

# Nonprofit Board Standard of Care, Risk Management, and Audit Committee Responsibility (Updated May 19, 2011)

David Tate, Esq. (San Francisco), <http://davidtate.us> (additional board and committee materials)  
Tate's Blog: Law – Governance – Risk - Business, <http://davidtate.wordpress.com>  
California Estate & Trust Litigation, <http://californiaestatetrust.wordpress.com>

The following materials were written for nonprofit board members in general, but also include an overview of important provisions of the Nonprofit Integrity Act which applies to nonprofits in California. Please feel free to pass this paper to other people who would be interested.

## Overview of Contents:

1. The Business Judgment Standard of Care and Fiduciary Duty
2. The California Nonprofit Integrity Act
3. Risk Management
4. Outside Auditor Communications with the Board or Audit Committee
5. Compliance Programs—Key Components
6. Annual Self-Evaluation, Board and Committees (in a word, yes, do it)

The obligatory disclaimer: These materials do not provide legal, accounting or other professional advice, and are not a solicitation for work. These materials do not apply to any particular person, entity, event, transaction or situation. As these materials are only a summary of technical and detailed subject matters, and are updated and changed periodically, 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 these summary materials to guide your situation or your actions.

## **1. The Business Judgment Standard of Care and Fiduciary duty**

### **The Business Judgment Rule**

The business judgment rule provides a director with a defense to personal liability, holding that as a general principle of law, a director, including a director who serves as a member of a board committee, who satisfies the business judgment rule has satisfied his or her duties. Thus, the business judgment rule provides one general standard of care, although other standards may also apply. In some states the business judgment rule is codified by statute, such as Cal. Corp. Code §309 for California corporations; in other states the rule is established by case law. The rule also applies to directors as board committee members.

In summary, as a general principle the business judgment rule provides that a director should undertake his or her duties:

- In good faith, with honesty and without self-dealing or improper personal benefit;
- In a manner that the committee member believes to be in the best interests of the corporation and its shareholders; and
- With the care, including reasonable inquiry, that an ordinarily prudent person in a like position would use under similar circumstances.

### **Reliance Upon Other People Under the Business Judgment Rule**

In the course and scope of performing his or her duties, a director must necessarily obtain information from and rely upon other people. The director is not involved in the day-to-day operations of the business. The director provides an oversight function. Pursuant to the business judgment rule, a director is entitled to rely on information, opinions, reports or statements, including financial statements and other financial data, prepared or presented by any of the following:

- Officers or employees of the corporation whom the director believes to be reliable and competent in the relevant matters;
- Legal counsel, independent accountants or other persons as to matters that the director believes are within the person's professional or expert competence; or
- A committee of the board on which the director does not serve, as to matters within that committee's designated authority, so long as the director acts in good faith, after reasonable inquiry as warranted by the circumstances, and without knowledge that would cause reliance to be unwarranted.

### **The Business Judgment Rule for California Nonprofits**

California Corporations Code §5231, for nonprofit public benefit corporations, and §7231, for nonprofit mutual benefit corporations, in pertinent part provide that:

- (a) A director shall perform the duties of a director, including duties as a member of any committee of the board upon which the director may serve, in good faith, in a manner such director believes to be in the best interests of the corporation and with such care, including reasonable inquiry, as an ordinarily prudent person in a like position would use under similar circumstances.

### **Reliance Upon Other People Under the Business Judgment Rule for California Nonprofits**

California Corporations Code §5231, for nonprofit public benefit corporations, and §7231, for nonprofit mutual benefit corporations, in pertinent part provide that:

(b) In performing the duties of a director, a director shall be entitled to rely on information, opinions, reports or statements, including financial statements and other financial data, in each case prepared or presented by: (1) one or more officers or employees of the corporation whom the director believes to be reliable and competent in the matters presented; (2) counsel, independent accountants or other persons as to matters which the director believes to be within such person's professional or expert competence; or (3) a committee of the board upon which the director does not serve, as to matters within its designated authority, which committee the director believes to merit confidence, so long as, in any such case, the director acts in good faith, after reasonable inquiry when the need therefore is indicated by the circumstances and without knowledge that would cause such reliance to be unwarranted. I have underlined part (3) above because it is important to understand that although a committee to which a task or responsibility has been delegated can do most of the work, the board still should receive a report or recommendation from the committee about the committee's important matters, prudently discuss and inquire about the report and/or recommendations, and approve them or refer for further work or considerations. In other words, the board should not simply punt decision making on important matters to the committee. Further, from a committee member's perspective, to ensure that everyone is on board and on the same page, I would want to make sure that the board is engaged, understands, and approves of the ongoing actions and recommendations of the committee close in time to when those actions and recommendations occur.

Thus, the business judgment standard for a board member of a nonprofit entity requires the director, including a board member who serves on a committee such as an audit committee member, to perform duties loyally, in good faith, without self interest, in a manner that the director believes to be in the best interests of the entity, and with the care, including reasonable inquiry, as an ordinary prudent person in a like position would use under similar circumstances.

A director may not close his or her eyes to what is going on with respect to the entity's business and financial affairs. The director has a duty to be proactive. In relying on the opinions or reports of other people, the director also must act in good faith, conduct reasonable inquiry, and be free of any knowledge that would cause reliance on data and reports received from others to be unwarranted. "In a like position . . . under similar circumstances" refers to the situation that exists at that time, including the individual director's knowledge, experience and expertise. Thus, cases have held that a director who has specific expertise may be expected to use that expertise.

### **The Business Judgment Rule for California Nonprofit Religious Corporations**

California Corporations Code §9241 contains similar language for nonprofit religious corporations. However, §9241 replaces ". . . as an ordinarily prudent person in a like position would use under similar circumstances", with ". . . as is appropriate under the circumstances." Section 9241 also allows for appropriate reliance on "religious authorities and ministers, priests, rabbis, or other persons . . . ."

Of course, the business judgment rule does not tell or educate a director about the specific tasks and actions to undertake to satisfy his or her director fiduciary duties. And except as otherwise discussed herein, those tasks and actions are too diverse and numerous to cover in this

paper; however, in broad terms I characterize a director's duty as being a member of the board which is responsible for oversight of the entity's processes and functions pertaining to strategy, governance, risk, compliance and talent/succession.

## **2. The California Nonprofit Integrity Act**

### **Provisions Pertaining to Financial Statements, Audits and Audit Committees**

The entire board is responsible for oversight of the nonprofit's accounting system and financial statements, including if there is an audit of the financial statements; however, as discussed above, the board may delegate responsibility to a committee such as the audit committee, but with continuing board oversight. If the board delegates responsibilities to the audit committee, the board nevertheless should be informed about the significant activities and recommendations of the audit committee, and should approve those activities and recommendations.

The audit committee is a sub-committee of the board. Members of the audit committee are directors, as a general matter, although in one instance I served as an audit committee chair of a nonprofit but not as an overall board member where the nonprofit wanted a completely independent audit committee chair. As the business judgment rule applies to directors, the rule also provides a general standard of care for audit committee members. For the most part, the activities that a nonprofit audit committee is required to perform are unspecified. The committee's activities will depend on the financial size of the nonprofit, the requirements and expectations of the sources of funds (governmental and non-governmental), the type of outside auditor financial statement evaluation required (i.e., audit, review, compilation), and the expertise of the board and audit committee members. Depending on the circumstances, the financial statements of a nonprofit may require an audit (and possibly an enhanced government OMB A-133, or single audit), review or compilation, or a combination thereof. In California the Nonprofit Integrity Act provides additional statutory requirements.

With respect to nonprofit financial statements, audits and audit committees, the California Nonprofit Integrity Act at Cal. Gov. Code §12586 in part requires:

-Specified charitable corporations, unincorporated associations and trustees, that receive or accrue in any fiscal year gross revenues of \$2,000,000 or more (exclusive of grants from, and contracts for services with, governmental entities for which the government requires an accounting of the funds received) to have annual financial statements, using generally accepted accounting principles, that are audited by an independent certified public accountant (adhering to the Government Auditing Standards, U.S. Comptroller General, Yellow Book) in conformity with generally accepted auditing standards. The Office of the Attorney General has stated that the audited financial statements and notes to the statements must be released to the public, but not the management letter which is not part of the audited financial statements; and that gross revenue is the same as total revenue which appears on Line 12 of IRS Form 990 for public charities, and Line 12, column (a) for private foundations (follow Form 990 and 990PF instructions).

-Each such nonprofit corporation must have an audit committee appointed by the board of directors. The audit committee may include people who are not members of the board, but may not include any members of the staff, including the president, chief executive officer, treasurer or chief financial officer. If the charitable corporation has a finance committee, the audit committee must be separate from the finance committee. Members of the finance committee may serve on the audit committee, but the chair of the audit committee may not be a member of the finance committee, and finance committee members must comprise less than one-half of the membership of the audit committee. The California Office of the Attorney General has stated that there is no requirement that the entity have a particular number of audit committee members—that one member may be sufficient—however, I suggest that there be three or more members to promote expertise, discussion, interaction and feedback.

-Members of the audit committee cannot receive any compensation from the charity in excess of the compensation, if any, received by members of the board for service on the board, and shall not have a material financial interest in any entity doing business with the charity.

-Subject to the supervision of the board, the audit committee shall recommend to the board the retention and termination of the outside auditor, and may negotiate the outside auditor's compensation, on behalf of the board.

-The audit committee shall confer with the outside auditor to satisfy its members that the financial affairs of the nonprofit are in order, and shall review and determine whether to accept the audit, shall assure that any non-audit services performed by the auditing firm conform with standards for auditor independence, and shall approve performance of any non-audit services by the auditing firm.

### **Provisions Pertaining to Executive Compensation**

California Government Code §12586(g) provides that the board of directors of a charitable corporation or an authorized committee of the board shall review and approve the compensation, including benefits, of the president or chief executive officer, and of the treasurer or chief financial officer to assure that it is just and reasonable. The review and approval shall occur initially upon hiring, whenever the term of employment is renewed or extended, and whenever the officer's compensation is modified. Separate review and approval is not required if a modification of compensation extends to substantially all employees. If the charitable corporation is affiliated with other charitable corporations, the review and approval requirements will be satisfied if review and approval is obtained from the board or from an authorized committee of the board of the charitable corporation that makes the retention and compensation decisions about the officer in question.

### **Provisions Pertaining to Fundraising**

California Government Code §§12599 through 12599.7 contain detailed requirements pertaining to certain fundraising activities. The following is an overview of the broad provisions.

- Commercial fundraisers must notify the California Attorney General before starting a solicitation campaign.
- Commercial fundraisers for charitable purposes must report and provide required information to the Attorney General's Registry of Charitable Trusts the start of a solicitation campaign or event not less than 10 working days prior to the start of a solicitation campaign or event or no later than the date on which the campaign begins if the proceeds are intended for victims of disasters or emergencies.
- For every solicitation campaign or event produced by a commercial fundraiser for a charitable organization, there must be a written contract, satisfying specific statutory terms and requirements, between the fundraiser and the charitable organization.
- The contract must be signed by the commercial fundraiser's authorized contracting officer and an official of the charitable organization authorized to sign by the governing board.
- Contracts between commercial fundraisers for charitable purposes and charitable organizations are voidable unless the commercial fundraiser is registered with the Attorney General's Registry of Charitable Trusts prior to the start of the solicitation campaign or event.
- Fundraising counsel must file a notice and provide information with the Attorney General's Registry of Charitable Trusts not less than 10 working days prior to the start of a solicitation campaign or event; or if the purpose is to raise funds for victims of disasters or emergencies, no later than the date on which the campaign begins.
- For every solicitation campaign or event, there must be a written contract, satisfying specific statutory terms and requirements, between the fundraising counsel and the charitable organization. The contract must be signed by the fundraising counsel's authorized contracting officer and an official of the charitable organization authorized to sign by the governing board.
- Charitable organizations have the right to cancel a contract with a commercial fundraiser without liability for 10 days following the date the contract is executed.
- Following the initial 10-day period, charitable organizations have the right to cancel a contract with a commercial fundraiser by providing 30-day notice. The charitable organization is liable for services provided by the commercial fundraiser up to 30 days after the notice is served.
- Following the initial 10-day period, a charitable organization has the right to cancel a contract with a commercial fundraiser without liability if the commercial fundraiser or its agents make material misrepresentations during a solicitation, harm the charitable organization's reputation during a solicitation, or are found to have been convicted of a crime arising from fundraising activities.
- Charitable organizations and commercial fundraisers cannot misrepresent the purpose of a charitable organization, or the nature or purpose of the beneficiary of a solicitation.

- Charitable organizations must establish and exercise control over fundraising activities conducted for their benefit. This obligation includes approving all written contracts and agreements, and assuring fundraising activities are conducted without coercion.
- Charitable organizations cannot enter into any contract or agreement with a commercial fundraiser that is not registered with the Attorney Generals Registry of Charitable Trusts.
- Charitable organizations cannot raise funds for any charitable organization required to be registered with the Attorney Generals Registry of Charitable Trusts unless the charitable organization is so registered or, if not, agrees to register prior to the start of a solicitation.
- Commercial fundraisers must, within five working days, either deposit in a bank account controlled by the charitable organization or deliver personally to the charitable organization all contributions received on behalf of the charitable organization.
- The following acts are prohibited in the planning, conduct or execution of solicitation campaigns:
  - Operating in violation of the Supervision of Trustees and Fundraisers for Charitable Purposes Act (Cal. Gov. Code §12580, et seq.), regulations and orders issued by the Attorney General.
  - Committing unfair or deceptive acts, or engaging in fraudulent conduct.
  - Using any name, symbol, emblem or other information that falsely suggests or implies a contribution is for a particular charitable organization.
  - Falsely telling donors that a contribution is for a charitable organization or will be used for a charitable purpose.
  - Telling donors that a person sponsors, endorses or approves a charitable solicitation when that person has not agreed in writing to have their name used for such a purpose.
  - Misrepresenting that goods or services have endorsements, sponsorships, approvals, characteristics or qualities they do not have.
  - Misrepresenting that a person has endorsements, approvals, sponsorships, status or affiliations they do not have.
  - Misrepresenting that registration with the Attorney Generals Registry of Charitable Trusts constitutes an endorsement or approval by the Attorney General.
  - Representing that a charitable organization will receive an amount greater than the reasonably estimated net proceeds from a solicitation campaign or event.

-Issuing cards, stickers, emblems, plates or other items that can be used for display on a motor vehicle, and which suggest an affiliation with, or endorsement by, public safety personnel or a group of public safety personnel.

-Representing that any portion of contributions solicited by a charitable organization will be given to another charitable organization unless the second charitable organization provides prior written consent for such use of its name.

-Representing that tickets to events will be donated for use by another person or entity unless: the charitable organization or commercial fundraiser has obtained written commitments from charitable organizations that they will accept a specific number of donated tickets; and the donated tickets, when combined with other ticket donations, do exceed either the ticket donations received from charitable organizations or the total capacity of the event site.

-Commercials must maintain for at least 10 years following each solicitation campaign records that contain:

-The date and amount of each cash contribution.

-The date, amount, name and address of each non-cash contributor.

-The name and address of each employee or agent involved.

-Documentation of all revenue received and expenses incurred.

-For each account into which the fundraiser deposited revenue, the account number and name and location of the bank or other financial institution in which the account was maintained.

### **3. Risk Management**

Risk management is a broad subject matter area—there is also no agreed upon definition or process for risk management. While there is no statutory requirement that the nonprofit board exercise oversight of risk management, it is, or is becoming, an accepted practice that risk oversight is a board function. Further, by statute or rule (and/or accepted prudence or standard in the industry) many organizations are now legally or quasi-legally required to exercise formal risk management, with board oversight. It is also not uncommon for the board to delegate risk oversight to a board committee, such as the audit committee; however, the board should remain engaged in risk management oversight even if preliminary responsibility is delegated to a board committee.

What is risk management and what does it include? There is no standard answer, and I am not going to propose one in this paper as that is not the objective here. The objective here is for the organization to consider and improve upon its risk management processes. Risk management is a process—or, more correctly stated, risk management is the processes—that are designed and implemented to help the organization achieve its mission, objectives and strategies—to get to where it wants to go. There can be a tendency to view risk management only

from a liability avoidance perspective. While it is true that in part an aspect of risk management does involve avoiding and handling liability or potential liability situations, risk management is considerably broader in scope. Every organization has risk. Risk is a part of operations and business. Simplistically, there is risk that an event or an objective might not occur or might not occur as desired, when desired or to the extent desired—there is risk that an objective might be exceeded or that an unexpected desirable event occurs or opportunity arises—there is risk that a negative event may occur or that an event or objective will not be achieved. Of course, even with the “best” of risk management processes unexpectancies will occur—the occurrence of an unexpectancy, even a negative unexpectancy, does not mean that someone is at fault or that someone acted improperly.

Some risks and risk management processes are generally shared or similar across organizations and industries, whereas, of course, within organizations and industries risks and risk management processes obviously will vary.

For the purpose of this paper, I am going to use some discussions about enterprise risk management by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Many other professional risk, audit and accounting organizations also regularly publish articles and guidance on risk management. The COSO website is <http://www.coso.org>; additional guidance from COSO can be found at <http://www.coso.org/guidance.htm>.

Pursuant to COSO, 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. COSO describes enterprise risk management as:

- 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.

COSO further details enterprise risk management:

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* – 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 (and I would add a ninth component: *Ongoing Improvement*):

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 risk management monitoring occurs, and modifications are made as warranted.

Enough of the technical discussion, start by listing the organization's mission, objectives, strategies, and projects, and identifying and preparing a list of the risk factors that impact or could impact the organization in relation to achieving its mission, objectives, strategies and projects. The list is endless. First concentrate on what I would consider the most significant ones based on likelihood of occurrence (based on current conditions), likelihood of occurrence within a particular time frame, and potential for impact upon occurrence. An event or unexpectancy with a high likelihood of occurrence, even within the immediate future, but with little likely impact, probably is not as important to deal with right away as an event that has much less likelihood of occurrence (based on current conditions) but that carries the potential for high impact. This gets into the areas of risk assessment, appetite and tolerance. Simplistically, management, with the board's oversight, needs to evaluate not only the risks, but also the organization's level of appetite for the risk, and if there is a further level of tolerance for allowing the risk if the risk begins to exceed the appetite.

For example, by historical standards the likelihood of a gulf oil spill might be slight, but the likely impact could be catastrophic. Of course, historical standards of likelihood could be an erroneous criteria as based on then existing current conditions (i.e., then existing conditions of the equipment being used, training, and safety procedures—possible leading indicators of the risk event), the likelihood of occurrence might have been higher. There would be little or no appetite or tolerance for the occurrence of a significant spill—presumably processes for addressing and preventing the risk of possible spill occurrence, and processes for emergency containment and remedial actions in the event of such a spill would be given the highest priorities.

We don't want to get bogged down here in a technical discussion about risk management as the objective is for the organization to consider and improve upon its risk management processes. For the purpose of an exercise, let's take the example of a hypothetical nonprofit that

provides assistance to people in need who are of low or no income. In part, the nonprofit runs a care clinic. The clinic is staffed with volunteers and with licensed care professionals who provide their time and services at a reduced rate. The nonprofit primarily receives revenue/receipts from money/cash, personal property, real property and estate/trust donations, from a government contract with the city which pays for care provided to qualifying patients who access the clinic, on a per-patient basis—the city contract covers approximately 55% of the cost of operating the clinic (approximately \$1.5 million per year), and from insurance reimbursements. The nonprofit also has a religious basis as an aspect of its mission.

Some of the nonprofit’s objectives that quickly come to mind are: securing stream of revenues/receipts from the various different sources; maintaining quality and timeliness of diagnosis and care provided at the clinic, by practice area, issue presented or other breakdown; proper referral of patients from the clinic to appropriate other care resources; satisfying the specific requirements of the contract with the city; meeting human resources needs and requirements; maintaining the religious aspect of its mission; obtaining appropriate liability/insurance risks and coverage; and proper and timely transaction recording, accounting records, internal controls and financial reports and statements.

The following chart is one possible approach for identifying an objective, strategy and risk process.

Objective	Strategic Initiative / Revised Strategic Initiative	Potential Risk to Strategy	Likelihood of Risk Occurring / Period of Time	Potential Impact if Risk Occurs	Appetite for the Risk	Tolerance for the Risk	Key Risk Indicators	Strategic Response to Risks	People and Processes for Monitoring / Trigger Points	Revised Strategic Response

#### **4. Outside Auditor Communications with the Board or Audit Committee**

The following discussion covers required outside auditor communications with the board and/or audit committee. What an audit is and the information that it provides, in addition to review and compilation services, is discussed in other materials that can be found at <http://davidtate.us>, where you will also find discussions about public companies and public company audit committees, internal controls, fraud, and other related topics.

**Statement on Auditing Standards (SAS) 114**, Auditor's Communications with those Charged with Governance, requires the outside auditor to determine that certain matters relating to the audit of the financial statements are communicated to those charged with governance, which at least includes the audit committee, and may include the board of directors.

-The auditor should have access to the audit committee, the chair and other members of the audit committee should meet with the auditor periodically, and the audit committee should meet with the auditor without management present at least annually.

-The auditor must communicate regarding the auditor's responsibilities under generally accepted auditing standards; the planned scope, performance and timing of the audit (including matters relating to internal controls); the extent that the auditor may use work of internal audit or outside accountants; and significant findings from the audit including but not limited to possible fraud, possible illegal acts, material deficiencies or errors, significant difficulties, qualitative aspects of the accounting practices, uncorrected misstatements, disagreements with management, material corrected misstatements, and other significant issues that come to the auditor's attention.

-Other matters that the auditor may consider discussing with the audit committee include the committee members' views about the company's governance; objectives and strategies relating to risks that may result in material misstatement; internal controls and the committee's oversight of internal controls; the possibility of fraud; communications with regulators; the committee's actions in response to previous communications with the auditor; the committee's actions in response to developments in financial reporting, laws, accounting standards, and corporate governance practices; and other matters that the audit committee members believe are relevant to the audit of the financial statements.

-The auditor should evaluate whether the two-way communication between the auditor and those charged with governance has been adequate for the purpose of the audit. Inadequate two-way communications may indicate an unsatisfactory control environment, which may influence the auditor's assessment of the risks of material misstatement, or the auditor's ability to perform that audit.

**Statement on Auditing Standards 54**, Illegal Acts by Clients, requires that the outside auditor design the audit to provide reasonable assurance that illegal acts that would have a direct and material effect on the financial statements will be detected. SAS 54 further provides that the outside auditor must be sure that the audit committee is adequately informed about illegal acts that come to the auditor's attention, and discusses the possible impact that the discovery of illegal acts may have for reporting and audit opinion purposes.

**Statement on Auditing Standards 99**, Consideration of Fraud in a Financial Statement specifies that:

-The outside auditor must ask management about knowledge or allegations of any fraud or suspected fraud; management's understanding about the risks of fraud; programs and controls established to mitigate specific identified fraud risks, or that prevent, deter, and detect fraud, and how management communicates to employees its views on business practices and ethics; and whether management has reported to the audit committee on how the company's internal control serves to prevent, deter, or detect material misstatements due to fraud.

-The outside auditor also must inquire of the audit committee or the audit committee chair regarding the committee's views about the risks of fraud, the committee's oversight of the entity's assessment of the risks of fraud, the programs and controls the entity has established to mitigate those risks, and whether the committee has any knowledge of any fraud or suspected fraud.

**Statement on Auditing Standards 109**, Understanding the Entity and Its Environment, requires the outside auditor to obtain an understanding of the entity and its environment, including its internal control, to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures. The auditor's understanding of the entity and its environment consists of an understanding of the following aspects:

- The industry, regulatory, and other external factors;
- The nature of the entity;
- Objectives and strategies and the related business risks that may result in a material misstatement of the financial statements;
- The measurement and review of the entity's financial performance; and
- Internal control, which includes the selection and application of accounting policies.

With respect to the relevant industry, regulatory and other factors, the outside auditor should obtain an understanding of factors that include, for example, industry conditions, such as the competitive environment, supplier and customer relationships, and technological developments; the regulatory environment encompassing, among other matters, relevant accounting pronouncements, the legal and political environment, and environmental requirements affecting the industry and the entity; and other external factors, such as general economic conditions.

In pertinent part, with respect to the entity, the outside auditor is required to obtain an understanding of the five components of internal control (control environment; risk assessment; information and communication; control activities; and monitoring) sufficient to assess the risk of material misstatement for the purpose of the audit. SAS 109 applies to all audits, and is not limited to an evaluation of internal control under Sarbanes-Oxley §404. Statement on Auditing Standards 109 describes “internal control” as a process—effected by those charged with governance, management, and other personnel—that is designed to provide reasonable assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. Internal control consists of five interrelated components: control environment, risk assessment, information and communication, control activities, and monitoring.

Regarding “control environment,” the control environment sets the tone of the organization. The outside auditor is required to consider the entity’s processes relating to communication and enforcement of integrity and ethical values; commitment to competence; participation of those charged with governance; management’s philosophy and operating style; organizational structure; assignment of authority and responsibility; and human resource policies and practices.

SAS 109 further provides that the responsibilities of those charged with governance are of considerable importance. This is recognized in codes of practice and other regulations or guidance produced for the benefit of those charged with governance. In understanding the control environment, the auditor should consider such matters as the independence of the directors and their ability to evaluate the actions of management. The auditor also should consider whether there is a group of those charged with governance that understands the entity's business transactions and evaluates whether the financial statements are presented fairly in conformity with generally accepted accounting principles.

With respect to evaluating the participation of those charged with governance, SAS 109 specifically identifies the following criteria: (1) independence from management, (2) the experience and stature of those charged with governance, (3) the extent of their involvement in and scrutiny of activities, (4) the information that those charged with governance are provided, (5) the degree to which difficult questions are raised and pursued with management, (6) the ability of those charged with governance to evaluate the actions of management, (7) interaction with internal and outside auditors, (8) communications between management and those charged with governance, and (9) the ability of those charged with governance to understand the company's business transactions and evaluate whether financial statements are presented fairly in conformity with generally accepted accounting principles.

The outside auditor is required to evaluate whether a deficiency in internal control is significant enough to require communication of the deficiency to the audit committee, pursuant to SAS 112. Additionally, SAS 109 states that a significant internal control deficiency, or a lack of appropriate corrective response by management to a material deficiency, may raise doubt about the integrity of management, and whether it is possible to audit the financial statements.

Please also note that SAS 109 is a detailed pronouncement, which is too detailed to completely summarize in these materials.

**Statement on Auditing Standards 112**, Communicating Internal Control Related Matters Identified in an Audit, is applicable for all audits, and is not limited to audits performed for the purpose of Sarbanes-Oxley §404. SAS 112 specifies that:

-The outside auditor must communicate in writing to management and the audit committee (and perhaps the board) significant control deficiencies and material weaknesses in controls identified during the audit. The auditor's responsibility to communicate significant deficiencies and material weaknesses exists even if management or those charged with governance decided to accept that degree of risk.

Each of the following is an indicator of a control deficiency that should be regarded as at least a significant deficiency and a strong indicator of a material weakness in internal control:

-Ineffective oversight of the company's financial reporting and internal control by those charged with governance;

- Restatement of previously issued financial statements to reflect the correction of a material misstatement due to error or fraud;
- Identification by the auditor of a material misstatement in the financial statements for the period under audit that was not initially identified by the company's internal control, even if management subsequently corrects the misstatement;
- An ineffective internal audit or risk assessment function for a company for which those functions are important to the monitoring or risk assessment of internal control;
- For complex entities in highly regulated industries, an ineffective regulatory compliance function for which associated violations of laws and regulations could have a material effect on the reliability of financial reporting;
- Identification of fraud of any magnitude on the part of senior management;
- Failure by management or those charged with governance to assess the effect of a significant deficiency, and either correct it or conclude that it will not be corrected; and
- An ineffective control environment.

Significant control deficiencies or material weaknesses in control identified during the audit must be communicated in writing to management and to the audit committee (and perhaps the board), including significant deficiencies and material weaknesses that were communicated in the previous audits, and that have not yet been remedied. The auditor's responsibility to communicate significant deficiencies and material weaknesses exists even if there has been a decision by management or those charged with governance to accept that degree of risk.

A significant deficiency is a control deficiency or combination of control deficiencies that adversely affects the company's ability to initiate, authorize, record, process or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected.

A material weakness is a significant deficiency or combination of significant deficiencies that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A misstatement is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, individually or when aggregated with other misstatements, would clearly be qualitatively and quantitatively immaterial to the financial statements.

Financial Accounting Standards Board Statement of Financial Accounting Standards No. 5, Accounting for Contingencies, provides for three degrees of likelihood: probable, which means that the future event or events are likely to occur; reasonably possible, which means that the chance of the future event or events occurring is more than remote but less than likely; and remote, which means that the chance of the future event or events occurring is slight.

**Statement on Auditing Standards 100**, Interim Financial Information (i.e., review engagements).

There is very little public discussion about the value of a review engagement, such as the quarterly review performed by the outside auditor for public companies. In a review engagement the outside auditor performs required procedures that may cause the auditor to become aware of significant information regarding the financial statements. If the outside auditor does become aware of certain information during the course of a review engagement, SAS 100 requires the auditor to communicate that information to management and the audit committee as appropriate. When performing a review, the auditor should also determine whether any of the matters described in SAS 114 have been identified, and, if so, the auditor should communicate them to the audit committee or be satisfied that those matters have been communicated to the audit committee by management. See additional information about review and compilation services at <http://davidtate.us>.

## **5. Compliance Programs—Key Components**

Generally, the following are key organizational compliance program component areas—you may also want to refer to the Federal Sentencing Guidelines and the Foreign Corrupt Practice Act. Of course, each of the below components must also have subparts, and program standards and procedures must be developed to meet the needs of the specific organization for potential different substantive areas such as the foreign corrupt practices act; governmental billings and receipts; fraud; HR and the ADA; accounting; disclosures; environmental; quality assurance (such as with respect to products, materials, services or care); bribes/kickbacks; and other areas of potential liability and risk exposure.

- High-level personnel of the organization (tone at the top) must ensure that the organization has an effective compliance and ethics program. A specific individual, or individuals, within high-level personnel shall be assigned overall responsibility for the compliance and ethics program. 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.
- The organization's governing authority, i.e., the Board or other highest-level governing body (tone at the top) shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise oversight with respect to implementation and effectiveness.
- A specific individual, or individuals, within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program, and shall report periodically to high-level personnel and to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. The person or persons to whom responsibility is delegated shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.

- Delineate lines of reporting and authority that are designed to effectively accomplish the goals and objectives of the compliance and ethics program.
- Design the compliance and ethics program standards and procedures to prevent and detect criminal conduct.
- Implement the standards and procedures.
- Promote and incentivize the compliance and ethics program consistently throughout the organization, and promote an organizational culture of ethical conduct and compliance with laws, regulations and rules. Periodically communicate the program's standards and procedures, and other aspects of the compliance and ethics program, to the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents. 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).
- Monitor the program to ensure that it is being followed to prevent and detect criminal conduct. Review and improve the program when needed.
- Periodically audit and evaluate the effectiveness of the standards and procedures to prevent and detect criminal conduct. Review and improve the program when needed.
- Periodically assess and reassess the risk of criminal conduct and take appropriate steps to design, implement, or modify each requirement in the program to reduce the risk of criminal conduct identified through this process.
- Have and enforce an effective progressive disciplinary system to encourage compliance with the goals and objectives of the compliance and ethics program.
- Enforce the compliance and ethics program's standards and procedures consistently throughout the organization including appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.
- Implement policies and procedures to facilitate prompt appropriate organizational reaction to possible unlawful conduct, and potential damage mitigation, control and remedy.
- After potential or actual criminal conduct has been detected, take necessary steps to promptly and appropriately respond to and investigate the conduct and to prevent further similar conduct,

including making any necessary modifications to the organization's compliance and ethics program.

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

## **6. Annual Self-Evaluation, Board and Committees**

Should the board and its committees have or perform an annual self-evaluation? Short and sweet: YES. It is good for the members to consider the positive aspects of the board's activities and processes, and possible improvements including additional or different information, processes and education that might be helpful to the board members. No particular self-evaluation process is required. You can find self-evaluation suggestions at <http://davidtate.us>.

I hope you found this information helpful and useful to prompt discussions about these topics. I have kept this paper relatively short. Additional materials on many of these topics are available.

David Tate, Esq.