEC may bring a civil action seeking a fine up to $10,000 against any firm, officer, director, employee, or agent of a firm, or any stockholder acting on behalf of the firm, for violation of the antibribery provisions. Additionally, in an action brought by the SEC, the court may impose an additional fine not to exceed the greater of the gross amount of the monetary gain to the defendant as a result of the violation, or a specified dollar limitation based on the egregiousness of the violation, ranging from $5,000 to $100,000 for a natural person and $50,000 to $500,000 for any other person.

The Attorney General or the SEC may also bring a civil action to enjoin (i.e., stop or prevent) any act or practice of a firm whenever it appears that the firm, or an officer, director, employee, agent, or stockholder acting on behalf of the firm, is in violation, or about to be, in violation of the antibribery provisions.

Private cause of action. A private cause of action may also be brought against the wrongful firm or person, such as by an aggrieved business competitor, for treble damages under the Racketeer Influenced and Corrupt Organizations Act (RICO), and under various other federal or state laws.

Additional possible penalties and sanctions:

A person or firm found in violation of the FCPA may be barred from doing business with the Federal government. An indictment can lead to the suspension of the right to do business with the government.

A person or firm that is guilty of violating the FCPA can be held ineligible to receive export licenses.

The SEC may suspend or bar a person or firm from the securities business and impose civil penalties on firms or persons in the securities business for violation of the FCPA.

The Commodity Futures Trading Commission and the Overseas Private Investment Corporation may suspension or debarment a person or firm from agency programs for violation of the FCPA.

And, a payment made to a foreign government official that is unlawful under the FCPA cannot be deducted for tax purposes.

VI. INTERNAL INVESTIGATIONS AND REVIEWS

Internal corporate investigations and reviews have become much more common, particularly in

situations involving possible unlawful activities or unacceptable risk exposure, including both quantitative and qualitative risk. The circumstances in which an investigation or review might be warranted are numerous and diverse, including, for example, situations involving corporate derivative litigation, or possible fraud, accounting impropriety, misappropriation, misrepresentation, workplace discrimination or harassment, bribery, and other unlawful acts. Members of the audit committee and other independent directors often are naturally considered to serve on investigation or review committees.

It is beyond the scope of this paper to discuss this topic in detail. However, members of a special committee or panel should consider the sufficiency of their own independence and qualifications to serve, and the independence and qualifications of counsel and consultants that they engage for representation and assistance. There have been several recent cases involving special committee member independence issues. A prospective special committee member who lacks independence from either the person or the situation being investigated or reviewed is incompetent to serve as a committee member. When evaluating the issue of independence, courts now are evaluating all direct and indirect relationships and associations, including not only business and family relationships, but also social relationship activities including clubs and other associations.

* * * * *