



Wednesday, October 21
9:00 am–10:30 am

909 Begin with the End in Mind

Julie A. Bell

Vice President, Law & Compliance
Kratos Defense & Security Solutions, Inc.

Paul G. Levenson

Assistant United States Attorney, Chief, Economic Crimes Unit
US Attorney's Office for the District of Massachusetts

Stephen Martin

General Counsel
Corpedia

Jennifer A. Short

Partner
Holland & Knight

Faculty Biographies

Julie A. Bell

Julie A. Bell is vice president of law and compliance for Kratos Defense & Security Solutions, Inc., a publicly traded provider of weapons systems support, IT solutions, defense engineering and range operation support to the federal government, state governments and commercial customers. Formerly known as Wireless Facilities, Inc., the company was a provider of design, engineering and deployment services to commercial wireless carriers and equipment manufacturers until 2007. Ms. Bell's responsibilities include providing legal counsel to the company and directing its formal ethics and compliance program.

Prior to joining Kratos, Ms. Bell was an associate attorney at the Washington, DC offices of Robins, Kaplan, Miller & Ciresi LLP and Zuckerman Spaeder LLP. Ms. Bell recently served as general counsel of the Ski Club of Washington, DC.

Ms. Bell received a BS from the University of Denver and is a graduate of the New York University School of Law.

Paul G. Levenson

Paul G. Levenson is chief of the economic crimes unit of the Office of the US Attorney for the District of Massachusetts. Since joining the US Attorney's Office, he has prosecuted a variety of white collar crimes, including securities fraud, bank fraud, bribery and kickback schemes, public employee fraud, insurance fraud, tax fraud, environmental violations, foreign corrupt practices, intellectual property crimes, procurement fraud, embezzlement, telemarketing fraud and money laundering.

Previously, he has served in the civil, economic crimes and public corruption units of the US Attorney's Office. Before joining the US Attorney's Office, Mr. Levenson was in private practice in Washington, DC and in New York.

Mr. Levenson is a magna cum laude graduate of Harvard College and of Harvard Law School, where he served as an editor of the Harvard Law Review.

Stephen Martin

General Counsel
Corpedia

Jennifer A. Short

Jennifer A. Short is a partner with the law firm of Holland & Knight LLP, where she concentrates her practice on civil and white-collar criminal litigation matters on behalf of companies and individuals. Ms. Short routinely assists companies in responding to

government investigations and inquiries, conducting internal investigations, and preparing disclosures of potential violations to appropriate enforcement authorities. She also aids companies, particularly those in highly regulated industries such as health care and government contracts, in designing, implementing, reviewing, and revising their corporate compliance and ethics programs.

Ms. Short is recognized as a leading white-collar litigator by Chambers USA (2006-2009), and was named a Virginia Super Lawyers "Rising Star" in 2007 and 2008. She co-chairs two ABA subcommittees of the criminal justice section's white collar crime committee, and serves on the steering committee for the Women's Business Council of the Fairfax County (Virginia) Chamber of Commerce.

Ms. Short earned her BA from Duke University and her JD from the University of Virginia School of Law.

ACC Association of Corporate Counsel

HYPOTHETICAL 1: FastCo – Background

- FastCo is a U.S. reporting engineering and construction services company with operations around the world.
- The company is headquartered in Iowa, where the CEO, CFO, General Counsel and Chief Accounting Officer are based.
- FastCo grows mostly by acquiring smaller, privately-held companies, and in the past several years has closed several acquisitions per year, many of them as earn-outs, where the prior ownership and management must achieve specific financial results for the three years immediately following the acquisition in order to receive the bulk of the acquisition consideration.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

FastCo – Background

- One morning, two FBI agents arrive at the Iowa office with a search warrant for a large number of accounting documents, with a particular focus on financial records relating to FastCo's subsidiary LooseCo, a Malaysian company that FastCo acquired about 2 years earlier.
- The receptionist immediately phoned the Facilities Manager, a burly fellow, who demanded of the FBI agents that they go away and leave FastCo alone.
- At this point, the General Counsel entered the building for the workday and, coming upon the scene, asked the agents for identification and the warrant. Seeing that all looked to be in order, the GC escorted the agents to the Accounting Department and watched them collect documents.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!


ACC Association of Corporate Counsel

FastCo – Documents

- The GC was busy with many things and concerns that day. For one thing, he was helping the HR Director get the commission and bonus schedules together. As a result, he was not able to issue any kind of document hold order to the IT, Accounting, Finance and other relevant staff. He meant to do it the next day but it slipped his mind.
- FastCo's document destruction software continued to purge emails according to its 90-day schedule and backup tapes were overwritten as usual.
- Thinking something might be up, the Treasury Manager shredded whatever records of cash requests and disbursements she had processed for LooseCo since it had been acquired. She figured that since there was no system at FastCo to audit these cash disbursement requests, they would not be missed anyway.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!




FastCo – Investigation

- After about a month, once the CEO returned from vacation, the GC recommended that FastCo undertake an internal investigation.
- The CEO would not allow the GC to hire outside counsel, so they agreed that the Accounting Manager at LooseCo would be perfect for the job. She was a loyal employee, and although she had never really conducted an investigation, she was seen as someone with a real “can do” attitude who was gunning for a promotion.
- The LooseCo Accounting Manager had a lot of work to do but eventually she looked over the cash request and disbursement records, since that seemed to be what all the fuss was about. She concluded that everything on her end looked just the way it had always looked at LooseCo – after all, the scribbled signatures on the signature blocks indicated the right titles from the Authority Matrix for requesting certain dollar amounts.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!




FastCo – Investigation

- The LooseCo Accounting Manager did not review any of the FastCo policies that now applied to LooseCo, such as those requiring Legal Department review of sales agent contracts and payment terms, since nobody had ever told her about those FastCo policies.
- In any event, she reported back to the LooseCo Controller and the FastCo CEO in the monthly FastCo-LooseCo a conference call that everything looked normal. This monthly conference call included several levels of management at both companies as well as the FastCo Treasury Assistant and other non-management staff, including an assistant to the Directors of Business Development at LooseCo.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!



FastCo

- The Business Development Director's assistant, who had attended because her boss was on vacation, thought about the subject matter of the FastCo's Accounting Manager's report.
- The BD Director's assistant remembered that her boss had, on several occasions, had the assistant sign the expense reports on the VP approval line to facilitate timely reimbursement of some large entertainment expenses. The assistant did not question her boss' directive, since it was well known at LooseCo, and at FastCo, as far as she could tell, that everyone was expected to respect authority and do what they were told. So, she had signed these reports in his name and submitted them for reimbursement.
- One of those expense reports, where the attendees at a lavish party were Malaysian Ministry of Defense officials and their families, now caused the assistant to think again.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

FastCo – Compliance Program

- The BD Director's assistant thought very hard about what it all meant. She really didn't have any guidance or experience with this kind of thing – no training, no Code of Conduct, no posted policies – so after a week or so, she let it drop.
- She also remembered reading her boss's commission plan, which was signed by both LooseCo's General Manager and FastCo's CEO, and which stated that "Your job and the success of both FastCo and LooseCo depend upon your achievement of the sales targets set forth in this commission plan." It seemed that achievement of sales goals was the most important thing, and she didn't want to face retaliation for not supporting management's directive.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

FastCo – Compliance Program

- In fact, she had heard that her boss was about to be promoted to a VP himself, since he had produced such strong sales, especially in the Defense area.
- She had also heard that LooseCo's General Manager had pleaded guilty to some sort of money-laundering charge several years back, before the acquisition by FastCo.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

FastCo – Compliance Program

- Back in the U.S., the Assistant U.S. Attorney contacted FastCo's GC and informed him that LooseCo and FastCo, were subjects of an international bribery investigation. The AUSA asked the GC if he would make several employees available to be interviewed. The GC, the CEO and the CFO discussed this request and decided that it would be best if they didn't give the AUSA any help, since the AUSA had various powers at her disposal anyway.
- The GC advised the CEO and the CFO that FastCo was not at risk, since it had a compliance program, all of the day-to-day elements of which were run by the GC's assistant, that included a policy statement against bribery of foreign public officials.
- As it was never FastCo's practice to discuss such operational matters with its Board of Directors, the Board was not advised of these matters.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

FastCo – Internal Controls

- It did not occur to the CEO, the GC and the CFO to conduct a review of internal controls in an effort to prevent similar situations elsewhere in the FastCo group of companies.
- They were very busy because they were about to close on a new acquisition of a construction company in Nigeria with terrific sales numbers – so busy that there just had not been time to perform much due diligence on that company.
- Plus, the bonus and commission checks were about to receive final sign-off so they could be paid, which some of the BD and Sales people had been clamoring for. One of these checks would be sent to the Director of BD at LooseCo, due to his having met and exceeded his goals for the prior year.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

HYPOTHETICAL 2: Boncorp – Background

- Boncorp is a large, publicly-traded engineering and construction company
 - 80% of revenues come from contracts with federal, state, local authorities related to transportation and other infrastructure development
 - Operations in a number of states in the Mid-Atlantic and Southeast U.S.; corporate headquarters in Alabama

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

Boncorp – Compliance Efforts

- In 2002, Boncorp establishes an independent audit committee
 - Audit committee recommends (and company adopts) a "Code of Ethics" in May 2003
- In 2005, Boncorp hires a Chief Compliance and Ethics Officer (CCEO).
 - CCEO reports to the General Counsel on a day-to-day basis, and also reports directly to the Board of Directors at their quarterly meetings
 - CCEO is authorized to contact the chair of the independent audit committee if an issue arises involving either senior management or a Board member.
- Also in 2005, Boncorp establishes an ethics hotline which is monitored by an outside vendor to ensure anonymity

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

Boncorp – Potential Impact on Contracts

- In October 2007, Boncorp's continuing internal investigation reveals that the embezzlement scheme largely impacted the company's overhead accounts, and through them, the rates charged to its government customers
- Outside counsel recommends meeting with the government to make a prompt voluntary disclosure of possible overcharges and false claims

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

Boncorp – How does that meeting go?

- Who does Boncorp approach about overpayment/false claims issues?
- What are government's likely questions?
- Boncorp as "victim"? Boncorp as "responsible contractor"?
- What are risk areas? Did Boncorp respond appropriately and/or anticipate those risk areas?
- What compliance measures should Boncorp highlight?
- What is the government's reaction?

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ABC Corp. Compliance Plan	Policies and Procedures for Responding to Government Investigations and Inquiries S.O.P. No. ABC-7.3 Replaces 5.1
------------------------------	--

POLICIES AND PROCEDURES FOR RESPONDING TO GOVERNMENT INVESTIGATIONS AND INQUIRIES

OUR PURPOSE

At ABC Corp., we are committed to operating our business with the utmost integrity and highest ethical standards. We must treat our customers, government agencies and their employees, and each other fairly and honestly in all our dealings.

The purpose of this policy is to provide basic guidance to our employees regarding responding to governmental investigations and inquiries. Companies like ABC Corp. that do business with the government occasionally face audits and investigations. We want to make certain that ABC Corp. and its employees cooperate with government investigations while at the same time protect the interests our company and employees.

OUR POLICY

ABC Corp. and its employees will comply with all applicable laws, rules, and regulations of federal, state, local and provincial governments, and other appropriate private and public regulatory agencies. ABC Corp. expects its employees to deal in an honest, fair, and ethical manner with government representatives and to avoid circumstances that could be considered deceitful, wasteful, fraudulent, or create the appearance of an impropriety or conflict of interest.

ABC Corp. will fully cooperate with any appropriately authorized government investigation, inquiry or audit. ABC Corp. will assert all protections afforded it by law in any such investigation, inquiry or audit.

APPOINTMENTS OF DESIGNATED CORPORATE COUNSEL

ABC Corp. has appointed Designated Corporate Counsel to handle issues related to investigations, audits, and requests from government investigators. The Designated Corporate Counsel will ensure that ABC Corp. appropriately and timely responds to all governmental requests and speaks with a unified voice to investigators. The Designated Corporate Counsel, and their contact information, are as follows:

DATE ISSUED: 1/01/01	DATE REVIEWED: 9/09/09	APPROVED BY: Board of Directors	Page #
-------------------------	---------------------------	------------------------------------	--------

ABC Corp. Compliance Plan	Policies and Procedures for Responding to Government Investigations and Inquiries S.O.P. No. ABC-7.3 Replaces 5.1
------------------------------	--

John B. Goode (101) 555-5555
Jane R. Diligent (101) 555-1111

DEFINITIONS

Civil Investigative Demand. A formal demand issued by a U.S. government investigator or a state attorney general related to a potential false claim investigation requesting an entity to produce records or documents, respond to written interrogatories, and provide testimony.

Subpoena. A subpoena is an order, issued by a court of law through a Grand Jury or the Office of an Inspector General (Administrative subpoena), which demands the disclosure of documents, records, physical evidence, or in the case of an individual, testimonial information, for use in criminal, civil or administrative investigations. A subpoena may be addressed to a company or to an individual within a company. It is important to note that a Grand Jury subpoena is a court order that must be followed. If you are served with either a Grand Jury or Administrative subpoena you must notify a Designated Corporate Counsel immediately.

Search Warrant. Government investigators may request a search warrant in order to obtain records and physical evidence. Search warrants are authorized by a federal or local judge or magistrate. A search warrant may be issued if the judicial officer finds probable cause to believe that evidence of a crime exists at a specific location. With a search warrant, investigators may confiscate documents, computers, and other data believed to be relevant to their case. During the execution of a search warrant, investigators may arrive in large numbers, armed, and wearing raid jackets. Employees should cooperate with investigators when a search warrant is executed, but not provide any information outside the presence of corporate counsel. An employee should immediately contact Designated Corporate Counsel if a search warrant is executed at ABC Corp.'s offices.

OUR PROCEDURES

Governmental Requests for Documents for an Investigation or Inquiry

DATE ISSUED: 1/01/01	DATE REVIEWED: 9/09/09	APPROVED BY: Board of Directors	Page #
-------------------------	---------------------------	------------------------------------	--------

ABC Corp. Compliance Plan	Policies and Procedures for Responding to Government Investigations and Inquiries S.O.P. No. ABC-7.3 Replaces 5.1
------------------------------	--

ABC Corp. personnel may be asked by government investigators to provide documents related to a government inquiry or investigation. ABC Corp. personnel must undertake and follow the steps below before disclosing any documentation to the investigating agency:

1. Contact the Designated Corporate Counsel immediately to notify them of the request for documents from the investigating agency.
2. Contact your immediate supervisor to notify them of the request for documents from the investigating agency.

DATE ISSUED: 1/01/01	DATE REVIEWED: 9/09/09	APPROVED BY: Board of Directors	Page #
-------------------------	---------------------------	------------------------------------	--------

ABC Corp. Compliance Plan	Policies and Procedures for Responding to Government Investigations and Inquiries S.O.P. No. ABC-7.3 Replaces 5.1
------------------------------	--

3. Cooperate with the government investigator but do not consent to provide any documentation or records.

4. Ask the investigator if a civil investigative demand, subpoena, or search warrant accompanies the request for the records. If a civil investigative demand, subpoena, or search warrant has been issued or ordered, please request a copy of the document. If a search warrant is presented for the documents, please follow the instructions below in the section titled "Governmental Request to Search ABC Corp. Premises with a Search Warrant."

5. Employees should never give any documents, copies of documents, or other tangible evidence to investigators during the initial service of a subpoena or during an interview. Documents that are subject to a subpoena will need to be reviewed for certain legal privileges by counsel before being disclosed to the government. Wait for a Designated Corporate Counsel to provide instruction on how to move forward with the request for documents from government investigators.

6. Law enforcement may serve a subpoena on an employee regarding matters that have nothing to do with the company. These matters could include a lawsuit unrelated to the employee's job, divorce, child support, or a car accident. Investigators could also execute a search warrant at an employee's workplace or home or attempt to garnish the wages of the employee. If the purpose of the visit relates solely to an individual employee, the major concerns are the privacy rights of the employee and the potential disruption to the company. Prior to the release of any personal information or records regarding an employee, Designated Corporate Counsel must be consulted.

Governmental Request for an Interview for an Investigation or Inquiry

DATE ISSUED: 1/01/01	DATE REVIEWED: 9/09/09	APPROVED BY: Board of Directors	Page #
-------------------------	---------------------------	------------------------------------	--------

ABC Corp. Compliance Plan	Policies and Procedures for Responding to Government Investigations and Inquiries S.O.P. No. ABC-7.3 Replaces 5.1
------------------------------	--

Government investigators may attempt to interview company employees without first obtaining a subpoena or notifying our legal department. These interviews may be attempted at our offices or at an employee's home. Employees should understand that despite the potentially coercive setting, employees are not required to answer questions, may decline to answer questions, and may delay answering any questions until they have corporate or individual counsel present. Delaying or postponing an investigator's request for an interview is perfectly appropriate and will not be viewed as a refusal to cooperate. ABC Corp. personnel must read and understand the following section before deciding to speak to government investigators.

1. ABC Corp. personnel have the option of speaking with government investigators with or without the presence of an attorney. ABC Corp. personnel may decide to forgo any discussions with an investigator until securing legal counsel. If an employee desires to have an attorney present at any meeting with a government investigator, ABC Corp. employees may request to consult with a private attorney or an attorney from the company's legal department prior to conducting an interview with an investigator.

2. If a ABC Corp. employee decides to speak with a government investigator without an attorney from the company's legal department present, the employee may be liable for any of the information provided to the investigator even if the employee retained private legal counsel. An employee must only make truthful, accurate statements when discussing the business's activities. Any failure to be truthful and accurate may result in serious legal consequences.

3. If a ABC Corp. employee decides to speak with a government investigator the employee should notify a Designed Corporate Counsel of the request for an interview and provide the following information.
 - a. The name, agency affiliation, business telephone number, and address of the government investigator, and

 - b. the reason for the interview, if known.

DATE ISSUED: 1/01/01	DATE REVIEWED: 9/09/09	APPROVED BY: Board of Directors	Page #
-------------------------	---------------------------	------------------------------------	--------

ABC Corp. Compliance Plan	Policies and Procedures for Responding to Government Investigations and Inquiries S.O.P. No. ABC-7.3 Replaces 5.1
------------------------------	--

4. During an interview, employees should not respond to any question unless they are certain that their responses are complete and accurate. An employee should not guess if unsure of an answer, be careful of informal or "off-the-record" discussions, and immediately report to your supervisor, manager, or the Designated Corporate Counsel, any non-routine contact with a government investigator that relates to ABC Corp..

Governmental Request to Search ABC Corp.'s Premises Without a Search Warrant

Government investigators may request permission to search ABC Corp.'s premises without obtaining a search warrant. If a government investigator requests to search the premises of ABC Corp. without a search warrant, a ABC Corp. employee **must**:

1. Contact a Designated Corporate Counsel immediately to notify them of the request for the search by the government investigator.
2. Contact your immediate supervisor to notify them of the government's request for permission to conduct a search.
3. Cooperate with the government official but **do not consent to a search without permission of a Designated Corporate Counsel.**
4. Avoid and prevent the altering, removing or destroying of records, documents or other tangible evidence.

Governmental Request to Search ABC Corp.'s Premises With a Search Warrant

When government investigators request to search ABC Corp.'s premises with a search warrant, the investigators have the authority to enter the premises, search for criminal activity, and seize documents, records, and other tangible evidence listed in the warrant. ABC Corp.'s employees are not required to answer investigators' questions, but they must provide the records requested in the warrant. When a government investigator presents a search warrant to search the premises, ABC Corp.'s personnel must:

DATE ISSUED: 1/01/01	DATE REVIEWED: 9/09/09	APPROVED BY: Board of Directors	Page #
-------------------------	---------------------------	------------------------------------	--------

ABC Corp. Compliance Plan	Policies and Procedures for Responding to Government Investigations and Inquiries S.O.P. No. ABC-7.3 Replaces 5.1
------------------------------	--

1. Contact a Designated Corporate Counsel immediately to notify them of the search warrant and the activities of the investigators.
2. Request a copy of the search warrant.
3. Request that the search be conducted after a Designed Corporate Counsel is present. Employees should understand this request will routinely be denied.
4. Employees must cooperate and under no circumstances should employees attempt to obstruct or interfere with the search. If investigators refuse to delay the search until counsel is present, the employees must allow the investigators to execute the search warrant.
5. Contact the supervisor of your department and notify them of the warrant and search.
6. A supervisor should accompany the lead government investigator during the search and take notes of what documents, records, and other tangible evidence were reviewed or taken and also take notes on the questions that were asked by investigators to employees.
7. The search warrant will include an attachment listing things that can be seized and places that may be searched. If government investigators search areas or records that are not listed in the warrant or seize documents or other tangible evidence that are not included in the warrant, the supervisor should note these deviations from the warrant in writing and give them to a Designated Corporate Counsel.
8. Government investigators may seize original documents and other tangible evidence, including computers. The ABC Corp. is entitled to a detailed inventory of the seized materials, and investigators are required to provide a receipt of the materials taken pursuant to the search warrant.

DATE ISSUED: 1/01/01	DATE REVIEWED: 9/09/09	APPROVED BY: Board of Directors	Page #
-------------------------	---------------------------	------------------------------------	--------

ABC Corp. Compliance Plan	Policies and Procedures for Responding to Government Investigations and Inquiries S.O.P. No. ABC-7.3 Replaces 5.1
------------------------------	--

9. Investigators may attempt to interview employees during the execution of a search warrant. Employees may agree to be interviewed, but they are not required to do so. It is solely their decision. An employee also may request to delay the interview until an attorney is present. If an employee agrees to be interviewed, he or she must tell the truth and should ask for a copy of any statement he or she signs.

8781197_v4

DATE ISSUED: 1/01/01	DATE REVIEWED: 9/09/09	APPROVED BY: Board of Directors	Page #
-------------------------	---------------------------	------------------------------------	--------

	Global Policy Manual	Effective Date: October 4, 2007	Page #
	Title: Compliance with Foreign Corrupt Practices Act	GPM No.	Old Rev 0.2 New Rev 0.3
Department / Author, Typed Name: Legal/			Date: 10/04/07
Approval, Typed Name: Sr. VP, General Counsel/			Date: 10/04/07

1.0 SCOPE AND PURPOSE

The Foreign Corrupt Practices Act ("FCPA") is a United States federal law that applies to U.S. individuals, companies and businesses, including their controlled international subsidiaries. All Company Business Segments around the world fall within the scope of the FCPA. The purpose of this policy is to alert all employees to the requirements of the FCPA and to establish codes of conduct and record-keeping procedures that assure that all transactions undertaken by Company are in compliance with the FCPA. This policy is designed to help employees recognize situations and payments that might raise legal issues under the FCPA. It is important that each person with responsibilities that might give rise to potential FCPA liabilities comply with the procedures contained in this policy and also work closely with Company's Law Department to ensure compliance with the FCPA.

2.0 RESPONSIBILITY AND AUTHORITY

Each employee is responsible for recognizing, avoiding and reporting any situation involving practices that may be illegal under the FCPA. Employees are further responsible for complying with the reporting and record-keeping procedures set forth in this policy. All managers are responsible for communicating this policy to all employees under their supervision. The Law Department is authorized to advise the Company concerning activities that fall within the scope of the FCPA. To ensure compliance with this policy, employees involved in retaining foreign sales agents and consultants are required to certify their compliance with this policy and the procedures set forth by the Law Department. Each Reporting Entity Controller and Vice President (or higher) providing quarterly management representations is responsible for affirming that, to his/her knowledge, no payments in violation of the FCPA have been made during that period.

3.0 POLICY

- 3.1 All Company personnel (including employees of subsidiaries of Company) who have any management, operational, or sales responsibilities for activities outside of the United States, and all accounting personnel throughout Company, are expected to be aware of the FCPA and its potential impact on Company's operations, and to conduct their business activities consistently with this policy.
- 3.2 Violations of the FCPA subject the offending parties to severe criminal and civil penalties. Consequently, Company is committed to full compliance with the letter and spirit of the FCPA.
- 3.3 The FCPA specifically prohibits United States companies and individuals acting on their behalf (including individuals acting in other countries) from paying or offering to pay "any

	Global Policy Manual	Page: 2 of 2
Title:	Compliance with Foreign Corrupt Practices Act	GPM No. Rev - 0.3

money ... gift ... or anything of value” to any foreign official, political party official, or candidate for political office in order to influence a business decision.

- 3.4 The FCPA also requires U.S. companies to maintain books and records that accurately and fairly reflect corporate transactions and also requires that companies establish a system of internal accounting controls to provide reasonable assurance to management of the type of financial transactions undertaken by Company and its employees.
- 3.5 Certain payments to foreign officials are not prohibited by the FCPA. These include payments made to an official to expedite or facilitate a decision in which the official has no ability to exercise discretion, payments for bona fide expenses relating to promoting products or performing or executing contracts, or payments permitted by the written laws of the official's country. However, it is often extremely difficult to distinguish between payments that are legal under the FCPA and illegal bribes under the FCPA. Consequently, every effort should be made to eliminate payments to foreign officials. At the very least, extreme care and consultation with the Law Department should be taken before any such payment is authorized.
- 3.6 Moreover, under the accounting standards provisions of the FCPA, even payments that are legal under the FCPA must be properly recorded in the accounts and records of Company. Recording of such payments in any way that would conceal their true nature constitutes an independent violation of FCPA accounting standards.

4.0 PROCEDURE

- 4.1 To ensure that Company and its employees remain in compliance with the FCPA, Company employees must follow the following procedural guidelines relating to FCPA compliance:
- 4.1.1 Company's relationship with all foreign governmental agencies and their officials and personnel in the United States and in each foreign country in which business is conducted shall be in all respects such that public disclosure of the full details thereof will not impugn Company's integrity and reputation. Accordingly, payments, regardless of amount, to foreign governmental officials and personnel for obtaining, maintaining or directing Company business, including gifts of substantial value or lavish entertainment, are not permitted.
- 4.1.2 The foregoing prohibition applies to the use of corporate as well as personal funds or assets. It also applies with equal force to indirect contributions, payments or gifts made through any medium, such as through consultants, advisors, suppliers, customers or other third parties.
- 4.1.3 Company personnel are to conduct Company business in compliance with the written laws of all countries in which Company does business.
- 4.1.4 The use of Company funds or assets for any unlawful, improper or unethical purpose is prohibited.

	Global Policy Manual	Page: 3 of 3
Title:	Compliance with Foreign Corrupt Practices Act	GPM No. Rev - 0.3

- 4.1.5 No undisclosed or unrecorded funds or assets of Company are to be established for any purpose (i.e., scrap funds, vending machine funds, etc.).
- 4.1.6 False, inflated or artificial entries are not to be made in the books and records of Company for any reason, and no employee shall engage in any arrangement that results in such entries.
- 4.1.7 No accounting record or document relating to any transaction shall be falsified in any manner that may obscure or disguise the true nature of the transaction.
- 4.1.8 No payment on behalf of Company shall be approved without adequate supporting documentation or made with the intention or understanding that any part of such payment is to be used for any purpose other than that described by the documents supporting the payment.
- 4.1.9 Compliance with generally accepted accounting principles and established internal audit controls and procedures shall be required at all times.
- 4.1.10 A Company employee is not to become involved in any arrangement or activities that result in any of the previously stated prohibited acts.
- 4.1.11 As with other laws, it is Company' policy to encourage compliance with not only the letter but the spirit of the law. All employees of Company and its subsidiaries shall refrain from any acts that are prohibited by the FCPA, and employees suspecting violations should report their concerns to the Law Department. Compliance with the provisions and requirements of the FCPA will be evaluated by the Law Department.
- 4.1.12 Role of the Law Department in FCPA Compliance. The Law Department shall direct the performance of due diligence on the proposed foreign agent or consulting organization and its principals. The level of due diligence to be performed may vary, in the Law Department's discretion, depending upon the nature of the proposed relationship, the amount of compensation proposed, the location of the agent and other factors. At a minimum, the Law Department will search the databases available from the U.S. Departments of State, Treasury and Commerce to ensure that the organization and its principals are not listed as debarred, denied or specially designated nationals.
- 4.1.13 If, as a result of its due diligence, the Law Department approves the engagement of the agent or consultant, then the Law Department, together with the businessperson requesting the engagement, shall obtain from the agent or consultant a signed agreement in a form acceptable to the Law Department. The signed agreement will include, among other terms, the agent or consultant's acknowledgement and certification that it has received a copy of this policy and will take all reasonable steps to ensure that its staff working on an engagement for Company act consistently with this policy, the FCPA and other applicable

	Global Policy Manual	Page: 4 of 4
Title:	Compliance with Foreign Corrupt Practices Act	GPM No. Rev - 0.3

laws.

4.1.13.1 The businessperson requesting the engagement is required to certify that, to the best of his/her knowledge, no transactions under the agency or consulting agreement violate or are anticipated to violate the FCPA and this policy.

4.1.13.2 Foreign agents or consultants engaged by Company for more than one year should be asked to certify their compliance with this policy in writing, on an annual basis.

4.1.13.3 If doubt exists as to the legality under the FCPA or this policy of any planned payment to a foreign official, or the accuracy of financial reporting with respect to any transaction, the matter must be referred immediately to Company' Law Department prior to making any such payment or recording such financial information.

4.2 Procedures for Permitting Payments to Foreign Officials. In those limited circumstances in which payments to foreign officials are permitted under the FCPA, and such payments are necessary and appropriate to protect the legitimate business interests of Company, the procedures in the following table must be followed.

Responsibility of:

- | | |
|-------------------|---|
| Employee or Agent | 1. (a) Determines the need for a payment to facilitate movement of goods or personnel, or to facilitate administrative or other ministerial or clerical activity.
(b) Determines the need for a payment relating to bona fide expenses for promoting products or performing or executing contracts.
(c) Determines the need and appropriateness for a payment where the only justification is that the payment is permitted under the written laws and regulations of the recipient's nation. <i>Use of this type of payment is to be discouraged and will only be permitted in the most limited circumstances.</i>
(d) Employee certifies in writing to Company that, to employee's knowledge, the facilitating payment complies with Company' Policy on Compliance with Foreign Corrupt Practices Act. |
|-------------------|---|

	Global Policy Manual	Page: 5 of 5
Title:	Compliance with Foreign Corrupt Practices Act	GPM No. Rev - 0.3

- | | |
|---|---|
| 2. | Seeks written approval for the facilitating payment in 1(a), the bona fide business payment in 1(b), or the payment permitted by written law in 1(c) from the appropriate Vice President or subsidiary head. Request for approval shall include information concerning the circumstances surrounding the payment and must clearly and fully demonstrate the necessity of the payment. For payments under 1(c), the request for approval must also include reference and citation to the written foreign law permitting the payment. |
| NOTE: | Recurring payments (i.e., certain facilitating payments) may receive standing written approval in advance to avoid unnecessary delay and inconvenience. When such approval is given, the appropriate Vice President or subsidiary head must periodically review the types of pre-approved recurring payments and payments actually made. <i>Standing written approval cannot be given for payments under 1(c) above.</i> |
| Corporate Officers and Business Segment Heads | 3. Analyzes the request and determines whether the payment is clearly within the provisions of the FCPA and Company' corporate policy. If there is any question as to whether a particular payment is legal under the FCPA or this policy, the matter must be referred to the Company Law Department for review prior to making the payment. Any request for payment approval under 1(c) must be directed to the Law Department for review and approval <i>prior to making the payment.</i> |
| Employee or Agent | 4. Advises employee of decision in writing and maintains permanent files for all written requests and the corresponding written decisions on said requests.
5. If payment is approved, the responsible employee makes arrangements for the disbursement of funds and makes required payment. |
| Accounting Department | 6. The employee reports the payment as a "facilitating payment," "bona fide business payment" or a "payment permitted by written law" to the accounting department so that the transaction is properly recorded in the accounting records of Company or the appropriate subsidiary's records.
7. The appropriate accounting department shall assure that all facilitating payments, bona fide business payments and payments permitted by written law are accurately reflected in its accounting records and should use a separate accounting code for such payments. The entity controller and manager making management representations as part of the internal financial package shall affirm that to his/her knowledge, no payments have been made in violation of the FCPA, and that all bona fide business payments have been classified appropriately in the Financial Package. |

	Global Policy Manual		Page: 6 of 6
Title:	Compliance with Foreign Corrupt Practices Act	GPM No.	Rev - 0.3

- | | | |
|---|-----|--|
| Corporate Officers and Business Segment Heads | 8. | Reviews facilitating payments, bona fide business payments and payments permitted by written law made at each location within his jurisdiction. |
| Agents | 9. | Signs contract with the Company which includes provision in which the Agent pledges compliance with the FCPA and the Company's policy and procedures related thereto. Annually certifies compliance in writing to Company. |
| Internal Audit/Audit Committee | 10. | When brought for review by executive management, Internal Audit or Audit Committee reviews reports of facilitating payments, bona fide business payments and payments permitted by written law. |

5.0 EXHIBITS

5.1 Reference Manual

5.2 Certifications for Employees Engaging Foreign Agents and Consultants

6.0 REVISION NOTES

6.1 Company name change.

	Global Policy Manual	Page: 7 of 7
Title:	Compliance with Foreign Corrupt Practices Act	GPM No. Rev - 0.3

**COMPANY, INC.
GLOBAL POLICY ON COMPLIANCE WITH FOREIGN CORRUPT PRACTICES ACT
REFERENCE MANUAL FOR EMPLOYEES ENGAGING NON-U.S. SALES AGENTS AND
PARTNERS**

September 23, 2009

1.0 PURPOSE AND SCOPE

All U.S. and foreign-based employees of Company, Inc., its subsidiaries and controlled affiliates (collectively, "Company") are required to comply with Company' policy on compliance with the Foreign Corrupt Practices Act ("FCPA"). In support of that compliance, Company employees must follow the procedures outlined below before engaging non-U.S. sales agents and partners.

2.0 PROCEDURE

- 2.1 Identification of Foreign Sales Agent or Partner. Any employee of Company who intends to engage a non-U.S. sales agent or partner for Company shall first notify the Company Law Department of such intention. The Company Law Department will assign an attorney to work with the employee on the matter.
- 2.2 Preliminary Information. When identifying the potential foreign sales agent or partner to be engaged, the Company employee must provide the following preliminary information to the assigned attorney:
- 2.2.1 Name and location of company, principals and staff who will be performing the services. Are any principals or staff government officials?
 - 2.2.2 Company business address and entity designation.
 - 2.2.3 Proposed type of relationship (e.g., agent, distributor, consultant, teaming partner); scope and location of services.
 - 2.2.4 Source of referral and at least two business references. Does Company have any past experience with the consultant or its representatives?
 - 2.2.5 Banking and credit references.
 - 2.2.6 Requested fee or commission and method of payment.
 - 2.2.7 Website address or marketing materials, if any exist.

	Global Policy Manual	Page: 8 of 8
Title:	Compliance with Foreign Corrupt Practices Act	GPM No. Rev - 0.3

2.3 Preliminary U.S. Government Database Search. Once the assigned attorney has received the preliminary information identified in Section 2.2 above, the assigned attorney will search the following U.S. government databases for the names of the foreign entity and its principals and staff members with whom Company is proposing to enter a relationship:

2.3.1 U.S. Department of Commerce, Bureau of Industry and Security:
(<http://207.96.48.13/complianceandenforcement/index.htm>)

2.3.1.1 Denied Persons List (HTML Version)
<http://www.bis.doc.gov/dpl/Default.shtm>

2.3.1.2 List of Recent Changes to Denied Persons List
<http://www.bis.doc.gov/dpl/recentchanges.asp>

2.3.1.3 Unverified List
http://www.bis.doc.gov/Enforcement/UnverifiedList/unverified_parties.html

2.3.1.4 Entity List <http://www.bis.doc.gov/Entities/Default.htm>

2.3.2 U.S. Department of State Debarred List
<http://www.pmddtc.state.gov/debar059.htm>

2.3.3 U.S. Department of Treasury, Office of Foreign Assets Control
<http://www.treas.gov/offices/enforcement/ofac/sdn/>

2.3.3.1 Specially Designated Nationals (SDN) List (Current)

2.3.3.2 SDN Changes List (Current)

2.4 Red Flag Analysis. After the assigned attorney has both (a) reviewed the preliminary information supplied by the Company business or sales employee and (b) conducted the preliminary U.S. government database search, the attorney will determine whether sufficient "red flags" exist to warrant further investigation into the background of the proposed agent or partner.

2.4.1 If the assigned attorney determines that sufficient red flags exist, s/he may recommend that Company not enter into a business engagement with the foreign party, or that such engagement be withheld pending further due diligence with satisfactory results. Company's General Counsel and the Business Segment Head requesting the engagement will determine the scope, supplier and cost of such due diligence investigation.

2.4.2 If the assigned attorney determines that there are not sufficient red flags to warrant a further investigation, or if an investigation is performed and satisfactory

	Global Policy Manual	Page: 9 of 9
Title:	Compliance with Foreign Corrupt Practices Act	GPM No. Rev - 0.3

results received, the attorney approves the engagement of the foreign agent or partner.

2.5 Contract with Proposed Non-U.S. Agent or Partner. Once the assigned attorney approves the engagement:

- 2.5.1 The attorney develops an approved form of written contract to be signed by the foreign agent or partner. All such contracts will contain, among other things, the agent or partner's certification of its review of and adherence to Company's Global Policy on FCPA Compliance.
- 2.5.2 When submitted for Company' signature, the contract package must contain the Company business or sales employee's certification that, to the best of his/her knowledge, information and belief, no transactions under or in furtherance of the requested contract violate or are intended to violate Company's Global Policy on FCPA Compliance.

2.6 Certificate of Compliance.

- 2.6.1 Each foreign agent or partner under contract with Company should be asked to re-certify annually to Company in writing that it has read and complies with Company's Global Policy on FCPA Compliance.
- 2.6.2 Each business or sales employee within Company who recommends that Company retain any foreign agent, consultant or partner must certify to Company in writing that s/he has read and understood Company's Global Policy on FCPA Compliance, and pledges compliance therewith.

	Global Policy Manual	Page: 10 of 10
Title:	Compliance with Foreign Corrupt Practices Act	GPM No. Rev - 0.3

**COMPANY, INC.
GLOBAL POLICY ON COMPLIANCE WITH FOREIGN CORRUPT PRACTICES ACT
FORM OF ANNUAL CERTIFICATION FOR NON-U.S. SALES AGENTS AND PARTNERS**

I, [Name of Individual or Entity] hereby certify that:

- I have received a copy of the written compliance policy and procedures of Company, Inc. and I understand agree to follow such policy and procedures;
- I agree to take no action that might cause Company, Inc. or any of its subsidiary or affiliated entities (collectively, "Company ") to be in violation of the U.S. Foreign Corrupt Practices Act or the laws of other countries that prohibit corrupt payments to public officials;
- Neither I, [Consultant entity name], nor to my knowledge any other person, including but not limited to every employee, representative and agent of [Consultant entity name], has made, offered to make or agreed to make any loan, gift, donation or other payment, directly or indirectly, whether in cash or in kind to or for the benefit of any government official, political party, political party official or candidate for political office in order to obtain or retain business; and
- Should I learn of or have reason to know of any such payment, offer or agreement to make a payment to a government official, political party official or candidate for the purpose of obtaining or retaining business for Company, I will immediately advise Company of my knowledge or suspicion.

By: _____

Title: _____

Date: _____

	Global Policy Manual	Page: 11 of 11
Title:	Compliance with Foreign Corrupt Practices Act	GPM No. Rev - 0.3

**COMPANY, INC.
GLOBAL POLICY ON COMPLIANCE WITH FOREIGN CORRUPT PRACTICES ACT
FORM OF CERTIFICATION FOR EMPLOYEES ENGAGING NON-U.S. SALES AGENTS AND PARTNERS**

I, [Name] hereby certify that:

- I have received a copy of the written compliance policy and procedures of Company, Inc., and I understand agree to follow such policy and procedures;
- I agree to take no action that might cause Company, Inc. or any of its subsidiary or affiliated entities (collectively, "Company") to be in violation of the U.S. Foreign Corrupt Practices Act or the laws of other countries that prohibit corrupt payments to public officials;
- Neither I, nor to my knowledge any other person, including but not limited to [Name of consultant if an individual] [and] every employee, representative and agent of [Consultant entity name], has made, offered to make or agreed to make any loan, gift, donation or other payment, directly or indirectly, whether in cash or in kind to or for the benefit of any government official, political party, political party official or candidate for political office in order to obtain or retain business; and
- Should I learn of or have reason to know of any such payment, offer or agreement to make a payment to a government official, political party official or candidate for the purpose of obtaining or retaining business for Company, I will immediately advise the office of the General Counsel of Company of my knowledge or suspicion.

By: _____

Title: _____

Date: _____



By in-house counsel, for in-house counsel.®

InfoPAKSM

Framework for Conducting Effective Compliance and Ethics Risk Assessments

Sponsored by:



Framework for Conducting Effective Compliance and Ethics Risk Assessments

August 2008

Provided by the Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036
Tel 202.293.4103
Fax 202.293.4701
www.acc.com

This InfoPAKSM is designed to provide corporate counsel with a general overview of the concept of risk assessment and to suggest useful practices for the handling of such in the corporate setting. It is based upon examination of more than a dozen leading organizations' risk assessment methodologies and was authored/compiled by Corpedia, Inc., the leading provider of ethics and compliance program solutions.

The information in this InfoPAK should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of Corpedia, Inc. or of ACC or any of its lawyers, unless so stated. Further, this InfoPAK is not intended as a definitive statement on the subject and should not be construed as legal advice. Rather, this InfoPAK is intended to serve as a tool for readers, providing practical information to the in-house practitioner.

This material was compiled by **Corpedia, Inc.**

For more information about Corpedia, please visit their website at www.corpedia.com or see the "About the Author" section of this document.

Contents

I.	Glossary.....	6
II.	Introduction and Overview.....	7
III.	What is a Risk Assessment and Why is it Important?.....	8
	A. Goals of Risk Assessment	9
	B. Legal Defense and Federal Sentencing Guidelines	9
	C. Benefits	9
IV.	Leading Practices.....	10
	A. Examine All Major Areas of Potential Misconduct	10
	B. Examine Risk Contextually	10
	C. Address Current and Potential Risks	11
	D. Industry Information and Historical Incidence Reports	11
	E. Participants From All Levels of the Organization	11
	F. Impact and Likelihood of Occurrence	11
	G. Document the Outcome	12
	H. Be Defensibly Objective.	12
	I. "Quantification" of Each Risk Area.	13
	J. Be Sufficiently Periodic	14
	K. Measure of Employee Knowledge	14
	L. Benchmarking.	14
	M. Coordinating with Internal Audits.	15
V.	Major Universal Components of an Effective Risk Assessment	16
	A. Sufficiently Flexible to Add Unforeseen Risks Introduced During Assessment Execution	17
	B. Measures and Ranks Risk in Accordance with Enterprise Impact	17
	C. Has a Standardized and Documented Approach that is Defensible and Repeatable	18
	D. Enterprise Wide to Accommodate Global Risks	18
	E. Distinct from Sarbanes-Oxley 404 Assessments	18
VI.	What to Examine in a Risk Assessment.....	19
VII.	The 10-Step Risk Assessment Process	21
	A. Step 1: Definition of Objectives, Criteria, Process, and Documentation	22
	1. Desired Outcome	
	2. Target Audience	
	3. Use of Report	
	4. The Issue of Document Creation and Privilege	
	B. Step 2: Planning of the Process	25
	1. Appoint a Risk Assessment Leader	
	2. Identify and Select Team Members	

	3. Decide Which Steps to Include/Perform	
	4. Will You Quantify Risk or Just Write a Qualitative Report?	
	5. Will You Be Conducting Workshops?	
	6. Will You Be Conducting an Employee Survey?	
	7. Estimate Resources	
	8. Set Milestones	
C.	Step 3: Profile the Organization	29
D.	Step 4: Catalogue Risk Area Universe.	30
	1. Tips	
E.	Step 5: Rate Risk Areas for Severity.	31
	1. Rating System	
	2. Leverage Peer Data	
F.	Step 6: Conduct Interviews, Surveys, and Assessments	32
	1. Interviews	
	2. Assessments	
G.	Step 7: Catalog and Measure Mitigating/Aggravating (M&A) Factors.	33
H.	Step 8: Determine Risk-Event Probability or Likelihood	34
I.	Step 9: Determine Aggregate Risk Scores and Final Ranking	34
J.	Step 10: Finalize Risk Assessment Report and Create Mitigation Action Plan	35
	1. Report	
	2. Mitigation Action Plan	
VIII.	In-House vs. Outsourcing the Risk Assessment	37
A.	In-House	37
	1. Inadequate Process Knowledge	
	2. Ineffective Survey Knowledge and/or Interviewing Skills	
	3. Weak Data Analysis and Interpretation	
	4. Biased Judgment	
B.	Hire Outside Advisors.	38
	1. Who Are They?	
	2. Why is it a Good Idea?	
IX.	About the Author	41
X.	Additional Resources.	42
XI.	Sample Forms.	43
XII.	Endnotes	45

TABLE OF FIGURES

Figure 1	Percentage of Organizations that Conducted Periodic Risk Assessments
Figure 2	Percentage of Organizations that Examine Risk by both Likelihood and Severity in Risk Assessments
Figure 3	Level of Involvement of Independent Parties in Compliance Risk Assessment
Figure 4	Percentage of Organizations that Quantify Risk as Part of Risk Assessment Process Outcome
Figure 5	Percentage of Organizations That Coordinate Compliance Activities with Internal Audit
Figure 6	Risk Assessment Process Grid
Figure 7	Target Audiences for the Risk Assessment
Figure 8	Percentage of Organizations that Believe Attorney-Client Privilege Protections Still Exist
Figure 9	Percentage of Organizations that Prioritize Risk in a Quantitative Manner
Figure 10	Percentage of Publicly-Traded Companies in the U.S. that Prioritize Risk in a Quantitative Manner
Figure 11	Risk Universe
Figure 12	Compliance Diagnostic Assessment
Figure 13	Risk Likelihood Scale Example
Figure 14	Risk Likelihood-Severity Matrix
Figure 15	Percentage of Organizations that Conducted Risk Assessments In-House vs. Using External Advisors or a Combination of Both
Figure 16	Types of Outside Advisors Hired to Help Conduct Risk Assessments

I. Glossary

Below are summary definitions of some of the terms used in this InfoPAKSM.

A. Enterprise Impact

A product of risk severity and likelihood of occurrence, Enterprise Impact is the significance or effect (either positive or negative) that a unique risk or risks can have on an organization.

B. External Aggravating Factors

The factors (political, legal, environmental, socioeconomic, etc.) outside of the actual organization, which play a role in subjecting the organization to heightened risk.

C. Internal Aggravating Factors

The factors specific to an organization's unique circumstances or operation. Such factors can be identified through a number of methods, including, but not limited to, interviews, assessments/surveys, examination of available policies and procedures, financial reporting, etc.

D. Internal Mitigating Factors

These pertain to specific elements unique to the organization that can provide a reduction effect to identified risk areas relevant to the organization.

E. Occurrence Likelihood

The reasonable likelihood of a risk event occurring for a typical or average company in a given industry.

F. Risk Severity

The maximum potential economic outcome of violation or misconduct for a typical company in a given industry, measured in terms of total enterprise impact.

G. Risk Area Weighting

Practice of assigning unique values or ratings to areas of risk, where the specific weights are quantified by both impact and likelihood of occurrence.

H. Risk Assessment Team

Collection of individuals or employees of an organization tasked with the re-

sponsibility of researching and evaluating the overall environment of risk in the organization, as well as recommending future action to manage identified risk areas.

I. Risk Universe

This term pertains to a catalog or inventory of identified risk areas relevant to the subject organization.

J. Sarbanes-Oxley § 404

Pertains to the information detailed in Section 404 of the Sarbanes-Oxley Act of 2002 (“SOX 404”). This section outlines the requirements for a publicly traded organization to present a Management Assessment of Internal Controls when issuing an annual report.

K. PCAOB Auditing Standard #5

Pertains to AS#5 that recently replaced AS#2. Approved by the SEC in July 2007, AS#2 is aimed at improving the accuracy of financial reports while reducing unnecessary costs, especially for smaller companies. The standard allows management to rely on assessment of internal controls by other independent managers when certifying to the effectiveness of internal controls to meet SOX 404 requirements.

II. Introduction and Overview

In this era of heightened expectations for proactive corporate governance and compliance with the Federal Sentencing Guidelines for Organizations (FSG) and the Sarbanes-Oxley Act, more institutions are looking to develop effective risk assessment procedures to help: (1) meet Federal Sentencing Guidelines; (2) prioritize compliance program initiatives and spending; (3) provide a roadmap for improving compliance programs to reduce the likelihood of any material violations of federal, state, and foreign jurisdiction laws and regulations; and (4) demonstrate good-faith compliance efforts in the event of civil or criminal proceedings.

While the reasons for conducting a risk assessment are apparent, the overall process and methodology for developing and implementing such an endeavor are less clear. Some of the questions commonly posed by ethics and compliance professionals include:

- How often should risk assessments be performed?
- Should the process be managed by an external third party or can it be performed internally?
- How should risk areas be prioritized, weighted, or ranked?
- Which internal stakeholders should be involved?
- What type of report should be generated and for which audience?
- How should a risk assessment be conducted to provide a strong legal defense in criminal or civil proceedings?
- What type of risk assessment will meet Federal Sentencing Guidelines criteria?

This InfoPAK, based upon examination of more than a dozen leading organizations' risk assessment methodologies, will help address the above questions.

III. What is a Risk Assessment and Why is it Important?

Risk is defined as an uncertain event or condition that, if it occurs, has a positive or negative effect on the entity to which it is tied. The key word is "uncertainty," and as such, it is incumbent upon organizations to proactively and responsibly engage in a process where risks are identified and analyzed, and where strategy is developed to manage or mitigate those risks. The process is commonly known as "risk assessment." It is important to note that other disciplines consider risk assessment and its related activities as an element of a larger enterprise risk management program. Such a claim is valid, but for the purposes

of this paper, we will focus on the specific role and associated tactics and processes of risk assessment as they apply to completing an ethics and legal compliance risk assessment.

Parsing the actual components of a risk assessment, we have the following¹:

- *Risk Identification* – determining which risks are relevant to the organization and documenting their characteristics.
- *Qualitative Analysis* – prioritizing risks for subsequent further analysis or action by assessing and combining their probability of occurrence and impact.
- *Quantitative Analysis* – numerically analyzing the overall effect of risks on the organization.
- *Defining Risk Appetite* – To properly prioritize risks for setting compliance priorities, management must define its risk appetite (whether financial, legal, operational or reputational).
- *Risk Mitigation* – developing options and actions to enhance opportunities and/or reduce threats to the organization.

A. Goals of Risk Assessment

For organizations intent on completing an ethical and legal compliance risk assessment, the primary goals are as follows:

- To evaluate, quantify, and prioritize legal/ethics misconduct and compliance risks specific to current organizational operations;
- To provide rationale for planned compliance and ethics programs, including ethics and compliance training;
- To develop risk mitigation plans, including corporate policies and controls
- To align an organizational compliance program with the Federal Sentencing Guidelines for Organizations
- To develop a benchmark for ongoing risk assessment and measurement of the program's effectiveness.

B. Legal Defense and Federal Sentencing Guidelines

The concept of assessing risk is a critical underpinning to any corporate compliance program. In fact, the Federal Sentencing Guidelines for Organizations explicitly state:

In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.²

C. Benefits

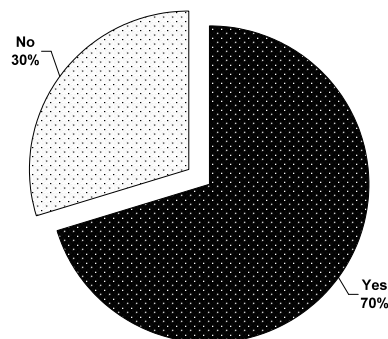
The associated benefits of conducting an effective risk assessment include:

- Helping organizations prioritize compliance budget spending by identifying those areas most in need.
- Enabling the organization to modify and improve compliance program components to reduce risk and increase the likelihood of preventing criminal conduct.
- Providing an affirmative defense to allegations of deficiencies in the design and administration of a compliance program.

Given these benefits, more organizations are conducting periodic risk assessments. As illustrated in Figure 1, in 2007, 70 percent of all surveyed U.S.-based organizations conducted periodic risk assessments.

Figure 1: Percentage of Organizations that Conducted Periodic Risk Assessments

Does your organization conduct periodic Risk Assessments?



Source: ACC-Corpedia 2007 Compliance Program Benchmarking Survey

IV. Leading Practices

Many organizations are confused as to the scope, frequency and structure of an effective risk assessment. However, as more and more organizations have embarked on compliance risk assessments and started to develop their methodologies, leading practices are emerging, which are outlined below.

A. Examine All Major Areas of Potential Misconduct

An effective risk assessment examines all major areas of potential misconduct. A common mistake made by organizations when conducting a risk assessment is to limit the potential risk universe to a preconceived short list of likely high impact risks. However, a proper risk assessment includes the full realm of potential risks, both systemic to the average organization, as well as those that are unique to the industry within which the organization operates. A good risk assessment would seek to catalogue and examine risks of non-compliance with every applicable federal, state, and local law or regulation, as well as other ethics-related areas which may have an adverse impact on organization's image and reputation.

B. Examine Risk Contextually

To be most effective, a risk assessment must examine risk within the context of the ability of the organization to plan for, prevent, or mitigate each risk area. This means including an examination of the controls, processes and procedures designed to prevent compliance failure. It may also entail assessing the capabilities of the individuals in positions of substantial authority from the standpoint of their effectiveness in recognizing and preventing a compliance breakdown.

C. Address Current and Potential Risks

An effective risk assessment should address both current and potential risks. It should not only address risks that exist today, but also address those risks which may not yet be deemed illegal but could reasonably be called into question in the future. Moreover, acceptable industry practices today could be called into question tomorrow.

D. Industry Information and Historical Incidence Reports

Risk assessments should include an examination of industry information as well as historical incidence reports. Document review should not be limited to internal corporate documents, but should also look externally. To be adequately predictive, an effective risk assessment should not only include "compliance breakdowns and failures," but "near misses," as well. This is particularly important when it comes to modifying the compliance program as outlined under FSG.

E. Participants From All Levels of the Organization

Risk assessments should involve participants from all levels of the organization. The leader of the risk assessment process should solicit the involvement of both functional (e.g., sales, marketing, finance) and line (e.g., division heads, executive team) leadership in collecting and assessing potential risk areas. This is

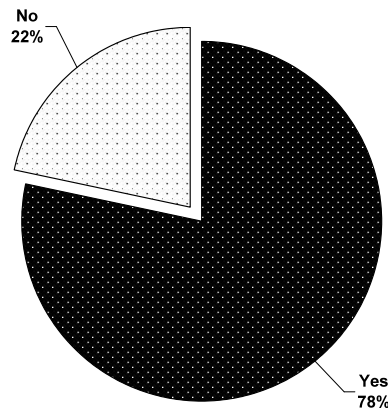
commonly done through workshops, focus groups, surveys, and interviews.

F. Impact and Likelihood of Occurrence

Risk areas should be weighted to account for impact and likelihood of occurrence. When conducting the risk assessment, the organization should assign quantifiable “likelihood” and “severity” weights or ratings to each relevant risk area. Utilizing this type of analysis helps organizations rank relevant risk areas (from minor to severe impact and low to high chance of occurrence). Performing such an activity is becoming a more common trend among organizations. As Figure 2 illustrates, nearly 80 percent of all surveyed U.S.-based companies now analyze risk for both likelihood of occurrence and severity basis.

Figure 2: Percentage of Organizations that Examine Risk by both Likelihood and Severity in Risk Assessments

Is the risk prioritized from BOTH the likelihood and the impact of violation standpoints?



Source: ACC-Corpedia 2007 Benchmarking Survey

G. Document the Outcome

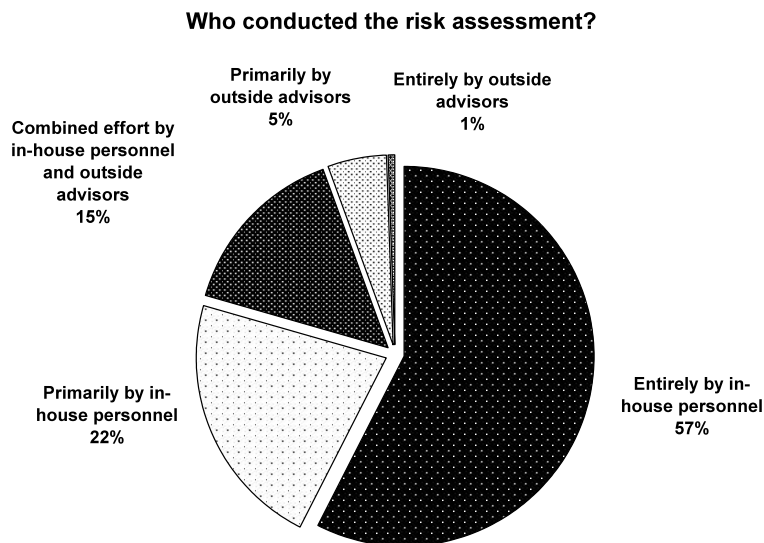
The organization should document the outcome of the risk assessment into a defensible action plan. Good documentation may be introduced as an affirmative defense, supporting the existence of an effective compliance and ethics program in the event of misconduct. Such documentation should not only include the risk assessment process followed; more importantly, it should also specify what actions were taken to design and implement a new compliance program or modify the existing one.

H. Be Defensibly Objective

The process methodology behind the risk assessment must be defensibly objec-

tive. This includes fairly assessing the full universe of potential risks, including existing acceptable industry practices. An organization needs to resist any temptation to ignore or de-emphasize risks simply because they may be costly to address (either from a financial or internal political vantage point). To help ensure objectivity, an increasing number of companies are involving domain-expert outside advisors in the assessment. As shown in Figure 3, 43 percent of all surveyed organizations currently involve independent outside parties in conducting risk assessments.

Figure 3: Level of Involvement of Independent Parties in Compliance Risk Assessment



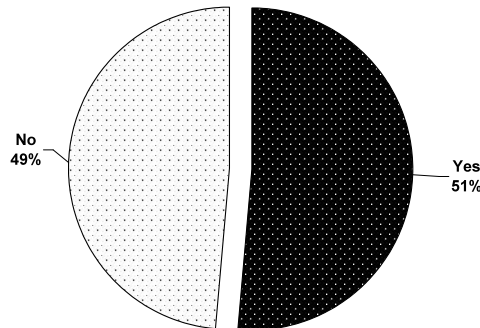
Source: ACC-Corpedia 2007 Benchmarking Survey

I. “Quantification” of Each Risk Area

The process in which the risk assessment is conducted should allow for specific “quantification” of each risk area. A risk assessment that goes beyond examining mere “likelihood” and “severity” can be more useful in prioritizing compliance budget spending and activities, as well as justify any incremental controls, policies, processes or costs that need to be implemented. Furthermore, if executed correctly, such quantification can be used to measure program effectiveness (another FSG criterion for effective compliance and ethics programs). For example, of the 78 percent of organizations that rank risk by likelihood and severity of impact, 51 percent of these companies also quantify each risk area.

Figure 4: Percentage of Organizations that Quantify Risk as Part of Risk Assessment Process Outcome

Does your organization's risk assessment prioritize risk in a quantitative way?



Source: ACC-Corpedia 2007 Benchmarking Survey

J. Be Sufficiently Periodic

The risk assessment should be sufficiently periodic. Risk assessments should not be a one-time activity. The frequency at which an organization chooses to conduct risk assessments and schedule follow-up risk reviews may depend on the nature of the organization's industry. However, if the methodology and process for the risk assessment is adequately defined, a risk assessment can be conducted on an annual basis. Operating environments, regulations and government enforcement priorities routinely change. As such, it is inadvisable to conduct risk assessments less frequently than every two years. Furthermore, infrequent risk assessments are of less value when they are used to measure the effectiveness of a compliance program.

K. Measure of Employee Knowledge

The risk assessment should include measurement of employee knowledge and awareness of the compliance program and supporting controls. Most companies include employee knowledge and awareness as a measurement factor in their risk assessments.³ Doing so can help pinpoint where communications and training programs need to be improved. One of the most common ways of accomplishing this is through online employee surveys, either as part of a COSO-aligned self-assessment, or run independently.

L. Benchmarking

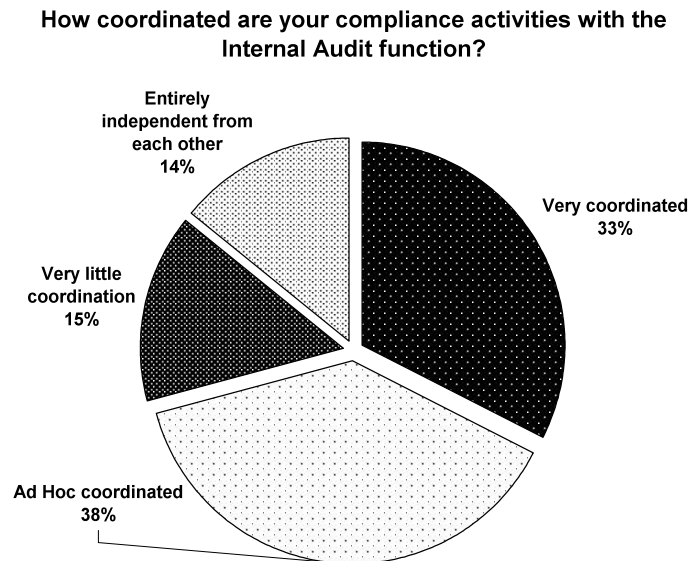
The risk assessment should benchmark against peer organizations. If it is feasible and such information is accessible, companies should compare their risk

areas and compliance program activities with others within their industry or with other companies that may have a similar size and operational profile. This is of particular importance as it ensures that the organization meets “accepted or applicable industry practice” as outlined in the application notes to the U.S. Federal Sentencing Guidelines Manual⁴ Although a company may reach out directly to a competitor to conduct a benchmarking survey, this is not advised due to antitrust concerns. Another resource that is commonly used by organizations for benchmarking data is Corpedia’s ECERA™ (Enterprise Compliance and Ethics Risk Assessment) database on hundreds of organizations’ compliance programs.⁵

M. Coordinating with Internal Audits

It is common and often useful to coordinate the risk assessment with internal audits. More and more companies these days are taking steps to increase coordination between the internal audit and ethics and legal compliance risk assessment. After all, a risk assessment is used to identify, measure, and rank risk areas. Completing one produces the following results for the internal audit: (1) aligns company focus and resources to address areas of greatest significance to the organization; and (2) allows the auditor to design a program that tests the most important internal controls. According to the 2007 ACC/Corpedia Benchmarking Survey, approximately one-third of respondents said that their risk assessment process was very coordinated with internal audit (see Figure 5). Moreover, a significantly higher percentage of publicly-traded companies (82 percent) reported that some form of coordination on risk assessment with internal audit existed, either in a formal or ad hoc basis, compared to private organizations.⁶

Figure 5: Percentage of Organizations that Coordinate Compliance Activities with Internal Audit



Source: ACC-Corpedia 2007 Benchmarking Survey

Using information from one in the preparation for the other is acceptable and recommended. However, the organization must never confuse the primary purpose of either, and the associated analysis must be kept separate and distinct. Remember, an internal audit focuses primarily on internal controls and financial risks, whereas an effective risk assessment will look at a much broader universe of compliance and ethics risks (such as employment law, antitrust, environment, safety, health, trade compliance, privacy, etc.).

V. Major Universal Components of an Effective Risk Assessment

Before commencing your risk assessment, it is important to understand some of the key components that comprise the design of any effective risk assessment. These components help ensure that a risk assessment will capture and measure all risk, both apparent and unforeseen, and they provide a framework for a repeatable process that can be used effectively for planning and improving any compliance program.

Below are the five fundamental components that a risk assessment plan should include:

<input checked="" type="checkbox"/>	Sufficiently Flexible to Add Unforeseen Risks Introduced During Assessment Execution
<input checked="" type="checkbox"/>	Measures and Ranks Risk in Accordance with Enterprise Impact
<input checked="" type="checkbox"/>	Has a Standardized and Documented Approach that is Defensible and Repeatable
<input checked="" type="checkbox"/>	Enterprise-Wide to Accommodate Global Risks
<input checked="" type="checkbox"/>	Distinct from Sarbanes-Oxley 404 Assessments

A. Sufficiently Flexible to Add Unforeseen Risks Introduced During Assessment Execution

Naturally, organizations attempt to catalogue a portfolio of potential risk areas when embarking on a risk assessment. This risk portfolio may be independently derived, or alternatively, the organization may leverage an external resource (for example, a risk database that bears information on common risk areas). Regardless of how comprehensive a “risk universe catalog” may appear to be, a good risk assessment process is flexible enough to allow for the addition of new or unforeseen risks. New risk areas may be identified by the risk assessment team, advisory councils, business leadership, or employee surveys, but there may also be an “alternative interpretation” of a catalogued risk that needs to be addressed. For example, it is not unusual for established commonly-accepted business practices in any industry to come under new scrutiny given increased awareness and sensitivity to compliance and corporate governance.

B. Measures and Ranks Risk in Accordance with Enterprise Impact

Not all compliance failures that could result in violations of the law are equal. While one “material violation of law” may result in a fine or penalty as well as substantial legal defense costs, a different “material violation of law” can have a far greater impact on an organization’s operations through substantial customer and contract losses, reputation damage or even necessitated changes to the business model. The varied impact of various compliance failures by area or category of risk are not the same for all organizations, but may depend on such factors as the industry in which an organization operates, any historical incidence of compliance failures, and judicial enforcement trends. OMB Auditing Standard 133 translates the internal control deficiencies defined in SAS 112 into compliance terms (e.g., defines substantial deficiency and material weakness to possible compliance risks), and these are useful for standardizing and comparing compliance risks. The compliance risk assessment should also define standard “risk appetites” across risk areas (financial, operational, legal, and reputational),

so that different risks may be objectively compared.

C. Has a Standardized and Documented Approach that is Defensible and Repeatable

A common failing of risk assessment efforts is when they are treated as a one-time event and lack sufficient process and documentation. Federal Sentencing Guidelines criteria for an “effective compliance and ethics program” set forth expectations that risk assessments are a recurring activity within an organization’s overall compliance program. A well-designed risk assessment has a systematic methodology and well-documented process, and therefore is more likely to be deemed objective. Organizations should be concerned about objectivity because imputed subjective bias on the part of those conducting the risk assessment (particularly if conducted by internal personnel) can undermine the credibility of the final outcome.

Documented and standardized processes allow for more cost-effective repetition of the risk assessment processes as the inevitable endemic change occurs both within the organization, as well as the business environment in which it operates (e.g., new laws or interpretations of existing laws come into existence; compliance and legal departments experience personnel turnover; organizations divest operations or enter into new business activities or markets). Additionally, with a standardized and documented process towards assessing and prioritizing risk, a risk assessment may be sufficiently defensible as to be able to “measure effectiveness” of an organization’s compliance and ethics program through comparing outcomes over a series of sequential risk assessments.

D. Enterprise Wide to Accommodate Global Risks

When examined through the lens of an “effective compliance and ethics program,” limiting a risk assessment to an organizational “silo,” such as specific geographic regions or unique functional areas, can leave the organization open to exposed risks. For example, in recent years, some of the most costly compliance failures (in terms of out-of-pocket and reputational damage) for U.S. organizations have occurred overseas. While it is tempting to focus an assessment on those areas with which the legal department is most familiar, doing so would undermine the defensibility of the analysis outcome.

E. Distinct from Sarbanes-Oxley § 404 Assessments

While there are certainly correlations between work performed by the internal audit function of any organization and a risk assessment undertaken by the compliance, ethics or legal department, analyses must still be kept separate and distinct. Sarbanes-Oxley § 404 requires management to document and assess the effectiveness of their internal controls over financial reporting. With the advent of new guidance from the SEC in the form of the May 25, 2005 Bulletin,

organizations may use a risk prioritization approach to conducting their § 404 work in the future. While such risk prioritizations may interlay with risk assessment, the fundamental elements being examined under § 404 (effectiveness of internal controls, which may include processes and procedures to detect material violations of law that could affect financial statements) are very different from an assessment of risk areas from a weighted, occurrence likelihood and deterrence element, which are essential to any effective risk assessment.

In short, the type of “risk” from the internal audit viewpoint is fundamentally different from the type of “risk” that should be applied by the legal compliance function. Using information from one analysis or assessment in the preparation of the other is acceptable and recommended. However, allowing the two to become interchangeable is a mistake as these are not identical types of “risk.” While internal audit may participate in, or possibly even lead a legal compliance risk assessment, a legal compliance risk assessment must be sufficiently distinct and independent from the material disclosure work done for Sarbanes-Oxley § 404. However, the assessment of internal controls conducted in the course of a § 404 audit can be effectively used as a part of the risk assessment, and vice versa. Many companies successfully use COSO methodology for conducting internal control surveys, including surveys of compliance internal controls to the extent that they may potentially impact on financial statements. Compliance risk assessment can be aligned with internal audit by using COSO methodology to conduct broader compliance risk analysis, which requires an assessment of internal controls. Under PCAOB AS #5, management can use our independent assessment of compliance internal controls to support their annual certifications. Conducted properly, compliance risk assessments can, in part, serve this dual purpose.

VI. What to Examine in a Risk Assessment

So what exactly does an organization examine in a risk assessment? When conducting the risk assessment, the organization should assign quantifiable “likelihood” and “severity” weights or ratings to each identified risk area. There are numerous resources, both internal and external, that are extremely useful in helping to determine likelihood and severity of any given risk. When looking at severity of risk, a good approach is to compute maximum potential severity, or the worst that could happen to the organization should a particular type of misconduct occur. The factors that drive the severity are almost too numerous to be listed. However, we list here the most obvious ones that should be considered.

- Civil and criminal penalties potentially resulting from violations

- Legal defense costs
- Litigation settlements
- Impact on a company's revenue, earnings, and bottom line
- Impact on a company's stock value
- Impact on credit rating and cost of capital
- Employee turnover
- Customer loss
- Change in business model and operations, such as shutdown of various business operations or product or service lines
- Debarment from participation in government contract or grant programs
- Change in market share
- Reputation damage
- Negative media coverage
- NGO/advocacy group pressure
- Increased future costs of compliance
- Current and anticipated regulatory initiatives and enforcement/prosecution priorities.

We recognize that most organizations lack internal data or internal experience from prior incidences to accurately determine severity of risk areas under examination. However, industry experience, as well as broader corporate experience, can provide adequate information for reasonably accurate analysis of risk severity. There are a number of studies available that seek to statistically measure severity of various risk areas for major industries. It is important to note that while it is very important to have an accurate understanding of risk severity, in reality there is little an organization can do to reduce the risk severity. What the organization can do, however, is to reduce the likelihood of risk. Therefore, an accurate assessment of the likelihood and a good understanding of the underlying factors are key elements of any good risk assessment methodology.

The risk likelihood is a combination of internal factors which determine the probability that a particular type of misconduct will occur. The following major factors affect—indeed, create—the risk probability:

- Organization's business activities;
- Organization's policies, processes, and controls;
- Organizational culture and ethics;
- Employee knowledge, awareness and intent.

Below is a sample of some of the key tools and activities an organization can utilize to aid the risk assessment process:

- Executive interviews and focus groups
- Organizational health survey

- Employee awareness/knowledge assessment
- Examination of corporate policies, processes and controls per risk area
- Examination of the anonymous reporting system statistics
- Review of other historical incidence
- Evaluation of existing training inventory and courseware
- Interviews with training “owners”
- Examination of prior audits, surveys and reports
- Review corporate publications (Code of Business Conduct, Employee Guides, New Hire Kits, etc.)
- Examination of organizational charts and reporting relationships
- Review of Audit Committee Charter and Corporate Governance Principles
- Assessment of employee disclosure and acknowledgement forms
- Analyst reports.

VII. The 10-Step Risk Assessment Process

The following is a discussion on the ten key steps in an effective risk assessment process. This process represents an amalgamation of best practices and methodologies employed by leading organizations that Corpedia has either observed or worked with via prior engagements. Depending on resources and facility with risk analysis, some companies may eliminate or combine certain steps. Others may wish to add incremental steps, such as peer analysis and benchmarking.

<u>Step</u>	<u>Description</u>
1.	Definition of Objectives, Criteria, and Documentation
2.	Planning the Process
3.	Profile the Organization
4.	Catalogue Risk Area Universe
5.	Rate Risk Areas for Severity
6.	Conduct Interviews, Surveys, and Assessments
7.	Catalogue and Measure Mitigating & Aggravating Factors
8.	Determine Risk Event Probability or Likelihood
9.	Determine Aggregate Risk Scores (Enterprise Impact) and Final Ranking
10.	Finalize Risk Assessment Report and Create Mitigation Action Plan

Although your organization may deviate from these steps, the fundamental sequential principles are the same in any effective risk assessment. These principles include: plan, profile, assess, rank, and report.

Figure 6: Risk Assessment Process Grid

A. Step I: Definition of Objectives, Criteria, Process, and Documentation

The first step in commencing a risk assessment is to define the process. The proposed methodology needs to be specified as to the desired outcomes and supporting processes for communication and handling documentation. The critical questions that you will need to address are:

- What is the desired outcome?
- Who is the target audience for the final report?
- How will this report be used?
- How will your organization manage the documents to be created?
- How will the issue of “privilege” be addressed?

I. Desired Outcome

For most, the practical role of a risk assessment is to meet the criteria of an “effective compliance and ethics program” set forth in the Federal Sentencing Guidelines. However, taking it one step further, your risk assessment should reaffirm the priorities of and the emphasis on an existing compliance program, or

it can serve as a guidepost for the creation of a new program where none exists. Knowing the parameters of the outcome may sound simple, but in reality the answer to the above questions will determine the scope, depth and breadth of your risk assessment. For example, if you are reaffirming priorities of an established program, then the risk assessment might be built around a focus on the risk categories and areas already contained and set forth in your organization's Code of Conduct. On the other hand, in the absence of a mature compliance program, in order to use the risk assessment for purposes of budgeting and building a new or reestablished compliance program, it is preferable to:

- Examine a far greater range of risk areas;
- Research what peers of similar size or industry are doing; and
- Broaden the scope of the risk assessment team to include key functional areas and business leaders.

2. Target Audience

It is quite possible to have several target audiences. Knowing your target audience will better prepare you for the type of data that needs to be collected in the risk assessment itself. In our experience and review of leading organizations' risk assessment reports, some common target audiences include those featured below:

Figure 7: Target Audiences for the Risk Assessment

More Common ↓ Less Common	Audit Committee
	Internal Legal Counsel
	Executive Leadership
	External Legal Counsel
	Internal Audit/CFO
	Insurance Carriers/Underwriters
	Human Resources/Training
	Employee Base
	Shareholders

3. Use of Report

This report can be and is used to address/support such things as:

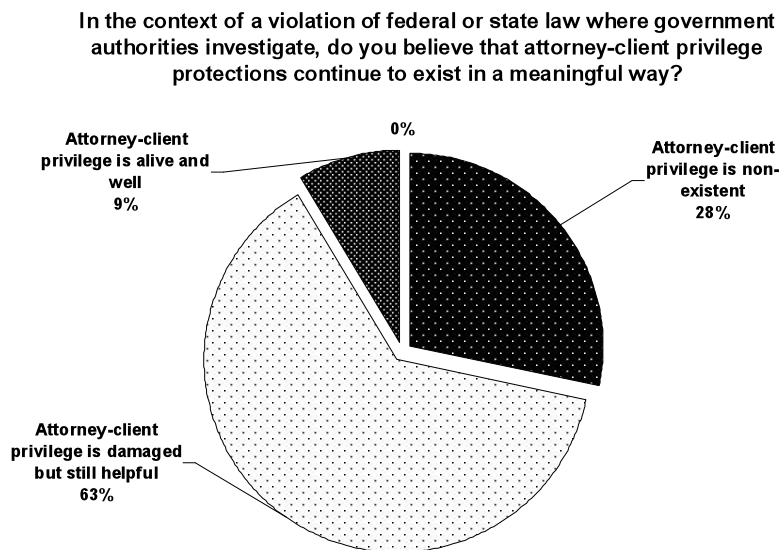
- Policy and process creation
- Training initiatives
- Sarbanes-Oxley § 404 work prioritization
- Purchase of incremental insurance
- Divestment of product lines, customers or markets, etc.

4. The Issue of Document Creation and Privilege

While completing a risk assessment can be very beneficial, organizations should be aware that, if poorly executed, the sensitive information collected as part of the risk assessment can potentially subject the organization to harm. One of the most vexing issues facing any legal department today when it comes to conducting a risk assessment is making sure that the form, content, and tone of any document created by the risk assessment team does not subject the organization to any unintended harm. Assuming that all created documents are protected by attorney-client or work product privilege is a flawed and dangerous assumption, as many documents may fall outside of the established privilege parameters in how they are generated or shared.

Privilege is very hard to maintain in today's legal environment, and the veil of privilege is commonly pierced through waiver in regulatory and judicial investigations. In light of these issues, many corporate counsels embrace an operating assumption that privilege is of limited use or thereby should not be relied upon. As illustrated in Figure 8, twenty-eight percent of organizations feel that attorney-client privilege within the context of a government investigation no longer exists in a meaningful form.

Figure 8: Percentage of Organizations that Believe Attorney-Client Privilege Protections Still Exist and Are Meaningful



Source: ACC-Corpedia 2007 Benchmarking Survey

Any risk assessment will contain lists, descriptions, and theoretical suggestions about current or possible future compliance problems. For example, envisioning

“what could go wrong” is a useful exercise in helping to prevent such an occurrence. At the same time, should such an envisioned compliance problem later occur, a written document from such an exercise could be taken out of context as “evidence” of preexisting knowledge of a compliance problem or deficiency that an organization failed to address.

An additional complication is that an effective risk assessment commonly includes a diverse team of individuals, including employees and non-company personnel. It is likely that the majority of these individuals will not be attorneys, and many of them may not be knowledgeable about the concept of privilege and the associated dangers of document and content creation. Furthermore, some of these individuals, bearing an intention of wishing to grandstand their participation or simply being misguided, can lend themselves to dramatic verbiage and pronouncements about potential risk areas in their documentation creation. As a result, at this stage in the risk assessment process, guidelines and protocols for document creation should be established for the risk assessment team and any other key contributors. At a minimum, documentation guidelines should include the following:

■ **Detailed Guidelines on Document Creation**

Guidelines should focus on counseling participants to be clear in their writing and to use neutral language that avoids hyperboles and exaggeration. Participants should also understand that any document might be taken out of context. Furthermore, participants need to understand that these guidelines also apply to shorthand, margin and handwritten comments and notes.

■ **Limitations on Document Distribution**

Naturally, the more broadly that drafts and documents are copied and distributed, the greater the risks of losing control over what exists. There should be clear parameters for where documents are submitted and stored after creation.

■ **Provide Guideline Templates**

Should participants be part of ranking risks and creating hypotheticals, it is best to provide a description template with which they should work.

B. Step 2: Planning of the Process

Once the organization has clearly defined the purpose, process, and desired outcomes of the risk assessment, it is important to map out a plan for how the organization plans to execute the process.

I. Appoint a Risk Assessment Leader

Important to any new endeavor, a leader must be selected to oversee the risk assessment process. Depending on the organization, this individual could be drawn from any number of roles including general counsel, chief compliance

officer, ethics officer, head of risk management, or possibly the director of human resources. It is also possible that this individual could be appointed by any of the individuals listed above. Regardless of the level, the leader of the risk assessment process must be empowered to control the process from inception through final implementation.

2. Identify and Select Team Members

No leader can succeed without effective team members. As such, it is important to identify key individuals in the organization who will serve as members of the risk assessment team.

Some of the more common ones include:

- General Counsel and/or Chief Compliance Officer
- Legal and/or Compliance Subject Matter Experts
- Business Unit or Functional Heads
- Outside attorneys or consultants (as necessary).

When selecting team members, it is important “to ensure participants are familiar with the purpose, scope and elements of a risk assessment process and possess relevant functional and/or business unit background information and experience.”⁷

3. Decide Which Steps to Include/Perform

Each organization is unique and therefore is likely to be at a different stage or maturity level in terms of conducting risk assessments. Novice organizations that are implementing or planning to implement a risk assessment for the first time would be advised to complete each step, while other more experienced entities that have completed multiple risk assessments may decide to limit the process.

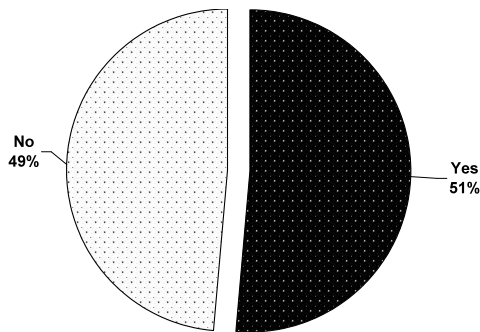
4. Will You Quantify Risk or Just Write a Qualitative Report?

Another decision to be made by the organization is whether or not the portfolio of risks will be quantified or assigned a value based on impact to the organization as well as likelihood of occurrence. The value in conducting a risk assessment is the ability to measure the degree to which a specific risk can impact the organization, either positively or negatively. Positive risks present opportunities for the organization while negative risks naturally serve as potential threats. Depending on the type of organization and its associated industry, the number of potential risk areas for the organization can vary. As such, the quantification of risk areas provides a mechanism to allow for the ranking of risk areas.

Incidentally, based on recent research, many companies still decline to quantify their risk areas and instead rely on a more subjective, qualitative analysis where they base their risk assessment and corresponding mitigating strategies on opinions and feedback from personnel in their organization. As illustrated in Figure 9, a little over half (51 percent) of all organizations actually quantify risk in their risk assessments.⁸

Figure 9: Percentage of Organizations that Prioritize Risk in a Quantitative Manner

Does your organization's risk assessment prioritize risk in a quantitative way?

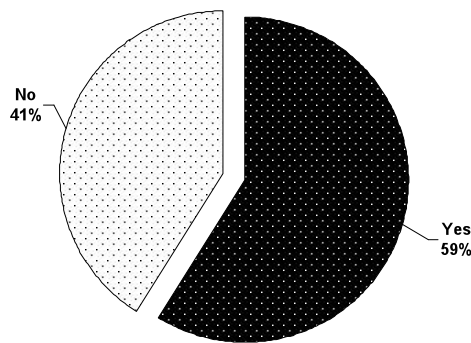


Source: ACC-Corpedia 2007 Benchmarking Survey

Moreover, as shown in Figure 10, publicly-traded companies in the United States are 59 percent more likely to quantify risk versus foreign or private organizations.

Figure 10: Percentage of Publicly-Traded Companies in the U.S. that Prioritize Risk in a Quantitative Manner

Does your organization's risk assessment prioritize risk in a quantitative way?



Source: ACC-Corpedia 2007 Benchmarking Survey

5. Will You Be Conducting Workshops?

Some organizations choose to conduct group meetings or workshops to identify, evaluate and prioritize risk areas. These meetings are managed by the risk assessment leader with the aid of the risk assessment team. All of the relevant risks to the organization are examined, and a severity and likelihood score is assigned to each risk. Whether or not workshops will be a productive activity really depends on the organization. In order for them to work, it is important for the risk assessment leader to fully manage the process. This includes selecting the right participants, defining both guidelines and expectations for these participants, providing sufficient background material and guidance and creating an effective schedule and agenda for the meeting.

6. Will You Be Conducting an Employee Survey?

In the past, when conducting risk assessments, some firms have chosen to exclude the broad employee base and focused their risk assessment queries on key functional area and business leaders of the organization. In fact, recent research conducted by Corpedia and the Association of Corporate Counsel found that less than 24 percent of organizations actually use workforce surveys as part of the risk assessment process.⁹ Taking the time to perform an employee survey can help protect the organization from premature dismissal or a failure to recognize certain risk areas. It is not uncommon, especially in highly decentralized organizations, for gaps in information and communication failures to exist. As such, including an employee survey as part of the overall risk assessment will

lessen the chance of omitting a key risk area.

7. Estimate Resources

When planning the scope of the risk assessment, decisions will need to be made on what resources are needed, estimates on how much time is required of those resources, and verification of availability of those resources. It is important for all participants of the risk assessment to make an honest and effective contribution to the process. Given the importance of the risk assessment to the organization, any weakened participation can lead to holes in the overall risk assessment effort. As part of the resource identification and planning, another important decision will be whether to conduct the risk assessment entirely in-house or in association with an external party or advisor (law firm, audit firm, etc.). A more in-depth discussion of the associated costs/benefits is available below in Section VIII, In-house vs. Outsourcing the Risk Assessment.

8. Set Milestones

An effective risk assessment involves a significant number of interrelated tasks necessitating the active involvement of many individuals. Moreover, depending on the actual number of risk areas assessed, the process can become a very complicated activity. As such, it is important for the overall leader of the risk assessment to set specific measurable goals and checkpoints throughout the process. The use of milestones will help guide individual contribution as well as place structure around a process with multiple diverse inputs.

C. Step 3: Profile the Organization

Once the planning stage has been completed, the next step is to develop an accurate profile of the organization. This step is not to be underestimated as it effectively drives the rest of the risk assessment process. Moreover, diligence and care should be taken when performing this step of the process. A company's profile dictates the types of risk areas, relevant to the organization. A weakened organizational profile will only lead to an ineffective risk assessment.

Some of the typical elements addressed in a company profile include specifications of the organization in the following areas:

- Industry Type
- Company Size
- Classification (public versus private)
- Key aspects of business operations (e.g., consumer products, government contracting, union environment, etc.)
- International operations

Profiling the organization includes a comprehensive review of business activities, strategy and priorities, industry and geography of operations, workforce

composition, and other operational circumstances that generate exposure to particular risk areas.

D. Step 4: Catalogue Risk Area Universe

Completion of the organizational profile enables the development of a complete catalog of risks also commonly known as a *risk universe*. There are many risks that an organization is exposed to on a daily basis. Many individuals associate risk to the organization with business risks or those risks that affect the delivery of a product or service by affecting the critical constraints of schedule, budget and quality. Our analysis here focuses specifically on ethics and legal compliance risks—that is, those risks related to the potential for business misconduct and/or violations of federal, state and/or local laws and regulations. A robust risk assessment process would attempt to map out every business process, the associated ethics, and the associated compliance risks for an organization. This process would be updated annually and used for conducting risk assessment.

I. Tips

When developing the risk universe, it is necessary to take a comprehensive view. The organization must strive to first identify and scrutinize risks to pinpoint the root cause and then widen the examination to account for systemic risks (common to the average organization), industry-specific risks, and finally, organization-specific risks. It is also useful to rely on the experience of peer groups and review historical incidence.

Figure II: Risk Universe



Moreover, it is useful to display the entire set of risks in an Excel grid format. Doing so enables risk assessment leaders or team members to capture, sort and rank the risk areas later in the process, once they have been rated for severity and likelihood of occurrence. An example of this type of grid is available in Section XI, Sample Forms.

E. Step 5: Rate Risk Areas for Severity

Once the risk area universe is fully developed and you are confident that all relevant risk areas to the organization have been addressed, the next step in the process is to rate those risk areas for severity. Industry severity can be described as the maximum potential outcome of violation or misconduct for a typical or average company in a given industry, measured in terms of total enterprise impact.

Risk event severity is a product of many factors including:

- Civil/criminal penalties, such as SEC/DOJ settlements, lawsuits, etc.;
- Impact on stock price and bottom line;
- Employee turnover and loss of intellectual property;
- Loss of customers and market reputation;
- Systemic business model impact;
- Increased future cost of compliance;
- Current and anticipated future enforcement trends and priorities.

1. Rating System

Risk areas can be rated for severity both subjectively and statistically. The former will typically scale the level of a risk from minor to moderate to severe impact while the latter will rely on a numeric rating or weight assigned to the risk. The scale can vary but often appears in a range of either 1-5 or 1-10 where the level of severity is ranked in ascending order. Furthermore, once the risk likelihood is calculated later in the process, organizations often process both data sets and visually map them on a probability-impact matrix. An example of this matrix is available later in this document.

2. Leverage Peer Data

When evaluating the complete portfolio of risk areas for impact to the organization, one may find it helpful to research available benchmark information on how their industry peers rate or have rated specific risk areas to their organizations. Obviously, when benchmarking, it is important to choose one or more peer organizations that closely match the subject organization in terms of size, industry type, etc. Organizations commonly rely on Corpedia's ECERA™ database for such a benchmarking activity, as it contains specific critical risk severity metric data for over fifty unique industries, collected as a result of in-depth research of over 1,000 U.S. and international corporations.

Another alternative is to actually design a customized industry peer survey and distribute it among a selection of peer organizations in order to obtain common

severity metrics. However, this process may be lengthy and requires effective planning and design by the host organization. Some companies opt to develop an internal database of news items from multiple media sources, which identify potential or actual risks relevant to those companies so they will be “remembered” at the time of periodic risk assessment.

F. Step 6: Conduct Interviews, Surveys, and Assessments

Once the risk universe has been fully developed, the next step in the process is conducting interviews and/or assessments with senior and mid-level managers and key functional area leaders (finance, sales, etc.) of the organization, as well as a sample of the workforce. The prime goal of such interviews and assessments is to collect information that will enable you to determine the likelihood of misconduct with sufficient accuracy. The secondary goal is to verify the integrity of the risk-area universe constructed earlier, and to see whether there are any material risk-areas that may be missing from it. Sometimes, interviews and assessments uncover totally unforeseen yet *material* risks.

I. Interviews

For organizations that do conduct employee interviews as part of the risk assessment process, the three most common groups to be interviewed (based on the survey results) are: 1) Executive Team (81%); 2) HQ Functional Department Management (73%); and 3) Operational Field Management (66%). However, there is a significant drop-off before involving additional lower-level employees in the risk assessment process, with only 37% of organizations interviewing any line employees.

2. Assessments

Two general types of assessments can be utilized: *Compliance Diagnostic Assessments* and *Employee Surveys/Assessments*.

- **Compliance Diagnostic Assessments** evaluate such things as organizational policies, processes, procedures and controls, cases of historical incidence, the quality and extent of existing compliance efforts, existing ethics/compliance training programs, current compliance issues, corporate culture (as viewed by senior management), business priorities, an evaluation of the overall compliance and ethics environment, and the commitment to ethics and compliance. While some components of the Compliance Diagnostic are examined through comprehensive analysis of existing data—like training curriculum, code of conduct, management communications, written policies, internal audits, reporting hotline statistics, prior surveys, etc.—a significant portion of data is collected through targeted surveys, questionnaires, and interviews. (See Figure 12 for a snapshot of a typical compliance diagnostic assessment.)

Figure 1 **corpedia**  stic Assessment
ETHICS. ELEVATED.

CORPEDIA
in partnership with

COMPLIANCE DIAGNOSTIC ASSESSMENT
Survey# CD-ATL4

Job Level: **Manager, Non-Manager** Business Unit: **EMERGING BIZ**
Job Function: **SALES** Business Location: **UNITED STATES**

Risk Segment: **ANTI-TRUST**
Risk Area: **COLLUSION**

Q1: My organization has a written policy on fair competition, antitrust and communication with competitors

Yes
 No
 Don't Know

If YES, proceed to Q2. If NO, please skip to Q11.

Q2: The organizational policy on competition prohibits communication with competitors in order to (select all that apply)

Fix prices or other terms of sale
 Allocate or divide customers or markets
 Collaborate on competitive bids
 Agree to boycott certain customers or suppliers

Q3: The organizational policy on competition is effectively communicated to all employees in my business unit

Strongly agree
 Agree
 Neutral
 Disagree
 Strongly disagree
 Don't know

Q4: I am confident in my ability to recognize behavior that violates the policy on competition

Strongly Agree
 Agree
 Neutral
 Disagree
 Strongly Disagree
 Don't Know

Q5: I'm familiar with the contents of the policy on competition

Strongly agree
 Agree
 Neutral
 Disagree
 Strongly disagree

- **Employee Surveys/Assessments**, on the other hand, consist of both organizational health and knowledge assessments. The former seek broad impressions of the organization in regards to the ethics and compliance environment, culture, and overall ethical health, while the latter seek to determine employee comprehension of compliance issues with respect to their specific functional area.

G. Step 7: Catalog and Measure Mitigating/Aggravating (M&A) Factors

The next step of the process involves identifying those specific factors relevant to the organization that can serve to either reduce or increase the level of risk for the organization. Recall that this information is derived from the internal and external factors originally examined in earlier stages of the risk assessment.

H. Step 8: Determine Risk-Event Probability or Likelihood

Information gathered during interviews, surveys, and assessments helps to accurately determine the “risk-likelihood.” Risk-likelihood is defined as a reasonable likelihood of a risk-event occurring for a typical company in a given industry. “Risk event likelihood” is a product of mainly internal organizational factors, including:

- Organizational culture and ethics;
- Compliance initiatives;
- Organizational policies;
- Internal controls;
- Workforce awareness and knowledge; and
- Employee intent.

In terms of an actual scale for rating the likelihood of a risk event, it is common to use a scale of 1-5, as shown in Figure 13 below:

Figure 13: Risk Likelihood Scale Example

Rating	Scale	Description
1	Rare	Highly unlikely, but it may occur in unique circumstances
2	Unlikely	Not expected but there's a slight possibility it may occur
3	Possible	Event may occur at some point – typically there is history to support it
4	Likely	Strong possibility that an event will occur and there is sufficient historical incidence to support it
5	Almost Certain	Highly likely, this event is expected to occur

I. Step 9: Determine Aggregate Risk Scores and Final Ranking

Once risk severity and likelihood is known, an aggregate risk score (Enterprise Impact Score) can be developed. This risk score is essentially the product of risk area severity and likelihood of occurrence. It reflects the significance of a par-

particular risk area to the organization. It is important to note here that this aggregate risk score is only used to facilitate the ranking of the risk areas. This score is *not* a measure of compliance effectiveness of the organization, nor is it intended to compare, rate, or grade the organization's compliance efforts, controls and programs against peers, the market as a whole, or industry best-practices. In practice, it is also common to map these risk scores visually, often in a grid format, like the one featured in Figure 14 below. Mapping the scores will enable the organization to quickly view the most critical risk areas (highlighted in red) and will enable the risk management team to deploy a phased approach to risk mitigation.

Figure 14: Risk Likelihood-Severity Matrix

LIKELIHOOD											
High	5.0	Yellow	Yellow	Yellow	Yellow	Red	Red	Red	Red	Red*	Red*
	4.0	Green	Yellow	Yellow	Yellow	Yellow*	Red	Red*	Red	Red	Red
Medium	3.0	Green	Green*	Yellow	Yellow	Yellow	Yellow	Red	Red	Red	Red
	2.0	Green	Green	Green	Yellow*	Yellow	Yellow	Yellow	Red	Red*	Red
Low	1.0	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Red	Red
		1	2	3	4	5	6	7	8	9	10
		Minor			Moderate				Severe		
		SEVERITY									

- **Level Green:** Risks at this level should be monitored but do not necessarily pose any serious threat to the organization at the present time.
- **Level Yellow:** Organization should proactively take steps to actively monitor and further evaluate these risk areas and likely engage mitigation strategies.
- **Level Red:** Immediate action is required to address these risk areas as the potential for violations or damage to the organization is significant.

J. Step 10: Finalize Risk Assessment Report and Create Mitigation Action Plan

The last phase of the process is the development of a formal written risk assessment report and the creation of the risk mitigation action plan.

I. Report

A risk assessment report should be a comprehensive yet easy to understand document that should reflect a completed compliance risk assessment process which reasonably meets or exceeds Federal Sentencing Guidelines' risk assessment criteria under the definition of an "effective compliance and ethics pro-

gram.” The report and supporting documentation must be created, maintained, and delivered in a methodology that decreases the likelihood of information, as well as surrounding collection of data inputs, being misconstrued or used out of context. This is particularly important for “discovery” reasons, in the event the organization must later serve as a party, a witness, or a principal in litigation or a government investigation.

Some of the key elements of an effective risk assessment report may include:

- **Top Risk Areas.** The report should highlight a specified number of key risk areas.
- **Quantification and Ranking of Risk.** Each risk area should be weighted for severity and likelihood, and ranked according to significance of risk to the organization.
- **Supporting Documentation for Risk Quantification.** Each risk area and its relative weighting are supported by critical information that factors into the final report, including existing key risk aggravating and mitigating factors, such as employee knowledge measurement, existence or lack of a specific policy or control, etc.
- **Specific Risk-Reducing Steps and Recommendations.** Each of the top risk areas is accompanied by specific actions that the organization can take to reduce its contribution to the quantified risk score and “manage” its risks on an ongoing basis.
- **Year-Over-Year Effectiveness Measurement.** As the organization begins to conduct multiple annual risk assessments, the report includes measurements of effectiveness by analyzing and tracking the quantification of each major risk area on a year-over-year basis.
- **Compliance Program Benchmark.** A benchmark of the organization’s compliance program and activities versus its industry peers.

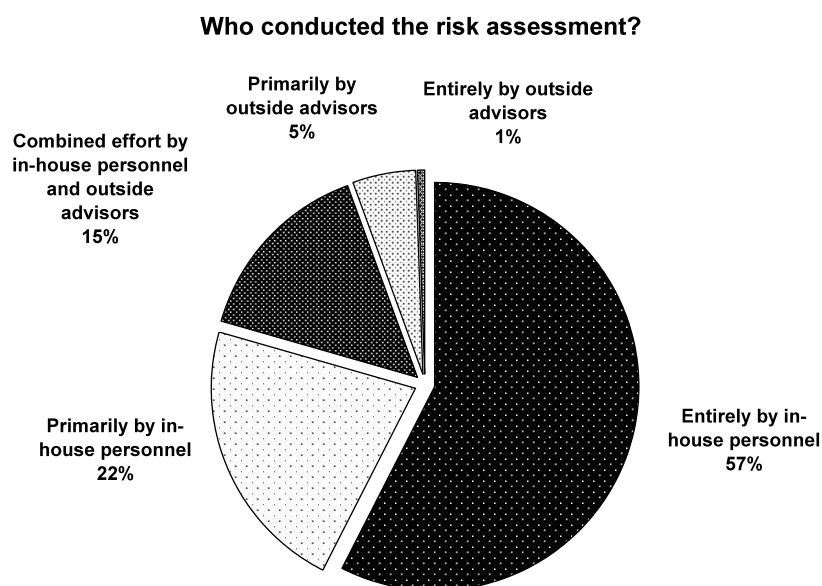
2. Mitigation Action Plan

Once developed, the formal risk assessment report serves as the guide for the creation of an Action Plan to mitigate the top risk areas to the organization. This action plan will enable the risk assessment leader to assign specific risk owners who will lead the process in managing each critical risk area. For each risk, milestones should be developed and tracking of these milestones will help ensure that the process is successfully completed. The action plan itself can take many forms, depending on the desired investment of the subject organization. Types of tools that have been used by organizations range from simple documents and Excel-based workbooks to more advanced risk management software packages and/or web-based applications.

VIII. In-house vs. Outsourcing the Risk Assessment

A decision any organization faces when planning for and implementing an organizational risk assessment is whether the activity should be conducted entirely in-house or if the organization would be better served by hiring external expertise. This decision should not be taken lightly and there are positives and negatives to both approaches. In a recent survey (conducted by ACC and Corpedia), results showed that over half (57 percent) of all organizations conduct their risk assessments entirely in-house, while the remainder (43 percent) use an outside advisor in the process.

Figure 15: Percentage of Organizations that Conducted Risk Assessments
In-House vs. Using External Advisors or a Combination of Both



Source: ACC-Corpedia 2007 Benchmarking Survey

A. In-House

Organizations may choose to conduct a risk assessment purely in-house. There are various reasons why an organization may choose to follow this path including:

- Size of the organization

- Budgetary constraints
- Concerns over confidentiality

However, there are also limitations when opting to conduct risk assessments internally.

I. Inadequate Process Knowledge

One of those concerns is whether or not there exists adequate process knowledge of conducting an effective risk assessment within the organization. As demonstrated in this paper, conducting a risk assessment is a methodical engagement with numerous phases requiring the coordination and participation of various individuals across the organization.

2. Ineffective Survey Knowledge and/or Interviewing Skills

A significant part of any risk assessment process is the ability to extract the most relevant information from individuals in the organization who have domain expertise in their functional area. To do this, individuals on the risk assessment team must be equipped to ask the right types of questions in order to obtain the critical information needed to examine. Without this, certain risk areas must actually be understated and the organization may be exposing itself to future harm.

3. Weak Data Analysis and Interpretation

A good risk assessment process generates a vast amount of data, a large amount of which is qualitative. The inability to accurately quantify all collected data and/or properly analyze and interpret it can significantly undermine the quality of the results.

4. Biased Judgment

Objectivity of the risk assessment includes fairly assessing the full universe of potential risks. An organization needs to resist any temptation to ignore or de-emphasize risks simply because they may be costly to address (either from a financial or internal political vantage point). To help ensure objectivity, an increasing number of companies are involving domain-expert external advisors in the assessment.

B. Hire Outside Advisors

Organizations may also choose to hire the expertise of outside advisors or experts to help them conduct the organizational risk assessment.

I. Who Are They?

When deciding among outside advisors, depending on the level of knowledge or expertise required, an organization can seek to hire the resources of:

- Outside lawyers or law firm
- Audit firms
- Other compliance experts, consultants, etc.

2. Why is it a Good Idea?

There are several reasons, not always readily apparent, why utilizing the advice, counsel, or services of an external advisor is a good idea. A few of those are detailed below.

a. Document/Information Security

One of the benefits of using an outside advisor is the ability to keep sensitive or potentially damaging information off of company premises. By utilizing an independent third party, much of the information that is generated can be stored, maintained, or held by the third party. This is important because the various documents that are created may detail potential compliance problems of varying levels of severity. By keeping the information with a third party, the organization can better protect itself from private litigants and/or regulatory bodies obtaining this information and using it as evidence of pre-existing knowledge of compliance failures.

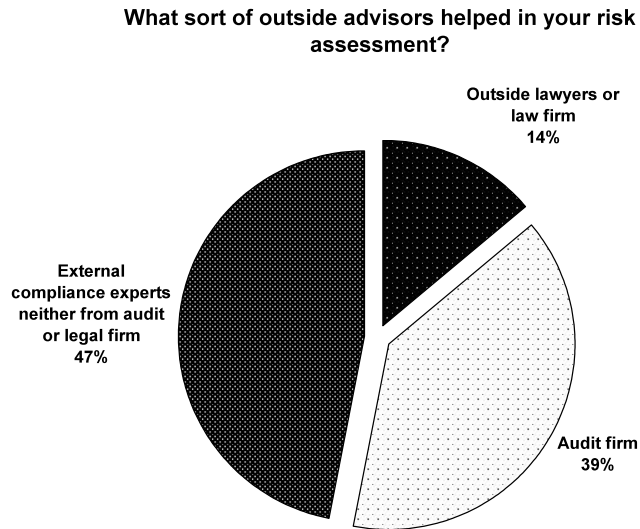
b. Analytical and/or Statistical Expertise

There is a high level of analytical and statistical expertise required for an effective risk assessment. Although some organizations may be more adept and experienced when conducting risk assessments, often, a wise choice may be to rely on the available skills and experience of outside consultants, who have current knowledge of the intricacies and frequent changes in the risk management field.

c. Non-Biased

When conducting a risk assessment internally, a natural bias will always exist. Individuals who are too close to the business operations have a tendency to misinterpret information and might overestimate or underestimate the degree of potential risk to the organization. This can introduce questions regarding the credibility of the risk assessment itself. As such, hiring an independent outside observer to help manage part or all of the risk assessment will help prevent the disillusioned effects of organizational bias.

Figure 16: Types of Outside Advisors Hired to Help Conduct Risk Assessments



Source: ACC-Corpedia 2005 Benchmarking Survey

X. Additional Resources

Alexander F. Brigham and Robert Leffel, "Benchmarking Compliance, Risk and Anticorruption Efforts—How Does Your Company Compare," ACC Presentation Transcript (Jan. 16, 2000) *available at* <http://www.acc.com/resource/index.php?key=9537>.

"2007 Compliance Program and Risk Assessment Benchmarking Survey," ACC Survey (2007), *available at* <http://www.acc.com/resource/v8530>.

John Beccia III ET AL., "Challenges Faced When Establishing an Enterprise-Wide Compliance Risk Management Program," ACC 2007 Annual Meeting, Session 208, *available at* <http://www.acc.com/resource/v9046>.

"Strategic Issues in Intellectual Property Risk Management," Briefing Material, ACC CLO Think Tank Series (2007), *available at* <http://www.acc.com/resource/v8713>.

XI. Sample Forms

A. Risk Universe Chart

Risk Areas	Industry Severity (1-10)	Industry Likelihood (1-5)	Organization Likelihood (1-5)	Organization Impact Score	Rank
Risk Area	7.4	2.8	2.7	100.9	1
Risk Area	8.4	2.9	2.3	95.3	2
Risk Area	6.3	2.1	2.9	90.5	3
Risk Area	6.1	2.2	2.9	89.5	4
Risk Area	7.5	2.0	2.4	88.1	5
Risk Area	5.6	2.3	3.1	86.5	6
Risk Area	5.2	2.6	3.2	81.7	7
Risk Area	6.0	2.5	2.7	80.6	8
Risk Area	5.9	2.7	2.7	78.4	9
Risk Area	4.4	3.4	3.3	73.4	10
Risk Area	5.0	2.8	2.9	71.7	11
Risk Area	6.2	2.9	2.3	71.1	12
Risk Area	5.9	2.8	2.3	67.0	13
Risk Area	5.7	2.7	2.3	66.3	14
Risk Area	4.5	2.0	2.5	56.3	15
Risk Area	8.5	1.9	1.3	54.6	16
Risk Area	4.0	3.7	2.6	51.0	17
Risk Area	5.8	1.8	1.7	48.2	18
Risk Area	5.0	2.1	1.9	47.8	19
Risk Area	4.9	2.1	1.9	47.5	20
Risk Area	5.0	2.4	1.8	46.2	21
Risk Area	5.6	1.6	1.5	43.0	22
Risk Area	4.0	2.2	1.9	38.0	23
Risk Area	4.5	1.6	1.6	35.8	24
Risk Area	6.9	1.6	1.0	34.9	25
Risk Area	4.4	2.3	1.6	34.8	26
Risk Area	3.0	2.1	2.3	34.5	27
Risk Area	4.0	1.9	1.7	31.0	28
Risk Area	4.8	1.4	1.3	30.9	29
Risk Area	5.2	1.7	1.2	30.0	30
Risk Area	3.0	2.0	1.9	28.5	31
Risk Area	3.6	1.9	1.4	25.3	32
Risk Area	4.4	2.0	1.1	23.3	33
Risk Area	2.0	3.2	1.9	19.5	34
Risk Area	1.0	2.9	3.6	18.0	35
Risk Area	3.2	1.3	1.0	16.4	36
Risk Area	1.9	1.6	1.5	15.0	37
Risk Area	2.1	2.5	1.5	15.0	38
Risk Area	2.0	1.6	1.3	12.8	39
Risk Area	2.0	2.2	1.1	11.0	40
Risk Area	1.1	1.0	1.6	8.0	41

B. Risk Severity Scale – Example

Score	1	2	3	4	5
	Descriptive				
Reputation	<i>No reputation damage</i>	<i>Extremely minor reputation damage</i>	<i>Very minor negative impact; easily recoverable</i>	<i>Minor but noticeable localized negative impact; generally recoverable</i>	<i>Moderate reputation damage on a regional level; negative national media coverage (minor); generally recoverable over time</i>
Loss of stock value (%)	~0	<1	1-2	2-5	5-10
Damages, fines, settlements & legal costs (% of revenues)	~0	<1	1-2	2-3	3-4
Operations	<i>No operational impact or loss of business</i>	<i>Extremely minor operational impact or loss of business</i>	<i>Very minor impact on operations; easily recoverable</i>	<i>Limited impact on operations; minor loss of business; generally recoverable</i>	<i>Moderate impact on operations; minor to moderate loss of business; moderate changes in business model may be required; requires serious attention at the senior level</i>
Score	6	7	8	9	10
	Descriptive				
Reputation	<i>Moderate to serious reputation damage; nationwide negative media coverage</i>	<i>Serious reputation damage; nationwide negative media coverage (serious); serious regulatory harm; partially recoverable over time with considerable effort</i>	<i>Severe reputation damage; negative national media coverage (severe); severe regulatory harm; low chance of recovery</i>	<i>Extremely severe damage to reputation; sustained and extremely negative national and international media coverage (front page); very low chance of recovery</i>	<i>Irreversible damage to reputation. Sustained and extremely negative national and international media coverage</i>
Loss of stock value (%)	10-20	20-40	40-60%	60-90%	>90
Damages, fines, settlements & legal costs (% of revenues)	4-5%	5-7%	7-10%	10-15%	>15%
Operations	<i>Moderate to serious impact on operations; moderate loss of business</i>	<i>Significant impact on operations; serious loss of business; possible elimination of business lines</i>	<i>Severe impact on business; significant loss of competitive positions; exit from significant market segments</i>	<i>Very severe impact on business with massive loss of revenue; exit from key market segments</i>	<i>Catastrophic impact on business with near total loss of revenue; recovery impossible</i>

XII. Endnotes

¹ See generally PROJECT MANAGEMENT INSTITUTE, A GUIDE TO THE PROJECT MANAGEMENT BODY OF KNOWLEDGE (PMBOK® GUIDE) (3d ed. 2004).

² U.S. FEDERAL SENTENCING GUIDELINES MANUAL § 8B2.1(c) (2005).

³ “2007 Compliance Program and Risk Assessment Benchmarking Survey,” ACC Survey (2007), available at <http://www.acc.com/resource/v8530>.

⁴ U.S. FEDERAL SENTENCING GUIDELINES MANUAL § 8B2.1, app. n. 6 (2007).

⁵ For more information on ECERA™, see CORPEDIA, INC., available at <http://www.corpedia.com>.

⁶ “2005 Compliance Program and Risk Assessment Benchmarking Survey,” ACC Survey (2005), available at <http://www.acc.com/resource/v6454>.

⁷ General Counsel Roundtable: “Performing a Legal and Compliance Risk Assessment,” 1-5.

⁸ “2007 Compliance Program and Risk Assessment Benchmarking Survey,” ACC Survey (2007), available at <http://www.acc.com/resource/v8530>.

⁹ “2005 Compliance Program and Risk Assessment Benchmarking Survey,” ACC Survey (2005), available at <http://www.acc.com/resource/v6454>.

Effective Compliance and Ethics Programs for the Small Law Department — Doing More With Less

This InfoPAKSM is designed to provide corporate counsel with a general overview of the requirements of an effective ethics and compliance program under the Federal Sentencing Guidelines and to suggest useful strategies for the Small Legal Department for creating and maintaining such a program. This information should not be construed as legal advice or legal opinion on specific facts, or representative of the views of ACC or any of its lawyers, unless so stated. This is not intended as a definitive statement on the subject but a tool, providing practical information for the reader. We hope that you find this material useful. Thank you for contacting the Association of Corporate Counsel.

This InfoPAK was developed by:

Deborah M. House,
Vice President and Deputy General Counsel for Legal Resources
and Strategic Initiatives, Association of Corporate Counsel.

ACC wishes to thank Meredith Stone, Vice President, General Counsel, Americas, NACCO Materials Handling Group, Inc., and Chair of the ACC Small Law Department Committee, for her contribution to the development of this InfoPAK.

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

InfoPAK

Effective Compliance and Ethics Programs
for the Small Law Department—Doing
More With Less



Association of Corporate Counsel
1025 Connecticut Avenue NW, Suite 200, Washington, DC 20036,
ph: 202.293.4103 www.acca.com

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

Effective Compliance and Ethics Programs for the Small Law Department

Contents

- I. Introduction and Overview 5
- II. The Federal Sentencing Guidelines: Not Just About Crime and Not Just About Sentencing 6
- III. One Size Does Not Fit All 8
- IV. The Top Ten Essential Tasks 10
 - A. Task #1: Create an Appropriate Organizational Structure.....10
 - B. Task #2: Assure that Individuals Responsible for the Program have Adequate Resources, Appropriate Authority, and Direct Access to the Board.....12
 - C. Task #3: Educate Your Board.....16
 - D. Task #4: Assess Your Legal and Regulatory Risk.....17
 - E. Task #5: Establish Appropriate Standards and Procedures.....22
 - F. Task #6: Establish an Effective Training and Communications Program...30
 - G. Task #7: Establish a Reporting Mechanism (Hotline).....34
 - H. Task #8: Implement the Carrot and Stick Approach.....39
 - I. Task #9: Screen Your Employees.....42
 - J. Task #10: Keep Your Program Effective—Monitoring and Auditing, Assessments, and Revisions.....44
- V. Conclusion 48
- VI. Sample Forms and Policies 48
 - A. Tool #1: Sample Organizational Structures for Corporate Compliance..48
 - B. Tool #2: Sample Chief Compliance Officer Position Description.....50
 - C. Tool #3: Sample Charter for Corporate Compliance Committee.....53
 - D. Tool #4: Sample Compliance Policy and Procedures.....54
 - E. Tool #5: Sample Annual Certification Form.....58
 - F. Tool #6: Sample Periodic Report to the Board.....59
 - G. Tool #7: Sample PowerPoint Presentation for Board.....62

- H. Tool #8: Top Ten Things Your Board Needs to Know About Effective Compliance and Ethics Programs.....62
- I. Tool #9: Sample Risk Assessment Tool.....65
- J. Tool #10: Sample Employee Compliance Survey.....65
- K. Tool #11: Sample Employee Exit Interview Questions.....73

- VII. About the Author74

- VIII. Endnotes.....75

Appendix A: Roadmap for an Effective Compliance and Ethics Program
 Appendix B: Sample Risk Assessment Tool

I. Introduction And Overview

Providing advice for Small Law Departments (SLD) on how to implement and maintain an effective compliance and ethics program (Program) reminds one of a cartoon. It depicts a smiling supervisor leaning over his desk delivering an annual review to his obviously beleaguered subordinate, saying: "Jones last year you did so much more with less than this year we are going to have you do more with nothing!" For while a lack of resources also besieges lawyers in large legal departments, the burden falls more heavily on the SLD which is required to be "chief cook and bottle washer" in meeting the legal needs of the company. In fact, in the 2005 ACC/Serengeti Survey where over 80% of the respondents came from legal departments with less than five lawyers, one of the top five concerns expressed by in-house counsel was "too much work for too little resources/legal budget."¹

Thus when the task of implementing and maintaining a Program falls on the SLD, or the SLD is otherwise significantly responsible for the Program, it is an extra serving on an already full plate. The notion that the SLD is likely to have a significant role in the Program is supported by data which indicates that even where the compliance function is a stand alone operation (65.6% of all respondents) the function frequently reports to the Chief Legal Officer (CLO) (32.6% of all respondents) or secondarily to the CLO (15.4% of all respondents). In over 50% of the firms surveyed, the chief compliance officer reported either primarily or secondarily to the CLO.² Moreover, even if there is no reporting relationship, given that legal and regulatory compliance is the lynchpin of the Program, the legal department plays a significant role in providing counsel and advice.³

Accordingly, the purposes of this paper are to provide SLDs with: (1) background information about the requirements for a Program; (2) practical advice on doing more with less when it comes to establishing and running a Program; and (3) tools for SLDs to utilize to facilitate the tasks associated with the Program. The information provided contemplates that there is no Program in place or it is in its earliest stages of development. However, it also may be used as a basis for reviewing and enhancing an existing Program. The good news is that having an effective Program means clients have a better understanding of their ethical, legal, and regulatory obligations. This result should ease the overall burden for the SLD and help avoid the all consuming corporate crisis.

II. The Federal Sentencing Guidelines: Not Just About Crimes and Not Just About Sentencing

The U.S. Sentencing Commission (USSC) was created in 1985 for the purpose of developing sentencing guidelines to assure that comparable misconduct by similar offenders received similar sentences. The first guidelines for the sentencing of organizations (e.g., partnerships, corporations, not-for-profits, etc.) became effective in 1991 (Guidelines).⁴

A critical component of the Guidelines is that organizations are given a sentencing credit if they have an effective Program.⁵ An effective Program is one where the company will "exercise due diligence to prevent and detect criminal conduct; and ... otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law..." (i.e., setting the appropriate "tone at the top").⁶

In October of 2003, after 18 months of study which included public hearings, an Ad Hoc Advisory Group to the USSC (Advisory Group), made up of 15 practicing lawyers, academics, compliance professionals, and public officials, made recommendations to the USSC for modifying and expanding the Guidelines for organizations to make them more effective.⁷ As explained by the Advisory Group, the purpose of these changes was to:

... eliminate ambiguities revealed by twelve years of sentencing experience and to describe more fully those essential attributes of successful compliance programs revealed by many years of program development and testing. They are also designed to respond to the lessons learned through the experience of national corporate scandals over the last two years and to synchronize the organizational sentencing guidelines with new federal legislation and emerging public and private regulatory requirements.⁸

Among other things, these changes:

- Emphasized the importance of a corporate culture committed to compliance with the law;
- Specified the responsibilities of a company's Board and senior management for having an effective Program.
- Highlighted that personnel heading Programs must have adequate resources and effective authority.

- Indicated that effective Programs must have compliance training for the Board, employees, and agents as appropriate.
- Required Programs to establish a mechanism for anonymous reporting.
- Added a requirement for periodic evaluation of the Program itself.
- Introduced ongoing risk assessments as a component of the Program.

In April of 2004, the USSC recommended significant additions and modifications to the Guidelines to Congress. The revised Guidelines became effective on November 1, 2004.⁹

The Guidelines are understood to be and are regularly cited as the benchmark for effective corporate ethics and compliance programs.¹⁰ For example, in the derivative shareholder action known as the Caremark case the Court was asked to approve the settlement that had its genesis in the criminal conviction of Caremark for mail fraud.¹¹ The conviction resulted in Caremark's payment of \$250 million in criminal and civil fines.

In determining whether the Caremark directors had breached their duty of care in their oversight of the corporation's activities, the Chancery Court addressed the question of "[W]hat is the board's responsibility with respect to the organizations and monitoring of the enterprise to assure that the corporation functions within the law to achieve its purposes?" In response to its own inquiry, the Court recognized the impact of the Guidelines stating that "Any rational person attempting in good faith to meet an organizational governance responsibility would be bound to take into account this development [of the Guidelines] and the enhanced penalties and the opportunities for reduced sanctions that it offers."¹²

Taking the position that the Guidelines are irrelevant except in a sentencing scenario puts a corporation at extreme risk. To evaluate whether you have an effective Program at the time of sentencing is too little, too late, to say the least. In fact, the USSC reported for Fiscal Year 2005 that 100% of the corporations sentenced had no program at all, let alone an effective or ineffective one.¹³ One interpretation of this data is that companies that have Programs don't find themselves being prosecuted for one of two reasons.

The first reason is that the Guidelines create a roadmap for a company to implement an effective Program that is designed to prevent and detect non-compliant activities and address them if they do occur. The result is that the misconduct never occurs or is suitably remedied.

Alternatively, if the company has an effective Program, although the misconduct occurs, prosecution may be avoided. This conclusion is buttressed by the fact that long before sentencing ever comes into play one of the factors the Department of Justice takes into consideration in "conducting an investigation, determining whether to bring charges, and negotiating plea agreements" is "the existence and

adequacy of the corporation's compliance program" for which the Guidelines are used as a benchmark.¹⁴ This analysis includes addressing such matters as:

- Is the corporation's program well designed?
- Does the corporation's compliance program work?
- Is it merely a "paper program" or is it designed and implemented in an effective manner?
- Has the corporation provided for a staff sufficient to audit, document, analyze and utilize the results of the corporation's compliance efforts?
- Are the corporation's employees adequately informed about the compliance program and are they convinced of the corporation's commitment to it?

Moreover, deferred prosecution agreements, of which there have been a number over the past several years, have permitted companies like KPMG, AOL, AIG, and MCI to avoid prosecution dependent on, among other things, their successful establishment or enhancement of compliance programs.

The importance of the Guidelines and their role as the principle benchmark for effective Programs is implicitly or explicitly observed by other entities of the federal government. Like the Department of Justice, the Securities and Exchange Commission (SEC) also considers what compliance activities were in place to prevent misconduct in determining whether to bring charges and what charges to bring.¹⁵ The Department of Health and Human Services (HHS), the Environmental Protection Agency (EPA), the Department of State, and the Equal Employment Opportunity Commission (EEOC) exercise similar considerations.

Effective Programs regularly address activities that do not carry criminal liability. One of the reasons for this is that certain acts, while criminal in their most egregious form (e.g., insider trading) often carry civil and regulatory liability with them as well. Other activities which may not carry criminal, civil or regulatory liability (e.g., conflict of interests) may nonetheless be very problematic for the company and precursors to activities to which criminal liability attaches. Finally, corporate wrongdoing in any form undercuts the necessary commitment to ethical conduct. Therefore, efforts to prevent and detect all misconduct are very important. It is for this reason that references herein are not just to criminal conduct, but misconduct generally.

III. One Size Does Not Fit All

Most explorations of the requirements of the Guidelines dutifully recite the components of an effective program. Because this piece is designed to walk you through the process of establishing (or enhancing) a Program, the components are reorganized into the top ten essential tasks. Resource issues are addressed and tools

are supplied as they relate to each task. Before creating or enhancing your Program, however, there are several issues you should take into consideration in the initial planning to “size” your undertaking.

First, what are the governmental regulations and industry practices that are applicable to your company? If your company or an area of its operations is highly regulated (e.g., banking, health care, food & drug, consumer protection, handling hazardous wastes etc.) your Program, its focus, and the resources dedicated to it, need to reflect this fact. A company’s “failure to incorporate and follow applicable industry practices or the standards called for by any applicable governmental regulation weighs against a finding of an effective compliance and ethics program.”¹⁶

Second, what is the size of your company? The Guidelines clearly recognize that the obligations for a large company are different than those for a small company: “The formality and scope of actions that an organization shall take to meet the requirements of this guideline, including the necessary features of the organization’s standards and procedures, depend on the size of the organization.”¹⁷

Large companies are expected to generally “devote more formal operations and greater resources in meeting the requirements of this guideline than shall a small organization.” Further, “a large organization should encourage small organizations (especially those that have, or seek to have, a business relationship with the large organization) to implement effective compliance and ethics programs.”¹⁸

Small companies are expected to “demonstrate the same degree of commitment to ethical conduct and compliance with the law as large organizations.” However in contrast to large companies, “a small organization may meet the requirements of this guideline with less formality and fewer resources than would be expected of large organizations. In appropriate circumstances, reliance on existing resources and simple systems can demonstrate a degree of commitment that, for a large organization, would only be demonstrated through more formally planned and implemented systems.”¹⁹

The Guidelines’ Commentary goes on to give more specific examples illustrating the differences.

Examples of the informality and use of fewer resources with which a small organization may meet the requirements of this guideline include the following: (I) the governing authority’s [Board’s] discharge of its responsibility for oversight of the compliance and ethics program by directly managing the organization’s compliance and ethics efforts; (II) training employees through informal staff meetings, and monitoring through regular “walk-arounds” or continuous observation while managing the organization; (III) using available personnel, rather than employing separate staff, to carry out the compliance and ethics program;

and (IV) modeling its own compliance and ethics program on existing, well-regarded compliance and ethics programs and best practices of other similar organizations.²⁰

Caveat: Unfortunately, the requirements for an effective Program for a large company need to be met even if the large company has a SLD. Thus, if you are an SLD within a large company — focusing on getting the resources that you need to meet these requirements is an important task.

Third, any prior misconduct by the organization should be considered so as to avoid a repeat performance. Recurrence of similar misconduct creates doubt regarding whether the organization took reasonable steps to meet the requirements of the Guidelines.²¹ Your efforts to structure the Program to prevent and detect such misconduct should not be too narrow (i.e., designed simply to detect or prevent just the previous misconduct.) Rather, they should be designed to address all “similar misconduct.” The Guidelines illustrate this concept by way of example, noting that if the organization had previously engaged in Medicare fraud, efforts should be made to avoid other types of fraud.²²

IV. The Top Ten Essential Tasks

A. Task # 1: Create an Appropriate Organizational Structure

1. Guidelines Requirements

USSG §8B2.1 (b) (2) (B) requires that “High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program as described in this guideline.”

‘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.²³

USSG §8B2.1 (b) (2) (C) requires that “Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program.”

When you first report to the Board on its responsibility for overseeing the Program it is contemplated that you will do so with a proposal or plan for the Program for comment or approval. Essential to such a Plan is the identification of persons within the company who will be responsible for overseeing the Program. There are a wide variety of compliance organizational structures that could be considered for a company. These variations take into consideration the requirements of the Guidelines and are driven by such factors as:

- Resources for the program.
- Size of the company.
- Whether compliance is a stand alone function.
- Which “High-level” personnel will be responsible for supervision of the Program.
- Whether “High-level” personnel responsible for the Program will also be responsible for its day to day operation.
- The role of business personnel in meeting compliance requirements.
- Whether the company is highly regulated.

It should be noted, particularly in educating the Board about the role of senior management in assuring there is an effective Program, that the responsibility for the Program does not lie just with those members of senior management who have oversight responsibility (e.g., the CLO, Chief Compliance Officer). Rather, high-level personnel and substantial authority personnel²⁴ are also charged with being “knowledgeable about the content and operation of the compliance and ethics program” and performing their assigned duties consistent with the exercise of due diligence” and with “promot[ing] an organizational culture that encourages ethical conduct and a commitment to compliance with the law.”²⁵

This sentiment is echoed by the Business Roundtable in its Principles of Corporate Governance where all of senior management is similarly vested with compliance related responsibilities.

The CEO and senior management are responsible for operating the corporation in an ethical manner. They should never put individual, personal interests before those of the corporation or its shareholders. Business Roundtable believes that when carrying out this function, corporations should have:

- A CEO of integrity. The CEO should be a person of integrity who takes responsibility for the corporation adhering to the highest ethical standards.
- A strong, ethical “tone at the top.” The CEO and senior management should set a “tone at the top” that establishes a culture of legal compliance and integrity communicated to personnel at all levels of the corporation.

- An effective compliance program. Senior management should take responsibility for implementing and managing an effective compliance program relating to legal and ethical conduct.²⁶

2. Doing More with Less: Staffing Your Program

- Staff Smart, Part I. Use non-lawyers. A large part of compliance is creating and maintaining proper documentation that training has occurred, the appropriate people attended, certifications were made, etc. You don't need a law degree to do this. Use paralegals and other professionals, (business analysts, program administrators, trainers, project managers, administrative assistants, etc.) to manage these tasks.
- Staff Smart, Part II. Limit the use of your lawyers. Whenever possible, use your lawyers only to provide legal advice, review final documents for legal and regulatory adequacy, or participate in and/or manage projects where legal input is necessary.
- Share the Challenge. Trainers exist in HR, technology experts may be secured from information systems, writers for policy and intranet communication may be available in your office of communications, and subject matter experts who can provide training and address other compliance related tasks exist in other departments.
- Use Outside Resources. Because it is often easier to secure funding than staff positions, use outside resources wherever possible; compliance training vendors, outside counsel (look for counsel with in-house compliance experience for the best value), temps to manage paperwork, etc. can supplement your staff.
- Use these Tools
 - Sample Organizational Structures for Corporate Compliance appear as Tool 1.
 - A Sample Chief Compliance Officer Position Description appears as Tool 2.

B. Task #2: Assure That Individuals Responsible For The Program Have Adequate Resources, Appropriate Authority, and Access To The Board

1. Guidelines Requirements

USSG §8B2.1 (b) (2) (C) requires that “Individual(s) with operational respon-

sibility shall report periodically to high-level personnel and, as appropriate to the [Board], on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the [Board] or an appropriate subgroup of the [Board].”

a. Adequate Resources

In determining whether the Program has adequate resources a number of factors should be taken into consideration. These might include:

- (a) size of the company (by number of employees or assets);
- (b) whether the company is highly regulated;
- (c) complexity of the company’s transactions;
- (d) geographic range (i.e., local v. international);
- (e) applicable industry practices;
- (f) nature of the company’s activities; and
- (g) potential areas of significant risk/liability and the need to address them.

The purpose of the Guidelines’ requirement that the organization provide “adequate resources” is to “ensure that a company’s compliance program is not just a paper program, but rather a substantial management effort with the resources needed to succeed.”²⁷

b. Appropriate Authority

The proposed version of the Guidelines offered by the Advisory Group would have required the individual responsible for the day to day operations of the Program to be from the ranks of the high level personnel. In the final version of the Guidelines there is no such requirement. However, the requirement that the individual have “appropriate authority” to run the Program continues to carry with it the notion that day to day operations should not be delegated to a low level employee for several reasons:

- (1) such a designation might undercut the establishment of an appropriate “tone at the top” and the organization’s commitment to compliance;
- (2) low level employees may have difficulty securing the assistance, cooperation, and attention of high level personnel needed to accomplish the

objectives of the Program;

- (3) delegation to a low level employee carries with it a risk that the Program might be viewed as a paper tiger; and
- (4) given the requirement that the individual responsible for the day-to-day operations of the Program has access to the Board or a Board Committee, a low level employee may not be the most suitable choice.

c. Direct Access to the Board

The Advisory Group Report is very clear as to why the individual responsible for day to day operations should have direct access to the Board, namely, “to bring two types of information directly from the head of the program to the members of the [Board] without the potential filtering or censoring influence of senior organization members.”²⁸ The first type of information is identified as reports to update the board on the current features of the Program and the compliance problems that are being addressed. These reports should be designed to assist the Board in meeting its “responsibilities to keep knowledgeable about program features and operations.”²⁹ The second type of information which immediately should be supplied to the Board or an appropriate subgroup of the Board is “in cases of actual or apparent involvement in, or support for, illegal conduct by top level organizational executives” which will “help the [Board] fulfill its proper role in assuring accountability on the part of senior organizational managers and preventing the initiation or continuation of misconduct at upper organizational levels.”³⁰

2. Doing More with Less: Appropriate Authority, Access, and Resources³¹

- Create a Company–Wide Compliance Committee. Such committees are created for a variety of reasons, but one of their more practical uses is to keep “high-level” and “substantial authority” personnel in the company apprised of the need to establish and maintain an effective Program and to secure their assistance and support in securing adequate resources and implementing the Program. Committees are typically comprised of senior level officers and above. This level of participation also helps establish the appropriate “tone at the top.” (See Tool #3).
- Create Compliance Policies and Procedures. While this initially may be a time consuming effort it will keep everyone engaged in compliance activities on the same page. This is particularly important if you are going to successfully delegate activities outside the Legal Department. (See Tool #4).
- Consolidate Tasks. When you have your employees annually certify to the Code, also have them certify (or provide information demonstrating) that they know how to find your Hotline. (Hotlines are discussed in more detail in Part IV (G)). At the same time have them make any conflict of interest disclosures. The more tasks that can reasonably be consolidated, the less resources will be

used. (See Tool #5).

- **Employ Your Risk Assessment.** It is important to understand that the Guidelines contemplate that your Program's activities will be based on your risk analysis. Accordingly, focus compliance resources where you have the greatest risks. The benefit of this approach is it is likely to keep the company out of trouble and if the worst happens, you will have a basis to defend your Program. For example, if the activities of your large competitive sales force causes you to rate the operation at high risk under the anti-trust laws, or there has been "similar misconduct" in this arena, make sure that you have an anti-trust policy, that anti-trust training is provided, that activities are monitored and audited, and that other effective steps for preventing and detecting misconduct are taken.
- **Plan Ahead.** Consider not only what the task is at hand, but what the task for the future might be. For example, when you create a program to obtain and track code certifications for current employees — consider how you are going to process certifications for new employees or even contractors. Otherwise you will find yourself backtracking and reinventing the wheel as new aspects of the same issue arise which burns resources and can be very frustrating as well.
- **Put it in Writing.** Reports to the Board (or a subgroup) may largely be made in writing. This eliminates the need to undertake such time consuming efforts as creating PowerPoints, practicing presentations, etc. and also serves as appropriate documentation for the activity. Care should be taken to properly document that the report was actually provided to the Board, that its author was available, and, as appropriate, the fact that it was discussed should be reflected in the minutes.
- **Share the Challenge, Part I.** Get other business units in the company to assist you in your tasks or even take responsibility for them! For example, a copy of the employee code of conduct and a code certification form might be distributed with new employee offer letters. The certifications could then be collected by HR when it conducts new employee orientations.
- **Share the Challenge, Part II.** Seek other financial resources. For example, if HR has a budget for company wide training — negotiate with them to cover part of the cost of compliance training. One CLO who is responsible for the Program managed to get the costs of the Program completely assigned to the CEO's budget. This not only increased the budget, but underscored the importance of the Program, thus helping to set the appropriate "tone at the top." A related tactic might be to get the costs of the Program (or the Program itself — which would have the same effect) as a separate line item from that of the Legal Department. Otherwise the Legal Department might be asked to make trade-offs in its staffing and other resources in order to support the Program.

- **Staff Smart.** As discussed above, don't use lawyers when you don't have to, leverage personnel in other Departments, and use outside resources when you can.
- **Use Technology.** Reminders to take training can be set up to be issued electronically and automatically, compliance communications may be distributed by e/mails to 1000s of employees with just one click, policies and communications regarding policies can be put on the company's intranet website.
- **Use these Tools**
 - A Sample Charter for Corporate Compliance Committee appears as Tool # 3.
 - A Sample Compliance Policy and Procedure appears as Tool # 4.
 - A Sample Annual Certification Form appears as Tool #5.
 - A Sample Periodic Report to the Board appears as Tool # 6.

C. Task #3: Educate Your Board

1. Guidelines Requirements

USSG §8B2.1 (b) (2) (A) requires that "The [Board] shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program."

The CLO of a company is traditionally responsible for overseeing all legal matters relating to the company. Accordingly, it is logical that the CLO will have some role in keeping the Board apprised of its obligations under the Guidelines particularly if the CLO has a principal role in overseeing and/or operating the Program.

Minimally the Board should be educated so that the members will know the following about the Guidelines³² and their implications for the company:

- The Guidelines serve as the benchmark for effective ethics and compliance programs, including outside of the criminal sentencing context, and it is in the company's best interests to have such a Program in place.
- The Board has a responsibility to be knowledgeable about and exercise reasonable oversight with respect to the Program.
- The company is responsible for establishing an appropriate culture and "tone at the top" that "encourages ethical conduct and a commitment to compliance with the law."
- Individuals responsible for the day-to-day operations of the Program must have effective authority and access to the Board or a subgroup of the Board.
- The Program must have adequate resources.
- The company must adopt standards of conduct and internal controls that are

designed to prevent and detect misconduct and reduce the likelihood that misconduct will occur.

- The company needs to have effective compliance training and the Board is expected to participate.
- The Program should be independently evaluated periodically.
- The approach to achieving compliance in the company should incorporate incentives for appropriate behavior and disincentives for inappropriate behavior (i.e., both “carrots and sticks”).
- A confidential or anonymous reporting mechanism (“hotline”) should be established to allow employees to report and seek guidance about possible misconduct.
- Periodic risk assessment is required and drives the components of the Program.

2. Doing More with Less: Educating the Board

- Use these Tools.
 - A Sample PowerPoint Presentation for the Board to educate the members about their compliance related responsibilities appears as Tool 7. Note: This Presentation contemplates that you will discuss how your company is meeting each of these requirements. It could be revised to take out the “Implementation” discussion under each section and make it two or three slides at the end of the requirements if that makes better sense.
 - A short paper entitled the “Top Ten Things the Board Needs to Know About Effective Ethics and Compliance Programs” which can be used as a hand-out or as talking points appears as Tool 8.

D. Task #4: Assess Your Legal And Regulatory Risk

1. Guidelines Requirements

USSG §8B2.1(c) requires that as part of implementing its Program “the organization shall periodically assess the risk of [misconduct] and shall take appropriate steps to design, implement, or modify [the components of an effective ethics and compliance program] to reduce the risk of [misconduct] identified through this process.”

There are a number of reasons for performing a corporate risk assessment. Under the exchange listing requirements and Sarbanes-Oxley, public companies are required to establish and test a system of internal controls that, among other things, are aimed at assessing, deterring and monitoring risk. Other statutory and regulatory provisions require risk analysis as well. The Guidelines establish an obligation for all organizations, public and private, to undertake a risk assessment as it relates to the risk of criminal conduct. Finally, analyzing and assessing risks so that they might be addressed and mitigated is simply a good business practice.³³

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

Requirements of such assessment under the Guidelines include periodic³⁴ consideration of: the risk that misconduct will occur, including assessing the following:

- (i) The “nature and seriousness” of such misconduct
- (ii) The likelihood that [misconduct] may occur because of the nature of the organization’s business. If, because of the nature of an organization’s business, there is a substantial risk that certain types of [misconduct] may occur, the organization shall take reasonable steps to prevent and detect that type of [misconduct]. For example, an organization that, due to the nature of its business, employs sales personnel who have flexibility to set prices shall establish standards and procedures designed to prevent and detect price-fixing. An organization that, due to the nature of its business, employs sales personnel who have flexibility to represent the material characteristics of a product shall establish standards and procedures designed to prevent and detect fraud.
- (iii) The prior history of the organization. The prior history of an organization may indicate types of [misconduct] that it shall take actions to prevent and detect.³⁵

Additionally, the Guidelines require companies to incorporate the risk analysis into their Program by engaging in activities that will “focus on preventing and detecting the misconduct identified” in the risk analysis “as most serious, and most likely to occur” and modifying its Program to “reduce the risk of [misconduct]” identified as “most serious and most likely to occur.”³⁶ These directives are of particular importance where staff and budgetary resources may be limited. A risk assessment allows a company to justify its determinations as to what and what will not be a part of its Program.³⁷

For example, if a company has wide ranging contracting activities with foreign government employees, the risk of violation of the Foreign Corrupt Practices Act may be identified as serious and most likely to occur. Accordingly, activities designed to mitigate possible violations, in which the substantial number of employees who might be vulnerable to such an occurrence would participate, should be an essential component of the Program. The contrary would be true for a company which has no international activities or minor ones where employees are not working with foreign officials.

In addition to focusing the company’s compliance Program, risk assessments are advantageous in that they often bring problematic practices to the attention of the SLD. Once identified these practices might be modified so as to decrease the attendant risk or eliminate it all together.

For example, a standard component of a legal risk assessment is to evaluate the

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

company's activities for risks associated with the possible violation of the antitrust laws. As part of such an exercise it might be revealed that sales personnel with the ability to determine prices are informally exchanging market information with competitors. One Legal Department response to such activities might be simply to seek their termination. Another could be to change the practice to secure marketing information from a third non-competing party such as a trade association and only in an historical form. Once an option was chosen it could be reinforced through Program activities (e.g., training, monitoring etc.).

Most CLOs can rattle off the top five legal and regulatory risks facing their company without so much as taking a deep breath. However performing a formal assessment of the nature contemplated here is a much more intentional process.³⁸ It can be reduced, however, to several fairly simple tasks:

- Identification of the risk; (i.e., violation of an ethical, legal or regulatory requirement)
- Quantification of the likelihood of the risk occurring;
- Quantification of the severity of the impact to the company should the risk occur; and
- Prioritization of the risks to be addressed by the Program.

Successfully completing these tasks requires some planning, organization, and the development of tools that will appropriately document the process. The following steps may be helpful in moving you forward.

- (1) Get Management Support. Secure buy-in and support from Senior Management by educating them about the need for the analysis.
- (2) Secure Knowledgeable Participants. Participants in the process must be sufficiently senior and knowledgeable about their own and related business areas to meaningfully contribute to the analysis. The purpose of these non-lawyer participants will be to assist you in identifying all activities and operations in the company which should be considered to assure that the evaluation is comprehensive and historically problematic activities are addressed.

Functions where there are multiple activities that might pose significant risk (e.g., brokerage operations, handling hazardous waste, use of confidential consumer information, etc.) might be broken down into sub-groups that have more than one participant. Include "support functions" whose non-compliant activities may carry risk (e.g., Human Resources). Also be sure to include representatives from business units that have specialized knowledge of compliance related risks (e.g., internal audit, controllers, and risk management). Finally, include participants who have historical knowledge of risks that have actualized or were near misses in the past (e.g., litigators, insurance managers, internal investigators, health and safety officers, etc.).

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

In a smaller company participants can often be quickly identified by creating a list from a corporate organization chart. For a larger company senior management may need to identify them. In all instances you will need to get management to "appoint" these persons and assure their participation.

- (3) Identify Applicable Requirements. Identify the applicable ethical (usually found in your code of conduct although there are other sources), legal, and regulatory requirements for the company (Requirements). This is obviously the place where you will want to use the scarce resource of your in-house lawyers although outside counsel may also be helpful. Start off with general Requirements applicable to most companies (e.g., the antitrust laws). However, counsel should take care to be very comprehensive and even break down into sub-categories Requirements that may specifically apply to your company's activities and operations that are likely to pose a higher degree of risk (e.g., banking laws for a financial institution, consumer protection laws for a credit card company, etc.).

Certain Requirements may be "lumped" together to facilitate the process (e.g., all state anti-discrimination laws that fairly closely track federal laws). You may want to highlight any unique provisions (e.g., California sexual harassment education provisions, the broader protected classes found in the District of Columbia, etc.) if you know they need to be addressed specifically.³⁹

Requirements that might reasonably be applied to the company, but are not applicable now (e.g., anti-spam laws if the company were to start sending commercial electronic messages) should be identified for record-keeping purposes, but excluded from further consideration. However they might be added in a subsequent reassessment if they later become applicable.⁴⁰

- (4) Brief Participants. Notification to the participants of their selection for the project and a brief background piece on its goals (i.e., identification, quantification and prioritization of risks) should be sent out.
- (5) Create Tools to be used in the Process. Having a format to work from with clear instructions will greatly assist all those who participate in the process. Make sure you also create a system for dating and controlling the use of the tools. Otherwise you will end up with an unmanageable number of versions and a justified fear that you are not working off the most recent version. Distribute the tools to the participants in draft form as they are very likely to have helpful input as to how they might be improved. Last, distribute final versions of the tools in advance of any work sessions so the participants will have an opportunity to review them prior to meeting.

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

- (6) Start the Process. Hold a kick-off meeting including all participants where the goals, objectives, timelines, and other matters relating to the assessment will be discussed and tools will be distributed.

Once finished, the conclusions reached in the risk assessment (and other considerations) will be used to drive the components of the Program.

2. Doing More with Less: Risk Assessment

- Benchmark Whenever and Wherever You Can. Legal and regulatory risk assessments for even different types of companies may be very useful as a wide variety of Requirements apply to all companies. Analyses for similarly situated companies (e.g., health care, manufacturing, financial services, etc.) are likely to be even more helpful. Thus benchmarking with colleagues in your industry as to how they are going about this task will be useful. While their full assessment of their respective company's legal risks will be confidential, other helpful information may not be. In all events care should be taken not to exchange information that might violate the anti-trust laws or other Requirements.
- Consolidate Tasks, Part I. Risk analysis is an element of complying with Sarbanes-Oxley and other statutory and regulatory obligations. This analysis is likely to be more directed towards controls and other areas of risk that might not impact legal and regulatory risk. Nonetheless there will be overlap and aspects of this analysis that are relevant to legal and regulatory risk (e.g., CEO and CFO certifications). Accordingly, consider to what extent you may want legal and regulatory risk to be part of this overall assessment so that the SLD is not solely responsible for administering this task. Even if the legal and regulatory risk analysis is administered separately, the SLD is wise to participate to some extent in the overall effort because mitigants of non-legal risks may intentionally or coincidentally also be mitigants of legal and regulatory risks and you will want to be aware of them. If you are not and you duplicate efforts when the legal and regulatory risks are assessed, your clients participating in the process will not view it favorably.
- Consolidate Tasks, Part II. Information gathering tools like employee surveys or other risk analysis tools may be used by other departments in your company for other reasons. If they are in process you may be able to "piggyback" on those efforts (e.g., add risk assessment questions to an HR survey). If they have been completed, you should review them as they are likely to contain relevant information that will be useful to you or might be supplemented to become useful to you. In these ways the SLD may be able to get the information it needs, but avoid the burden of having to completely do the work itself.
- Company-Wide Compliance Committee. If you have created the Committee previously suggested this is a good opportunity to use them to assist you in

providing support (and staff) for the risk analysis.

- Use these Tools.
 - A Sample Risk Assessment Tool for formulating the process of evaluating legal and regulatory risk appears as Tool #9.

E. Task # 5: Establish Appropriate Standards and Procedures

1. Guidelines Requirements

USSG §8B2.1 (b) (1) requires that "The organization shall establish standards and procedures to prevent and detect [misconduct]." For these purposes "Standards and procedures" means standards of conduct and internal controls that are reasonably capable of reducing the likelihood of [misconduct.]⁹⁴

The requirement that companies adopt appropriate compliance standards and procedures is not limited to the Guidelines. Rather, it emerges from a number of sources. For example, the NYSE requires that NYSE listed companies adopt a code of business conduct and ethics for directors and officers and employees and make it publicly available. Codes must "address the most important topics", including:

- Conflicts of interest. A "conflict of interest" occurs when an individual's private interest interferes in any way — or even appears to interfere — with the interests of the corporation as a whole. A conflict situation can arise when an employee, officer or director takes actions or has interests that may make it difficult to perform his or her company work objectively and effectively. Conflicts of interest also arise when an employee, officer or director, or a member of his or her family, receives improper personal benefits as a result of his or her position in the company. Loans to, or guarantees of obligations of, such persons are of special concern. The company should have a policy prohibiting such conflicts of interest, and providing a means for employees, officers and directors to communicate potential conflicts to the company.
- Corporate opportunities. Employees, officers and directors should be prohibited from (a) taking for themselves personally opportunities that are discovered through the use of corporate property, information or position; (b) using corporate property, information, or position for personal gain; and (c) competing with the company. Employees, officers and directors owe a duty to the company to advance its legitimate interests when the opportunity to do so arises.
- Confidentiality. Employees, officers and directors should maintain the confidentiality of information entrusted to them by the company or its customers,

except when disclosure is authorized or legally mandated. Confidential information includes all non-public information that might be of use to competitors, or harmful to the company or its customers, if disclosed.

- Fair dealing. Each employee, officer and director should endeavor to deal fairly with the company's customers, suppliers, competitors and employees. None should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practice. Companies may write their codes in a manner that does not alter existing legal rights and obligations of companies and their employees, such as "at will" employment arrangements.
- Protection and proper use of company assets. All employees, officers and directors should protect the company's assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the company's profitability. All company assets should be used for legitimate business purposes.
- Compliance with laws, rules and regulations (including insider trading laws). The company should proactively promote compliance with laws, rules and regulations, including insider trading laws. Insider trading is both unethical and illegal, and should be dealt with decisively.⁴²

The Business Roundtable places responsibility for having appropriate standards and procedures squarely with senior management:

Senior management should take responsibility for implementing and managing an effective compliance program relating to legal and ethical conduct. As part of its compliance program, a corporation should have a code of conduct with effective reporting and enforcement mechanisms.⁴³

And a wide variety of federal agencies require that program participants establish appropriate standards and procedures. For example, the federal Department of Health and Human Services requires hospitals subject to its regulation to establish a compliance program that includes: "The development and distribution of written standards of conduct as well as written policies and procedures that promote the hospital's commitment to compliance."⁴⁴

Finally, even the Federal Courts consider whether companies have established appropriate standards and procedures in determining whether employers have made a good faith effort to comply with employment anti-discrimination laws. If the company can demonstrate that it has in fact done so its activities may be offered as a defense to liability.⁴⁵

Given this wide array of requirements, the Advisory Committee declined to rec-

ommend the types of standards or procedures that should be adopted noting that: "Experience has shown that different standards and procedures are utilized by different industries and are influenced by the size of the organization, its complexity, and the nature of the business function. For these reasons the provision was left very general."⁴⁶

Accordingly, to meet the Guidelines every company should have a code of conduct and underlying implementing policies and procedures that are tailored to applicable legal and regulatory requirements, its operations and activities, and driven by its risk assessment.

2. Doing More with Less: Standards and Procedures

Prosecutors and regulators who scrutinize the actual effectiveness of company Programs scoff at a letter from convicted Chairman and CEO Kenneth Lay that introduced the Enron Code of Conduct stating:

As officers and employees of Enron Corp...we are responsible for conducting the business affairs of the companies in accordance with all applicable laws and in a moral and honest manner. ...We want to be proud of Enron and to know that it enjoys a reputation for fairness and honesty and that it is respected...Enron's reputation finally depends on its people, on you and me. Let's keep that reputation high.

The criticism is valid. A paper program alone, which is what Enron appeared to have had, is not — literally — worth the paper it is written on. And, if Enron continues to serve as the example, having a paper policy is likely to cost the company and its shareholders a great deal more. Thus it cannot be emphasized enough that every effort must be undertaken to avoid creating a compliance paper tiger. Your code and policies and procedures have to be real, customized for your company, and you have to be ready to enforce them.

- Use these Tools

That said, it doesn't mean you have to use your SLD's scarce resources to reinvent the wheel. Codes of conduct that you might consider to create or revise your own are plentiful and easy to find as public companies are required to have them and post them on their websites. They can usually be found by drilling down on the company's website under topics such as "Investors" or "Shareholder Relations," then looking under "Corporate Governance" or similar topic. In seeking a useful code of conduct to review, you should consider looking at codes for peer companies which might address issues that are peculiar to your industry which you need to address as well.

Here are a few examples of codes of conduct that you might want to review:

- General Electric <http://www.ge.com/files/usa/en/commitment/social/integrity/downloads/english.pdf>
- Microsoft <http://www.microsoft.com/citizenship/businesspractices/businesscodes.aspx>
- Verizon <http://www22.verizon.com/about/careers/pdfs/CodeOfConduct.pdf> Pfizer http://www.pfizer.com/pfizer/download/investors/corporate/business_conduct_policies_summary_2003.pdf
- Bank of America http://media.corporate-ir.net/media_files/irol/71/71595/corpgov/Ethics_6_21_05_final.pdf
- Federal Express <http://ir.fedex.com/downloads/code.pdf>
- Starbucks http://www.starbucks.com/aboutus/US_English_full_kit.pdf
- Sallie Mae http://www2.salliemae.com/about/corp_governance/slmcorp_board/business_conduct.

Under Section 406 of Sarbanes-Oxley public companies are also required to have a code of ethics for senior financial officers. Here are some examples:

- Aon http://www.aon.com/about/corp_governance/sfo_code.jsp
- PepsiAmericas <http://investors.pepsiamericas.com/governance-coe.cfm>
- McGraw-Hill <http://investor.mcgraw-hill.com/phoenix.zhtml?c=96562&p=irol-govconduct>
- Marathon Oil <http://www.marathon.com/content/released/CodeOfEthics.pdf>

Most codes of conduct address a variety of subjects that are often addressed in more depth in internal policies and procedures. A laundry list of the subjects typically covered by codes of conduct and/or related policies that you may want to consider includes:

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

Code Overview Statement

States company policy of commitment to ethical conduct and compliance with all applicable laws and regulations. Typically set forth as a letter or introductory statement from the CEO which helps establish the appropriate "tone at the top."

Compliance with Laws and regulations	Interaction with the Government	Reporting (of misconduct) Mechanisms	Prohibition against Insider Trading
Conflicts of Interest (including corporate opportunities)	Political Activities	Intellectual Property Matters	Media and Other Inquiries
Gifts & Entertainment	Confidential and Propriety Information	Hotlines	Equal Opportunity.
Antitrust & Fair Competition	Internal Investigations (includes non-retaliation policy)	Use of Company Resources	Prohibition against Discrimination and Harassment (including reporting mechanisms).
Document Retention	Books and Record-Keeping	Substance Abuse	Health Safety & Working Environment
Prohibition Against Workplace Violence	Employment Requirements (e.g., Wage and Hour Laws)	Use of Corporate Technology and Monitoring of emails	Diversity

Companies with international operations may want to address additional requirements including:

- Foreign Corrupt Practices Act
- Export/Import Controls
- Customs
- Requirements of foreign countries in which the company is doing business.⁴⁷

Companies also may want to address issues specific to their particular business activities and operations, including such matters as:

- Consumer or patient privacy
- Hazardous materials issues
- Product liability matters including testing procedures
- Anti-Money Laundering
- Various other legal and regulatory requirements applicable to the company because of the nature of its activities and operations.
-

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

Finally, company policies often include information regarding the system by which the company interprets, administers, and review its standards and procedures, including:

- Definitions
- Applicability
- Publication
- Amendments and Waivers
- Non-Exclusivity
- Remedies for Violations
- Review and Revision Process

3. Policies

Policies which you might use as an example to create or revise your own are also available, although not as readily as codes of conduct. ACC and in-house colleagues are two of the best sources for corporate policies, particularly colleagues working in peer industries for policies related to laws and regulations specific to that industry.

ACC Website

Numerous examples of policies are available on the ACC web site www.acca.com. Some of the subjects they cover include:

Emails and Computer Use

http://www.acca.com/protected/forms/employment/internet_policy.pdf

<http://www.acca.com/protected/forms/employment/electron.pdf>

<http://www.acca.com/protected/infopaks/email/infopak.pdf> (Policy appears at page 46)

Workplace Behavior and Security

<http://www.acca.com/protected/forms/employment/workbehavior.pdf>

<http://www.acca.com/protected/forms/security/workplace.pdf>

Substance Abuse

<http://www.acca.com/protected/policy/employment/substance.pdf>

Military Leave

<http://www.acca.com/protected/forms/leaveofabsence/military.html>

Anti-Harassment

http://www.acca.com/protected/forms/harassment/harass_imp.html

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

Smoking

<http://www.acca.com/protected/forms/smoking/smokepipjaff.html>

<http://www.acca.com/protected/forms/smoking/smokeirvine.html>

<http://www.acca.com/protected/forms/smoking/smokalrweil.html>

Privacy of Personal Data

<http://www.acca.com/protected/forms/privacy/personaldata.pdf>

Standards of Professional Conduct for Attorneys

<http://www.acca.com/protected/policy/conduct/unionbanca.pdf>

http://www.acca.com/protected/policy/conduct/rules_sample1.pdf

http://www.acca.com/protected/policy/conduct/rules_sample3.pdf

http://www.acca.com/protected/policy/conduct/wilmer_inhousepolicy.pdf

<http://www.acca.com/protected/policy/conduct/xerox.pdf>

Document Retention

<http://www.acca.com/protected/infopaks/quickreference/goodemailpractices.pdf>

http://www.acca.com/protected/forms/records/retention_fae.pdf

Foreign Corrupt Practices Act

<http://www.omm.com/webdata/content/publications/fcpa2003.final.pdf> (Policy appears at page 72 of document)

Internet

Many policies also may be found through a simple internet search. Some subjects located in this manner include:

Various Corporate Policies

http://www.baxter.com/about_baxter/sustainability/our_values_and_standards/global_business_practice_standards/standards.html

Conflicts of Interest

<http://www.americanheart.org/presenter.jhtml?identifier=3023759>

<http://www.cmu.edu/policies/documents/IntConflict.html>

<http://www.hms.harvard.edu/integrity/conf.html>

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

Entertainment and Gifts

<http://www.boeing.com/companyoffices/aboutus/ethics/pro6.pdf>

<http://www.frequelec.com/codeofethics.htm>

http://www.bbgroup.com/pdf/GiftsBusinessCourtesiesGratuitiesandFavours_1999.pdf

Antitrust

http://www.spe.org/spe/jsp/basic/0,,1104_1898,00.html

http://www.osdl.org/docs/antitrust_policy_document.pdf

http://www.yale.edu/provost/Yale_Antitrust_Compliance.pdf

<http://www.pennnationalinsurance.com/PORTAL/Documents/PDF/Corporate%20Governance/Antitrust%20Compliance%20Policy.pdf>

<http://www.acca.com/protected/forms/compliance/ashland/index.html>

Insider Trading

http://www.radioshackcorporation.com/it/ethics/insider_policy.html

<http://www.delmonte.com/company/Governance/InsiderTrading.pdf>

http://www.gm.com/company/investor_information/docs/corp_gov/insider_trading_pol.pdf

Document Retention

<http://www.abanet.org/lpm/lpt/articles/sampledocumentretentionpolicy.pdf>

Non-Retaliation

<http://www.ohiou.edu/policy/03-006.html#procedure>

<http://www.ncna.org/index.cfm?fuseaction=page.viewPage&pageID=430>

<http://www.inlandrealstate.com/investor/IRECW/WHISTLEBLOWERPOLICY.pdf>

Confidential Information

<http://www.mace.com/media/pdf/governances/confidential.pdf>

http://www.amgen.com/about/corporate_compliance_confidential_proprietary.html

<http://www.scu.edu/humanresources/policy/305.cfm?menu=300>

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

Foreign Corrupt Practices Act

http://www.devonenergy.com/corpgov/GP-Foreign_Corrupt_Practices_Act.pdf

http://www.willbros.com/fw/main/Foreign_Corrupt_Practices_Act_Compliance_Policy-95.html

<http://www.cbi.com/ir/cg/documents/CBIRedBookStandard121-5.pdf>

Sexual Harassment

<http://www.cu.edu/policies/Personnel/sexharass.html> <http://www.mass.gov/mcad/harassment.html>

http://www.officedepot.com/renderStaticPage.do;10gg9eb56?context=/content&file=/BusinessTools/tools/sxhst_m.jsp

Intellectual Property

<http://www.utsystem.edu/OGC/intellectualproperty/ippol.htm>

F. Task # 6: Establish An Effective Training And Communications Program**1. Guidelines Requirements**

USSG §8B2.1(b) (4) (A) requires that: “The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to [the Board, high level personnel, substantial authority personnel, the company’s employees, and as appropriate, the company’s agents] by conducting effective training programs and otherwise disseminating information appropriate to such individual’s respective roles and responsibilities.”

As explained by the Advisory Group, compliance training “should not be merely considered as one of the many ways to communicate effectively [organizational] standards and procedures.” Rather, “The Advisory Group believes that effective training has two components: (1) educating all employees about compliance requirements, *and* (2) motivating all employees to comply” [emphasis in original]. As the Advisory Group observes “Simply communicating standard procedures through written documentation may satisfy the first, but is unlikely to be effective in motivating employees to comply over time.” Consequentially, it is expected that “all organizations should engage in some sort of active compliance training.”⁴⁸

In the area of training, as in others, the Advisory Group declined to specify what type of compliance training should be provided. Rather, it stated that:

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

...organizations should have the flexibility to determine the types of compliance training and information dissemination that are appropriate given the size of their workforces, the types of misconduct that are of concern given the organizations' operations and fields of activity, and other factors such as the job responsibilities of the person being trained.⁴⁹

Here are some basic rules about training and communications that you should consider.

- Document, document, document. You are what you document. In order to demonstrate the effectiveness of your training and communications program you are going to have to be able to produce documents or a database minimally showing:
 - When and how the training was offered and who took it (a schedule of trainings, the attendance list, and other availability of the training such as video versions. Note: documentation of the availability of the training is important to demonstrate that even if an employee did not take the training you gave them numerous opportunities to do so)
 - The substance of the training (e.g., a copy of the PowerPoint and any hand-outs);
 - When communications were issued, what they were, and who got them (e.g., a copy of what was posted on the intranet, a copy of the company wide email that went out, etc.)
- Everyone needs to be included. While its substance may or may not differ, training is appropriate for everyone from the corporate receptionist to the CEO. It is not unusual for an auditor to request that documentation be produced that every senior executive has taken their code of conduct training. This underscores the importance of components of the Program being applied equally to those at the top. Moreover, it provides Program staff with a good response to senior executives who haven't completed their training, e.g., "I understand you are busy and it is difficult to find the time to take the training, but I want you to know that on audit I have been asked whether senior officers have taken the training and I wouldn't want you to get in trouble, so..."
- Code of conduct training is essential. Your code of conduct should establish the "tone at the top," convey the ethical culture of your company, and serve as the umbrella for all your standards and procedures. Absent this training, a review of your Program is not likely to be favorable. Moreover, given that the courts, the EEOC, and state agencies regularly scrutinize an entity's compliance activities in connection with fair employment actions, training in this arena should also

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

be viewed as essential.⁵⁰

- Meet special requirements. Training may also specifically be required under certain regulatory frameworks (e.g., anti-money laundering) so you should take steps to assure that those requirements are met.

2. Doing More with Less: Effective Training and Communications

- Consolidate Tasks. For example, present a simple overview of a number of legal and regulatory subjects if that is sufficient for your purposes. It may be easier to get employees to attend a half day of training than three one hour sessions.
- Employ Your Risk Assessment. Carefully evaluate, based on risk, which employees need to take a particular course and limit your audience to a reasonably related group. For example, perhaps only your sales force is at risk for antitrust violations—not everyone down in the Distribution Department—so just provide it to the sales force.
- Plan Ahead. Record all of your training sessions. If you provide classroom training get it on video for later use for make-ups and new employees. Nothing burns up resources like having to teach a class over and over. Create a whole library of compliance courses. If you place them on a server, distribution can be facilitated by emailing a link to the course. Note: If an attorney is teaching a taped course save questions to the end — as the answers may be privileged — and don't record them. At training sessions about legal and regulatory matters employees always should be counseled to frame their questions generally or speak to the trainer privately.
- Use Communications to Reinforce Training. While the Advisory Group makes it clear that communications alone will not substitute for training, this should not preclude you from using them to reinforce the training (e.g., bulletins during the winter holiday season to remind employees of the Gifts and Entertainment Policy or to reinforce the Political Activities Policy during an election year). To save resources use corporate wide emails or postings on company intranet web sites.
- Use Outside Resources, Part I. Web-based training will provide you with a big bang for your buck. Thousands of employees may be trained — often at the time and place of their choice. Code of conduct and fair employment training are prime candidates for web-based training and are available from multiple vendors. The cost of training may significantly be reduced if you negotiate with the vendor for a contract with a longer term and more courses. Potential vendors include (in no particular order and without any endorsement):

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

Integrity Interactive <http://www.integrity-interactive.com>

LRN <http://www.lrn.com>

WeComply <http://www.wecomply.com>

Midi <http://www.midicorp.com>

Corpedia <http://welcome.corpedia.com>; and

WorkingValues <http://www.workingvalues.com>

- Use Outside Resources, Part II. ACC has an alliance with WeComply which allows ACC member companies a free 100-employee trial of any of WeComply's training programs. See <http://www.acca.com/practice/alliance.php#wecomply>
- Use Outside Resources, Part III. Outside counsel that provides services to your company may be more than happy to provide training for you in their area of expertise at a reduced rate or for free. Be sure to video it and get appropriate approvals and releases so it can be used again.
- Staff Smart. This is a good time to use the SLD's limited resources. If you use web-based or other "off the shelf" training---use your lawyers to tailor it to your company's needs if it is appropriate to do so. This will make it more meaningful to employees; irrelevant training is a great source of frustration. However, if the training is suitable in its "off the shelf" format, then use it "as is" and conserve your resources. In all events, use your non-legal resources to oversee the project (e.g. implementing edits, negotiating with the vendor, etc.).
- Share the Challenge, Part I. Provide training at employee orientations where HR can assist you in the presentation and tracking attendance. In small companies training may even occur "through informal staff meetings, and monitoring through regular "walk-arounds" or continuous observation while managing the organization."⁵¹ Even in large companies at the same time operational training is given compliance training can be provided as well by non-lawyers who are knowledgeable about the requirements they must meet. (e.g., when a new employee is trained about how wire transfers are made he/she can also be trained about anti-money laundering requirements). Just make sure the training is documented.
- Share the Challenge, Part II. Coordinate carefully with your HR. You cannot have a meaningful training tracking system unless you create a comprehensive list of current employees. This will require regular updating due to new hires, terminations, and people being unavailable for training because of maternity leave, long term disabilities, etc. Preferably the list should be able to be "crunched" in a number of ways (e.g., by division, job level, supervisor etc.)

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

which will greatly facilitate your training efforts (e.g., allowing you to identify groups of employees who require training, identifying supervisors to enable you to inform them when an employee has not completed training, etc.) and your monitoring and auditing of training.

- Consider Providing "Top Gun" Training. This is training that is made available only to senior executives at a regular meeting — preferably one where the CEO attends — thus guaranteeing other's attendance. This training is tailored to provide basic information about applicable statutes or regulations, rather than an in-depth analysis. Providing this type of training helps to assure that: (1) the proper "tone at the top" is established; (2) "high level personnel" are properly trained; and (3) executives have an opportunity to discuss what is being taught in a forum where discussion might be more candid. If done well, it also provides you with an opportunity to demonstrate the benefits of the Program. Modified Top Gun Training may be suitable for the Board.

Caveat: In depth training may still be required for high level personnel in their specific areas of operation where their attendance will also help to establish the appropriate "tone at the top" for their subordinates by showing their commitment to the Program.

- Use Technology, Part I. For example (and without endorsement), Microsoft® Live Meeting allows you to bring a classroom presentation to each employee's desktop-- allowing you to train dozens of employees without them leaving their offices. Other software solutions provide similar services.
- Use Technology, Part II. If you are using web-based training your vendor can issue reminder notices and track "attendance" for you. Other software solutions are available for this purpose and can be used to track both web-based and classroom training. Tracking training on paper can burn up resources and, if it is used, must be carefully planned. In determining how you track training you should consider how your system will document your training for monitoring and auditing purposes.

G. Task # 7: Establish A Reporting Mechanism (Hotline)⁵²

1. Guidelines Requirements

USSC § 8B2.1(b)(5)(C) requires that "The organization shall take reasonable steps — (C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual [misconduct] without fear of retaliation."

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

As is true with other provisions of the Guidelines, other sources may supplement these requirements and should be considered. Sarbanes-Oxley provides protection for whistleblowers as well, imposing civil or criminal liability for retaliating against employees who provide information which the employee reasonably believes constitutes a violation of securities laws or regulations or certain types of fraud. Sarbanes-Oxley also requires the Audit Committee of the company to provide for and oversee confidential, anonymous reporting procedures for employees and others to express concerns about questionable accounting, audit, and internal control matters.

Another example, the market listing rules of the NYSE, require:

Encouraging the reporting of any illegal or unethical behavior. The company should proactively promote ethical behavior. The company should encourage employees to talk to supervisors, managers or other appropriate personnel when in doubt about the best course of action in a particular situation. Additionally, employees should report violations of laws, rules, regulations or the code of business conduct to appropriate personnel. To encourage employees to report such violations, the company must ensure that employees know that the company will not allow retaliation for reports made in good faith.⁵³

Finally, companies must be attuned to the requirements of various regulatory agencies that may address this matter, requiring that program participants maintain a system "such as a hotline to receive complaints, and the adoption of procedures to protect the anonymity of complainants and to protect whistleblowers from retaliation."⁵⁴ These same agencies also maintain hotlines available to your employees⁵⁵ and have established whistleblower programs to allow employees to file complaints and offering them protection from retaliation if they do.⁵⁶

To meet these requirements and address other important compliance related issues, a company should adopt, distribute, publicize, and train its employees about the corporation's policy on this subject which should minimally contain the following:

- An overall statement of the company's commitment to:
 - operate ethically and in compliance with all applicable laws and regulations;
 - having employees raise issues of inappropriate behavior and non-compliance so that they may be addressed;
 - provide an environment in which employees may safely raise such concerns without fear of retaliation;

- take action against any employee who violates the prohibition against retaliation;
- other principles consistent with the company's culture and policies (e.g., management's "open door" policy, managers' obligation to create an "open working environment," management's commitment that ethical conduct and compliance with the law should come before meeting business objectives, etc.)

- A broad description of the types of matters which the company expects should be raised (e.g., violations of applicable law or regulation, code of conduct, company policies, accounting controls, or auditing matters, etc.) and the reasons why they should be raised (e.g., to allow the matter to be addressed for the benefit of the company, to protect shareholders, to do the right thing, etc.).
- A statement that either encourages or directs employees to raise such matter
Note: some companies require employees to raise issues of misconduct, others do not. Some require only managers or officers to raise them when they become aware of them first hand or as reported to them by a subordinate.
- The avenues through which these issues can be raised (e.g., reports to hotline, ombudsman, offices of ethics or investigations, Legal Department, Audit Committee, supervisor, through any management employee or officer, etc.). Note: some companies want to create as many reporting avenues as possible to facilitate reporting; others want to narrow the possibilities so that the reporting and response are better controlled.
- Complete information on how to raise a complaint (e.g., hotline numbers and hours, relevant mailing addresses, e/mail addresses etc.)
- Statement of the policy on confidentiality and anonymity including explaining any limitations (e.g., it may be impossible to process a complaint thoroughly without implicitly identifying the complainant, such as a sexual harassment complaint in a small office; that anonymous complaints that do not provide complete information may also present challenges; that regulators may have access to such complaints, etc.).
- Statement of the prohibition against retaliation including that any employee who retaliates against another employee for raising an issue or participating in an investigation will be subject to disciplinary action.

2. Doing More With Less: Hotlines

- Share the Challenge. You should "advertise" your policy and hotline through posters, stickers, an icon on your company's internal website, or some other means that makes the policy and hotline number readily available to your em-

employees. Get your communications office to assist you by creating the necessary graphics. Also be creative about how to get these “advertisements” out without using your resources (e.g., cleaning staff can staple posters to bulletin boards, phone stickers can be sent out as part of some other company-wide message or with pay checks, stickers can be applied to the backs of security badges as employees come through the door, coffee mugs with the number on them can be placed in office kitchens, pre-printed Rolodex™ cards can be distributed through administrative assistants, etc.) Remember — whatever your choice is — document how you did it.

- **Staff Smart.** Make decisions about placing limitations on your Hotline to preserve resources. Does it really need to be 24/7, or will regular business hours suffice? Does a real person need to be available to answer calls or will a 24 hour turnaround on a recorded message suffice? How about a combination of a real person during working hours and voicemail thereafter? How these questions are answered will need to take issues into considerations such as whether the company functions in multiple time zones and countries.
- **Use Technology, Part I.** Publicize your policy by posting it on the company's intranet and sending it out (or a link to it) with a company wide-e/mail. It is particularly desirable to have this policy introduced or transmitted by your CEO as it is an important part of establishing an appropriate “tone at the top.”
- **Use Technology, Part II.** Reinforce the existence of your reporting mechanisms at least annually. Send another e/mail from the CEO. Require employees, as part of their annual code certification, to certify that they know how to find the hotline number by requesting that they fill it in on the certification form; perhaps irritating, but effective. Note: Program auditors frequently ask employees to identify how they would report a concern. Employees who have the hotline number at their fingertips — literally — can easily respond.
- **Use Technology, Part III.** Keep your hotline system in-house, but work with your technical experts to enhance its operation. For example, for complainants who desire to be anonymous, a system employing temporary mailboxes may be set up so that arrangements for future contacts may be made. Systems also can be established so that calls may be initially screened to preserve resources (e.g., Press #1 to make a recorded anonymous complaint about possible misconduct; Press # 2 to anonymously or confidentially speak to a real person, etc.)

Note: If you use such a system all “Caller ID” mechanisms must be fully deactivated on all phones receiving the calls and employees should be advised of the same.

- **Use Outside Resources.** Farm out your hotline's operation to a vendor. If you do so, use your SLD resources to create guidelines to assure the vendor knows how to answer the calls, how to document complaints, what needs to be re-

ported to the company and when, procedures for re-contacting an anonymous complainant, etc. And trust but verify. At least quarterly, call the vendor and make a test complaint and assess how it is handled. Set forth below (in no particular order and without endorsement) are a number of vendors that provide third party hotlines.

Wackenhut:

<http://www.ci-wackenhut.com/S2S%20Compliance%20Hotline.htm>

EthicsPoint:

http://info.ethicspoint.com/ethics_hotline.asp

ReportIt:

<http://www.reportit.net/>

GlobalCompliance:

<http://www.globalcompliance.com/information-reporting.html>

- **Use these Tools.** Take a look at other policies regarding hotlines to consider in creating (or enhancing) one tailored for your company. Some statements regarding hotlines are contained within codes of conduct. Other policies are posted only on employee intranet web sites (sometimes in addition to what is stated in the code of conduct) and your colleagues are the best sources for those. Finally, some are available on the internet. Here are a few.

<http://www.admivc.ucla.edu/appm/public/whstlblw.pdf>

http://www.gerbescientific.com/governance/policy_complaints.htm

http://www.doa.virginia.gov/DSIA/Fraud_and_Abuse_Hotline.cfm

<http://www.yale.edu/resources/Feb06Memo.pdf>

<http://investors.portlandgeneral.com/communications.cfm>

http://www.mbakercorp.com/COBC_HotlinePamphlet.pdf

<http://www.boeing.com/companyoffices/aboutus/ethics/hotline.html>

<http://ir.teldta.com/phoenix.zhtml?c=67422&p=irol-govEthicsline>

http://www.morehouse.edu/Intranet/ethics/quest_answ.php

<http://www.agcocorp.com/default.cfm?PID=1.4.6.6>

<http://www.motorola.com/content.jsp?globalObjectId=75-107>

<http://www.dow.com/about/aboutdow/ethics.htm>

Note: Some organizations have separate hotlines for concerns regarding accounting, internal accounting controls and auditing matters. Here are some examples.

<http://www.ulticom.com/html/investors/corporate-governance-sarbanes-hotline.asp>

http://www.filenet.com/English/About_FileNet/Investor_Relations/Corporate_Governance/033630042.asp

<http://att.sbc.com/gen/investor-relations?pid=5621>

H. Task # 8: Implement The Carrot And Stick Approach

1. Guidelines Requirements

USSG §8B2.1(b)(6) requires that “The organization’s compliance and ethics program shall be 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 [misconduct] and for failing to take reasonable steps to prevent or detect [misconduct].”

Earlier versions of the Guidelines provided for the imposition of disciplinary measures for failure to comply with applicable requirements (i.e., “sticks”) which were retained in (B) above. The Advisory Group concluded, however, that this language should be changed by adding language “to promote compliance standards through positive incentives as well as through disciplinary mechanisms. A culture of compliance can be promoted where organizational actors are judged by, and rewarded for, their positive compliance performance.” Thus the Advisory Group proposed language that was ultimately adopted indicating that “compliance standards should be promoted through incentives as well as enforced through disciplinary measures, giving both a ‘carrot and stick’ to this component of the guidelines.”⁵⁷

This aspect of the Guidelines can be reduced to basically three elements:

1. There should be incentives for acceptable compliance related performance.
2. There should be disincentives for unacceptable compliance related performance.
3. Misconduct itself or failure to prevent or detect misconduct should result in discipline.

Much of what is addressed in this Guideline relates to basic employee performance standards. While different companies may slice and dice these standards different ways and call them different things, reduced to their simplest form there are basically two types of performance standards. The first standard relates to how an

employee performs (i.e., a qualitative standard). The second standard relates to what the employee accomplishes (i.e., a quantitative standard). The incentives/disincentives approach of the Guidelines may be implemented by wrapping it into the existing qualitative and quantitative performance standards of the company.

For example, “compliance with the letter and spirit of all applicable laws and regulations” or “exercising honesty and integrity in business transactions” are examples of compliance related qualitative standards of performance. They can easily be incorporated into existing criterion.

Similarly, just as a goal of “annually meeting production goals of manufacturing 1,000 widgets” may be established as a quantitative standard — so too compliance related quantitative performance standards may be implemented. Conducting thorough risk assessments, establishing anti-fraud programs, meeting the requirements of business unit compliance plans, etc., are all examples of compliance related quantitative performance standards.

Other considerations which might be incorporated into these performance standards include whether a manager: (1) is knowledgeable about the company’s compliance program; (2) communicates to employees that they are required to operate ethically, and comply with all applicable laws and regulations, the code of conduct and the company’s policies; (3) maintains an open working environment where he/she is reasonably accessible and where employees are encouraged to raise issues of concern and feel that they may do so without fear of retaliation; (4) serves as an example by participating in program activities such as certifying to the code, taking required training by attending in a timely manner and participating, adhering to company policy (e.g., not accepting or providing inappropriate gifts), making appropriate disclosures of potential conflicts of interest; addressing problem situations including referring them to the ethics, investigations or legal departments, as appropriate, and taking steps to assure that the employees he/she supervises do the same and holds them accountable when they do not; (5) fully cooperates with any review or investigation of compliance related matters and takes steps to assure that the employees he/she supervises does the same; and (6) incorporates compliance related performance standards into the performance appraisal he/she conducts of subordinates

Steps then have to be taken to effectuate and apply the standards and otherwise make them “real” for the employee. These steps may include:

- Incorporating the standards into an employee’s goals, objectives, plans, job descriptions, or whatever other instrument is appropriate for the company.
- Securing input for the appraisal process to determine whether the employee is meeting the compliance related standards which might be acquired through subordinate, peer and manager input into the performance appraisal process,

other evaluations such as 360 assessments, employee surveys, and input from the compliance function itself.

- Incorporating compliance related evaluations into compensation (salary, bonuses, stock options, etc) and other employment related actions (e.g., promotions, expansion of managerial responsibilities, opportunities to participate in leadership programs, etc.).

Whether or not compliance related performance standards are met will set the whole tone for the company. Success or lack thereof will contribute (or detract) from whether the company achieves and maintains a culture that “encourages ethical conduct and commitment to compliance with the law.”

As recently reported in the Wall Street Journal, the importance of meeting compliance related performance standards is being recognized at the top ranks of companies. In one article it was noted that Boeing Chairman & CEO James McNerney “has made it clear that he believes the incidents that led to [recent] criminal investigations were isolated lapses by a handful of employees, but he also has said Boeing’s previous management didn’t place enough stress on ethical behavior. He has since scrapped an executive-compensation plan under which executives were rewarded for meeting primarily financial goals, and replaced it with one tied to broader criteria, including integrity and ethical leadership.”⁵⁸

The third standard identified in this Guideline is basically the extreme version of a disincentive for failing to meet performance standards. When an employee not only fails to acceptably perform, but engages in misconduct or fails to prevent or detect misconduct, then appropriate discipline should be the result. Assumedly this discipline would be compensation related, but would carry additional stigma with it (e.g., suspension, demotion or termination). Finally, appropriate discipline could go beyond the notions of a compensation related disincentive such as referral of questionable activities to civil or criminal authorities.

2. Doing More with Less: Carrots and Sticks

- Share the Challenge. Implementing compliance related performance standards in many companies is principally the responsibility of HR. These efforts should be designed to achieve three objectives: (1) establishing the standards; (2) securing the information that is necessary to determine how an employee meets these standards; and (3) taking steps to assure that these standards are actually considered when the employee’s performance is evaluated and are reflected in compensation and other related matters.

Internal Audit and Risk Assessment can assist in this analysis by examining elements of compliance related performance in their work and taking steps to assure that their findings are considered in the performance appraisal process. For exam-

ple, if an audit reveals that a manager has failed to establish or properly maintain internal controls for financial reporting or failed to design and implement company required activities to prevent and detect misconduct (e.g., establishment of a business unit anti-fraud program) a mechanism should be designed to assure this information is incorporated into the performance appraisal process.

- Staff Smart. Depending on a company’s organizational structure the SLD’s contribution to this undertaking should as much as possible be limited to: (1) educating HR, Internal Audit, and Risk Management (and others as appropriate) about the requirements of the Guidelines; (2) providing such other legal advice and assistance as may be associated with establishing employment performance standards (e.g., union contract requirements, non-discriminatory application, etc); and (3) reviewing the final work product for completeness.

I. Task # 9: Screen Your Employees

1. Guidelines Requirements

§ 8B2.1 (b) (3) requires that “The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.”

For the purpose of determining who should be screened, the Guidelines define the subject personnel as follows:

“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 must be determined on a case-by-case basis.⁵⁹

“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, administra-

tion, or finance; and an individual with a substantial ownership interest.⁶⁰

The Guidelines also explain the purpose and application of this provision stating that:

[T]he organization shall hire and promote individuals so as to ensure that all individuals within the high-level personnel and substantial authority personnel of the organization will perform their assigned duties in a manner consistent with the exercise of due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law... With respect to the hiring or promotion of such individuals, an organization shall consider the relatedness of the individual's illegal activities and other misconduct (i.e., other conduct inconsistent with an effective compliance and ethics program) to the specific responsibilities the individual is anticipated to be assigned and other factors such as: (i) the recency of the individual's illegal activities and other misconduct; and (ii) whether the individual has engaged in other such illegal activities and other such misconduct.

2. Doing More with Less: Screening

- Share the Challenge. Overall implementation of this requirement is best left to HR and/or Security.
- Use Outside Resources. There are significant numbers of vendors who perform this work as well as some on-line screening processes. Reputation, experience, and appropriate databases should be principal considerations. Set forth below (in no particular order and without endorsement) are a number of vendors that provide employment screening services. Others may be identified by searching the term "background check" on the internet.

Wackenhut

<http://www.ci-wackenhut.com/Pre-employment.htm>

Kroll

<http://www.baionline.net/index.cfm?ContentID=13>

ChoicePoint

http://www.choicepoint.com/business/pre_employ/pre_employ.html

- Staff Smart. The SLD's contribution to this undertaking should as much as possible be limited to providing consultation and legal advice on:
 - Who should be screened that meets the definitions set forth above and who might otherwise make sense based on an appropriate risk assessment⁶²;

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

- What the scope of the screening should be, taking into consideration any requirement for obtaining permission from the potential or existing employee, and the application of any laws that might limit screening;⁶³
- When the screening should be done including pre-employment, when an existing employee moves to a position that meets the definitions or other appropriate risk profile, and perhaps periodically if the employee's responsibilities continue to fit the definitions (e.g., every 5 years); and
- How the screening is to be performed, including contractual arrangements with vendors which should be specific about the elements of the screening, cost, and turn around time.

J. Task # 10: Keep Your Program Effective: Monitoring And Auditing, Assessments, And Revisions

1. Guidelines Requirements

USSG §8B2.1 (b) (5) (A) requires that "The organization shall take reasonable steps—(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect [misconduct]; and

USSG §8B2.1 (b) (5) (B) requires that "The organization shall take reasonable steps—(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program."

USSG §8B2.1 (b) (7) requires that "After [misconduct] has been detected, the organization shall take reasonable steps to respond appropriately to the [misconduct] and to prevent further similar [misconduct]⁶⁴ including making any necessary modifications to the organization's compliance and ethics program."

In considering possible amendments to the Guidelines, the Advisory Group concluded that:

...an increased emphasis on monitoring, auditing, and evaluation practices is justified on three independently sufficient grounds: (1) the recognition of the importance of compliance monitoring, auditing, and evaluation in recent legal standards; (2) practical evidence of the importance of these practices in revealing recent incidents of major corporate misconduct; and (3) privately developed standards and expert opinions identifying monitoring, auditing, and evaluation efforts as important components of effective compliance programs.⁶⁵

In support of this conclusion, the Advisory Group cited a number of examples of regulators that impose such requirements including the Department of the Treasury, the Environmental Protection Agency, and the Department of Health and Human Services, the role of independent auditors in detecting and stopping corporate misconduct, and the opinions of experts in the compliance field.⁶⁶

Consequently, the Advisory Group recommended the addition of USSG §8B2.1 (b)(5)(A&B) for the following reasons.

First, the proposed changes...recognize that regular compliance evaluations through auditing and monitoring practices are essential features of every compliance program.

Second, the proposed changes indicate that organizations should regularly scrutinize two separate organizational characteristics: (1) the adherence of organizational activities to applicable laws and compliance program requirements; and (2) the sufficiency of managerial practices comprising an organization's compliance program to ensure a reasonable likelihood of success in preventing and detecting violations of law...

Third, through additional provisions contained in §8B2.1(c), the proposed changes specify that compliance monitoring, auditing, and evaluation practices should be based on compliance risk assessments. This change clarifies that characteristics of monitoring, auditing, and evaluation efforts, such as the targeting and frequency of compliance assessments, should correspond to the likelihood of compliance problems in particular organizational activities.⁶⁷

As in other instances, the Advisory Group did not prescribe what monitoring and auditing activities would be appropriate for the organization. It left that determination to the organization, significantly distinguishing between large and small organizations:

The proposed changes do not specify the precise sorts of monitoring or auditing practices that will constitute adequate steps under these standards. Determinations of the sorts of periodic compliance assessments that will compose sufficient monitoring, auditing, and evaluation practices will depend on the characteristics and activities of specific organizations. In small organizations, periodic evaluations of compliance in the course of day-to-day business operating practices will often be adequate monitoring steps so that further auditing or evaluations will not be needed. In larger organizations, however, separate audits of compliance performance will usually be warranted, with such audits being conducted by internal or external parties who are independent of

the managers overseeing the performance under scrutiny.

In general, a sufficient monitoring, auditing, and evaluation system will be one which provides organizational managers, on an ongoing basis, with sufficient information to determine if their organization's compliance program is generally effective in preventing and detecting violations of law. This degree of information, and the monitoring, auditing, and evaluation practices that are needed to obtain it, will depend on such features as an organization's compliance history, functional units, operating practices, and legal environment.⁶⁸

Finally, the Advisory Group confirmed that the components of Programs should be revisited and, if appropriate, revised following the detection of misconduct as set forth in USSG §8B2.1 (b) (7).⁶⁹

2. Doing More with Less: Monitoring and Auditing, Assessments, and Revisions

Caveat: Although the issue may arise at anytime, in the monitoring and auditing arena counsel should be particularly sensitive to possible conflicts of interest between the company and its employees. Attorneys should keep in mind their obligations under Model Rule of Professional Conduct 1.13 and its state counterparts. In sum, these rules make it clear that counsel are counsel to the corporation and not the corporation's employees and, where appropriate, need to inform the employees of the same and the implications of that fact. (i.e., provide the "Corporate Miranda.")⁷⁰

- **Employ Your Risk Assessment, Part I.** Monitoring and auditing should be focused on those activities and operations that present the highest areas of risk for misconduct or where the company is otherwise required under law or by regulation to monitor and audit (e.g., anti-money laundering programs).
- **Employ Your Risk Assessment, Part II.** As your risk assessment changes (based on changes in the applicable law and regulations, implementation of new business activities and cessation of others, etc.) your Program should be revised accordingly.
- **Plan Ahead.** Carefully tracking and documenting Program activities can vastly reduce the resources required for monitoring and auditing. For example, simply maintaining all Board communications, training materials and attendance lists, copies of company policies and communications relating thereto etc. in separate notebooks or files that can easily be produced will facilitate review. Use of pre-determined procedures for implementing aspects of the Program (e.g.,

procedures for certification processes) will create a clear map for monitoring and auditing purposes that will more easily demonstrate that those activities took place.


- Share the Challenge, Part I. So long as there is no conflict of interest (e.g., a system should not be monitored by the individual responsible for its implementation), other internal resources such as HR, internal audit, security, or information systems, as appropriate, can be used to perform the monitoring and auditing tasks. Internal Audit should be urged to regularly review the Program itself as well as reviewing compliance with the Program when separately reviewing business unit activities.
- Share the Challenge, Part II. Careful coordination between investigative, legal department, internal audit, business, and compliance activities will assure that Program revisions are made (and documented), as appropriate. For example, if the legal department identifies problems with the requirements imposed by the antitrust laws it should be reported to the compliance function. This should trigger corrective Program activities such as the provision of further training and the initiation of monitoring measures to assure the changes are effective.
- Share the Challenge, Part III. Piggyback on other company activities to evaluate your Program. For example, HR activities such as employee surveys, employee 360s, employee exit interviews etc. can be used to measure the effectiveness of Program activities.
- Use Technology. Technology can be used to set up systems to facilitate monitoring and audits (e.g., by setting up systems so that information can be “crunched” in various forms to identify possible misconduct and failures to comply with the requirements of the Program).
- Use Outside Resources. Monitoring and auditing can be contracted out. Review of the Program particularly for a large organization itself should regularly be performed by an independent third party.
- Use These Tools
 - Sample Employee Compliance Survey appears as Tool # 10.
 - Sample Employee Exit Interview Questions appearing as Tool # 11.

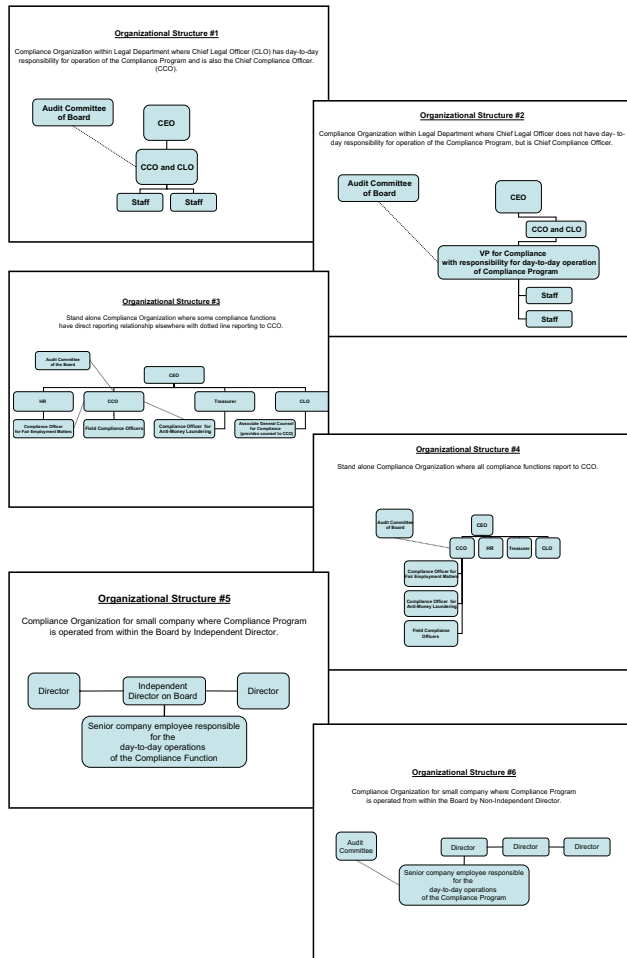
V. Conclusion

Unlike the person in the cartoon mentioned at the beginning of this piece, you really can't put together a Compliance Program with nothing. And it is important that your Board and senior management understand this fact and the significant liability for the company if it does not have an effective Program. However with reasonable resources and using the suggested strategies you really can do more with less.

VI. Sample Forms and Policies

A. Tool #1: Sample Organizational Structures for Corporate Compliance

<p>Organizational Structures for Corporate Compliance</p>  <p>InfoPAK Effective Compliance and Ethics Programs for the Small Law Department Doing More with Less Tool #1</p>	<p>Introduction</p> <p>The organization of the compliance function may be structured along lines that make the most sense for the company. It should, however, take into account a number of considerations that are reflected in the proposed structures:</p> <ul style="list-style-type: none"> • the Board and senior management have oversight responsibilities for the function; • individuals responsible for the day-to-day operations of the function should report to the Board (or appropriate subgroup); • individuals responsible for the day-to-day operations of the function should have “appropriate authority”; and • the structure should address conflicts of interest (e.g., overseeing the compliance of a supervisor).
---	---



B. Tool #2: Sample Chief Compliance Officer Position Description⁷¹

The Chief Compliance Officer is a Senior Vice President level position and head of the Office of Ethics and Compliance (OEC). The Chief Compliance Officer reports directly to the CEO and to the Audit Committee of the Board. The principal responsibility of the Chief Compliance Officer is to establish, maintain, and oversee an effective compliance and ethics program for the Company which is consistent with: (1) the provisions of the Federal Sentencing Guidelines established by the United States Sentencing Commission; and (2) such other statutory, regulatory and ethical requirements as may be applicable to the Company. (Compliance Program).

Duties

The duties of the Chief Compliance Officer include, but are not limited to, the following:

Tone at the Top. Working with other senior management to establish a “tone at the top” that reflects the company’s commitment to ethical business conduct and compliance with the letter and spirit of the law in all aspects of the Company’s operations.

Code of Conduct. Having principal responsibility for the administration of the Company’s Code of Conduct (Code), including:

- Revising and updating the Code, from time to time as may be appropriate, with any substantive revisions subject to the approval of the Audit Committee;
- Publishing the Code (and revisions to the Code) and otherwise making it readily available to Company employees;
- Providing Company employees with advice interpreting the provisions of the Code;
- Taking such actions as may be appropriate to investigate and enforce the Code;
- Creating, publishing, maintaining, and interpreting such additional policies and procedures as may be appropriate to fully implement the provisions of the Code or to otherwise meet the requirements of applicable statutes, regulations, or ethical standards.

Board. Working closely with the Audit Committee of the Board (and the full Board as appropriate) to undertake such compliance related activities as the Board may direct or may otherwise be required, including keeping the Board apprised of the following in a timely manner:

- the content and operation of the Compliance Program so as to enable the Board to exercise reasonable oversight for the Compliance Program;

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

- whether the Compliance Program has adequate resources;
- any allegations against an officer of the Company; where the allegations involve significant accounting or financial improprieties; or where, if proven true, the actions or failure to act would have a significant impact on the Company; or any other conduct by an employee which the Chief Compliance Officer believes should be brought to the Board's attention; and
- the compliance related performance of any senior personnel for whom the Board (or a subgroup thereof) evaluates performance and makes determinations regarding compensation.

Senior Management. Acting as the liaison with senior management, including:

- keeping them apprised of their obligations under the Compliance Program,
- including establishing and maintaining an appropriate "tone at the top:
- assisting and coordinating with them to implement compliance activities in their business operations; and
- evaluating their compliance related performance.

Risk Assessment. Directing and/or participating in regular risk assessments of the activities and operations of the Company, the results of which shall be used to, among other things, establish or appropriately modify the components of the Compliance Program.

Corporate Integrity Line. Managing the Corporate Integrity Line (CIL) and implementing activities relating to its underlying purpose, including:

- assuring that the CIL is operated in an effective manner (including that complaints may be made confidentially and anonymously) and employees are provided with access to the CIL at such times of day and in such manner as the Chief Compliance Officer determines appropriate;
- creating, publishing, and administering a policy regarding an employee's obligation to report conduct that possibly violates applicable laws, regulations, the Code and/or ethical standards and the avenues for reporting such misconduct including the CIL;
- training Company managers about how to maintain an open working environment where employees feel free to raise issues without fear of retaliation, how to respond to an employee's complaint and when to refer it to the OEC, and that retaliation against any employee raising a good faith complaint or participating in a Company authorized investigation is the basis for disciplinary action;
- screening the calls received by the CIL and directing those calls that are not appropriate for the CIL (e.g., questions regarding employee benefits)

to other places in the Company where they may be more appropriately handled, and initiating investigations in response to complaints;

- maintaining records on the number, nature, and resolution of the calls received and periodically providing reports to the Board and senior management of the same, provided, however, that where requested by the employee the confidentiality and/or anonymity of the caller shall be maintained;
- periodically analyzing and testing the effectiveness of the CIL and making such modifications to the CIL as may be appropriate; and
- based on an analysis of the complaints received through the CIL or through other reporting mechanisms, making appropriate changes to the Compliance Program and directing such other remedies as may be appropriate.

Investigations. Initiating and conducting internal corporate investigations as follows:

- As the primary investigator where the OEC's internal resources and expertise are sufficient, senior management (EVP and above) are not principally implicated, or the OEC does not have an apparent or actual conflict of interest;
- As the manager of outside independent investigators and experts where it is not appropriate for the OEC to conduct the investigation.
- The Chief Compliance Officer shall also be responsible for determining and causing remedial measures to be implemented, based on the findings of an investigation and for revising or modifying the Compliance Program, if appropriate, to prevent and deter future similar misconduct.
- Training and Communications Program. Implementing and conducting an effective compliance training and communications program, including:
- providing compliance related training for the Board, executive and senior level management, and all other employees which shall be appropriate for their respective roles and responsibilities;
- providing training for the Company's agents if the Chief Compliance Officer determines it is appropriate to do so; and
- disseminating other communications as may be appropriate to convey and reinforce applicable laws and regulations, ethical standards, the Code, and other Company policies and procedures.

Compliance Related Performance Standards.

- Coordinating with Human Resources to implement compliance related performance standards for all of the Company's employees so that the employee's failure or success in meeting such standards will be considered in compensation and related matters;
- Recommending appropriate disciplinary measures for a non-performing employee, as appropriate.

Screening Employees. Coordinating with Human Resources, Internal Security and the Chief Legal Officer to develop criteria for screening potential and current employees for misconduct inconsistent with an effective Compliance Program.

Maintenance, Modification and Assessment of the Compliance Program. Undertaking such actions as are necessary to assure the continued effectiveness of the Compliance Program, including:

- modifying the Compliance Program to reflect new laws and regulations applicable to the Company, new operations and activities undertaken by the Company, and such other changes as may require modification;
- modifying the Compliance Program after misconduct has been identified to enhance prevention and detection activities so that similar misconduct will not occur in the future;
- undertaking monitoring activities designed to prevent and detect misconduct including violations of the Compliance Program;
- coordinating with Internal Audit so that the Compliance Program itself is regularly audited and that when the operations and activities of the Company's business units and support functions are audited such audit regularly reviews whether such operations and activities are consistent with the Compliance Program; and
- not less than every three years engaging an independent third party to evaluate the Compliance Program and, based on that evaluation, undertaking appropriate modifications to the Compliance Program.

Compliance Committee. Serving as the chair of the Compliance Committee and regularly reporting to senior management and the Board on its activities.

C. Tool #3: Sample Charter for Corporate Compliance Committee

Purpose. The purpose of the Corporate Compliance Committee is to provide counsel and advice to the Chief Compliance Officer by high-level personnel in the Company in his/her implementation and administration of the Office of Ethics and Compliance and the Company's Compliance Program (Program) to ensure that the Program meets applicable legal and regulatory requirements and appropriate industry standards.

Membership. The Committee shall be comprised of the following:

- the Chief Compliance Officer who shall chair the Committee;
- the Chief Legal Officer;
- the Chief Financial Officer;
- the Senior Vice President for Internal Audit;

- the Senior Vice President for Human Resources; and
- two other Senior Vice Presidents as may be designated by the CEO and who shall serve rotating terms of two years.

Meetings. The Committee shall meet no less than quarterly and at such other times as may be determined by the Chief Compliance Officer or if requested by two other members of the Committee. The Chief Compliance Officer shall appoint a member of his/her staff who shall serve as the secretary for the Committee and maintain minutes for each meeting.

Quorum. Four members of the Committee shall constitute a quorum for purposes of determining whether a meeting can be held. Committee members may vote by proxy for another Committee member at a meeting, but the assignment of a proxy vote cannot be considered for purposes of determining whether a quorum exists. A proxy may not be assigned to anyone who is not otherwise a member of the Committee.

D. Tool #4: Sample Compliance Policy and Procedures

Policy and Procedures For Tracking Attendance at Customized Compliance Training Sessions

Statement of Purpose: All business units are required to track and document employee attendance at mandated customized compliance training sessions and report quarterly on the status of attendance to the Office of Ethics and Compliance (OEC). These procedures set forth the process for meeting this requirement. The OEC will, after appropriate consultation with the business unit, advise the business unit of what compliance training is mandated for the business unit. Certain compliance training may be mandated for all Company employees. The OEC (rather than the business unit) will be responsible for tracking and documenting web based compliance training that is required for all employees in the Company.

Forms: Attached for the use of the business unit are: (1) a blank quarterly reporting form (Exhibit A) and Attendance List (Exhibit B); and (2) a sample quarterly reporting form with a sample attachment that has been filled out as a guide (Exhibit C). Exhibit A needs to be filled out by the business unit and submitted to the OEC each quarter. However, business units are required to submit underlying training documentation (Form B) with their quarterly report only when they have achieved 100% accountability for attendance (this can include acceptable absences for persons on leave). Training documentation should include copies of training materials that were provided to employees.

Timeliness. All employees are required to take mandated compliance training in a timely fashion. To facilitate this process at least one live training session will be provided for each course and thereafter that training session will be made available

in a recorded form for employees who were unable to take the live training session. Training must be taken no later than thirty (30) business days after the date the recorded session is made available. The exception to this rule is for employees who are out of the office on approved extended leave (e.g., maternity, short term disability, leave under the Family and Medical Leave Act, etc.) who must take the recorded course no later than thirty (30) business days after their return to the office. In consideration of the fact that they may have multiple courses to take, new employees have ninety (90) business days to take a required course after they start work with the Company. Managers are responsible for assuring that their employees take their courses in a timely fashion.

Required Audience. Customized training courses may be mandated for an entire business unit or only certain individuals within the business unit. It is the responsibility of the business unit to identify those individuals who are required to take a mandated course.

Repository: All training documentation received by the OEC will be filed in the official OEC files. Business units should also keep a copy of the documentation.

EXHIBITS

- A. Quarterly Training Report
- B. Attendance Lists
- C. Sample Quarterly Training Report with Attendance List

Exhibit A

Quarterly Compliance Training Report

Business Unit: _____

Report for Quarter: ____

Compliance Training	Course	Business Unit Employees Required to take Training	Required Date of Completion	Percentage of Training Completed	Comment

Exhibit B

Attendance List for Live Session

Business Unit: _____

Compliance Training Course: _____

Date of Live Session: _____

Attachments (if any): _____

Required Attendees	Signature of Attending Employee	Employee Number
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

Attendance List for Recorded Session

Business Unit: _____

Compliance Training Course: _____

Required Attendees	Signature of Attending Employee	Employee Number	Date Course Taken
1.			
2.			
3.			
4.			
5.			
6.			
7.			

Exhibit C

Sample Quarterly Compliance Training Report
 Business Unit: Human Resources
 Report for Quarter: 2

Compliance Training	Course	Business Unit Employees Required to take Training	Required Date of Completion	Percentage of Training Completed	Comment
1. Insider Trading	All HR Officers	Q 1	100%	See attached attendance list	
2. Fair Employment and Recruiting	All HR Recruiters	Q3	75%	Attendance lists to be submitted end of Q3.	
3. Form I-9 and Employment Eligibility Verification	All HR Employees responsible for processing New Hires	Q4	0%	Course to be offered in Q4	

Attendance List for Live Session
 Business Unit: Human Resources
 Compliance Training Course: "Insider Trading: Don't Even Think About It!"

Date of Live Session: January 20, 2006

Attachments (if any): PowerPoint Slides from course

Required Attendees	Signature of Attending Employee	Employee Number
1. Jane Doe	Jane Doe	5555
2. Tom Jones	Tom Jones	3241
3. John Smith	John Smith	5346
4. Trevor Higgins	Trevor Higgins	9075
5. Susan Kent		

Attendance List for Recorded Session
 Business Unit: Human Resources
 Compliance Training Course: "Insider Trading: Don't Even Think About It!"

Required Attendees	Signature of Attending Employee	Employee Number	Date Course Taken
1. Susan Kent	Susan Kent	6789	2/15/06
2.			
3.			
4.			
5.			
6.			
7.			

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

E. Tool #5: Sample Annual Certification Form

I, _____, on
 [Print Name]

_____ do hereby certify that:
 [Date]

1. I have read and understand all provisions of the [Company's] Code of Conduct and agree to comply with its provisions as a condition of my employment at [the Company].
2. I agree to report any actions or failures to act which I in good faith believe to be a possible violation of the Code as soon as I become aware of them in the future. I also represent that I have reported such possible violations in the past, and am not aware of any possible violations of the Code that I have not reported as of the time I am signing this Certification. In this regard I understand that the Code requires that [Company] employees must comply with the provisions of applicable laws, regulations, and the Code.
3. I understand that the Code and related [Company] policies require me to submit annual disclosures (including repeat disclosures) of any possible conflict of interests that I might have with [the Company] and represent that I have already made or will fully make any such disclosures for this year to the Office of Ethics and Compliance (OEC) within ten (10) business days of the date of this Certification.
4. I am aware that the Company maintains the Corporate Integrity Line that I may use to report possible Code violations, including anonymously, at (XXX) XXX-XXXX and that further information about the Corporate Integrity Line is available on [the Company's] intranet website.
5. I also understand and agree that if I submit this Certification electronically it is as legally binding as if I were signing and submitting a paper version of this Certification. I also understand that it is a violation of the Code for me to ask anyone else to submit this Certification for me.

In the event that I have any questions about the Code, this Certification, or my annual disclosures I may contact the OEC at (XXX) XXX-XXXX or via e-mail to OEC@anycorpany.com.

 Employee's Signature

 Employee Number

F. Tool #6: Sample Periodic Report to the Board

MEMORANDUM

To: [Company] Board of Directors

From: [Name]
Chief Compliance Officer

Date: January 20, 2006

Re: Annual Report to the Board for 2005

I. Introduction and Background

As we discussed previously, the Federal Sentencing Guidelines set forth the components of an effective ethics and compliance program (Compliance Program). Among those components is that the Board be knowledgeable about the content and operation of the Compliance Program and reasonably oversee its implementation and effectiveness. This Report addresses this requirement by outlining the operations and activities of the Compliance Program for 2005 and providing additional information about our proposed activities for 2006.

II. Meeting the Requirements of the Guidelines

A. Tone at the Top

Senior Management has worked to develop and maintain an organizational culture that encourages ethical conduct and commitment to compliance with the law by establishing an appropriate "tone at the top." Included among [the Company's] activities for 2005 in this regard were:

- [Example: The company town hall meeting co-chaired by the CEO and the Chairman of the Audit Committee where they answered employee questions and talked about the standards of conduct that they expect employees to meet.]

B. Activities of Senior Management and the Chief Compliance Officer

Senior officials in the Company have been very active in overseeing the effective operation of the Compliance Program in 2005, including:

- [Example: The Corporate Compliance Committee has met six times in the past year to provide counsel and advice relating to the Compliance Program, including addressing such important matters as appropriate employee discipline,

subjects for required compliance training, and establishing compliance related performance standards. Minutes from Committee meetings are attached as Exhibit A.]

- [Example: Every Senior Vice President has been responsible for implementing a compliance plan for his/her business unit that addresses such matters as compliance training, internal policies and procedures, and implementing other compliance requirements for that business unit. A sample of a plan is attached as Exhibit B.]

In addition to my general responsibility for the day-to-day operations of the Compliance Program, in 2005 I have:

- [Example: At the request of the Chair of the Audit Committee, undertaken a review of five years of Company internal investigations for the purpose of identifying any possible systemic problems.]

C. Resources

[Example: The approved budget for the Office of Ethics and Compliance (OEC) for 2005 was \$_____ and its approved staffing was _____ fulltime employees. The approved budget for 2006 is \$_____ and its approved staffing is _____ full-time employees. The OEC budget request for 2006 was \$_____ and its staffing request was for _____ additional employee[s]. The OEC's budget request was based on the need for additional resources to: (1) provide new compliance training; (2) monitor internal compliance with our Document Retention and Confidentiality Policies; and (3) meet the new requirements of the Homeland Security Act applicable to [the Company] that go into effect in June of 2006.

OEC has a request into the Controller's office to reconsider our budget request. Action on that request is expected in the next month. If the approval is not granted, new compliance training will be restricted and one of the monitoring projects will be dropped.

For the Board's information attached as Exhibit C is a survey printed in XYZ Magazine that reflects the budgets for compliance programs for peer companies in our industry.]

D. Compliance Standards and Procedures

To meet the requirement that our Company have appropriate standards and procedures in place to prevent and detect misconduct, in 2005 the OEC issued and provided training for affected employees on the following new policies:

- [Example: the Foreign Corrupt Practices Act Policy, given our new operations

and activities outside of the United States. A copy of the Policy is attached as Exhibit D.]

The OEC also significantly revised and provided supplemental training for affected employees on existing policies, including:

- [Example: the Gifts and Entertainment Policy, given the changes in the federal law relating to Members of Congress. A copy of the Policy showing changes is attached as Exhibit E.]

E. Compliance Training Programs

In 2005, in addition to providing existing courses to new employees, the OEC provided the following new significant compliance related training courses to [Company] employees who required them:

- [Example: "Limitations on Corporate Political Activities" (45 attendees from the Office of Communications and the Office of Government Affairs).]
- [Example: "Sexual Harassment: Don't Try it Here" (required on a company-wide basis for all 6,000 employees).]

F. Compliance Program Evaluation

In 2005 the Compliance Program itself was evaluated in several respects:

- [Example: An employee survey seeking input on the Compliance Program was distributed to all employees. A copy of the results of the survey is attached as Exhibit E.]
- [Example: a sample monitoring of four business units was conducted by the OEC to determine their conformity with certain requirements of the Compliance Program. A summary of the OEC's findings is attached as Exhibit G.]

G. Matters Relating to Possible Employee Misconduct

[Example: In 2005 employees indicated their willingness to use the Corporate Integrity Line to raise issues of possible misconduct: 10 anonymous complaints were received and 15 complaints were made where the complainant was identified. Most reports are made directly to OEC staff. In 2005 the OEC investigated 85 matters relating to possible employee misconduct and oversaw one independent third party investigation of such allegations. A chart setting forth the nature of the matters reviewed and the resolution of them is attached as Exhibit H.]

The OEC provides the Chair of the Audit Committee with monthly updates of matters being reviewed by the OEC and reports immediately to the Chair if the allegations made: (1) are against a [Company] officer; (2) involve significant

accounting or financial improprieties; (3) if proven true would have significant impact on the Company; or (4) are of such a nature that the Chief Compliance Officer believes the Chair should be informed.]

H. Other Activities

- [Example: Compliance Standards: In mid 2005 the OEC began work with Human Resources to develop specific compliance related performance standards for all [Company] employees. These standards were published to employees in December of 2005. They will be considered and applied for employee performance appraisals for 2006. The OEC and HR also worked with the Board's Compensation Committee to incorporate the standards into evaluations of executive management and they will be considered and applied for executive management performance appraisals for 2006.]

I. Initiatives for 2006

In 2006 the OEC will direct and/or participate in the following new initiatives:

- [Example: Responding to the new regulation of the United States Department of the Treasury, effective January 2007, that will require [the Company] to create an anti-money laundering program for certain of the Company's financial operations.]

I look forward to meeting with the Audit Committee next week to further discuss this report and the operations and activities of the Compliance Program and answer any additional questions the Committee might have. In addition, I am happy to provide additional information to members of the Board who are not on the Audit Committee and may be contacted at (XXX) XXX-XXX or at *chiefcomplianceofficer@anycompany.com*.

G. Tool #7: Sample PowerPoint Presentation for Board (See Appendix A)

H. Tool #8: Top Ten Things Your Board Needs to Know About Effective Compliance and Ethics Programs

"Any rational person attempting in good faith to meet an organizational governance responsibility would be bound to take into account [the US Sentencing Guidelines]...." stated the Delaware Court of Chancery in the landmark Caremark case. And your company's board of directors (Board) needs to understand this given the Guidelines charge them with oversight and participation in corporate compliance programs. As in-house counsel you should understand these

requirements as well and make sure your Board is aware of them.

Make no mistake however---this isn't just about criminal misconduct and sentencing. Rather, whether an organization has an effective compliance and ethics program (Program) that meets the Guidelines is an important consideration utilized by the Department of Justice, the SEC, and other regulators to determine whether or what type of action should be taken for corporate misconduct.

Here is what your Board needs to know about what the Guidelines require.

1. The Board Needs to Know About and Oversee the Program

The Board is charged with being knowledgeable about the content and operation of the Program, and reasonably overseeing its implementation and effectiveness. Basic information should be made available to the Board about its responsibility for the Program. Regular reports should be supplied about the Program's operations, resources and effectiveness.

2. There Must Be An Appropriate "Tone at the Top"

The company must have an organizational culture that encourages ethical conduct and commitment to compliance with the law by establishing an appropriate "tone at the top." A paper program just won't do it. Companies must not only "talk the talk" but "walk the walk." Establishing this culture begins with the Board. It also requires making sure that corporate leaders behave appropriately or are held accountable by the Board.

3. Individuals Responsible for the Program Must Have Effective Authority and Access

"High level" corporate personnel (i.e., those who have "substantial control over the [company] or who have a substantial role in making policy") should be assigned overall responsibility for the Program. Otherwise it is likely to undercut the Program and the establishment of an appropriate "tone at the top." Lower level individuals in the company may be delegated day-to-day operational responsibility for the Program, but should have access to the Board or the subgroup responsible for oversight of the Program (e.g., Audit Committee).

4. The Program Must Have Adequate Resources

What is adequate? Resources should be sufficient to reasonably prevent and detect misconduct and promote an organizational culture that encourages a commitment to compliance with the law. Factors which might be considered in determining resource adequacy could include: (a) size of the company (by number of employees or assets); (b) whether the company is highly regulated; (c) complexity of the company's transactions; (d) geographic range (i.e., local v. international); (e) practices in the industry; (f) nature of the company's activities; or (g) potential areas of significant risk/liability and the need to address them.

5. The Company Must Adopt Compliance Standards and Procedures

An employee code of conduct is essential. Required standards common to all companies address such matters as conflicts of interests, entertainment and gifts, prohibition against insider trading, and non-compliance reporting mechanisms. Other compliance standards are tailored to the nature of the company's business activities such as antitrust, the foreign corrupt practices act, or reports related to government contracting. Sarbanes-oxley requirements such as up-the-ladder reporting for attorneys under section 307 should also be addressed. Finally, standards peculiar to the job duties of particular employees (e.g., Those handling hazardous wastes) should be included.

6. Companies Need to Have Effective Compliance Training Programs and the Board Should Participate

The Guidelines require that companies have effective training programs that communicate their compliance standards and procedures to the Board, all levels of employees, and the company's agents if appropriate. The purpose of the training is not just to educate employees about the compliance requirements, but also to motivate them to comply with them. Training should be tailored; there is no template. Small organizations could provide training at orientation, staff meetings, or even one on one. Larger companies should have a formally documented program with sufficient dedicated resources and tools to measure its effectiveness.

7. The Program Should Be Regularly Evaluated

Programs should not stagnate. They should be evaluated regularly and appropriately modified. This analysis may be internal (review by internal audit, self assessment, employee surveys, etc.), but periodic measurement by an outside third party is highly recommended. Evaluations of the program should take into consideration new laws and regulations, new business activities, and updated corporate risk assessments.

8. The Approach to Compliance Should Be Both Carrot and Stick.

The Program should be promoted consistently within the company with incentives provided for compliance with the Program and disincentives provided for engaging in misconduct. For example, whether managers participate in the Program (e.g. take training), properly administer compliance activities in their department, and set an example that contributes to the appropriate "tone at the top," should be considered in their performance evaluation and resulting compensation. Similarly, misconduct should be met with appropriate sanctions regardless of corporate position.

9. Company "Hotlines" with Anonymity Features Are Required

The Guidelines also require the implementation of a mechanism that allows employees to anonymously report potential misconduct without fear of retaliation. For those companies that operate outside the United States, special care should be taken in addressing this requirement. The availability of the hotline needs to be communicated to employees. Evaluation of the hotline should be part of the

regular assessment of the Program.

10. Risk Assessment Drives the Program

The elements of a company's Program will be driven by an analysis of the laws and regulations applicable to the operations of the company and the risks potential non-compliance creates. Periodically the company must reassess this risk and modify the Program accordingly.

Additional Resources

Text of the Federal Sentencing Guidelines for Organizations
http://www.ussc.gov/2005guid/8b2_1.htm

Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines
 (October 7, 2003) <http://www.ussc.gov/corp/advgrprpt/advgrprpt.htm>

I. Tool #9: Sample Risk Assessment Tool (See Appendix B)

J. Tool #10: Sample Employee Compliance Survey

The purpose of this survey is to secure your input about the Company's corporate culture and our Compliance Program. Your participation is totally anonymous. Please fill out the survey and deposit it in the designated receptacle in the company cafeteria or place it in interoffice mail directed to the attention of the Office of Ethics and Compliance, Room 452, Corporate Headquarters, Any town, USA.

Corporate ethics and compliance is everyone's business. Your input is essential for the Office of Ethics and Compliance (OEC) to improve our Compliance Program.

Thank you for your time.
 The Office of Ethics and Compliance

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

A. CODE OF BUSINESS CONDUCT (fill in one)

1. I have been given a copy of the Company's Code of Business Conduct (Code).

True	False	Don't Know
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2. I have taken training about the Code.

True	False	Don't Know
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. I refer to the Code for guidance...

Once a Week	Every 2 weeks	Once a month	Practically Never	Never
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4. I can find a printable copy of the Code on the Company's Intranet Home Page.

True	False	Don't Know
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. The last time my manager mentioned the Code was...

Less than a week ago	Within the past 2 weeks	Within the past month	Within the last 6 months	Never mentions it
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

B. REPORTING POSSIBLE WRONGDOING

1. The Company maintains a hotline ("Integrity Line") where employees can report good faith allegations of possible violations of law, regulations, the Code, or unethical conduct (Wrongdoing) anonymously.

True	False	Don't Know
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

2. The number for the Integrity Line appears on the Company's Intranet Home Page.

True	False	Don't Know
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. I believe I can make a truly anonymous report to the Integrity Line.

True	False	Don't Know
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4. Under Company policy I may report good faith allegations of possible Wrongdoing to any of the following (fill in all that apply).

- my supervisor
- the Office of Ethics and Compliance
- the Chief Compliance Officer
- any officer of the Company
- the HR representative assigned to my division.
- the Integrity Line
- the Audit Committee of the Board of Directors

5. I would be the most comfortable reporting good faith allegations of possible Wrongdoing to the following (Rank choices from 1-5; 1 being the place/person to whom you would be least likely to report and 5 being the place/person to whom you would be most likely to report. Rankings may be used more than once).

- ___ my supervisor
- ___ the Office of Ethics and Compliance
- ___ the Chief Compliance Officer
- ___ any officer of the Company
- ___ the HR representative assigned to my division.
- ___ the Integrity Line
- ___ the Audit Committee of the Board of Directors

6. I believe that if I made a good faith allegation of possible Wrongdoing the following would take place:

	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree	Don't Know
There would be a thorough investigation of my allegation regardless of the rank, position, productivity, etc. of the person being investigated.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If the allegation turned out to be true, the employee would be appropriately disciplined regardless of the rank, position, productivity, etc. of the employee.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I might be retaliated against (disciplined, demoted, transferred, etc.) for making the report.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I might be indirectly retaliated against (e.g., treated as not being a team player, subjected to unjustified criticism, etc.) for making the report.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7. I made a good faith report(s) of possible Wrongdoing in the past to the following (fill in all that apply). [If this question does not apply to you, please proceed to Section C]

- my supervisor
- the Office of Ethics and Compliance
- the Chief Compliance Officer
- an officer of the Company
- the HR representative assigned to my division.
- the Integrity Line
- the Audit Committee of the Board
- Other (please specify) _____

8. Fill in all of the responses/results that you believe apply to your previous report(s).

- I believe that I was directly retaliated against (e.g., disciplined, demoted, transferred, etc.) for making the report.
- I believe that I was indirectly retaliated against (e.g., not treated as a team player, subjected to unjustified criticism, etc.) for making the report.
- Nothing was done to my knowledge.
- I was satisfied with the result.
- Other (please specify) _____

C. CORPORATE CULTURE

1. Senior Management: At our company, the senior management (SVPs and above) demonstrates by both word and deed that they are committed to the following (fill in one):

	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree	Don't Know
Ethical business practices and compliance with all applicable laws, regulations, and provisions of our Code.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Putting compliance and ethical conduct before production goals or other corporate objectives.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Creating an open working environment where employees may raise issues of concern and have them fully addressed without fear of retaliation.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Taking the Compliance Program seriously by participating in training, talking about the Code, avoiding conflict of interests, etc.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Holding their subordinates accountable for ethical business practices and compliance with all applicable laws, regulations, and provisions of our Code.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Applying the Company's policies and Code consistently and fairly to all employees	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Raising issues of concern to their peers rather than just "going along to get along."	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2. Peers: At our company my Peers in my division demonstrate by both word and deed that they are committed to the following:

	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree	Don't Know
Ethical business practices and compliance with all applicable laws, regulations, and provisions of our Code.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Putting compliance and ethical conduct before production goals or other corporate objectives.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Holding their peers accountable for ethical business practices and compliance with all applicable laws, regulations, and provisions of our Code.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Raising issues of concern with their supervisor and having them fully addressed rather than just "going along to get along."	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. Supervisor: At our company my supervisor demonstrates by both word and deed that s/he is committed to the following:

	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree	Don't Know
Ethical business practices and compliance with all applicable laws, regulations, and provisions of our Code.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Putting compliance and ethical conduct before production goals or other corporate objectives.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Creating an open working environment where subordinates can raise issues of concern and have them fully addressed without fear of retaliation.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Taking the Compliance Program seriously by participating in training, talking about the Code, avoiding any conflict of interests, etc.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Holding his/her subordinates accountable for ethical business practices and compliance with all applicable laws, regulations, and provisions of our Code.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Applying the Company's policies and Code consistently and fairly to all employees.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Raising issues of concern with his/her supervisor or peers rather than just "going along to get along."	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

D. COMPLIANCE PROGRAM

1. OVERVIEW

	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree	Don't Know
I know where to go when I have questions about the Compliance Program, our Code, or our Company's Policies.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I know how to make a good faith report about possible Wrongdoing by a Company employee.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I know what my responsibility is for making a good faith report about possible Wrongdoing by a Company employee.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am knowledgeable about the responsibilities I have for compliance with applicable laws and regulations, the Code, and other matters relating to ethical conduct in my job position.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel that I have received adequate training regarding applicable laws and regulations, the Code, and other matters relating to ethical conduct that affect the Company's operations.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel that I have received adequate training regarding applicable laws and regulations, the Code, and other matters relating to ethical conduct that affect my job position.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I believe the Chief Compliance Officer is committed to complying with applicable laws and regulations, the Code, and other matters relating to ethical conduct that affect the Company's operations.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I believe the CEO is committed to complying with applicable laws and regulations, the Code, and other matters relating to ethical conduct that affect the Company's operations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2. INFORMATION AND TRAINING REQUIREMENTS

The following is a list of topics addressed in our Code and the related Policies that support the Code. The Code and the Policies are available online on the HomePage of the Company's intranet and are also posted in a pdf. version so that they may be printed in hard copy. Please indicate below whether you would like more information or training about these provisions of the Code or related Policies or if you feel you have had sufficient information or training on these subjects.

Topic	I would like more information or training on this subject.	I have sufficient information or training on this subject.
Code of Conduct	<input type="radio"/>	<input type="radio"/>
Fair Employment (equal employment, sexual harassment, etc.)	<input type="radio"/>	<input type="radio"/>
Ethical Responsibility Policy (duty to report Wrongdoing, reporting mechanisms, etc.)	<input type="radio"/>	<input type="radio"/>
Antifraud Policy	<input type="radio"/>	<input type="radio"/>
Antitrust and Fair Business Practices	<input type="radio"/>	<input type="radio"/>
Conflict of Interests and Disclosures	<input type="radio"/>	<input type="radio"/>
Customer Privacy	<input type="radio"/>	<input type="radio"/>
Confidentiality	<input type="radio"/>	<input type="radio"/>
Gifts and Entertainment	<input type="radio"/>	<input type="radio"/>
Government Inquiries and Investigations	<input type="radio"/>	<input type="radio"/>
Corporate Charitable Contributions	<input type="radio"/>	<input type="radio"/>
Political Activities	<input type="radio"/>	<input type="radio"/>
Insider Trading	<input type="radio"/>	<input type="radio"/>
Financial Standards and Accounting Practices	<input type="radio"/>	<input type="radio"/>
Workplace Standards of Conduct	<input type="radio"/>	<input type="radio"/>
Substance Abuse	<input type="radio"/>	<input type="radio"/>
Intellectual Property (Copyright, Trademarks, & Patents)	<input type="radio"/>	<input type="radio"/>
Technology Use	<input type="radio"/>	<input type="radio"/>
Leave Policies	<input type="radio"/>	<input type="radio"/>
Travel Policies	<input type="radio"/>	<input type="radio"/>
Corporate Communications Policies (speaking with the media, endorsements, use of Company name, etc.)	<input type="radio"/>	<input type="radio"/>
Other (please fill in) _____ _____	<input type="radio"/>	<input type="radio"/>

E. EMPLOYEE PROFILE

1. The following best describes my job level (check all that apply):
- Non-manager
 - Manager (1-5 employees)
 - Manager (5-10 employees)
 - Manager (10 + employees)
 - Vice President
 - Senior Vice President
 - Executive Vice President and above

2. I have been with the Company:

- less than a year
- 1-3 years
- 3-5 years.
- 5-10 years
- 10-15 years
- 15 + years

3. I work in (optional)

- the Executive Offices
- Human Resources
- Legal Department
- Controller's
- Internal Audit
- Compliance
- [Supplement with Other Departments]

4. Additional Information

If there is any additional information that you would like us to know about how the Company's culture and Compliance Program may be improved, please let us know by filling out the form below or by e/mailing us at OEC@anycompany.com or calling us at (XXX) XXX-XXXX. Please do NOT use this form to report possible Wrongdoing.

Thank you for your participation in this important process.

Jane Doright
Chief Compliance Officer

K. Tool #11: Sample Employee Exit Interview Questions

Background. The exit interview can present an excellent opportunity to measure the effectiveness of the compliance program and to secure information about possible misconduct. Employees who are leaving the company may feel more comfortable about sharing information and giving them an opportunity to do so may allow the company to identify and correct problems before or instead of having those problems referred to a regulator or other authorities.

The individual who is conducting the exit interview must be properly trained to ask follow-up questions to the ones posed below so that important matters will be appropriately explored. If misconduct is alleged, the interviewer must secure sufficient details to allow the company to pursue the matter. Such interviews are frequently conducted by company employees (HR or compliance or both), but other companies outsource the function in the belief that departing employees will be more candid with a third party. The following questions are suggested and they should be supplemented with inquiries tailored to your Company's operations and activities.

- Do you feel that you received adequate training regarding the Company's Code of Conduct, ethical standards, and related policies?
- Was there any training that you did not receive that you would have liked to receive?
- What was the most effective method that the Company used to provide you with training or other information about the Code of Conduct, ethical standards, or related policies?
- What do you think the Company can do to improve its communications with employees about the Code of Conduct, ethical standards, and related policies?
- Do you feel that senior management (SVPs and above) acts ethically and complies with the law, the Code of Conduct and related policies?
 - How about your peers?
 - How about the managers in your chain of command?
- Do you think this Company has an open working environment where employees feel comfortable raising issues for resolution without fear of retaliation?
- Are you leaving the Company because of any legal or ethical concern you have about its operations or activities?
- Were you ever asked to engage in any conduct that you thought was legally or ethically questionable?
- Did you know how to anonymously report possible misconduct at the Company?
- Did you ever observe or otherwise become aware of possible misconduct at the Company and decide not to report it?
 - Why did you decide not to report it?
 - What was the misconduct that you observed or became aware of?
- Is there anything about the Company's compliance program or possible misconduct at the Company that I did not ask you about that you think I should know?

For more ACC InfoPAKs, please visit www.acca.com/vl/infopak

VII About the Author

Deborah M. House, Vice President and Deputy General Counsel for Legal Resources and Strategic Initiatives for the Association of Corporate Counsel. Ms. House was previously Vice President and Deputy General Counsel for Corporate Compliance at Fannie Mae, a Fortune 100 corporation, where she designed, staffed, and implemented the corporation's centralized legal and regulatory compliance function, including creating tailored compliance plans for all business units and support functions within the company. Prior to taking that position Ms. House served as Fannie Mae's Vice President and Deputy General Counsel for Multifamily Legal Services where she managed 14 attorneys and \$9 million in annual outside legal services for this business unit with a \$112+ billion portfolio and 2002 production of \$22+ billion. Before joining Fannie Mae, Ms. House was Chief of the debarment section of the Resolution Trust Corporation which was the third largest government contracting agency at that time. Prior to that she was in private practice in Washington and London where she provided legal services to a wide variety of corporate and financial institution clients. Ms. House is co-chair of the ABA's subcommittee on Compliance Set-up and Structure of the Business Law Section's Compliance Committee. She holds a BS from the University of Illinois and a JD from the Washington College of Law of American University.

The opinions expressed in this document are solely those of Ms. House.

Copyright © 2006 Deborah M. House and Association of Corporate Counsel

Endnotes

¹ The reputation might be somewhat misleading. In the author's experience, Wayne County juries are as likely to deliver a "no-cause" verdict as any other. However, perhaps when they do render verdicts, they are larger.

² Discrimination actions are personal injury tort actions. *Slayton v Michigan Host*, 122 Mich App 414, 416, 332 NW2d 498 (1983).

³ "Familial status" (defined with regard to one's obligation to care for children under age 18) is declared as a civil right under the statute for purposes of employment (MCL 37.2102), but "familial status" is omitted from the section describing prohibited acts of employers (MCL 37.2206). Therefore, one unreported opinion, in a footnote, has observed that discrimination on the basis of familial status is only prohibited with respect to housing. *Saldana v American Red Cross*; 1997 WL 33341640 (Mich. App.).

⁴ Ann Arbor, Birmingham, Detroit, East Lansing, Flint, Grand Rapids, Huntington Woods, Saginaw, and Ypsilanti.

⁵ 2005 ACC/Serengeti Managing Outside Counsel Survey. www.acca.com/Surveys/partner/2005/

Compliance Occupies a More Strategic Role as Business Goes Global, Integrity Research Group and Altman Weil Compliance Survey—Analysis of Results, a publication of the Integrity Research Group (2005).

Law Department's Role in Developing and Implementing Compliance and Ethics Programs. www.acca.com/protected/article/ethics/lead_compliance.pdf

While the Guidelines are applicable to all "organizations," references herein are to companies or corporations as one type of organization subject to their application.

Organizations also previously qualified for a reduction in their culpability score if they waived the attorney client privilege when it was necessary to do so "to provide timely and thorough disclosure of all pertinent information." At the urging of the ACC and others, this requirement was eliminated earlier this year. See 71 FR 28063 (May 15, 2006).

USSG §8B2.1 (a) (1&2). The

⁶ Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines (October 7, 2003) (Advisory Group Report). http://www.uscc.gov/corpl/advgrp/AG_FINAL.pdf

⁷ Advisory Group Report at 3-4.

⁸ United States Sentencing Commission, Guidelines Manual, Chapter 8 - PART B - Remedying Harm from Criminal Conduct, and Effective Compliance and Ethics Program (Nov. 2004). http://www.uscc.gov/2005guid/8b2_1.htm

⁹ In the Booker case the Supreme Court ruled that the Sixth Amendment right to a jury trial requires that the Guidelines be treated as advisory, not mandatory, based on earlier decisions which had held that state judges could not consider facts not considered by the jury or admitted by the defendant. The consensus of the legal and compliance community, however, has been that notwithstanding the Court's actions the requirement for an effective compliance and ethics program remains firmly in place.

¹⁰ See *In re Caremark Int'l Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

¹¹ 698 A.2d 970.

¹² U.S. Sentencing Commission's Sourcebook of Federal Sentencing Statistics, Table 54 (2005). For this reason judicial interpretation of the effectiveness of a Program under the Guidelines is not readily available.

¹³ Memorandum from Larry D. Thompson, U.S. Department of Justice Deputy Attorney General to Head of Department Components, Principles of Federal Prosecution of Business Organizations (January 20, 2003). http://72.14.207.104/search?q=cache:4cx1QWLCStUJ:www.usdoj.gov/dag/cftf/business_organizations.pdf+thompson-memorandum&hl=en&gl=us&ct=clnk&cd=1

¹⁴ SEC Report of Investigation, Release No. 44969 (October 23, 2001). The SEC also requires entities it regulates to have compliance programs. See e.g., <http://www.sec.gov/rules/final/ia-2204.htm>

¹⁵ USSG §8B2.1, comment, (n.2 (B)).

¹⁶ USSG §8B2.1, comment (n.2 (C) (i)).

¹⁷ USSG §8B2.1, comment, (n.2 (C) (ii)).

¹⁸ USSG §8B2.1, comment, (n.2 (C) (iii)).

¹⁹ Id. "Governing authority" means the organization's Board of Directors or, if it does not have a Board, the highest level governing body of the organization. USSG §8B2.1, comment (n. 1). For simplicity's sake the term Board is used here.

²⁰ USSG §8B2.1, comment, (n.2 (D)).

²¹ USSG §8A1.2, comment, (n.3 (f)).

²² USSG §8A1.2, comment, (n.3 (b)).

²³ "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 must be determined on a case-by-case basis." USSG §8A1.2 comment, (n.3 (c)).

²⁴ USSG §8B2.1, comment, (n.3).

²⁵ The Business Roundtable's Principles of Corporate Governance at 12 (2005) is available at <http://www.businessroundtable.org/pdf/CorporateGovPrinciples.pdf> (Business Roundtable).

²⁶ Advisory Group Report at 62.

²⁷ Advisory Group Report at 62.

²⁸ Individual(s) with day-to-day operational responsibility for the Program are expected to provide reports about the implementation and effectiveness of the compliance and ethics program to the Board (or a subgroup) at least annually. USSG §8B2.1, comment, (n. 3).

²⁹ Advisory Group Report at 63.

³⁰ As reported in Compliance Program and Risk Assessment Benchmarking Survey 2005, prepared jointly by ACC and Corpedia, Inc., the top five challenges to Program implementation are: (1) the complexity of the legal and regulatory environment; (2) the complexity of the compliance process; (3) staffing issues; (4) the perception that compliance is not a strategic function; and (5) organizational resistance to change. See <http://www.acca.com/protected/Surveys/compliance/survey.pdf> at 29 (Compliance and Risk Survey).

³¹ Other sources require or encourage Board oversight of legal and regulatory compliance. The NYSE rules require that the Audit Committee assist in the Board's oversight of the company's legal and regulatory compliance (NYSE Rules at 13). http://www.nyse.com/pdfs/section303A_final_rules.pdf

³² The Business Roundtable's Principles of Corporate Governance indicate that the Board should set the "tone at the top" that "establishes the corporation's commitment to integrity and legal compliance" and oversee "the corporation's compliance program relating to legal and ethical conduct." In this regard, the board should be knowledgeable about the corporation's compliance program and should be satisfied that the program is effective in preventing and deterring violations." Business Roundtable at 10.

³³ Sixty-nine percent of 412 reporting companies indicated that they were conducting risk assessments consistent with the Guidelines. Compliance and Risk Survey at 3.

³⁴ What is determined to be an appropriate period for conducting overall risk assessments may depend on a number of factors such as changes in: the industry, applicable laws and regulatory frameworks, and the activities and operation of the company (including new activities acquired through mergers or acquisitions). "Mini" risk assessments should be conducted whenever there are significant changes that bring new requirements into play. Such changes may require immediate modifications of the Program (e.g., new policies and training)

³⁵ USSG § 82B.1, comment, (n.6 (A)). In a risk assessment it is also very instructive to consider the prior history of peer companies and instances where the company came perilously close to engaging in impermissible activity in the past.

³⁶ USSG § 82B.1 comment, (n.6 (B&C)).

³⁷ It is outside the scope of this paper to discuss the issues arising from creating the documentation associated with this analysis, or for that matter, having a Program at all. Suffice it to say the implications these issues may have for, among other things, regulatory oversight, potential future litigation, and preserving the attorney client privilege etc. are not insignificant. These issues, identified as the Litigation Dilemma³⁷ were discussed, although not resolved, at some length in the Advisory Group Report at 105-129.

³⁸ This process is discussed in significantly more detail in ACC's InfoPAK Conducting Effective Risk Assessments, available at <http://www.acca.com/resource/v7151>.

³⁹ California's Assembly Bill 1825 (California Government Code section 12950.1) requires that employers doing business in California and employing 50 or more workers provide sexual harassment prevention training and retraining for supervisors. The District of Columbia's Human Rights Act (Title II, Chapter 14) prohibits discrimination on the basis of race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, familial status, family responsibilities, matriculation, political affiliation, disability, source of income, and place of residence or business.

⁴⁰ There is some disagreement among experts in this area as to whether the documentation of the risk assessment should reflect laws and regulations that were considered but rejected as not being applicable so as to document the analytical process. Given the number of possible Requirements it seems that the rule of reason should be applied here or the process will get bogged down. However, creating a short list of Requirements that reflect significant risk is not sufficient either.

⁴¹ USSG § 82B.1, comment. (n.1).

⁴² NYSE Rules at 16-17.

⁴³ Business Roundtable at 12.

⁴⁴ "Publication of the Office of Inspector General's Compliance Program Guide for Hospitals" 63 Federal Register 63 (3 February 1998): 8987-8998, 8989.

⁴⁵ See e.g., *Burlington Industries v. Ellerth*, 524 U.S. 742 (1998) and *Faragher v. City of Boca Raton* 524 U.S. 775 (1998). *Kolstad v. American Dental Association*, 524 U.S. 775 (1999).

⁴⁶ Advisory Report at 56.

⁴⁷ For companies with operations abroad it should be noted that the Guidelines specify that "Nothing in [the requirement for standards and procedures] is intended to require conduct inconsistent with any...local law, including any law governing employment or hiring practices." USSG §82B2.1, comment (n. 6). Arguably "local law" includes foreign law applicable to a domestic corporation's operations outside of the United States.

⁴⁸ Advisory Report at 70-71.

⁴⁹ Advisory Report at 71.

⁵⁰ Code of conduct training (63%) and training associated with fair employment (e.g., sexual harassment training) (63%) are the training most frequently provided by organizations. Compliance and Risk Survey at 17.

⁵¹ USSG §8B2.1, comment. (n. 2 (C) (iii)).

⁵² There may be some limitations on the use of hotlines outside of the United States which you will need to consider if yours is an international organization. See e.g., *Clash of the Titans: Complying with US Whistleblowing Requirements While Respecting EU Privacy Rights*. <http://www.acca.com/protected/pubs/docket/apr06/beyer.pdf>

⁵³ NYSE Rules at 16.

⁵⁴ "Publication of the Office of Inspector General's Compliance Program Guide for Hospitals" Federal Register 63 (3 February 1998): 8987-8998, 8989.

⁵⁵ <http://www.oig.hhs.gov/hotline.html>

⁵⁶ See e.g., the whistleblower program established by OSHA under the Occupational Safety and Health Act as presented at <http://www.osha.gov/dep/oa/whistleblower/index>.

⁵⁷ Advisory Group Report at 86.

⁵⁸ Andy Pasztor, "Boeing to Settle Federal Probes For \$615 Million Deal Allows Defense Giant To Avoid Criminal Charges In Contracting Scandals," *Wall Street Journal*, May 15, 2006.

⁵⁹ USSG §8A1.2, comment. (n.3(c)).

⁶⁰ USSG §8A1.2, comment. (n. 3(b)).

⁶¹ USSG § 82B.1, comment. (n.4).

⁶² While not required under the Guidelines, some screening makes sense for the purpose of limiting overall legal liability. For example, if employees have access to consumers' homes (e.g., cable television installer), providing screening for substance abuse and a criminal record is appropriate even though these persons would not qualify as "high-level" nor "substantial authority" personnel.

⁶³ Depending on the nature of the employee's work activities, categories for screening might include substance abuse, criminal and educational history, and professional licensing requirements (e.g., bar membership). Consideration also needs to be given to geographical scope (e.g., what jurisdiction's records are screened) including whether to screen multiple geographical areas such as areas of former residences and employment sites, and where the employee attended college or graduate school. Some companies also review the credit records of employees, particularly those placed in positions of financial trust. If so, care must be taken to assure that there is compliance with the provisions of the Fair Credit Reporting Act.

⁶⁴ "Similar misconduct" means prior conduct that is similar in nature to the conduct underlying the instant offense, without regard to whether or not such conduct violated the same statutory provision. For example, prior Medicare fraud would be misconduct similar to an instant offense involving another type of fraud." USSG §8A1.2, comment. (n.3(f)).

⁶⁵ Advisory Group Report at 72.

⁶⁶ Id. at 72-76.

⁶⁷ Id. at 76-77.

⁶⁸ Id. at 77.

⁶⁹ Id. at 87.

⁷⁰ This Model Rule is found at http://www.abanet.org/cpr/mrpr/rule_1_13. See also *In House Ethical Conflicts: Recognizing and Responding to Them*, ACC Docket at 30-31 (February 2004), available at <http://www.acca.com/protected/pubs/docket/feb04/conflict.pdf>.

⁷¹ This position description contemplates that the compliance function will be a "stand alone" operation and that the Chief Compliance Officer will have responsibility for compliance, ethics, and investigations and act as the overall coordinator, but not have principal responsibility for certain compliance activities (e.g., anti-money laundering) that may be located outside of the compliance function. This position description is purposefully detailed to identify for consideration those duties that might be assigned to the Chief Compliance Officer.

⁷² For these purposes it is assumed that the Chief Compliance Officer will also be responsible for the day to day operations of the compliance function. If that function is delegated, the relationship with the Board will change.



InfoPAK
Effective Ethics and Compliance Programs
for the Small Law Department
Doing More with Less
Tool #10



Roadmap For An Effective Compliance And Ethics Program

The Top Ten Things the Board Must Know

[Name of Presenter]

[Title]

[Date]



Not Just About Sentencing

- United States Sentencing Guidelines (“Guidelines”), which address criminal conduct, are the foundation for compliance and ethics programs that address all misconduct (“Program”).
- 2004 Amendments to the Guidelines set forth specific goals for Programs.
- The Department of Justice and the SEC measure Programs against Guidelines’ standards when considering actions against entities.
- Other government agencies such as HHS, EPA and State also use the Guidelines as the principle benchmark for Programs.



Key Requirements for Program

1. Board needs to be knowledgeable about and oversee the Program.
2. Must establish a “tone at the top” that demonstrates corporate commitment to ethical conduct and compliance with the law.
3. Requires an organizational structure where senior personnel have overall responsibility for the Program and individual responsible for day-to-day operations has appropriate authority and access to the Board or subcommittee of the Board.
4. Program must have adequate resources.
5. The Company must have appropriate corporate standards and procedures designed to achieve compliance.



Key Requirements for Program (continued)

6. Effective compliance training should be provided and Board needs to participate.
7. A confidential and anonymous disclosure mechanism ("hotline") is required.
8. Must provide incentives to perform consistent with Program and apply consistent disciplinary measures for misconduct ("carrot and stick").
9. Risk Assessment drives the Program.
10. The Program needs to be kept effective and regularly evaluated and revised as appropriate.



Board Must Know About and Oversee Program

Guidelines Require

“The [Board] shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.” (§8B2.1(b) (2) (A)).

Implementation

- This training.
- Regular written reports
- [to be supplied]



Tone at the Top

Guidelines Require

- Establishment and maintenance of an organizational culture that “encourages ethical conduct and a commitment to compliance with the law.” (§8B2.1 (a) (2)).

Implementation

- [to be supplied]



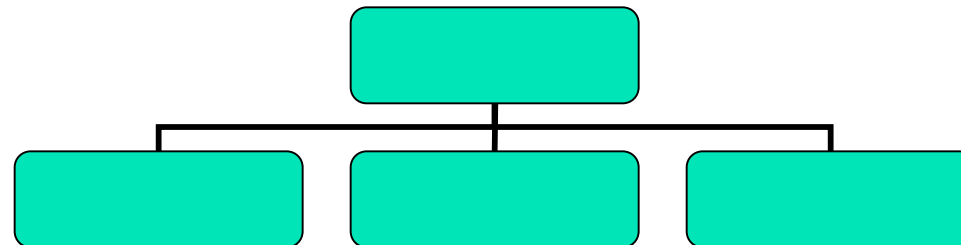
Organizational Structure

Guidelines Require

- High level personnel who have substantial control over the organization or who have a substantial role in making policy are responsible for the compliance program. (§ 8B2.1(b) (2) (B)).
- Day-to-day operational responsibility for the program delegated to individuals who report to high level personnel. Individuals responsible for day-to-day operations must have . . . appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority (§8B2.1(b) (2) (C)).

Implementation of Organizational Structure

[to be revised appropriately]





Program Must Have Adequate Resources

Guidelines Require

Individuals responsible for day-to-day operations must have adequate resources (§8B2.1(b) (2) (C)).

Implementation

- Budget for Program for last year: \$_____
- Staffing for Program for last year: _____
- Budget for Program this year: _____
- Staffing for Program this year: _____



Compliance Standards and Procedures

Guidelines Require

“The organization shall establish standards and procedures [standards of conduct and internal controls] designed to prevent and detect [misconduct].” (§8B2.1 (b) (1)).

Implementation

- [to be supplied—discussing code of conduct, policies etc.]



Compliance Training

Guidelines Requirements

“The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to [the Board, high level personnel, substantial authority personnel, the company’s employees, and as appropriate, the company’s agents] by conducting effective training programs and otherwise disseminating information appropriate to such individual’s respective roles and responsibilities.”
(§8B2.1(b) (4) (A)).



Compliance Training (continued)

Implementation

- [to be supplied—identifying training courses, when given, who took them (by category), what is to be provided in the future etc.]



Hotline

Guidelines Require

“The organization shall take reasonable steps---(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization’s employees and agents may report or seek guidance regarding potential or actual [misconduct] without fear of retaliation.”
(8B2.1(b)(5)(C)).

Sarbanes-Oxley imposes similar requirements.

Implementation

- [to be supplied]



Carrots & Sticks

Guidelines Require

“The organization’s compliance and ethics program shall be 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 [misconduct] and for failing to take reasonable steps to prevent or detect [misconduct].”
(§8B2.1(b)(6)).

Particularly important with regard to senior management who must set the “tone at the top” and whose performance and compensation may be considered by the Board.



Carrots & Sticks (continued)

Implementation

- [to be supplied]



Risk Assessment

Guidelines Require

“The organization shall periodically assess the risk of [misconduct] and shall take appropriate steps to design, implement, or modify [the Program] to reduce the risk of [misconduct] identified through this process.” (§8B2.1(c)).

Implementation

[to be supplied]



Program Needs to be Kept Effective and Regularly Evaluated

Guidelines Require

- “The organization shall take reasonable steps—(A) to ensure that the organization’s compliance and ethics program is followed, including monitoring and auditing to detect [misconduct]; and B) to evaluate periodically the effectiveness of the organization’s compliance and ethics program.” (§8B2.1 (b) (5) (A&B)).

- “After [misconduct] has been detected, the organization shall take reasonable steps to respond appropriately to the [misconduct] and to prevent further similar [misconduct] including making any necessary modifications to the organization’s compliance and ethics program.” (§8B2.1 (b) (7)).



Program Needs to be Kept Effective and Regularly Evaluated (continued)

Implementation

[to be supplied]



InfoPAK
 Effective Ethics and Compliance Programs
 for the Small Law Department
 Doing More with Less
 Tool #9

APPENDIX B

Sample Risk Assessment Tool¹

Instructions for Using the Risk Assessment Tool

“**Legal and Regulatory Risk**” means those laws and regulations that are applicable to the operations and activities of the Company and with which it must comply.

“**Excluded**” means where the laws and regulations cited may be applicable to the Company, but generally are not considered as presenting a reasonable risk for the reasons stated. Therefore they are excluded from full analysis, but the Tool documents that they were considered.

“**Business Area Affected**” means those business areas within the Company that could reasonably be expected to be at risk for violation of the law or regulation specified because of their operations and activities.

“**Likelihood of Risk Occurrence**” means the following categories, ranked from 1-5, that reflect the likelihood that the Legal and Regulatory Risk analyzed (i.e., violation of the law or regulation) will actually occur. These numerical rankings are inserted in the Risk Assessment Tool.

<u>Scale</u>	<u>Description</u>
1	Extremely unlikely, but could occur. Less than a 1% chance it will occur.
2	Unlikely, but could occur. A 1- 5% chance it will occur.
3	Possibly could occur. A 5-10% chance it will occur.
4	Likely to occur. A 10-25% chance it will occur.
5	Extremely likely to occur. A 25% or greater chance it will occur.

¹ The purpose of this tool is to suggest a process for performing a legal and compliance risk analysis consistent with the requirements of the U.S. Federal Sentencing Guidelines. The analytics presented here may not meet the risk assessment analytics required under other applicable statutes or regulations.

“Severity of Risk Occurrence” means the following categories, ranked from 1-5, that reflect the severity of the impact that the occurrence of the Legal and Regulatory Risk (i.e., violation of the law or regulation) will have on the Company. The nature of the impact is ranked in three categories: (1) Financial; (2) Reputational; and (3) Operational. These numerical rankings are inserted in the Risk Assessment Tool along with a letter indicating whether the severity is Financial (F), Reputational (R), and/or Operational (O).

Scale **Financial Risk (including damages, settlements, fines, cost of addressing violation)**

- 1 Less than 1% of Revenue.
- 2 1- 5% of Revenue.
- 3 5-10 % of Revenue.
- 4 10-15% of Revenue.
- 5 Greater than 15% of Revenue.

Scale **Reputational Risk (the risk that negative publicity about a Company may lead to a loss of revenue, regulatory impact, or litigation).**

- 1 Practically none.
- 2 Very minor with local coverage; easily remediable.
- 3 Moderate, with state and regional publicity.
- 4 Serious, national publicity with legal and regulatory impact.
- 5 Extremely severe, sustained and prominent national publicity with significant legal and regulatory impact

Scale **Operational Risk (the risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events).**

- 1 Practically none.
- 2 Identifiable, but minor and can be managed without impact on operations.
- 3 Moderate impact; can be managed with special attention.
- 4 Serious, affects ability of Company (or business area) to conduct business and remain competitive.
- 5 Catastrophic with continued viability of Company (or business area) seriously questionable

“Risk Score” is the product reached by multiplying the ranking given to the Likelihood of the Occurrence times the ranking given to the Severity of the Occurrence. If more than one category from the Severity of the Occurrence is utilized (e.g., Financial and Operational) the calculation should be done for each category and designated as such. (e.g., Likelihood of 3 x Severity of 3(O) = 9(O). Likelihood of 3 x Severity of 4(R) = 12(R).

“Risk Mitigants” are those controls or other actions designed to prevent and detect the Occurrence.

“Effectiveness of Mitigants” means the following categories, ranked from 1-4 that reflects the effectivity of the Risk Mitigants presented. The combined effect of all Risks Mitigants presented in any category should be considered in assigning a rank.

<u>Scale</u>	<u>Risk Mitigants</u>
1	Not Effective
2	Moderately Effective.
3	Substantially Effective.
4	Very Effective

“Prioritization to Address” means the following categories, ranked from 1-4, that should be assigned to creating or enhancing Risk Mitigants.

<u>Scale</u>	<u>Prioritization</u>
1	High Priority
2	Medium Priority
3	Low Priority
4	No action required.

#

Evaluation of Legal and Regulatory Risks²

Legal & Regulatory Risk	Excluded	Business Area(s) Affected	Likelihood of Risk Occurrence	Severity of Risk Occurrence	Risk Score	Risk Mitigants	Combined Effectiveness of Mitigants	Prioritization to Address
Antitrust and Fair Competition Laws								
Antitrust and Fair Competition Laws (Sherman Act, Clayton Act, Robinson- Patman Act , FTC Act, European Union Trade Laws and Regulations,		<ul style="list-style-type: none"> Sales (pricing and general practices) HR (use of employment related statistics such as industry salary information, etc.) Marketing (advertising claims) 	2	3 (F) 2(R) 1(O)	6(F) 4(R) 2(O)	-Antitrust Policy -Antitrust training for Sales -Division of duties and authority between employees setting price and employees selling product. -Legal Department pre review of HR acquired data. -Legal Department review of all advertisements.	3	3
Consumer Protection Laws								
Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN SPAM)	Co. does not use commerc. electronic messages							
Federal Telephone Consumer Protection Act (NO FAX ACT)	Company does not use faxes for advrtsng.							

² No attempt has been made to enumerate the multitude of legal and regulatory risks given that they will differ significantly for each company. Rather the intent here is just to suggest a few of the many considerations that would go into such an analysis. It may be advisable to break down some laws into subcategories to more thoroughly analyze them. A few categories are filled out completely to serve as a guide.

Legal & Regulatory Risk	Excluded	Business Area(s) Affected	Likelihood of Risk Occurrence	Severity of Risk Occurrence	Risk Score	Risk Mitigants	Combined Effectiveness of Mitigants	Prioritization to Address
Federal Fair Credit Reporting Act and related state laws		Credit Finance	4	4 (R) 2(F) 2(O)	16(R) 8(F) 8(O)	-FCRA Policy -FCRA training for all credit personnel -Legal review of all new credit related policies and procedures. - Established monitoring of requests for credit reports by Compliance. -Disposal policy for credit data. -Physical and system restrictions on access to credit data.	2	2
Federal Trade Commission Act (Section 5) and related state laws (fair advertising and marketing practices)		Marketing	2	2(R) 2(F) 2(O)	4 (R) 4(F) 4(O)	-Legal reviews all advertising prior to dissemination. -Legal is member of marketing committee that reviews activities.	2	3
California Data Security Laws (notification of computer security breach)		Technology	2	5 (R) 3(F) 4(O)	10 (R) 6(F) 8(O)	-Confidential Information Policy	1	1
Government Related Activities								
Federal, state and local election laws								
Government contracting requirements (kickbacks, bid-rigging, acquisition regs., affirm. action, billing, and record maintenance requirements, etc.)								

Legal & Regulatory Risk	Excluded	Business Area(s) Affected	Likelihood of Risk Occurrence	Severity of Risk Occurrence	Risk Score	Risk Mitigants	Combined Effectiveness of Mitigants	Prioritization to Address
Code of Conduct/Ethics Related Activities								
Conflicts of Interest								
Screening Employees								
Health and Safety								
Federal, state, and local hazardous materials requirements (e.g., RCRA)								
Product Safety (e.g., CPSA)								
International Operations								
Foreign Corrupt Practices Act								
Export Administration Regulations								
Intellectual Property								
Copyright Laws								
Patent Violations								

Legal & Regulatory Risk	Excluded	Business Area(s) Affected	Likelihood of Risk Occurrence	Severity of Risk Occurrence	Risk Score	Risk Mitigants	Combined Effectiveness of Mitigants	Prioritization to Address
Employment Laws								
Federal Wage and Hour Laws								
Health and Benefit Plans (ERISA, COBRA etc.)								
Family Medical Leave Act								
HIPPA								
Regulatory Reporting								
Disclosure Laws (SOX, SEC)								
Accounting Requirements (SOX, SEC)								
Tax Laws (federal, state and local)								
Other Specific Legal and Regulatory Requirements Based on Company's Operations and Activities (if not included above)								
1.								
2.								
3.								

2007 Compliance Program and Risk Assessment Benchmarking Survey

Executive Summary

The Association of Corporate Counsel (ACC) and Corpedia, Inc., jointly administered the 2007 Compliance Program and Risk Assessment Benchmarking survey during February and March of 2007.

The survey was "opt-in" and 458 inside corporate counsels participated in the survey. In terms of demographics, over 45 percent of the respondents were from organizations that are publicly traded on a major U.S. stock exchange, and 70 percent of the represented organizations conduct business operations outside of the United States.

The following key topics were covered in the survey:

- Compliance program leadership, staffing and spend
- Ethics and compliance awareness and training
- Challenges, privilege and the Board of Directors
- Risk assessments
- Hotlines, reports and organizational health surveys

Key Findings

- In terms of compliance program leadership, 58 percent of all organizations have a Chief Compliance Officer while 28 percent have a Chief Ethics Officer.
- Over one-third (35 percent) of all organizations revealed that the individual with daily operational responsibility for the compliance program reports directly to the CEO.
- The majority of organizations have fewer than five full-time equivalents (FTEs) dedicated to managing the ethics and compliance program.
- Thirty-seven percent of organizations with between 25,000 and 49,999 employees spend between \$1 million and \$5 million annually on their compliance program.
- About a quarter (26 percent) of all organizations rate their workforce awareness of ethics and compliance issues as "Average" while close to half (42 percent) believe their workforce maintains a "Good" level of awareness and understanding of ethics and compliance issues. Fewer than one in six organizations (17 percent) classify their workforce's level of awareness as "Excellent."
- Seventy-six percent of all organizations provide formal Code of Conduct training to employees and of those that do, 69 percent train more than 90 percent of their employees.
- More than half (54 percent) of the organizations surveyed are subject to Sarbanes-Oxley, and yet less than a quarter have formal training programs on "Financial Integrity" or "Sarbanes-Oxley."
- According to 68 percent of all organizations, the most significant challenge they face

2007 Compliance Program and Risk Assessment Benchmarking Survey



Conducted Jointly with  CORPEDIA
Ethics. Elevated



Association of Corporate Counsel
1025 Connecticut Avenue NW, Suite 200, Washington, DC, 20036
ph: 202.293.4103
www.acc.com

Copyright © 2007 Corpedia, Inc. and Association of Corporate Counsel

- when managing their compliance program is the “complexity of the legal and regulatory environment.”
- Twenty-eight percent of organizations felt that attorney-client privilege protections no longer exist in the context of a government investigation.
 - In over half (54 percent) of companies that are publicly traded in the United States, the person with daily operational responsibility for the compliance program reports to the Board of Directors quarterly.
 - For organizations that are not subject to Sarbanes-Oxley, only 26 percent offer training to their Board of Directors in compliance matters.
 - Seven out of every ten organizations conduct periodic risk assessments. Publicly traded organizations are more likely to do so than non-public ones (79 vs. 63 percent, respectively).
 - Almost one quarter (23 percent) of all organizations conduct risk assessments at least twice a year.
 - When conducting risk assessments, slightly more than half of all organizations quantify their risks and close to 80 percent of them prioritize risks using both the likelihood of occurrence and severity of impact.
 - Forty-six percent of all organizations offer a telephone-based anonymous reporting system. Email and websites were the next most common mediums (24 and 20 percent, respectively).
 - Forty-three percent of all organizations outsource their anonymous reporting systems to a third party, whereas 38 percent handle it in-house.
 - A high majority of organizations (71 percent) do not conduct regular organizational health surveys, which aim to evaluate the ethical culture of an organization and gauge employee perception of organizational commitment to ethical business conduct.

Contents

1. **About ACC and Corpedia, Inc.5**

2. **About the Survey.....6**
 2.1 Survey Breakdown

3. **Compliance Program: Leadership, Staffing and Spend.....7**
 3.1 Compliance Program Leadership
 3.2 Compliance Program Staffing
 3.3 Compliance Program Spend
 3.3 Compliance Program Spend

4. **Ethics and Compliance Awareness and Training20**
 4.1 Workforce Awareness of Ethics and Compliance Issues
 4.2 Formal Code of Conduct Training
 4.3 Percentage of Workforce Trained in Code of Conduct
 4.4 Formal and Mandatory Training Topics Beyond Code of Conduct

5. **Challenges, Privilege and the Board of Directors32**
 5.1 Top Challenges Encountered in Planning and Implementing Compliance Programs
 5.2 Attitude Toward Attorney-Client Privilege Protections
 5.3 Board of Directors Involvement

6. **Risk Assessments.....39**
 6.1 Prevalence of Risk Assessments
 6.2 Frequency of Risk Assessments
 6.3 Risk Assessment Methodologies
 6.4 Prioritization and Quantification of Risks
 6.5 Primary Parties to Risk Assessment
 6.6 Form and Distribution of Final Risk Assessment Report
 6.7 Risk Assessment Outcomes

7. **Hotlines, Reports and Organization Health Surveys.....51**
 7.1 Anonymous Reporting Systems
 7.2 Ethics Guidance Line
 7.3 Managing Cases and Reports of Misconduct
 7.4 Organizational Health Surveys

1. About ACC and Corpedia, Inc.

About ACC

The Association of Corporate Counsel is the in-house bar associationSM, serving the professional needs of attorneys who practice in the legal departments of corporations and other private sector organizations worldwide. The association promotes the common interests of its members, contributes to their continuing education, seeks to improve understanding of the role of in-house attorneys and encourages advancements in standards of corporate legal practice. Since its founding in 1982, the association has grown to more than 21,600 members in more than 73 countries who represent 9,416 corporations, with 48 Chapters and 14 Committees serving the membership. Its members represent all of the Fortune 50 companies and Fortune 100 companies. Internationally, its members represent 42 of the Global 50 and 74 of the Global 100 companies.

The Association of Corporate Counsel promotes the common professional and business interests of attorneys who are employed to practice law by corporations, associations and other private-sector organizations by developing and disseminating information, providing educational initiatives, facilitating networking opportunities, supporting collegiality and engaging in advocacy on behalf of the in-house bar. For more information, go to www.acc.com.

About Corpedia, Inc.

Corpedia, Inc., founded in 1998, is a leader in ethics and compliance e-learning, risk assessment, code of conduct services and many other areas of ethics and compliance consulting. Corpedia specializes in creating and implementing comprehensive and highly integrated compliance and ethics programs and solutions that exceed the requirements of Federal Sentencing Guidelines and Sarbanes-Oxley. Corpedia programs and services are provided in exclusive partnership with the Practising Law Institute (PLI), the premier provider of continuing legal education.

Corpedia serves on the Ethisphere Council and is a co-publisher of Ethisphere Magazine in partnership with the Practising Law Institute (PLI), the National Association of Corporate Directors (NACD) and LexisNexis. Ethisphere Magazine's circulation of 65,000 consists of CEOs, members of Boards of Directors, General Counsels and senior executives. Ethisphere also publishes the annual World's Most Ethical Companies™ ranking.

Corpedia prides itself in providing measurable and tailored solutions to companies to help them resolve complex compliance problems, allowing them to focus more

clearly on the business at hand. To find out more about how Corpedia's expertise and tailored solutions can help your organization resolve complex compliance issues, please visit the Corpedia website www.corpedia.com or call toll-free (877) 629-8724.

2. About the Survey

2.1 Survey Breakdown

The ACC-Corpedia Compliance Program and Risk Assessment Benchmarking Survey was administered online during February and March of 2007. The survey was "opt-in," and 458 individuals participated in the survey. A breakdown of participants by industry is as follows:

Aerospace & Defense	3%	Healthcare Products: Devices & Equipment	3%
Agriculture, Forestry, Fishing & Hunting	1%	Healthcare Services & Social Assistance	5%
Banking	2%	Industrial Manufacturing	9%
Beverages: Alcoholic	1%	Insurance	9%
Chemicals	3%	Leisure (Lodging, Restaurants, Entertainment)	3%
Computer Hardware, Software & Services	8%	Media	2%
Construction	2%	Non-Profit	3%
Consumer Products Manufacturing	3%	Pharmaceuticals and Biotechnology	4%
Consumer & Business Services	2%	Professional, Scientific & Technical Services	3%
Education	1%	Real Estate	1%
Electronics	5%	Retail	5%
Energy, Oil & Gas: (Exploration, Refinement & Distribution)	4%	Telecom Equipment & Services	4%
Environmental Services	1%	Transportation & Logistics Services	3%
Financial Services	7%	Utilities	3%
Food Product Manufacturing	1%	Wholesale Trade	1%

Over 70% represented organizations conduct business operations outside of the United States, including:

Africa	7.12%
Asia-Pacific	15.66%
Canada	15.73%
EU	16.05%
Europe - Non-EU country	11.00%
Latin America/Caribbean	13.66%
Middle East	9.64%
South Asia	11.13%

In terms of the size of the organization, the respondent breakdown was as follows:

Fewer than 50 employees	3.06%
50-249 employees	11.35%
250-999 employees	17.90%
1,000-4,999 employees	25.33%
5,000-9,999 employees	12.23%
10,000-24,999 employees	14.41%
25,000-49,999 employees	6.55%
Over 50,000 employees	9.17%

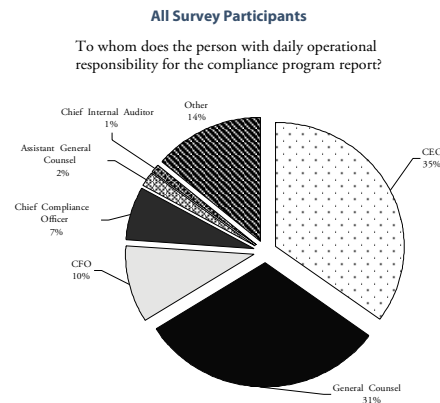
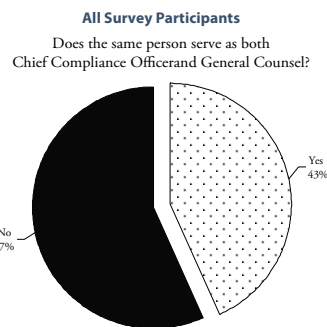
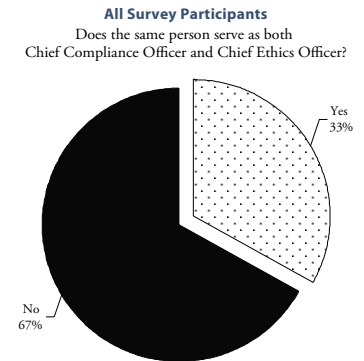
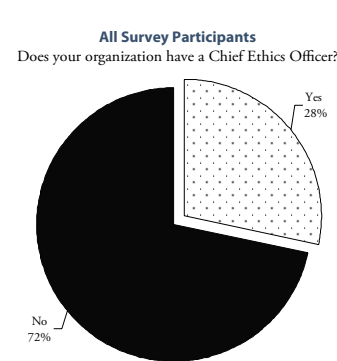
Participating organizations that are subject to the Sarbanes-Oxley Act:	
Yes	53.90%
No	46.10%

Participants that are publicly traded on a U.S. stock exchange (NYSE, NASDAQ, AMEX):	
Yes	45.90%
No	54.10%

3. Compliance Program: Leadership, Staffing and Spend

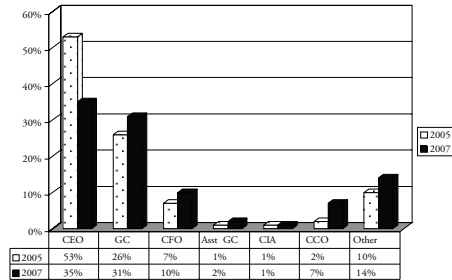
3.1 Compliance Program Leadership

- Fifty-eight percent of all organizations have a Chief Compliance Officer, with this person also serving as the General Counsel in slightly fewer than half of the organizations (43 percent). While this “dual-role” is more prevalent in smaller organizations, it is also common in larger ones.
- Twenty-eight percent of all organizations have a Chief Ethics Officer, and 33 percent of those hold the title and role of Chief Compliance Officer.
- In 35 percent of organizations, the individual with daily operational responsibility for the compliance and ethics function reports directly to the CEO.



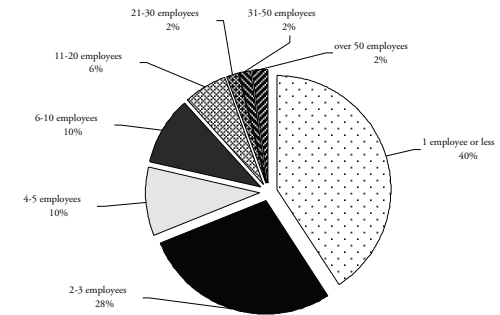
Year 2005 vs. Year 2007

To whom does the person with daily operational responsibility for the compliance program report?



All Survey Participants

What is the full-time employee equivalent in your organization dedicated to compliance and ethics activities or a formal compliance and ethics function?

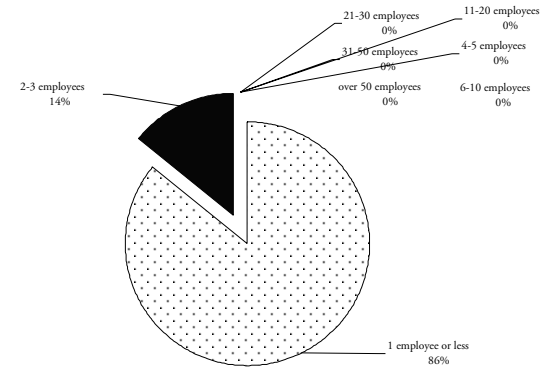


3.2 Compliance Program Staffing

- Overall, the majority of organizations have fewer than five full-time equivalents (FTEs) dedicated to managing the compliance and ethics function.
- A full 86 percent of compliance and ethics programs at organizations with 5,000-9,999 employees have less than five FTEs.
- Thirty percent of all organizations with workforce sizes of 25,000 to 49,999 employees have a minimum of 10 FTEs dedicated to the compliance and ethics function, with this percentage rising to 41 percent for companies having more than 50,000 employees.
- However, more than a third (36%) of companies with more than 50,000 employees have five or fewer FTEs dedicated to the compliance and ethics function.

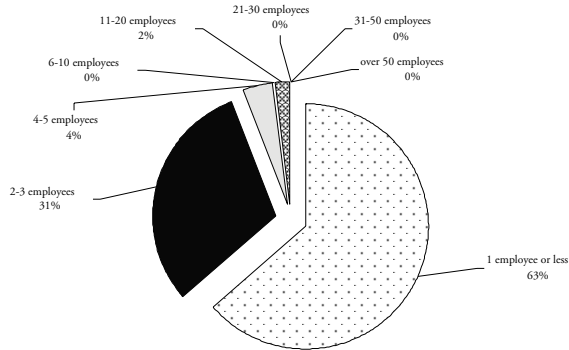
Organizations with less than 50 Employees

What is the full-time employee equivalent in your organization dedicated to compliance and ethics activities or a formal compliance and ethics function?



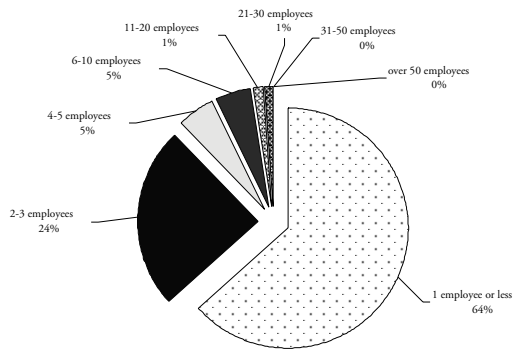
Organizations with 50-249 Employees

What is the full-time employee equivalent in your organization dedicated to compliance and ethics activities or a formal compliance and ethics function?



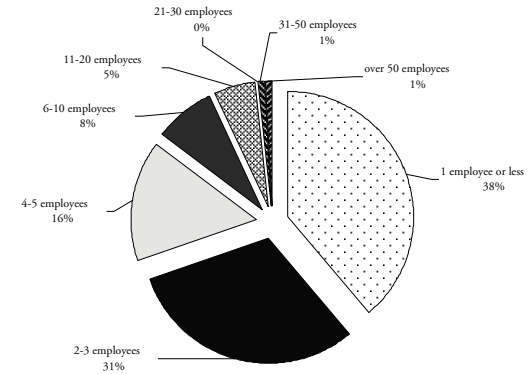
Organizations with 250-999 Employees

What is the full-time employee equivalent in your organization dedicated to compliance and ethics activities or a formal compliance and ethics function?



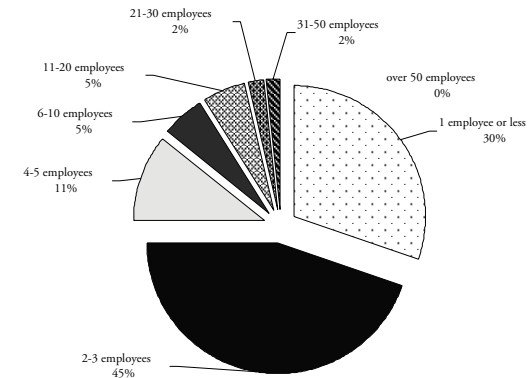
Organizations with 1,000-4,999 Employees

What is the full-time employee equivalent in your organization dedicated to compliance and ethics activities or a formal compliance and ethics function?



Organizations with 5,000-9,999 Employees

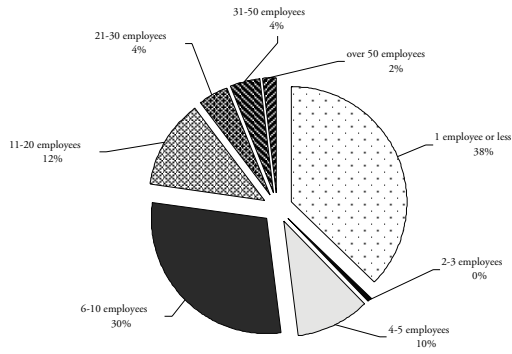
What is the full-time employee equivalent in your organization dedicated to compliance and ethics activities or a formal compliance and ethics function?



Copyright © 2007 Corpedia, Inc. and Association of Corporate Counsel

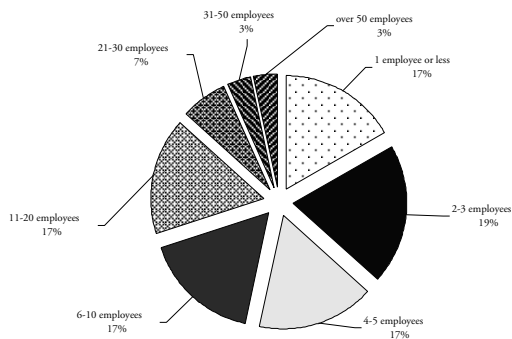
Organizations with 10,000-24,999 Employees

What is the full-time employee equivalent in your organization dedicated to compliance and ethics activities or a formal compliance and ethics function?



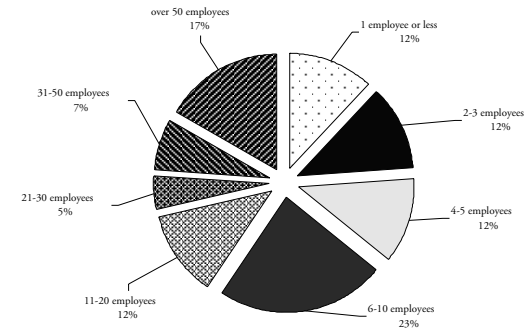
Organizations with 25,000-49,999 Employees

What is the full-time employee equivalent in your organization dedicated to compliance and ethics activities or a formal compliance and ethics function?



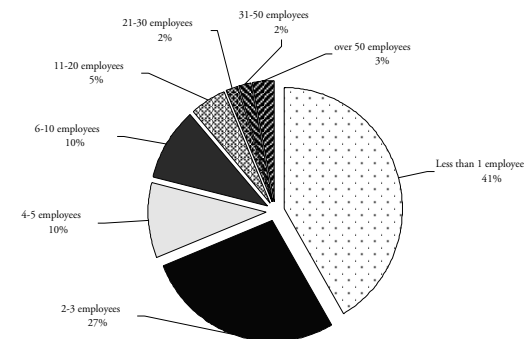
Organizations with 50,000+ Employees

What is the full-time employee equivalent in your organization dedicated to compliance and ethics activities or a formal compliance and ethics function?



Organizations with Operations Outside USA

What is the full-time employee equivalent in your organization dedicated to compliance and ethics activities or a formal compliance and ethics function?

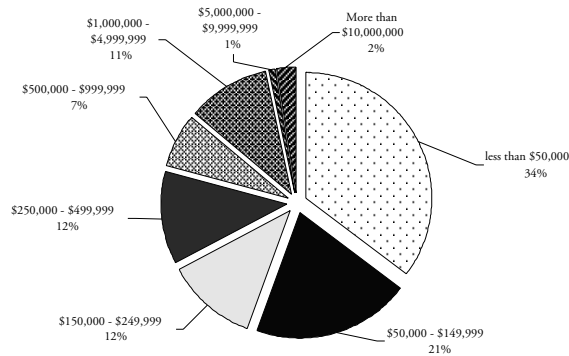


3.3 Compliance Program Spend

- While it is not surprising that larger organizations spend more money annually on the compliance ethics function than smaller organizations, it is interesting to note that the amount spent on compliance and ethics programs is more a function of industry type rather than the size of an organization.
- Two thirds of organizations (67 percent) spend up to \$250,000 annually on their ethics and compliance function, which is an increase of 17 percent from year 2005.
- Over one-third (37 percent) of organizations with workforce sizes of 25,000-49,999 employees spend between \$1 million and \$5 million annually on their compliance and ethics programs.

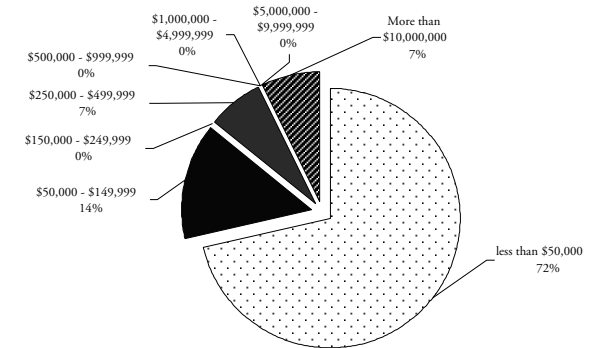
All Survey Participants

What is the approximate annual spend on your organization's legal compliance and ethics activities (excluding personnel)?



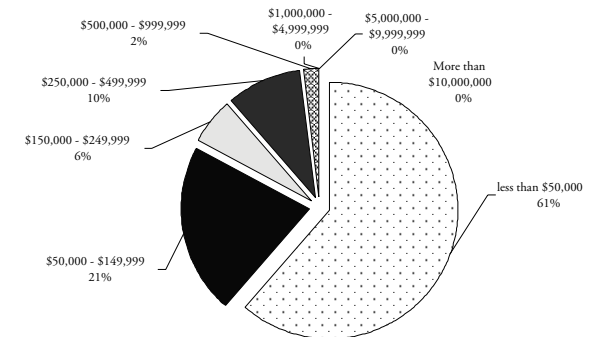
Organizations with Less than 50 Employees

What is the approximate annual spend on your organization's legal compliance and ethics activities (excluding personnel)?



Organizations with 50-249 Employees

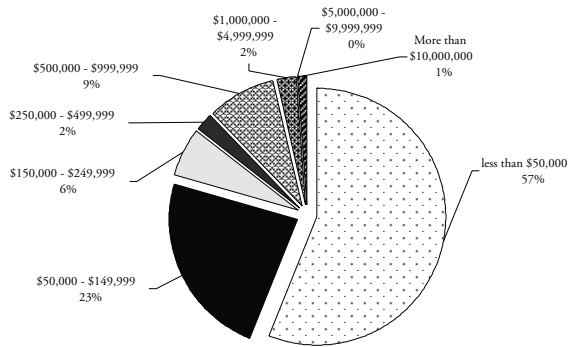
What is the approximate annual spend on your organization's legal compliance and ethics activities (excluding personnel)?



Copyright © 2007 Corpedia, Inc. and Association of Corporate Counsel

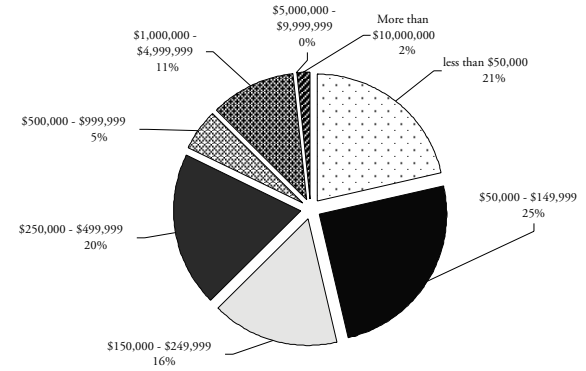
Organizations with 250-999 Employees

What is the approximate annual spend on your organization's legal compliance and ethics activities (excluding personnel)?



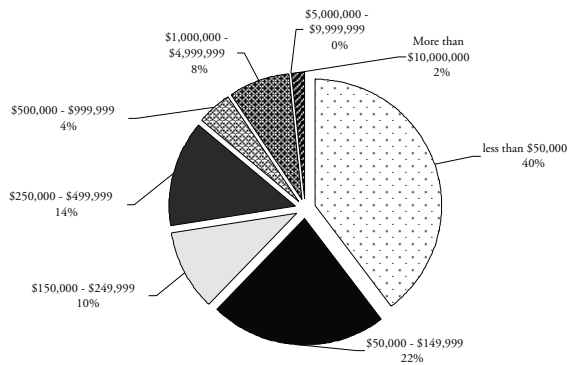
Organizations with 5,000-9,999 Employees

What is the approximate annual spend on your organization's legal compliance and ethics activities (excluding personnel)?



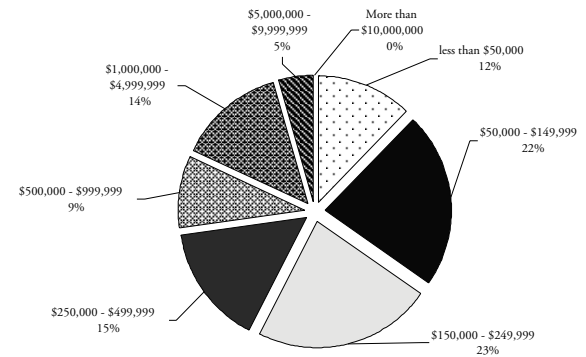
Organizations with 1,000-4,999 Employees

What is the approximate annual spend on your organization's legal compliance and ethics activities (excluding personnel)?



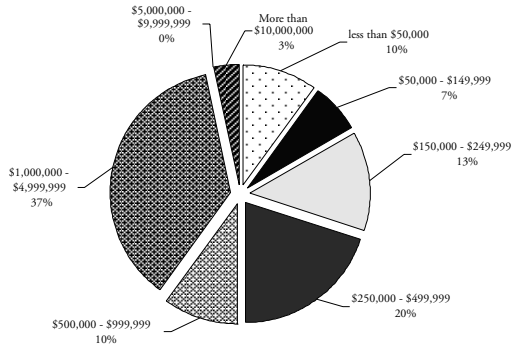
Organizations with 10,000-24,999 Employees

What is the approximate annual spend on your organization's legal compliance and ethics activities (excluding personnel)?



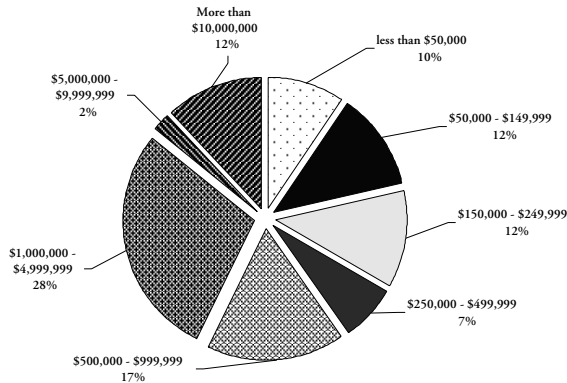
Organizations with 25,000-49,999 Employees

What is the approximate annual spend on your organization's legal compliance and ethics activities (excluding personnel)?



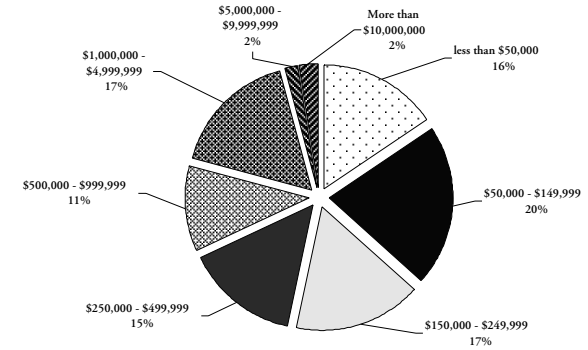
Organizations with 50,000+ Employees

What is the approximate annual spend on your organization's legal compliance and ethics activities (excluding personnel)?



Publicly Traded Companies (USA)

What is the approximate annual spend on your organization's legal compliance and ethics activities (excluding personnel)?

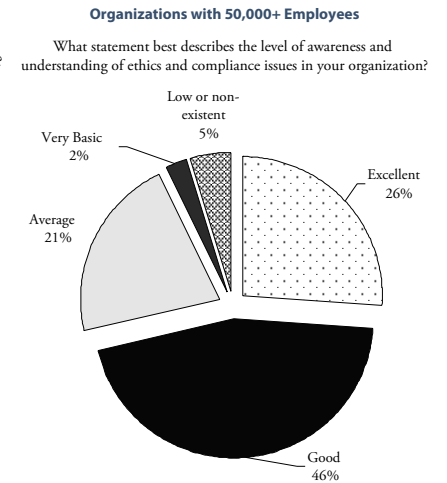
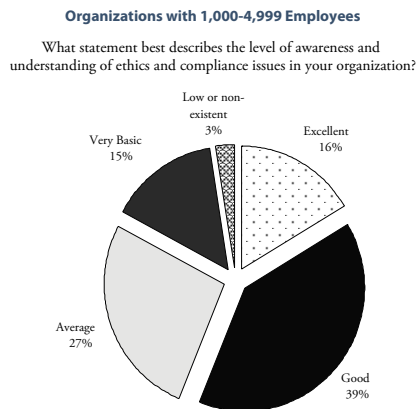
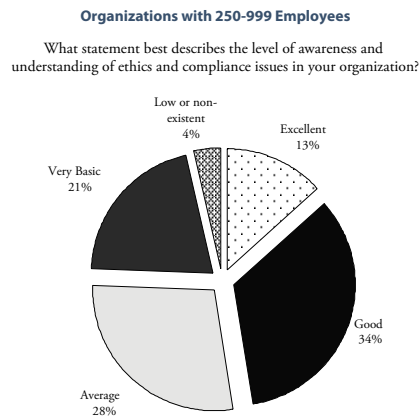
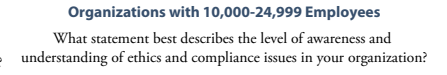
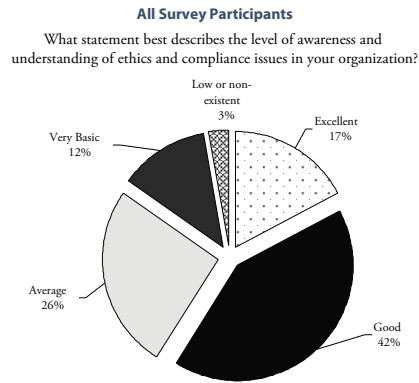


4. Ethics and Compliance Awareness and Training

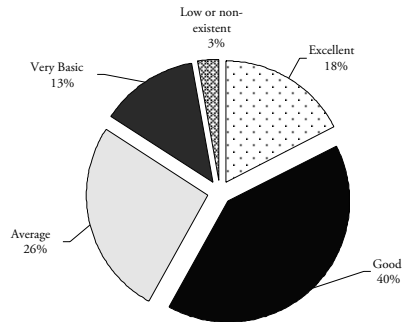
4.1 Workforce Awareness of Ethics and Compliance Issues

- For the typical organization, the level of awareness among the workforce about ethics and compliance issues is "Average" for over a quarter of all organizations (26%). While percent say that their workforce maintains a "Good" level of awareness and understanding of compliance and ethics issues, only 17 percent of all organizations classify their workforce as having an "Excellent" level of awareness and understanding of the issues.
- There is a definite correlation between the size of an organization and the level of workforce awareness of compliance and ethics issues. Only 15 percent of smaller organizations (with fewer than 1,000 employees) rate their workforce as having an "Excellent" understanding of the issues, and 34 percent report a "Good" understanding of the issues. However, among larger organizations (with more than 10,000 employees), the levels of "Excellent" and "Good" understanding of the issues jump to 21 percent and 47 percent, respectively.
- The higher levels of awareness and understanding among employees at larger organizations may be attributed, in part, to the fact that larger organizations tend to have a formal Code of Conduct training program in place for employees. While 87 percent of larger employers (with 10,000 or more

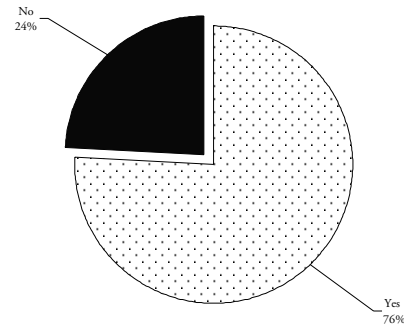
employees) have a formal Code of Conduct training program in place, only 60 percent of small employers do (under 1,000 employees).



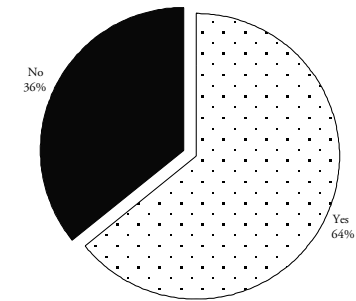
Organizations with Operations Outside USA
 What statement best describes the level of awareness and understanding of ethics and compliance issues in your organization?



All Survey Participants
 Does your organization provide formal Code of Conduct training to employees?



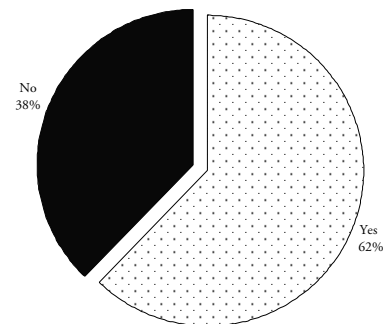
Organizations with less than 50 Employees
 Does your organization provide formal Code of Conduct training to employees?



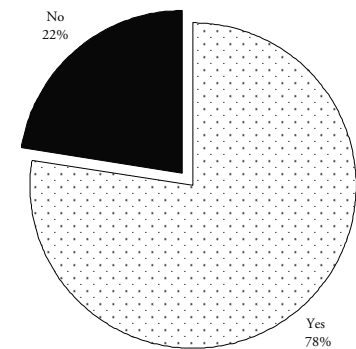
4.2 Formal Code of Conduct Training

- Overall, 76 percent of organizations provide formal code of conduct training to employees.
- Of organizations that are publicly traded in the United States, 85 percent provide formal code of conduct training to employees. Yet only 68 percent of non-publicly traded companies provide such training.
- For those organizations that conduct business operations outside of the United States, 78 percent provide formal code of conduct training to employees.
- Of organizations that have formal code of conduct training programs in place, the majority of such organizations (69 percent) train virtually the entire workforce (more than 90 percent of employees).
- Of organizations that have formal code of conduct training programs in place, the percentage of the workforce that is trained is relatively consistent regardless of the size of the organization, with only organizations with workforce sizes between 10,000-24,999 employees training a materially smaller proportion of the workforce.

Organizations with 250-999 Employees
 Does your organization provide formal Code of Conduct training to employees?

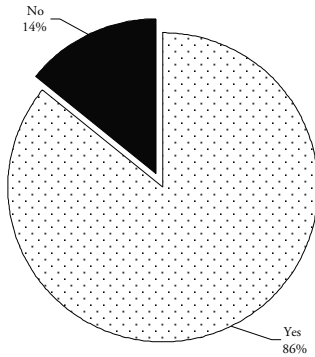


Organizations with 1,000-4,999 Employees
 Does your organization provide formal Code of Conduct training to employees?



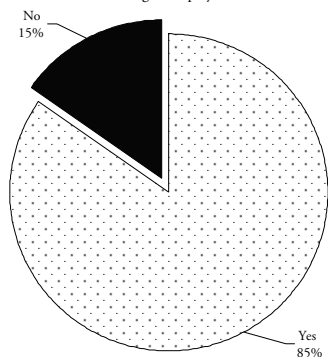
Organizations with 5,000-9,999 Employees

Does your organization provide formal Code of Conduct training to employees?



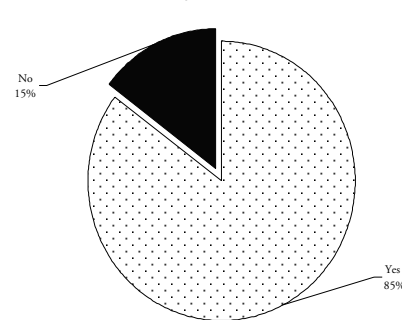
Organizations with 10,000-24,999 Employees

Does your organization provide formal Code of Conduct training to employees?



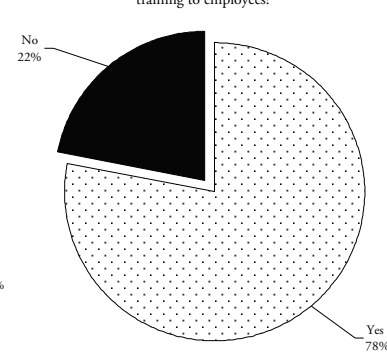
Publicly Traded Companies (USA)

Does your organization provide formal Code of Conduct training to employees?



Organizations with Operations Outside USA

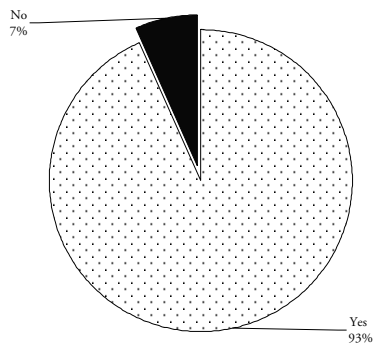
Does your organization provide formal Code of Conduct training to employees?



4.3 Percentage of Workforce Trained in Code of Conduct

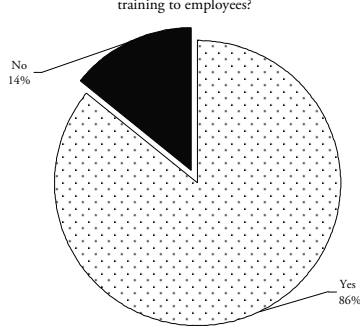
Organizations with 25,000-49,999 Employees

Does your organization provide formal Code of Conduct training to employees?



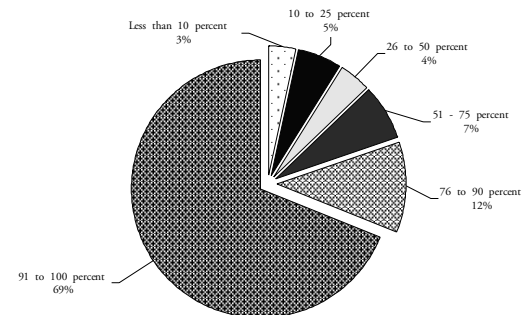
Organizations with 50,000+ Employees

Does your organization provide formal Code of Conduct training to employees?

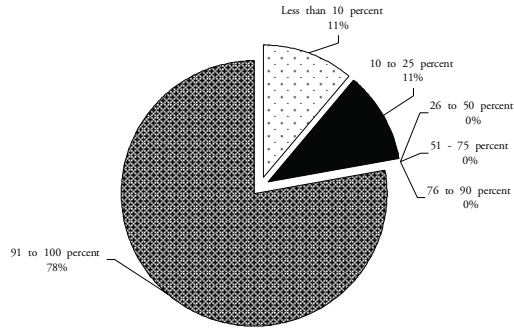


All Survey Participants

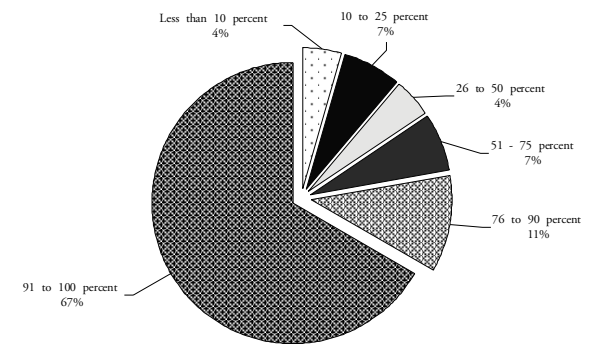
Approximately what percentage of all employees receive the Code of Conduct Training?



Organizations with less than 50 Employees
Approximately what percentage of all employees receive the Code of Conduct Training?

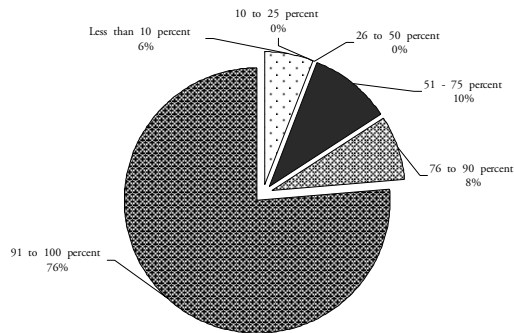


Organizations with 1,000-4,999 Employees
Approximately what percentage of all employees receive the Code of Conduct Training?



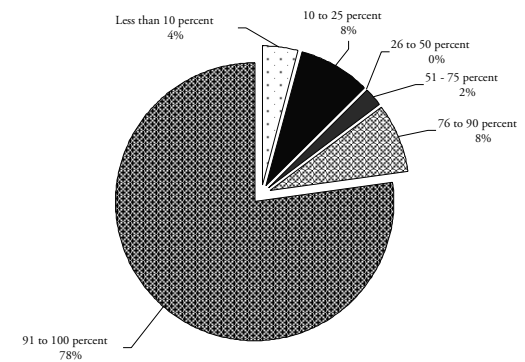
Organizations with 250-999 Employees

Approximately what percentage of all employees receive the Code of Conduct Training?



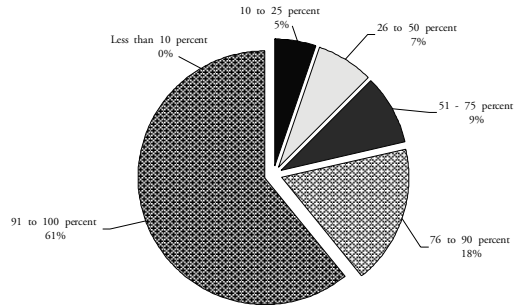
Organizations with 5,000-9,999 Employees

Approximately what percentage of all employees receive the Code of Conduct Training?



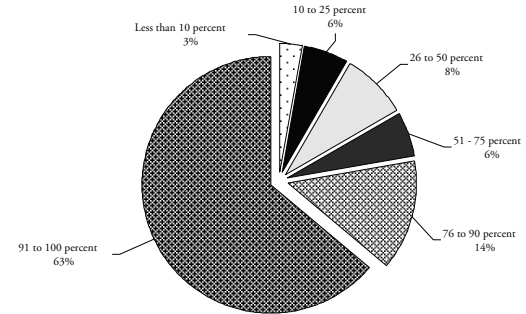
Organizations with 10,000-24,999 Employees

Approximately what percentage of all employees receive the Code of Conduct Training?



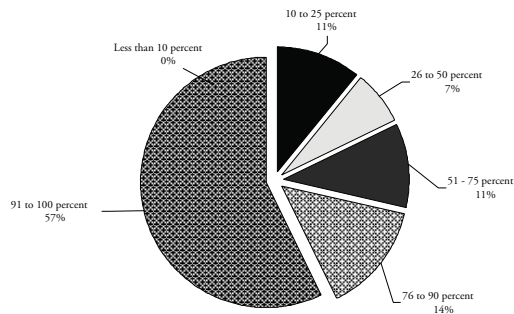
Organizations with 50,000+ Employees

Approximately what percentage of all employees receive the Code of Conduct Training?



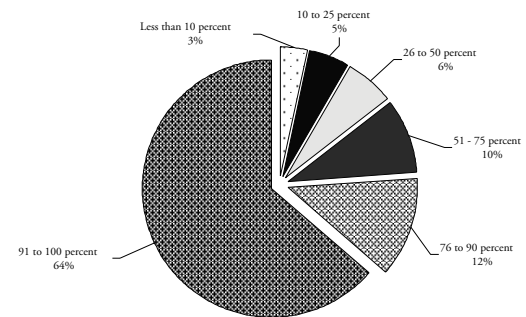
Organizations with 25,000-49,999 Employees

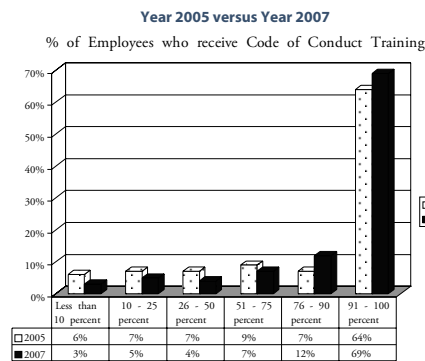
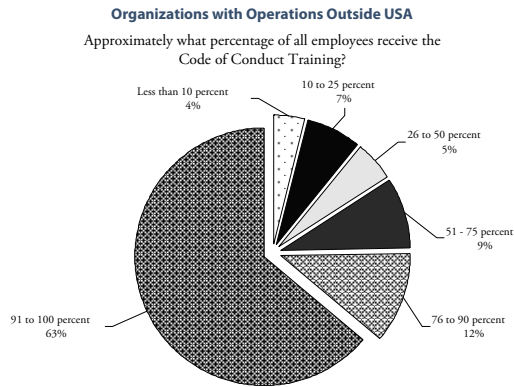
Approximately what percentage of all employees receive the Code of Conduct Training?



Publicly Traded Companies (USA)

Approximately what percentage of all employees receive the Code of Conduct Training?





4.4 Formal and Mandatory Training Topics Beyond Code of Conduct

- For all organizations, the top three topics of formal and mandatory training beyond the Code of Conduct include sexual harassment (66 percent), workplace harassment (53 percent) and conflicts of interest (53 percent).

- While 70 percent of survey respondents conduct business operations outside of the United States, only 39 percent of those organizations had a formal and mandatory training program in Foreign Corrupt Practices Act (FCPA), bribery and corruption.
- While 54 percent of all survey respondents are subject to the Sarbanes-Oxley Act, only 25 percent have formal and mandatory training programs in financial integrity, and only 21 percent offer training on compliance with the Sarbanes-Oxley Act.

TOPIC	%	TOPIC	%
Sexual Harassment	66%	Substance Abuse / Drug-Free Workplace	25%
Workplace Harassment	53%	Ethical Sales & Business Practices / Fair Dealing	24%
Conflicts of Interest	53%	Contracts & Contract Management	21%
Confidential Information Protection	53%	Intellectual Property	21%
Ethics	50%	Sarbanes-Oxley	21%
Equal Employment Opportunity / Discrimination	46%	Employee Privacy	19%
Gifts & Entertainment	42%	Export Controls	18%
Workplace Safety/OSHA	35%	Corporate Governance	18%
Antitrust/Competition	32%	Workplace Violence	16%
Whistleblowing and Investigations	31%	Political Activities/Lobbying	14%
Customer / Consumer Privacy	31%	Environmental Protection	14%
Diversity	30%	Government Contracting	14%
Foreign Corrupt Practices Act (FCPA) / Bribery & Corruption	29%	Money Laundering	12%
Industry-Specific Regulations	26%	Corporate Social Responsibility	12%
Insider Trading / Securities Law	26%	FLSA/Wage & Hour Rules	11%
Document / Record Management	26%	OFAC Regulations	9%
Employment Law for Managers	25%	Marketing/Advertising Law	9%
Financial Integrity	25%	Vendor Compliance	8%
		Product Liability	5%

5. Challenges, Privilege and the Board of Directors

5.1 Top Challenges Encountered in Planning and Implementing Compliance Programs

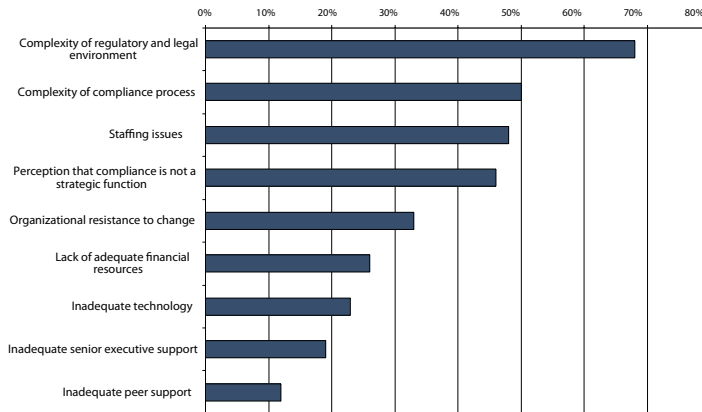
- Not surprisingly, the two most common challenges encountered by those responsible for the compliance and ethics function are "Complexity of Regulatory and Legal Environment" (cited by 68 percent) and the "Complexity

of the Compliance Process” (cited by 50 percent).

- Hiring and retaining qualified individuals for the ethics and compliance function is the third greatest challenge for nearly half of all organizations (48 percent).
- Only one in five respondents (19 percent) cited “Inadequate Senior Executive Support” as a significant challenge for their compliance and ethics program efforts. This figure is down 5 percent from our 2005 findings.

All Participants

What are the top challenges you have dealt with or are likely to deal with when planning or implementing your company's Compliance and Ethics function?



5.2 Attitude Toward Attorney-Client Privilege Protections

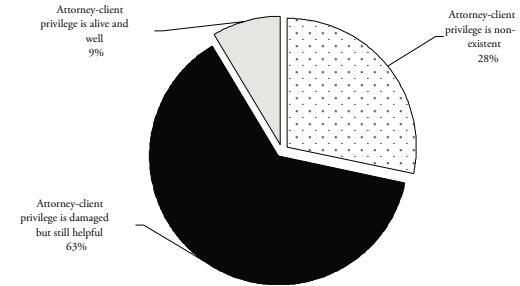
- The in-house corporate counsel believes that attorney-client privilege protection has been severely damaged in recent years. Close to one-third (28 percent) of survey respondents feel that attorney-client privilege no longer exists in the context of a government investigation. On the other hand, 63 percent feel that privilege is damaged but still helpful, while only 9 percent believe that attorney-

client privilege in the context of a government investigation remains alive and well.

- There is little difference of opinion regarding the presence of attorney-client privilege whether the respondent works for a private company or public company.

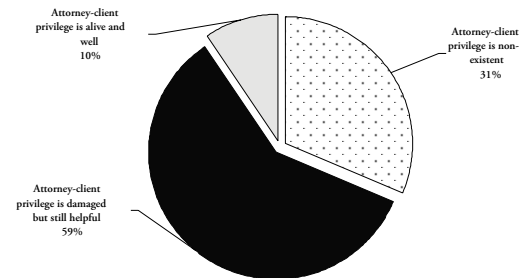
All Survey Participants

In the context of a violation of federal or state law where government authorities investigate, do you believe that attorney-client privilege protections continue to exist in a meaningful way?



Publicly Traded Companies (USA)

In the context of a violation of federal or state law where government authorities investigate, do you believe that attorney-client privilege protections continue to exist in a meaningful way?



Copyright © 2007 Corpedia, Inc. and Association of Corporate Counsel

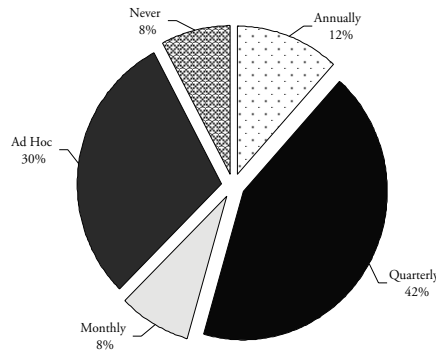
5.3 Board of Directors Involvement

Communication with the Board of Directors

- The person who has daily operational responsibility for the compliance and ethics program has high exposure to the Board of Directors. This is particularly significant at publicly traded companies, where 54 percent of ethics and compliance officers communicate with the Board of Directors at least quarterly.
- Only 8 percent of the persons who have daily operational responsibility for compliance and ethics never communicate directly with the Board of Directors.
- In organizations not subject to Sarbanes Oxley, communication with the Board of Directors tends to occur most often on an as-needed basis (39 percent).
- In organizations that conduct business operations outside of the United States, 43 percent report communication with the Board occurs on a quarterly basis while another 30 percent do so on an as needed basis.

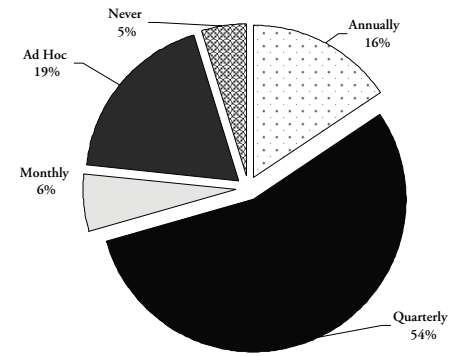
All Survey Participants

How often does the person with daily operational responsibility for the compliance and ethics program communicate with the Board of Directors?



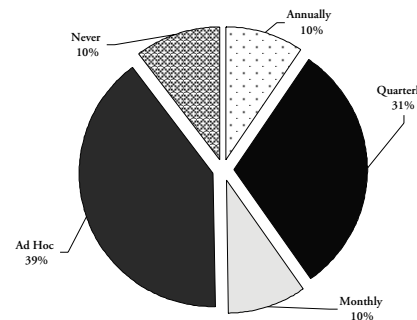
Publicly Traded Companies (USA)

How often does the person with daily operational responsibility for the compliance and ethics program communicate with the Board of Directors?



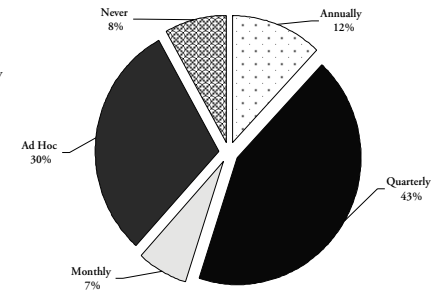
Organizations Not Subject to Sarbanes-Oxley

How often does the person with daily operational responsibility for the compliance and ethics program communicate with the Board of Directors?



Organizations with Operations Outside USA

How often does the person with daily operational responsibility for the compliance and ethics program communicate with the Board of Directors?



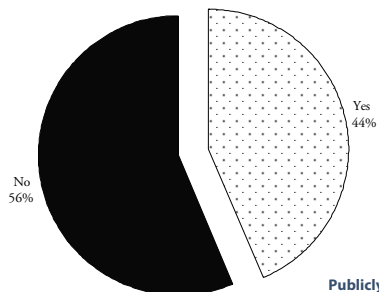
Copyright © 2007 Corpedia, Inc. and Association of Corporate Counsel

Board Training

- Nearly 44 percent of organizations confirmed that their Board of Directors has been trained in compliance consistent with Federal Sentencing Guidelines (FSG) criteria. Of that percentage, 73 percent provide 2 hours or less of training.
- For those respondents who work for a publicly traded company, 62 percent acknowledged that the Board has been trained in compliance with FSG criteria.
- For organizations that are **not** subject to Sarbanes-Oxley, only 26 percent offer training on compliance matters to the Board of Directors.

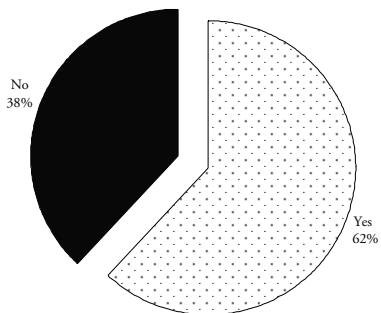
All Survey Participants

Has your Board of Directors been trained in compliance consistent with Federal Sentencing Guidelines criteria?



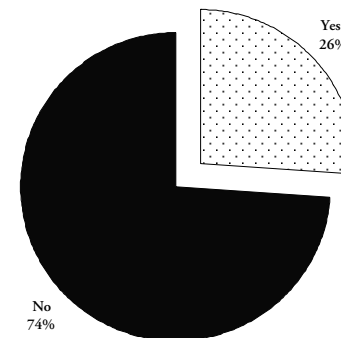
Publicly Traded Companies (USA)

Has your Board of Directors been trained in compliance consistent with Federal Sentencing Guidelines criteria?



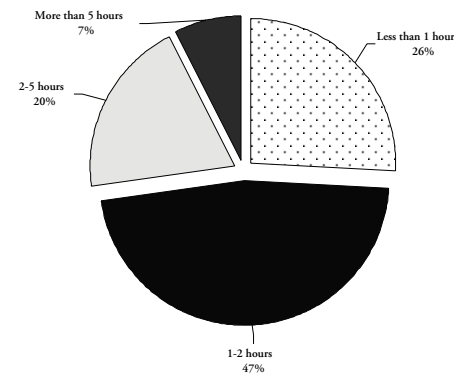
Organizations Not Subject to Sarbanes-Oxley

Has your Board of Directors been trained in compliance consistent with Federal Sentencing Guidelines criteria?



All Survey Participants

How many hours of compliance training does the Board of Directors receive on an annual basis?



Copyright © 2007 Corpedia, Inc. and Association of Corporate Counsel

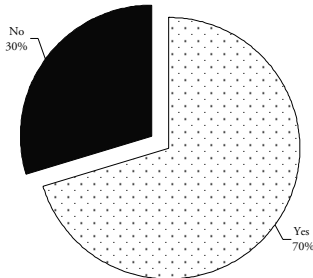
6. Risk Assessments

6.1 Prevalence of Risk Assessments

- A majority (70 percent) of all organizations conduct periodic risk assessments, regardless of organizational size. This is an increase of 12 percent from our 2005 findings. Publicly traded organizations are also more likely to conduct a periodic risk assessment than private organizations (79 percent vs. 63 percent).
- While smaller organizations are likely to conduct a periodic risk assessment (42 percent), the larger the organization, the higher the odds that it will conduct such an assessment. Four out of every five organizations (80 percent) with more than 25,000 employees conduct periodic risk assessments.

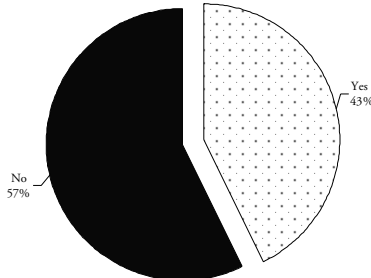
All Survey Participants

Does your organization conduct periodic Risk Assessments?



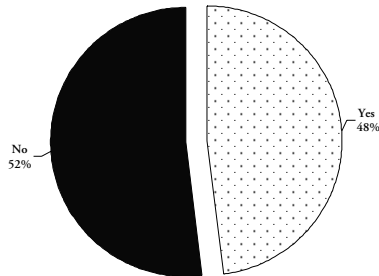
Organizations with less than 50 Employees

Does your organization conduct periodic Risk Assessments?



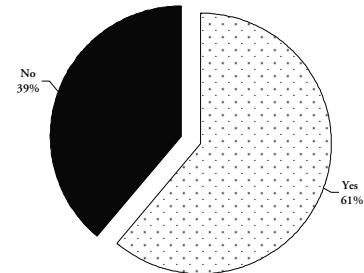
Organizations with 50-249 Employees

Does your organization conduct periodic Risk Assessments?



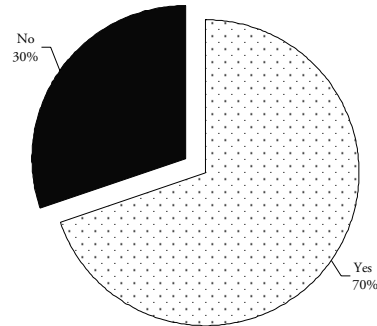
Organizations with 250-999 Employees

Does your organization conduct periodic Risk Assessments?



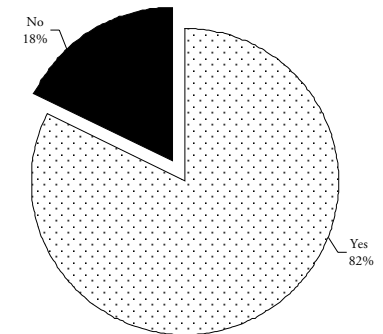
Organizations with 1,000-4,999 Employees

Does your organization conduct periodic Risk Assessments?



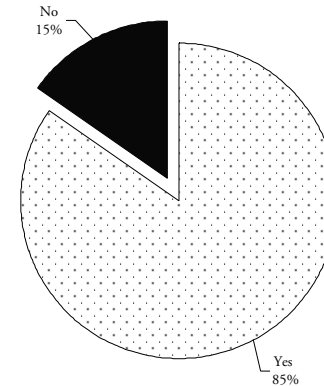
Organizations with 5,000-9,999 Employees

Does your organization conduct periodic Risk Assessments?



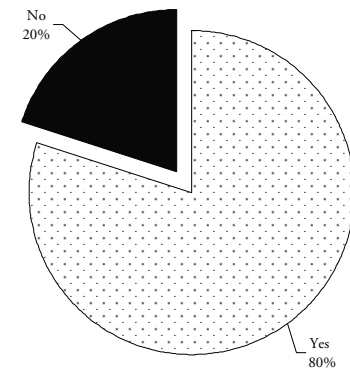
Organizations with 10,000-24,999 Employees

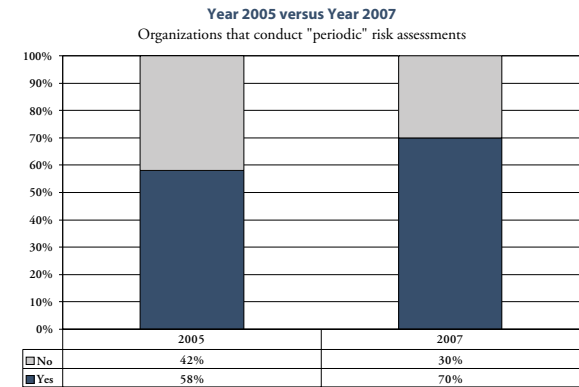
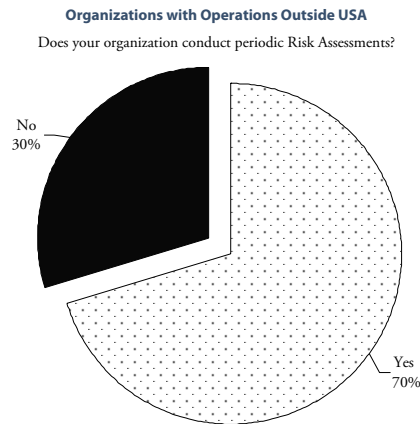
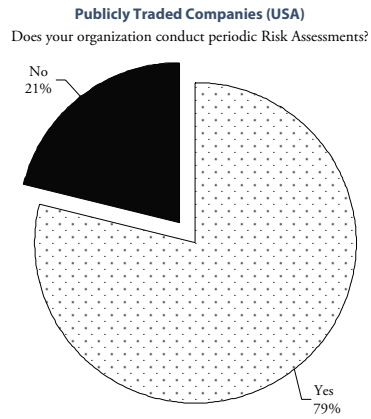
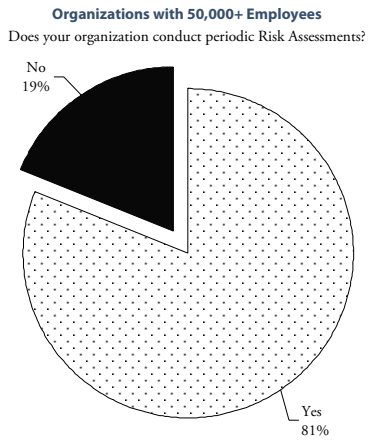
Does your organization conduct periodic Risk Assessments?



Organizations with 25,000-49,999 Employees

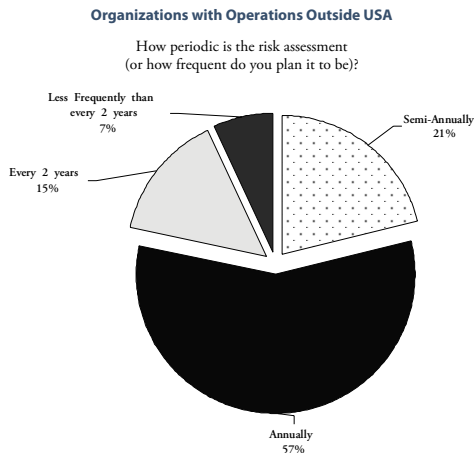
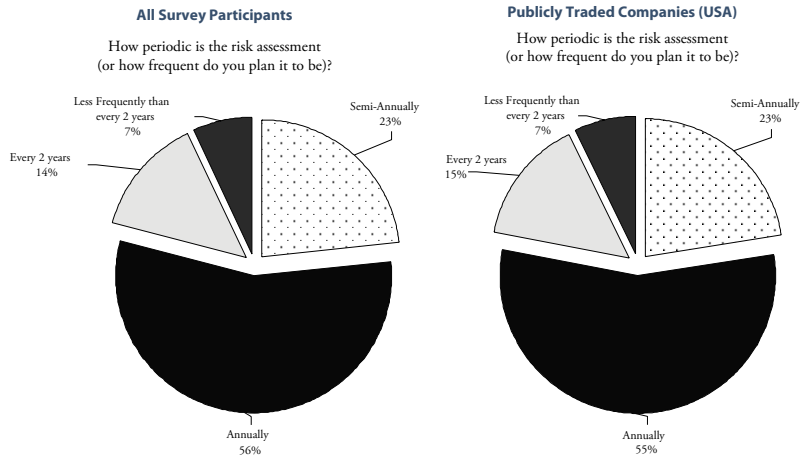
Does your organization conduct periodic Risk Assessments?





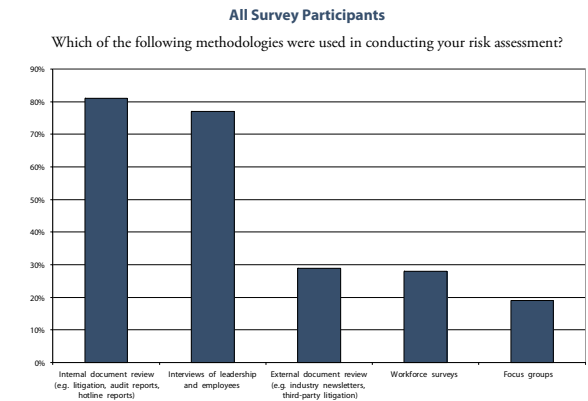
6.2 Frequency of Risk Assessments

- A slight majority (56 percent) of organizations conduct risk assessments on an annual basis, while just over 23 percent of organizations conduct them at least twice each year.
- There were no significant differences between public and private companies.
- For those organizations that have business operations outside of the United States, 57 percent conduct risk assessments annually.



6.3 Risk Assessment Methodologies

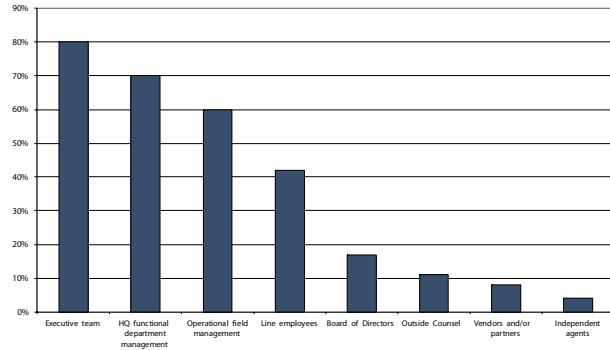
- The two most popular methodologies used in conducting risk assessment are “Internal Document Review”, such as litigation, audit and hotline reports, which were used by 81 percent of respondents, and “Interviews with Leadership and Employees”, which were used by 77 percent.
- Overall, only 28 percent use workforce surveys and even less (19 percent) employ focus groups as part of the risk assessment process.



- For organizations that conduct employee interviews as part of the risk assessment process, the three most commonly interviewed groups are Executive Team (80 percent), HQ Functional Department Management (70 percent) and Operational Field Management (60 percent). However, significantly fewer companies interview additional lower-level employees in the risk assessment process, specifically, only 42 percent.
- The Board of Directors is typically omitted from the interview process in most organizations. Only 17 percent of organizations that conduct interviews as part of the risk assessment include the Board of Directors in the interview pool.
- The areas that are most often reviewed in risk assessment interviews are “Internal policies & processes” (96 percent), “Employee awareness & understanding” (78 percent) and the “Anonymous reporting system” (71 percent).

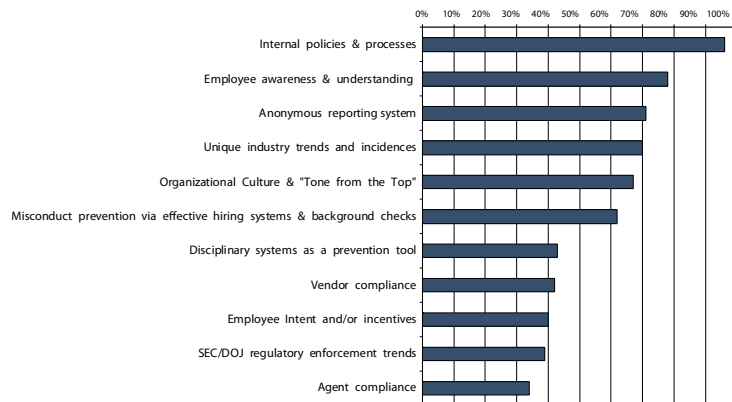
All Survey Participants

If you conducted interviews, surveys or focus groups in your risk assessment, which parties were represented in the interviews or focus groups?



All Survey Participants

Does the risk assessment take into account one or more of the following?

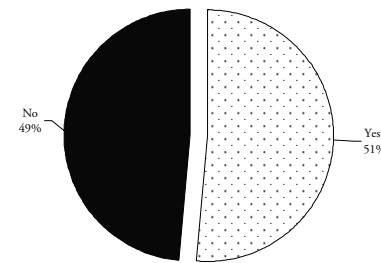


6.4 Prioritization and Quantification of Risks

- The majority (78 percent) of companies that conduct risk assessments prioritize risk using both the probability of occurrence and the severity of impact. This statistic does not vary significantly regardless of the size of the organization or whether it is publicly traded or private.
- Fifty-one percent of all organizations actually quantify their risks, up 7 percent from our 2005 findings. Publicly traded companies are more likely to quantify risk (59 percent) versus foreign or private organizations.

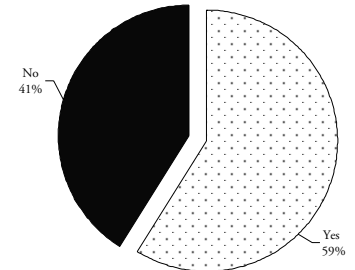
All Survey Participants

Does your organization's risk assessment prioritize risk in a quantitative way?



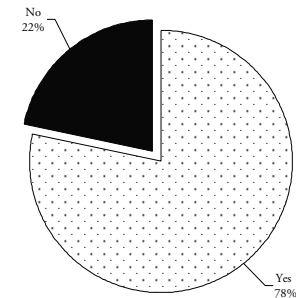
Publicly Traded Companies (USA)

Does your organization's risk assessment prioritize risk in a quantitative way?



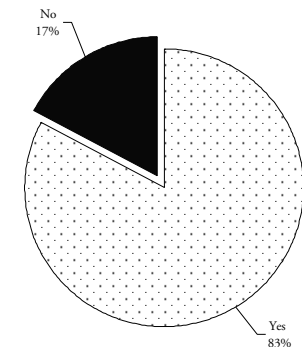
All Survey Participants

Is the risk prioritized from BOTH the likelihood and the impact of violation standpoints?

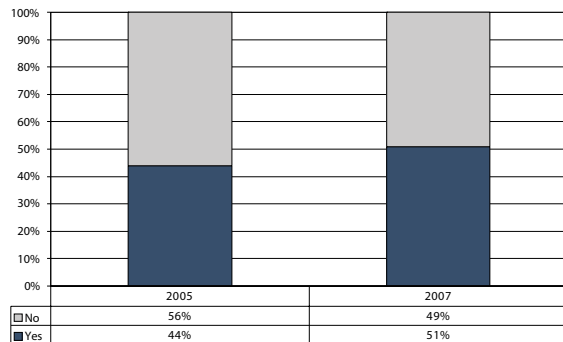


Publicly Traded Companies (USA)

Is the risk prioritized from BOTH the likelihood and the impact of violation standpoints?

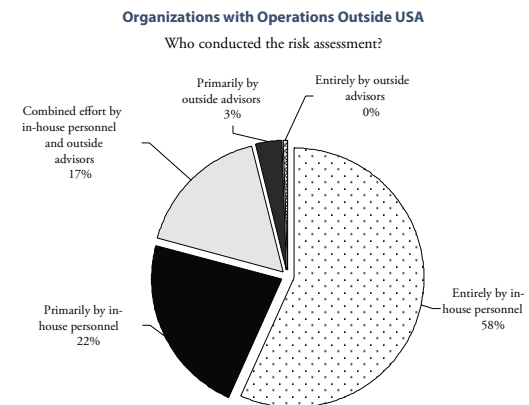
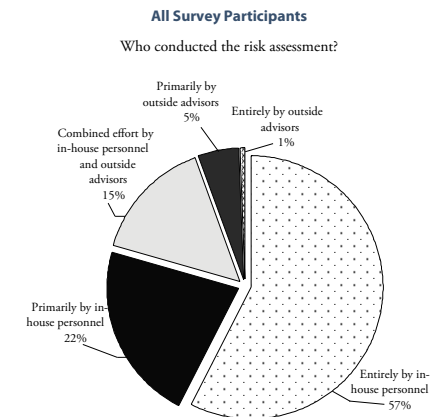


Year 2005 versus Year 2007
Organizations that prioritize risk in a quantitative manner



6.5 Primary Parties to Risk Assessment

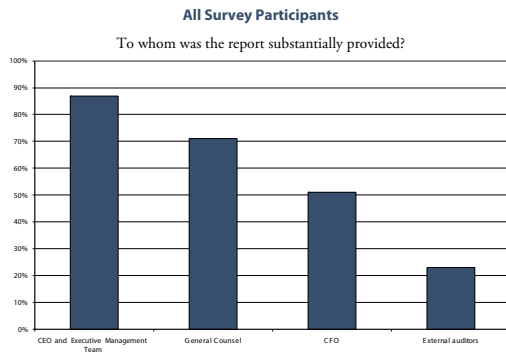
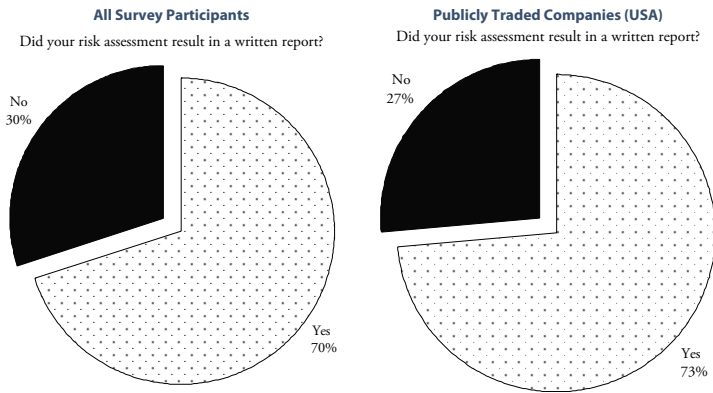
- Over half (57 percent) of all organizations handle risk assessments entirely in-house, while 21 percent use an outside advisor in the process.



Copyright © 2007 Corpedia, Inc. and Association of Corporate Counsel

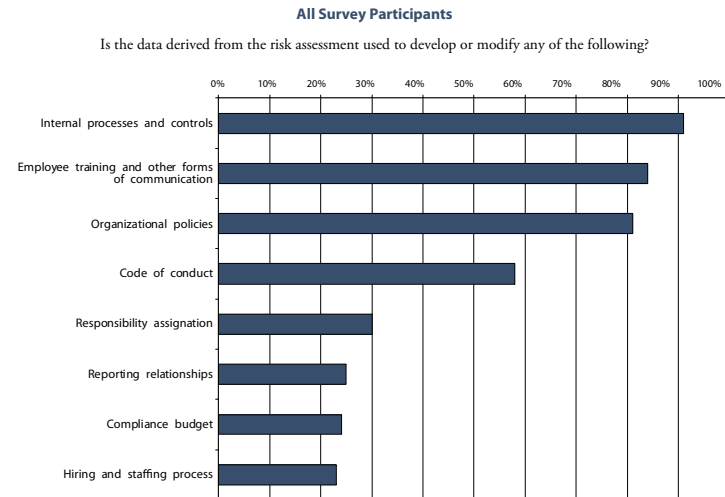
6.6 Form and Distribution of Final Risk Assessment Report

- Seventy percent of all organizations confirmed that their risk assessment resulted in a written report, with companies publicly traded in the United States reporting a slightly higher percentage.
- Not surprisingly, the top audience for the final risk assessment report is the CEO and Executive Management Team (87 percent). In contrast, only 23 percent of all organizations provide the results of their risk assessment to external auditors.



6.7 Risk Assessment Outcomes

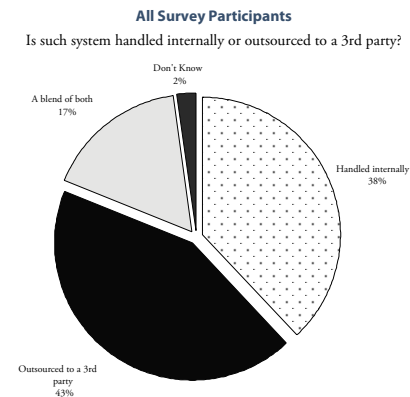
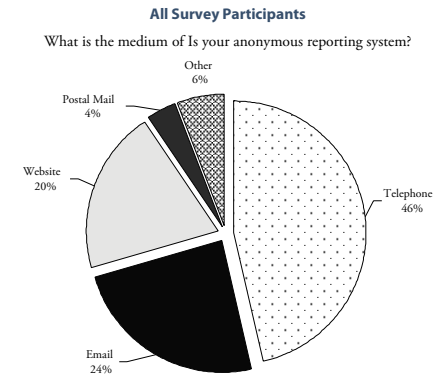
- For those organizations that conduct risk assessments, the most common outcomes were the development or modification "Internal Processes and Controls" (91 percent), "Employee Training and Other Forms of Communication" (84 percent), and "Organizational Policies" (81 percent).
- Risk assessments are also used by 58 percent of organizations to modify (or develop) the organization's written code of conduct.
- Infrequently, risk assessments may affect "Reporting Relationships" (25 percent), "Organizational Compliance Budget" (24 percent) or "Hiring and Staffing Process" (23 percent).



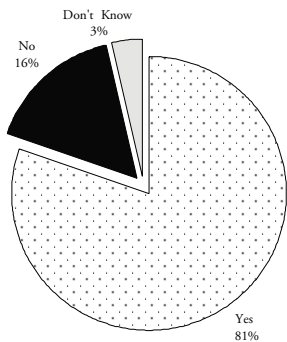
7. Hotlines, Reports and Organization Health Surveys

7.1 Anonymous Reporting Systems

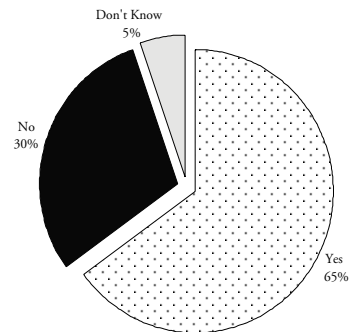
- The vast majority (81 percent) of organizations provide an anonymous reporting system for employees to report suspected misconduct.
- It is interesting to note that, while anonymous reporting systems are required for organizations subject to the Sarbanes-Oxley Act, a majority (65 percent) of organizations that are **not** subject to the Act also have such reporting systems in place. This may be due to the requirement (under Federal Sentencing Guidelines) of having such a system in order to capitalize on the affirmative defense available under FSG criteria for having an "effective compliance and ethics program."
- Of the organizations that provide an anonymous reporting system, 46 percent indicated the use of telephone-based hotlines, while 24 percent mentioned email, and another 20 percent offered a website.
- In terms of how organizations manage such anonymous reporting systems, 38 percent of all organizations operate their systems internally, 43 percent outsource the systems to an independent third party and 17 percent employ a blend of both insider- and outsider-operated systems. These statistics are relatively consistent across all sizes of organizations.



All Survey Participants
Do you have an anonymous reporting system where employees can report misconduct or raise concerns about illegal behavior or code violations?



Organizations Not Subject to Sarbanes-Oxley
Do you have an anonymous reporting system where employees can report misconduct or raise concerns about illegal behavior or code violations?

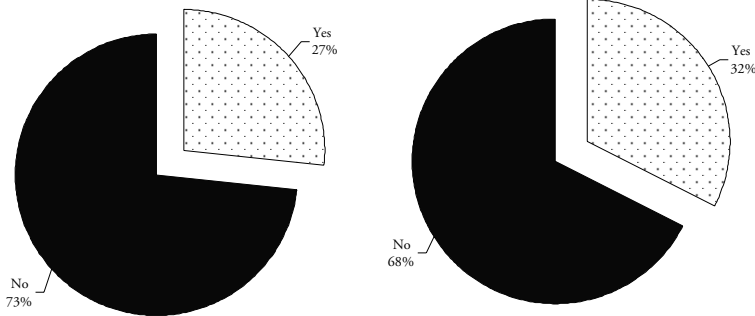


7.2 Ethics Guidance Line

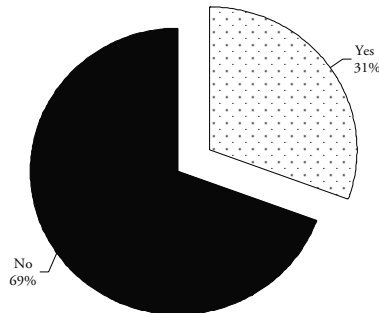
- Only a minority (27 percent) of organizations maintain a separate resource to provide advice or guidance on ethics issues in addition to anonymous reporting hotline.
- Publicly traded organizations are slightly more likely to maintain a separate ethics guidance line (32 percent).

All Survey Participants
Do you maintain an "Ethics Guidance" line, separate from the hotline, where employees can seek advice on ethical dilemmas?

Publicly Traded Companies
Do you maintain an "Ethics Guidance" line, separate from the hotline, where employees can seek advice on ethical dilemmas?

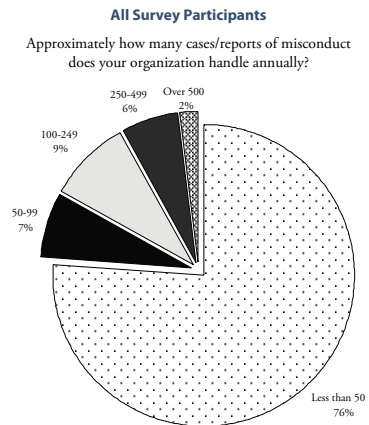
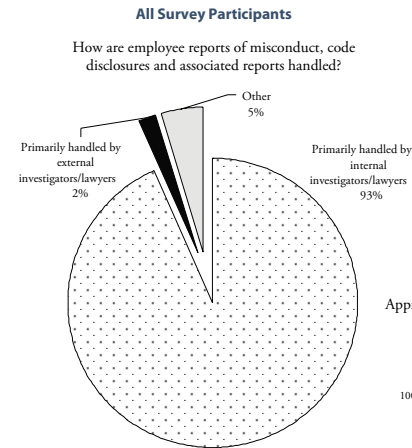


Organizations with Operations Outside USA
Do you maintain an "Ethics Guidance" line, separate from the hotline, where employees can seek advice on ethical dilemmas?



7.3 Managing Cases and Reports of Misconduct

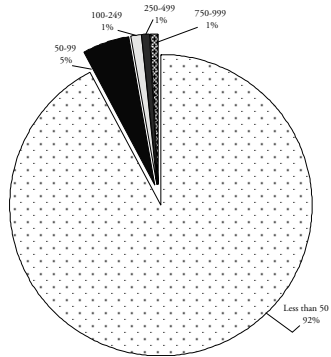
- The vast majority (93 percent) of all organizations assign responsibility for managing reports of misconduct, disclosures and related issues to internal investigators or lawyers.
- Overall, 76 percent of all survey participants deal with fewer than 50 reports or cases of misconduct each year. Not surprisingly, there is a direct correlation between size of the organization and the number of cases or reports handled. Smaller organizations, with under a thousand employees, typically deal with fewer than 50 cases a year, while organizations with more than 25,000 employees handle between 250 and 499 reports or cases annually.



Copyright © 2007 Corpedia, Inc. and Association of Corporate Counsel

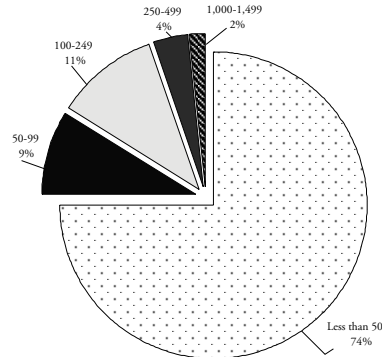
Organizations with 1,000-4,999 Employees

Approximately how many cases/reports of misconduct does your organization handle annually?



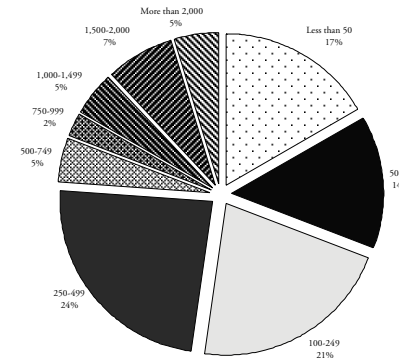
Organizations with 5,000-9,999 Employees

Approximately how many cases/reports of misconduct does your organization handle annually?



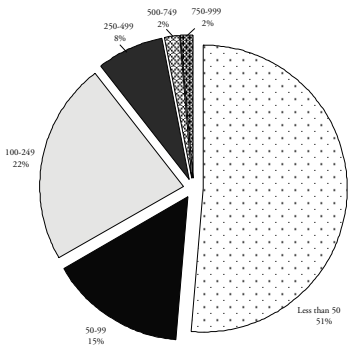
Organizations with 50,000+ Employees

Approximately how many cases/reports of misconduct does your organization handle annually?



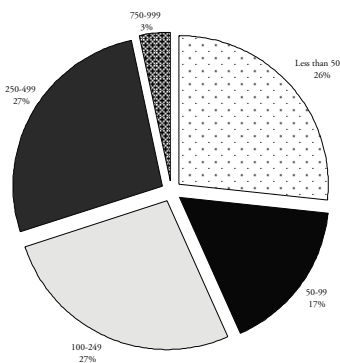
Organizations with 10,000-24,999 Employees

Approximately how many cases/reports of misconduct does your organization handle annually?



Organizations with 25,000-49,000 Employees

Approximately how many cases/reports of misconduct does your organization handle annually?

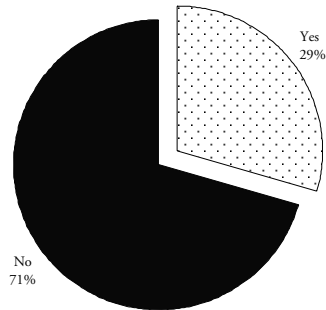


7.4 Organizational Health Surveys

- Only 29 percent of all respondent organizations reported that they regularly conduct organizational health surveys. However, in organizations with operations outside of the US, this number increases to 31 percent. In terms of publicly traded companies, this number jumps to 38 percent.
- For organizations that regularly conduct such surveys, the topics that are commonly measured include "Awareness of the organization's code of conduct" (76 percent), "Executive commitment" (74 percent) and "Supervisor commitment" (71 percent).
- Somewhat surprising is that not many organizational health surveys attempt to measure "Perceived accountability for misconduct" (41 percent) or actual "Misconduct observed in the workplace" (43 percent).

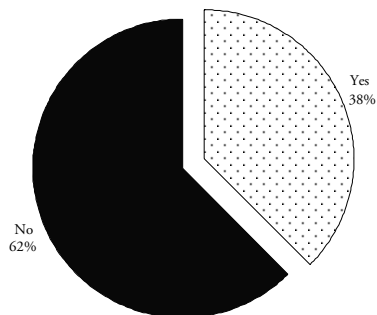
All Survey Participants

Does your organization regularly conduct an organizational health or ethics survey of employees?



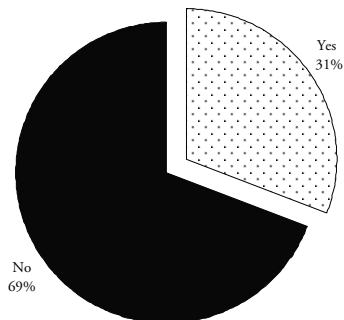
Publicly Traded Companies (USA)

Does your organization regularly conduct an organizational health or ethics survey of employees?

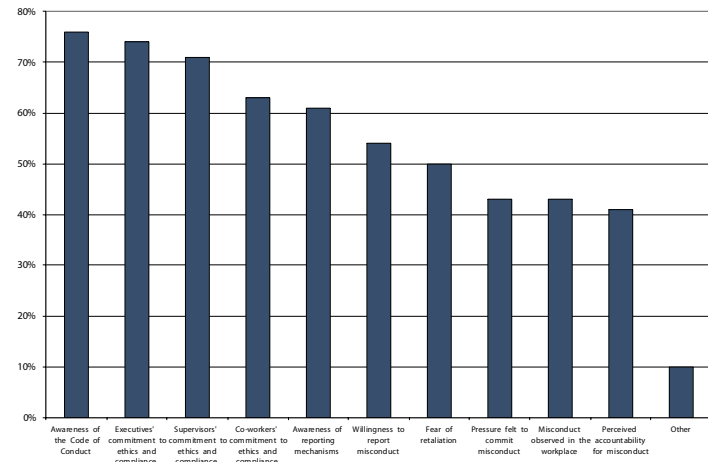


Organizations with Operations Outside USA

Does your organization regularly conduct an organizational health or ethics survey of employees?



Organizations that regularly conduct organizational health surveys address the following topics:



ETHISPHERE Government Contractor Ethics Program Questionnaire

Welcome to the 2009 Government Contractor Ethics Program Ranking, conducted by the Ethisphere Institute in partnership with Ethisphere Magazine. In order to participate in this survey, you must be an authorized representative of an organization that generates at least \$5 million in annual business with the United States Government.

This questionnaire consists of a mix of multiple-choice (both single and multiple-select) and open ended text questions.

Your participation is voluntary. You may skip any question if you so desire, but please remember that our analysis depends on the information you provide. The quality of that information including accuracy and breadth will directly impact your organization's overall ranking.

NOTE: All information in this questionnaire will be confidential. None of your responses will be made public or provided to another organization without your consent.

For your convenience, we have provided you with a hard-copy version of the questionnaire. In terms of completing the survey, you fill it out online by clicking the URL that was provided to you in the invitation email.

If you have any questions or experience technical difficulty or would like to submit the completed questionnaire, via email, please contact _____

Thank you for contributing your time to this valuable project.

GOOD. SMART. BUSINESS. PEOPLE.
ETHISPHERE Government Contractor Ethics Program Questionnaire

Part 1. Respondent Demographics

1. Please provide your name, business title and contact information

Your name _____
 Business title _____
 Email address _____
 Phone number _____

2. Please provide your organization's full name

3. Will you be answering these questions on behalf of the entire organization or only one division? (Select one)

- Entire
 Division only (please enter name of division-5 words _____)

IMPORTANT NOTE: If you selected "Division Only" above, when responding to the remainder of this questionnaire, please assume that all references to "organization" equates to the "division" for which you are responding.

4. Please indicate the type of your organization (Select one)

- Public company
 Private company
 Educational or research institution
 Other (please specify- 5 words)

5. Please select your primary industry (please select only **one** that most closely describes your primary activities)

- Aerospace and defense
 Agriculture, forestry, fishing and hunting
 Banking
 Business services
 Chemicals
 Computer software
 Computer hardware
 Computer services
 Construction
 Consumer products manufacturing
 Consumer
 Education
 Electronics
 Energy, oil and gas
 Environmental services, equipment and remediation
 Financial services
 Food and beverage products manufacturing
 Food service
 Healthcare products
 Healthcare services
 Industrial manufacturing
 Insurance
 Leisure and hospitality
 Media

GOOD. SMART. BUSINESS. PROVE IT.

ETHISPHERE Government Contractor Ethics Program Questionnaire

- Metals and mining
- Non-profit
- Pharmaceuticals and biotechnology
- Professional, scientific and technical services
- Real estate
- Retail
- Security products and services
- Telecommunication equipment
- Telecommunication services
- Transportation and logistics
- Utilities
- Wholesale trade
- Other (please specify- 5 words)_____

6. Please indicate the total size of your organization's workforce (Select one)

- Less than 50 employees
- 50-249 employees
- 250-499 employees
- 500-999 employees
- 1,000-9,999 employees
- 10,000-24,999 employees
- 25,000-49,999 employees
- 50,000-99,000 employees
- 100,000-149,999 employees
- Over 150,000 employees

7. Please indicate the size of your annual business with the U.S. government (Select one)

- \$5-20 million
- \$20-50 million
- \$50-100 million
- \$100-200 million
- \$200-500 million
- \$500 million- \$1 billion
- \$1-2 billion
- \$2-5 billion
- \$5-10 billion
- over \$10 billion

GOOD. SMART. BUSINESS. PROVE.
ETHISPHERE Government Contractor Ethics Program Questionnaire

Part 2 Code of Ethics and Business Conduct

8. Does your organization maintain an organization-wide written Code of Ethics and Business Conduct?

- YES
 NO

Skip logic: If NO, skip the next question

9. Is it available on your organization's internet and/or intranet site? (Select one)

- YES, both Internet and Intranet sites
 YES, but on the Internet site only
 YES, but on the Intranet site only (please email a copy to csindik@ethisphere.org and indicate "[your company name] code" in the subject line)
 NO (please email a copy to csindik@ethisphere.org and indicate "[your company name] code" in the subject line)

Part 3 Leadership and tone from the top

10. Does your organization have a formal compliance and ethics program?

- YES
 NO

11. Please specify the job title(s) of the person given primary responsibility for the compliance and ethics program/initiatives.

(open ended -10 words)

12. To whom does the person with responsibility for the compliance and ethics program/initiatives report? (Please indicate **primary** reporting relationship)

- President/CEO
 General Counsel
 CFO
 Head of Internal Audit
 Board of Directors of a Committee
 Other (please specify) _____ (10 words)

13. How often does the person with responsibility for the compliance and ethics program communicate with the Board of Directors of other Committee?

- QUARTERLY
 ANNUALLY
 OTHER (Please specify- 10 words) _____

14. Please indicate your level of agreement with the following statement:

"The person with responsibility for the compliance program has been given adequate authority and resources to perform the job effectively"

GOOD. SMART. BUSINESS. PROFIT.
ETHISPHERE Government Contractor Ethics Program Questionnaire

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- Not sure

15. Please indicate your level of agreement with the following statement:

"The Board of Directors is actively engaged in your organization's ethics and compliance program"

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- Not sure

16. Please indicate your level of agreement with the following statement:

"The organization's senior executives regularly and consistently communicate with the employees regarding the proper standards of conduct, ethics and compliance"

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- Not sure

17. Please indicate your level of agreement with the following statement:

"Communications from the executive level emphasize the importance of using the U.S. government resources efficiently"

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- Not sure

18. Please indicate your level of agreement with the following statement:

"Communications from the executive level emphasize the importance of using internal whistle-blowing system for reporting misconduct or concerns without fear of retaliation"

GOOD. SMART. BUSINESS. PROOF.
ETHISPHERE Government Contractor Ethics Program Questionnaire

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- Not sure

Part 4 Internal control systems

19. Does your organization maintain policies that address the following issues?
 (Select all that apply)

- Antitrust/competition
- Conflicts of Interest
- Gifts, entertainment and kickbacks
- Working with or hiring former government officials
- Political contributions, activities and lobbying
- Ensuring integrity of agents, consultants and representatives
- Bribery and corruption (FCPA)
- Truth in negotiations
- False claims
- Proper cost accounting (including labor charging)
- Cooperating with the government investigations
- Confidential information including procurement sensitive information and confidential competitor information
- Data privacy (employees, customers and/or consumers)
- Record retention
- Export controls and national security
- Insider trading
- EEO, discrimination and harassment
- Environmental protection
- Workplace health and safety

Please specify any other key policies relevant to your business that are not listed above (50 words)

Open ended text

20. Does your organization require periodic conflict of interest certifications/disclosure from certain employees?

- YES
- NO

Skip logic: if NO, skip the next question.

21. The following employee segments are subject to conflict of interest certification/disclosure in the past 24 months (please select all that apply)

- Executive level
- Vice Presidents
- Directors
- Managers
- All or most employees in sales function

GOOD. SMART. BUSINESS. PROOF.

ETHISPHERE Government Contractor Ethics Program Questionnaire

- All or most employees in procurement function
 All or most employees in finance function
 Other (PLEASE SPECIFY _____ 200 words)

22. Does your organization routinely perform background checks prior to hiring key personnel?

- YES
 NO

23. Does your organization routinely conduct exit interviews as people leave?

- YES
 NO

Skip logic: of NO skip the next question

24. Exit interviews used for the following purposes (select all that apply)

- To obtain information about possible misconduct or policy violations that may have taken place
 To obtain information concerning organizational health and the culture of ethics
 To remind employee about his or her responsibilities regarding confidentiality
 Other (PLEASE SPECIFY _____ 20 words)

25. What mechanisms does your organization use to ensure vendor compliance? (select all that apply)

- Our organization maintains a written vendor code of conduct
 Vendor acknowledgement and compliance with the vendor code is a required condition of doing business with the organization
 Our organization's hotline and other reporting mechanisms are available to use for vendor personnel
 Our organization encourages or requires vendors to maintain an anonymous reporting hotline
 Our organization conducts due diligence when selecting vendors
 Our organization conducts periodic vendor audits to ensure compliance
 Vendors are encouraged or required to obtain a third-party certification for ethics and compliance
 Our organization provides vendors with compliance and ethics training assistance or resources

26. How would you rate the level of oversight of your vendors and subcontractors?

- High
 Above average
 Average (neither high nor low)
 Below average
 Low

27. Does your organization display government fraud hotline poster at its workplace locations?

- YES
 NO
 SOME, BUT NOT ALL

GOOD. SMART. BUSINESS. PROVE.
ETHISPHERE Government Contractor Ethics Program Questionnaire

28. Does your organization have an FCPA compliance program?

- YES
 NO
 NOT APPLICABLE (We do not conduct business outside of the United States)

29. Does your organization conduct due diligence for third-party representatives (e.g. agents, distributors, joint venture partners)?

- YES
 NO
 SOME, BUT NOT ALL (please specify: 50 words)

30. Does your organization maintain a misconduct reporting system (whistle-blower system)?

- YES
 NO

If NO, skip the next 3 questions

31. The reporting mechanism permits the following (Select all that apply):

- Report potential or actual criminal misconduct
 Report potential or actual violations of organizational policy(s)
 Seek guidance regarding ethics and compliance issues
 Express concerns
 Other (PLEASE SPECIFY _____-50 words)

32. Please specify the type of reporting options available (Select all that apply):

- Phone number
 Website
 Email
 "Open door"
 Other (PLEASE SPECIFY _____)

33. Does any of the reporting options allow for anonymity?

- YES
 NO

34. How does your organization handle reports of alleged misconduct?

- Conduct internal investigations of all reports of alleged misconduct
 Conduct internal investigations of those reports that seem credible
 OTHER (please specify- 50 words)

35. Does your organization maintain a clear process for escalating certain types of allegations to senior management, the Board of Directors (or a Committee) or external auditors?

- YES
 NO

36. What kind of misconduct information is reported to the Board of a Committee? (select all that apply)

GOOD. SMART. BUSINESS. PROVE.
ETHISPHERE Government Contractor Ethics Program Questionnaire

- Overall misconduct reporting statistics in periodic (e.g. quarterly) reports
- Details of all key investigations after they have been completed
- Details of all key investigations in progress
- OTHER (please specify- 50 words)

37. Please indicate your level of agreement with the following statement:

"Our organization maintains a well-defined criteria and process for evaluating the internal reports to determine whether formal government disclosure is appropriate and warranted"

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- Not sure

38. Does your organization maintain a non-retaliation policy for a good-faith misconduct reporting?

- YES
- NO

Skip logic: If NO, skip the next question:

39. Please indicate your level of agreement with the following statement:

"Our organization's non-retaliation policy has been clearly communicated to all employees"

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- Not sure

40. Does your organization maintain a written policy and procedures on disciplinary actions?

- YES
- NO

Skip logic: if NO, skip the next question:

ETHISPHERE Government Contractor Ethics Program Questionnaire

41. Please indicate your level of agreement with the following statement:

"The policy and procedures on disciplinary action (for engaging in misconduct) is consistently applied/enforced throughout the organization"

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- Not sure

42. In your organization, is punitive action an option against both the individual who committed the serious misconduct as well as the individual's supervisor?

- YES
- NO

43. Does your organization offer any of the following incentives for employees for engaging in ethical conduct? (please select all that apply)

- Evaluation of ethical business conduct as a part of annual performance reviews
- Evaluation of ethical business conduct as a part of promotion decisions
- Awards and recognitions showcasing ethical business conduct
- Other (please specify- 50 words)

44. Within the past 24 months, has your organization conducted a risk assessment to determine compliance, regulatory and ethics related risks?

- YES
- NO

45. Within the past 24 months, has your organization conducted a formal evaluation or benchmarking of your overall compliance and ethics program/initiative to evaluate its relative effectiveness?

- YES
- NO

Skip logic: If NO, skip the next question

46. Which components of the compliance and ethics program have you evaluated within the past 24 months? (select all that apply)

- Code of Ethics and Business Conduct
- Policies, procedures and controls
- Training and communication
- Organizational health and culture of ethics
- Employee knowledge of compliance and ethics issues relevant to their jobs
- Whistle-blowing system
- Auditing system
- High level oversight
- Other (please specify- 50 words)

GOOD. SMART. BUSINESS. PEOPLE.
ETHISPHERE Government Contractor Ethics Program Questionnaire

47. How would you describe your organization's culture of ethics?

- Very strong
 Strong
 Fair
 Weak
 Very weak

Part 5. Training and communication

48. Does your organization maintain a training plan for ethics and compliance training?

- YES
 NO

49. How would you rate the average level of awareness of Code of Ethics and Business Conduct among employees in your organization?

- High
 Better than average
 Average (neither high nor low)
 Below average
 Low

50. Does your organization offer a dedicated training program on the organization's Code of Ethics and Business Conduct for employees?

- YES
 NO

Skip logic: if NO, skip next 6 questions

51. Please describe briefly the current audience and frequency for Code of Ethics and Business Conduct training as well as an approximate percentage of your total workforce that receive this training.

(open ended: 500 words)

52. Is the Code of Ethics and Business Conduct training mandatory?

- YES, for all employees
 YES, for some, but not all employees (please specify the mandatory groups of employees)
 NO

53. Does your organization track completion of the Code of Ethics and Business Conduct training?

- YES
 NO
 DEPENDS ON THE AUDIENCE

GOOD. SMART. BUSINESS. PEOPLE.
ETHISPHERE Government Contractor Ethics Program Questionnaire

54. Please indicate your level of agreement with the following statement:

"Code of Ethics and Business Conduct training in our organization strongly emphasizes the importance of reporting issues or concerns"

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- Not sure

55. Please indicate your level of agreement with the following statement:

"Code of Ethics and Business Conduct training in our organization properly emphasizes the importance of cooperating with the government investigations"

- Strongly agree
- Agree
- Neutral/not sure
- Disagree
- Strongly disagree
- Not sure

56. Does the Code of Ethics and Business Conduct training in your organization provide learners with a clear guidance on any of the following reporting options?

- Internal reporting options only
- External reporting options only
- Both external and internal options with an equal emphasis
- Both external and internal options with an emphasis on internal options

57. Has the Board of Directors been trained on the Code of Ethics and Business Conduct?

- YES
- NO

58. Beyond the Code of Ethics and Business Conduct training, does your organization offer targeted compliance training on any of the following topics to specific groups of employees? (Select all that apply)

- Antitrust/competition
- Conflicts of Interest
- Gifts, entertainment and kickbacks
- Working with or hiring former government officials
- Political contributions, activities and lobbying
- Ensuring integrity of agents, consultants and representatives
- Bribery and corruption (FCPA)
- Truth in negotiations
- False claims
- Proper cost accounting (including labor charging)

GOOD. SMART. BUSINESS. PROVE.
ETHISPHERE Government Contractor Ethics Program Questionnaire

- Cooperating with the government investigations
- Confidential information including procurement sensitive information and confidential information of competitors
- Data privacy (employees, customers and/or consumers)
- Record retention
- Export controls and national security
- Insider trading
- EEO, discrimination and harassment
- Environmental protection
- Workplace health and safety

59. Does your organization routinely offer ethics and compliance training for third-party representatives, such as agents, and business partners?

- YES
- NO

60. Does your organization routinely communicate with the employees on ethics and compliance training topics outside formal training program?

- YES
- NO

If NO, skip the next question

61. Please briefly describe your organization's ethics and compliance communication initiatives outside formal training program.

(open ended: 500 words)

62. The proposed FAR rule requires contractors to "***have a satisfactory record of integrity and business ethics***". Based on publicly available information, how would you rate your organization's overall record of integrity and business ethics in the past 5 years?

- Superior (better than most peers)
- Average
- Inferior (worse than most peers)
- Not sure/Decline to answer

63. Is there any additional information about your compliance and ethics program initiatives that you wish to share?

(open ended: 1000 words)

ETHISPHERE GOOD. SMART. BUSINESS. PROFIT. Government Contractor Ethics Program Questionnaire

Thank you for completing the survey.

We also encourage you to provide us with additional documents to support your responses and our analysis. Examples of such documents include:

- ***Code of Ethics and Business Conduct***
- ***Examples of employee ethics and compliance communication materials***
- ***Employee handbook***
- ***Vendor Code of Conduct***
- ***Summary of current compliance training curriculum***
- ***Copies of key policies***
- ***Summary results of Employee Surveys (Culture surveys)***
- ***Compliance reports to the Board of Directors or other Committee***

http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/28mcrm.htm US Attorneys Manual 9-28.000 PRINCIPLES OF FEDERAL PROSECUTION OF BUSINESS ORGANIZATIONS

<http://www.acc.com/vl/membersonly/InfoPAK/loader.cfm?csModule=security/getfile&pageid=77637&page=/legalresources/publications/infopaklistings.cfm&qstring=&title=Responding%20to%20Government%20Investigations> Infopak Aug 2008 Responding to Government Investigations – includes Thompson and McNulty memos and discussion of role of compliance programs

<http://www.acc.com/vl/membersonly/InfoPAK/loader.cfm?csModule=security/getfile&pageid=19675&page=/legalresources/publications/infopaklistings.cfm&qstring=startrow=21&title=Internal%20Investigations> (Internal Investigations)

<http://www.acc.com/vl/membersonly/ACCDocketArticle/loader.cfm?csModule=security/getfile&pageid=14543&page=/legalresources/publications/accdocket/archive.cfm&qstring=startrow=241&title=Managing%20an%20Internal%20Corporate%20Fraud%20Investigation%20and%20Prosecution>

<http://www.acc.com/vl/membersonly/SampleFormPolicy/loader.cfm?csModule=security/getfile&pageid=12447&page=/legalresources/forms/index.cfm&qstring=pafilterID=175&title=Internal%20Investigations%20Report%20Form>

<http://www.acc.com/vl/membersonly/SampleFormPolicy/loader.cfm?csModule=security/getfile&pageid=12522&page=/legalresources/forms/index.cfm&qstring=pafilterID=175&title=Sample%20Investigation%20Guidelines>

<http://www.acc.com/vl/membersonly/SampleFormPolicy/loader.cfm?csModule=security/getfile&pageid=12316&page=/legalresources/forms/index.cfm&qstring=startrow=41&pafilterID=5&title=Ethics%20Manual> (Business Conduct Handbook)

<http://www.acc.com/vl/membersonly/SampleFormPolicy/loader.cfm?csModule=security/getfile&pageid=12310&page=/legalresources/forms/index.cfm&qstring=startrow=41&pafilterID=5&title=Gifts%2C%20Gratutities%20%26amp%3B%20Conflicts%20of%20Interest> (Consultant or vendor contract clause regarding conflicts of interest)

<http://www.acc.com/vl/membersonly/QuickReference/loader.cfm?csModule=security/getfile&pageid=16462&page=/legalresources/forms/index.cfm&qstring=startrow=41&pafilterID=5&title=Code%20of%20Business%20Conduct%20and%20Ethics> (Sample Code of Business Conduct)

<http://www.acc.com/vl/membersonly/SampleFormPolicy/loader.cfm?csModule=security/getfile&pageid=12554&page=/legalresources/forms/index.cfm&qstring=startrow=61&pafilterID=5&title=Signature%20Authority%20Form%20> (Signature Authority Policy)

<http://www.acc.com/vl/membersonly/SampleFormPolicy/loader.cfm?csModule=security/getfile&pageid=12588&page=/legalresources/forms/index.cfm&qstring=startrow=81&pafilterID=5&title=Conflict%20of%20Interest%20Policy%20%232> (Conflict of Interest and Gift Policy and Disclosure Forms)

<http://www.acc.com/vl/membersonly/SampleFormPolicy/loader.cfm?csModule=security/getfile&pageid=12689&page=/legalresources/forms/index.cfm&qstring=startrow=81&pafilterID=5&title=Code%20of%20Ethics%20and%20Conflicts%20of%20Interest%20Policy%20for%20Directors%2C%20Officers%20and%20Senior%20Team%20Leaders> (Code of Ethics AND CONFLICTS OF INTEREST POLICY FOR DIRECTORS, OFFICERS AND SENIOR TEAM LEADERS)

<http://www.acc.com/vl/membersonly/SampleFormPolicy/loader.cfm?csModule=security/getfile&pageid=12751&page=/legalresources/resource.cfm&qstring=show=12751&title=International%20Business%20Ethics%20And%20Conduct%20Policy%20> (International Business Ethics and Conduct Policy – Non-Profit)

<http://www.acc.com/vl/membersonly/InfoPAK/loader.cfm?csModule=security/getfile&pageid=19684&page=/legalresources/publications/infopaklistings.cfm&qstring=startrow=61&title=Corporate%20Compliance> (Corporate Compliance Program Development)

<http://www.acc.com/vl/membersonly/InfoPAK/loader.cfm?csModule=security/getfile&pageid=19710&page=/legalresources/publications/infopaklistings.cfm&qstring=startrow=21&title=Compliance%20Training%20and%20E%20Learning%20Programs%3A%20Leading%20Practices%20in%20Designing%2C%20Implementing%2C%20and%20Supporting%20Risk%20Assessment%20and%20Communication%20Strategies> (Compliance Training and E-Learning Programs Leading Practices in Designing, Implementing, and Supporting Risk Assessment and Communication Strategies)

<http://www.acc.com/vl/membersonly/ACCDocketArticle/loader.cfm?csModule=security/getfile&pageid=14371&page=/legalresources/resource.cfm&qstring=show=14371&title=Business%20Ethics%3A%20Ethics%20Resource%20Center%20Sounds%20Alarm%20with%20its%202007%20National%20Business%20Ethics%20Survey> (Short Docket Article)

<http://www.acc.com/vl/membersonly/ACCDocketArticle/loader.cfm?csModule=security/getfile&pageid=14456&page=/legalresources/resource.cfm&qstring=show=14456&title=Business%20Ethics%3A%20The%20Alphabet%20Soup%20of%20Risk%20Management> (Short Docket Article)

<http://www.acc.com/vl/membersonly/ACCDocketArticle/loader.cfm?csModule=security/getfile&pageid=306110&page=/practiceareas/international.cfm&qstring=paid=84&title=1%2E6%20Billion%20Reasons%20to%20Get%20Anti%2DBribery%20Compliance%20Right> (Anti-Bribery Compliance)

<http://www.acc.com/vl/membersonly/ACCDocketArticle/loader.cfm?csModule=security/getfile&pageid=14459&page=/legalresources/resource.cfm&qstring=show=14459&title=The%20Challenges%20of%20Global%20Compliance%20in%20Emerging%20Markets%20> (Compliance in Emerging Markets)

ACC Extras

Supplemental resources available on www.acc.com

What Corporate Counsel Should Remember When the State Attorney General Calls.

QuickCounsel. August 2009

<http://www.acc.com/legalresources/quickcounsel/wccsrwtsage.cfm>

Corporate Compliance.

InfoPak. August 2009

<http://www.acc.com/legalresources/resource.cfm?show=19684>

Effective Corporate Ethics and Compliance Programs.

Program Material. May 2009

<http://www.acc.com/legalresources/resource.cfm?show=358240>

Please note, these additional resources are provided by the Association of Corporate Counsel and not by the faculty of this session.