International Compliance

Dana G. Nahlen
Assistant General Counsel

16 June 2017, for the Academy of American and International Law
What Do We Mean by “Compliance” as a Legal Discipline?

What is Compliance?

- Dictionary: the act or process of complying to a desire, demand, proposal, or regimen or to coercion; conformity in fulfilling official requirements

- Legal Discipline: the establishment of programs to deter and detect wrongful conduct and promote an organizational culture to assure compliance with all applicable laws

Compliance with all applicable law has always been necessary

Increasingly, it is not enough to simply comply with the law, but it is also necessary for a company to be able to establish the controls it has in place to be sure it is complying. Development and administration of those controls is what we mean by “Compliance”.
El implosion de Enron en 2001 y la reacción a los delitos corporativos que surgieron como resultado dejó a los reguladores de EE.UU. y al público en general dudando de la capacidad de las grandes corporaciones para cumplir con la ley aplicable.

- Muchos otros escándalos similares han seguido y han agregado presión para que las empresas tengan programas de cumplimiento adecuados:

  - Volkswagen
  - Takata
  - Arthur Andersen
  - Wells Fargo
Trends in Anti-Corruption Enforcement Show Why Assuring Compliance is Necessary

Total Aggregate Corporate Cases: 2002–2016

Source: Shearman & Sterling FCPA Digest
Total FCPA Cases Over Time by DOJ and SEC
The “Outliers” are cases where the total fines were significantly larger than would be considered normal: Siemens (2008); KBR (2009); BAE, Snamprogetti, and Technip (2010); JGC (2011); Alstom (2014); and Odebrecht/Braskem, Teva, VimpelCom, Och-Ziff, JP Morgan, Embraer (2016).
The US Sentencing Guidelines Set the Standard

➢ The Sentencing Guidelines are the product of the US Sentencing Commission, so they are not binding laws or regulations

➢ The primary goal of the Sentencing Guidelines was to alleviate sentencing disparities in the existing US federal sentencing system

➢ Chapter 8 of the Sentencing Guidelines deals with the sentencing of “Organizations”, first published in 1991 and revised in 2004

➢ The Sentencing Guidelines authorized a significant reduction in penalty for an organization that could demonstrate it had an effective compliance and ethics program in place to prevent and detect criminal conduct

➢ The Sentencing Guidelines include standards for determining the sufficiency of an organization’s compliance program to be considered “effective” and therefore entitled to that reduction in sentence

➢ The Sentencing Guidelines are now recognized as setting the “floor” for effective compliance programs
Is Having a Compliance Program a Legal Defense?

➢ In some jurisdictions: YES
   – UK Bribery Act 2010
   – Mexican anti-corruption laws
   – European anti-money laundering laws
   – Others?

➢ In the US: NO
   – Having an effective compliance program will reduce the penalty in the event of a violation, but by how much is uncertain
   – Development of a compliance program may be ordered as part of the penalty in the event of a violation
   – In determining whether to charge a company, the US Department of Justice will factor in the existence and effectiveness of the organization’s existing compliance program in making that decision
What do the US Sentencing Guidelines Require?

➢ Established standards and procedures to prevent and detect criminal conduct

➢ The organization’s governing authority must accept and exercise responsibilities of oversight

➢ Identification of persons with direct responsibility for the program and adequate resources, authority, and access to the governing authority to assure program effectiveness

➢ Due care in delegation of authority and employee screening

➢ Effective training and communication of compliance standards and procedures

➢ Monitoring and auditing of the effectiveness of the program

➢ A system for employees to report or seek guidance regarding actual / potential violations without fear of retaliation

➢ Consistent enforcement with incentives and discipline

➢ Periodic risk assessments

➢ If criminal conduct is detected, appropriate action to address the violation and prevent future violations
US Sentencing Guidelines Recognize the Compliance Program Must be Custom Tailored to the Company

“The formality and scope of actions that an organization shall take . . . depend on the size of the organization.”

“A large organization generally shall devote more formal operations and greater resources in meeting the requirements of this guideline than shall a small organization.”

“[S]mall organizations shall demonstrate the same degree of commitment to ethical conduct and compliance with the law as large organizations. However, a small organization may meet the requirements of this guideline with less formality and fewer resources than would be expected of large organizations.”
Other Guidance on Compliance Programs

➢ Good Practice Guidance on Internal Controls, Ethics and Compliance, published by the OECD
➢ ISO / DIS 37001, International Standard on Anti-Bribery Management Systems
➢ The COSO Internal Control Framework published by the Treadway Commission
➢ UK Bribery Act 2010 Guidance issued by the UK Ministry of Justice
➢ The Resource Guide to the US Foreign Corrupt Practices Act published by the US Department of Justice and Securities and Exchange Commission
➢ Export Compliance Guidelines published by the US Department of Commerce
➢ New York Stock Exchange Listing Requirements
➢ Sarbanes / Oxley Requirements
➢ The Brazilian Clean Company Act
All the Standards Provide Consistent Advice
Building Blocks of an Effective Ethics & Compliance Program

- Board Oversight
- Responsibility
- Risk Assessment
- Policies & Procedures
- Training & Communications
- Incentives, Investigations, Discipline
- Employee Screening, Selection, Evaluation
- Monitoring, Audit, Modification
US Sentencing Guidelines
Board Oversight

“The organization's governing authority 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.”

“Governing authority" means (A) the Board of Directors; or (B) if the organization does not have a Board of Directors, the highest-level governing body of the organization.”

➢ Under US law, directors can have personal liability for not meeting their assigned responsibilities
“Specific individuals with the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.”

- Most often, if a subgroup of the governing authority is given oversight responsibility it is the Audit Committee of the Board. Such responsibility should be documented in the Board Charter, or in the Audit Committee Charter if delegated.
“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.”

“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.”

Many organizations screen all employees on hire, without establishing criteria for which positions will be considered to have substantial authority.
COSO Framework

The COSO Framework requires that an organization:

➢ Demonstrate a commitment to integrity and ethical values
➢ Ensure that the board exercises oversight responsibility
➢ Establish structures, reporting lines, authorities and responsibilities
What Does that Mean in Practice?

➢ **Board Responsibilities:**
  - Stay informed about risks to the enterprise and the content and operations of the ethics and compliance program
  - Provide oversight of operational implementation of the program
  - Ensure the program functions effectively with adequate resources
  - Understand the board members’ responsibilities to honor the organization’s ethical standards and code of conduct

➢ **Activities this involves:**
  - Attend briefings and training about the compliance program
  - Ask probing questions of senior management
  - Assure the Chief Ethics and Compliance Officer (CECO) has direct access to the Board
  - Meet with the CECO regularly and as needed
  - Serve as role models of ethical and compliant conduct – set the “Tone from the Top”
What Does that Mean in Practice?

➢ Executive Management Responsibilities:
  − Provide leadership for operation of the ethics and compliance program
  − Ensure the ethics and compliance program has adequate resources and sufficient authority within the organization to act as needed
  − Promote and advocate the organization’s ethical values and legal commitments

➢ Activities this involves:
  − Track and use appropriate benchmarks and measures to gauge the effectiveness of the ethics and compliance program
  − Review and approve the program’s annual goals and budget and assure funding and staffing are adequate for the goals
  − Consider the ethical and compliance implications of strategic initiatives, such as acquisitions or the opening of new markets
  − Cultivate an organizational culture that supports ethical decisions
  − Advocate and practice “Tone from the Top”
  − Deal with all violations with promptly and without special treatment
What Does that Mean in Practice?

➢ CECO Responsibilities:
  - Implement the ethics and compliance program and make day to day decisions required by the program
  - Report periodically to senior management and the Board about program effectiveness and activities
  - Determine resources needed to implement and maintain the program

➢ Activities this involves:
  - Determine appropriate benchmarks and measures to gauge the effectiveness of the ethics and compliance program
  - Prioritize training and communication needs
  - Identify emerging issues and trends that present compliance risks
  - Provide the Board and senior management information about program management, accomplishments and results
  - Nurture an organizational culture that supports ethical decisions
  - Model “Tone from the Top”
What is “Tone from the Top” or “Tone from the Middle”?

➢ The Board and, particularly senior management, should have specific goals to communicate the need for compliance and its importance to the organization
- If necessary make communication part of the Key Performance Indicators for Senior Management
- Declare ethics and compliance publicly as a core value of the organization
- Use ethics and compliance as a criteria for determining promotion and/or compensation
- Ensure consistent discipline of all personnel for the same offenses, including senior personnel and best performers
- Encourage personnel to report concerns

➢ Studies show that employees are most significantly influenced by the expectations of their direct management
If You Are, or Advise, the CECO What Do You Report to the Board?

- Your risk assessment findings – whatever they are
- The introduction of new compliance programs or procedures
- Distribution and affirmation of the Code of Conduct
- Distribution and affirmation of other important compliance policies
- Update on investigations that have been disclosed
- Results of communication campaigns and training initiatives
- The number of cases reported, investigated and resolved based on employee reports, by type of allegation
- Budget and resource needs
- Benchmarking results
- Performance metrics
To Whom Should the CECO Report?

➢ Most traditional US response is that the CECO is a lawyer and reports to the General Counsel.

➢ Alternative developing in the financial industry and others is that the CECO is not in Legal and reports to the Chief Risk Officer or the CEO.

➢ Independence of CECO is key. The Board should have hiring / firing decisions and compensation decisions – not executive managers.

➢ An organization should have a set of principles that are documented and control the escalation procedure to executive management and to the Board, considerations include:
  - Potential financial impact
  - Likely reputational harm or adverse publicity
  - Potential for legal or regulatory proceedings
  - Potential for outside investigation
  - Level or rank of individuals involved
  - Egregious, deliberate or willful violations
Governance of an Ethics and Compliance Program

- Executive Committee
- CEO
- General Counsel
- Chief Ethics & Compliance Officer
- Business Conduct Office
- Reporting
- Risk Assessment
- Training
- Communication
- Code of Conduct
- Policies & Procedures
- Inquiries & Investigations
- Hotline
- Conflicts of Interest
- Monitoring & Audit
- Monitor & Audit
- Corporate Social Responsibility
- Product Regulatory Compliance
- Business Conduct Advisory Council
  - Internal Audit, Treasury, Accounting, Asset Protection, Environmental, Human Resources, Product Regulatory

- Board of Directors
- Audit Committee
Building Blocks of an Effective Ethics & Compliance Program

- Board Oversight
- Responsibility
- Risk Assessment
- Policies & Procedures
- Training & Communications
- Incentives, Investigations, Discipline
- Employee Screening, Selection, Evaluation
- Monitoring, Audit, Modification
The US Sentencing Guidelines
Risk Assessment

“The organization shall periodically assess the risk of criminal conduct. . . including assessing the following:

(i) The nature and seriousness of such criminal conduct.

(ii) The likelihood that certain criminal conduct may occur because of the nature of the organization’s business. . .

(iii) The prior history of the organization. The prior history . . . may indicate the types of criminal conduct that it shall take actions to prevent and detect.”

➢ An organization shall “[p]riortitize periodically, as appropriate, the actions taken. . . In order to focus on preventing and detecting the criminal conduct identified. . . as most serious, and most likely, to occur.”
The COSO Framework defines enterprise risk management as a process “designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”
Factors to Consider in Assessing Risk

➢ Size of the organization
➢ Nature of its business
➢ Locations and markets
➢ Organizational structure
➢ Workforce composition
➢ Prior Audit findings
➢ Political environment
➢ Geographic disposition of employees
➢ History of claims and litigation
➢ History of reports to the “hotline”
➢ Applicable laws and regulations

Ownership structure
Reputational vulnerability
Use of third parties
Sales model
Gifts and entertainment
Personal data processed
Controls in place
Industry history
Common practices
Risk Assessment Best Practices

➢ The risk assessment should examine not only the potential for criminal conduct, but also the likelihood that unethical decisions will be made

➢ The risk assessment should result in an action plan to mitigate the high priority risks that are identified

➢ Risk assessments should be conducted regularly to accommodate changes in the business environment as well as changes in law and the organization’s activities

➢ Risks should be prioritized according to the likelihood of occurrence and the seriousness of the impact on the organization, as well as the factors that contribute to the risk

➢ The risk assessment should be kept confidential, and possibly protected by privilege as attorney work product
Risk Analysis for UnivEnergy

- Risk: Anticorruption
- Potential: Antitrust
- Business Impact: Human Rights
- Data Privacy: Export

High Probability of Occurrence

Low Probability of Occurrence
Third Party Risk – A Special Kind of Risk

Vast Third-Party Networks
Median Number of Third Parties per Respondent Company

Expected Growth in Third Parties

- **92%** Companies that will either increase their use of third parties or remain steady in the next twelve months.
- **79%** Companies are currently outsourcing core corporate function or plan to do so in future.
- **5.5%** Expected growth rate in the business process outsourcing market through 2015.

Why We Use Third Parties
Select Benefits of Third-Party Use

- **Cost Savings**
- **Market Access**
- **Increased Speed to Market**
- **Local Expertise**

Source: CEB 2015 Third-Party Risk Diagnostic.
FOCUSED ON ENFORCING STANDARDS

Compliance’s Standard Third-Party Risk Management Process

68% of compliance executives agree that Compliance and Ethics’ most important third-party role is creating and enforcing standards, requirements, and controls.

1. Review Business Justification Form
2. Segment and Conduct Due Diligence
3. Contract, Remediate Risk, and Certify
4. Monitor and Audit
5. Recertify or Terminate Relationship

Source: CEB 2015 Third-Party Risk Diagnostic.
Third Party Due Diligence Review Program Elements

Prerequisite Steps

1. Establish a Due Diligence Process
   - Due Diligence Program Manuals
   - Due Diligence Procedures

2. Understand Business Sponsor Role and Responsibilities
   - Training and Communications for Internal Partners

3. Complete the Business Justification Form
   - Questionnaires for Internal Employees

4. Respond to Due Diligence Questionnaires
   - Questionnaires for Third Parties
   - Onboarding Training

5. Evaluate and Segment Third-Party Risk
   - Risk Criteria

6. Understand Compliance Expectations
   - Third-Party Codes of Conduct
   - Policies and Standards
   - Risk-Specific Training
   - Quick Guides/FAQs
   - Newsletters

7. Certify to Expectations
   - Certification Language

8. Contract with Third Party
   - Contractual Language

9. Monitor and Audit Risk
   - Allegation Reporting Support
   - Risk Assessments
   - Control Assessments
   - Audit Plans

Business Sponsor (Internal Employee)

Third Party

Compliance Program

Source: CEB 2015 Third-Party Risk Diagnostic.
Building Blocks of an Effective Ethics & Compliance Program
US Sentencing Guidelines
Policies and Procedures

“The organization shall establish standards and procedures to prevent and detect criminal conduct”

“‘Standards and procedures’ means standards of conduct and internal controls that are reasonably capable of reducing the likelihood of criminal conduct”

➢ The Control Standards component of the COSO Framework requires written policies and procedures as part of expected internal controls

➢ The Sarbanes-Oxley Act and the listing standards of the New York Stock Exchange and the NASDAQ all require that companies have a public code of conduct addressing certain issues
POLICIES, STANDARDS AND GUIDELINES

POLICY

What
- Code of Conduct
- Anti-Corruption Policy

How
- Vendor Diligence
- Gift Registry

Why
- Approval matrix
- Education

STANDARDS/PROCEDURES/PROCESSES

GUIDELINES
What is a Code of Conduct?

➢ Per Wikipedia.org*:
  − “A set of rules outlining the social norms and rules and responsibilities of, or proper practices for, an individual, party or organization”

➢ Per the International Federation of Accountants**:
  − “Principals, values, standards or rules of behavior that guide the decisions, procedures and systems of an organization in a way that (a) contributes to the welfare of its key stakeholders, and (b) respects the rights of all constituents affected by its operations”

➢ Per most CECOs:
  − The basic foundation of an ethics and compliance program

* en.m.wikipedia.org
** http://www.ifac.org
What Should the Code of Conduct Cover?

- Code of Conduct should instruct employees on the organization’s expectations for employee behavior
- Primary purpose is to assure employees do not act in ways that will create a legal violation by the organization
- Employee relations and ethics issues also addressed
- Summarize or reference the most important policies, rules and laws that cover organization operations
  - Use risk analysis as a guide to what to address
- Advise employees of reporting obligations and mechanisms
- Advise employees of prohibition on retaliation
- Advise employees of consequences of failure to comply
- Must be both comprehensive and comprehensible
Two Basic Models for Policies and Codes of Conduct

➢ Rules Based
  – Focuses on specific rules that apply
  – Focus on penalties for violation of those rules

➢ Values Based
  – Leaves more judgement to the employees on how to comply
  – Focus is on core values of the organization

➢ Most Codes and Policies have elements of both
  – Consider your employee base location and culture
  – Consider what risk areas must be absolutely followed and which ones allow more latitude for compliance
Best Practices for Policies and Codes

➢ Translate into all organization relevant languages
➢ Organize so that relevant portions can be easily identified and reviewed as needed
➢ The Code of Conduct will reference, but does not replace, more detailed and specific policies on high risk issues, such as anti-corruption or privacy
➢ Consider and tailor to the average reading level of the primary target audience within the organization
➢ Code and Policies must be fully adopted, supported and modeled by executive management of the organization – make sure they buy in
➢ Enforceable under local law as the basis for an employment action if violated
➢ Living documents, updated and acknowledged annually
More than One Code of Conduct?

➢ Best practice for the code to apply broadly to all employees/contractors with as few deviations by country, management level or business unit as possible

➢ Common practice to have separate code of conduct for vendors
  - Different issues to address
  - Different authority over constituents
  - Different consequences for violation

➢ Also somewhat common, but less so, to have a separate code of conduct for Board of Directors and/or owners or shareholders

➢ Avoid separate Code of Conduct for management!
Building Blocks of an Effective Ethics & Compliance Program
“The organization shall take reasonable steps to communicate periodically and in a practical manner its standards, procedures and other aspects of its compliance and ethics program. . . by conducting effective training programs and otherwise disseminating information appropriate to [each] individuals’ respective roles and responsibilities.”

➢ Although various categories of employees are listed as required recipients of such training and communication, the Sentencing Guidelines make it clear that all employees must receive some training, as appropriate to their respective roles and responsibilities

➢ Non-employee agents must also be trained, as appropriate
COSO Framework
Training and Communication

The COSO Framework requires that:

➢ The organization obtains or generates and uses relevant, quality information to support the functioning of its internal controls
➢ The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal controls
➢ The organization communicates with external parties regarding matters affecting the functioning of internal controls
Training v. Communication – Both Are Required

- All training and communication must be reviewed carefully to assure it is consistent with the Code of Conduct and other Policies
- Determine training topics based upon the risk assessment
- Communicate frequently and do not be afraid of repetition
- Involve senior leadership in training and communication efforts, even when the Compliance Office writes the message for them
- Frequency and duration of required training must be targeted to the audience, their tools and other demands on their time
- Segment target audience based upon roles and responsibilities
- Vary training delivery methods over time to reach all styles of learning in the same target audience
- Always communicate how to ask questions and make reports
- Provide training and communications in an appropriate language for the audience
Communicate Knowledge, Values, or Both?

➢ Do not fall into the trap of trying to teach everyone the law – everyone you train is not a lawyer, and does not want to be!

➢ Communicate what the target audience needs to do, or not do, in order to stay compliant

➢ Providing hypotheticals, case studies and real-life scenarios similar to situations the target audience will encounter is effective

➢ Real-life problems can be very effectively used in training and communication, but be careful about privilege and privacy

➢ Communicate the rules, but also communicate ethical values and company expectations because there will not be a rule for every situation an employee may encounter

➢ Training and communication must empower employees to make the decisions the organization expects them to make

➢ Live training, in-person or by WebEx, allows questions and discussion relevant to the target audience in addition to the direct training
Create Records of Training and Communication Provided

- To enforce the policies and procedures it may be necessary to establish that training and communication were provided
- Create a record of date, time, duration, participants and all materials used or distributed
- If training is described as mandatory, be prepared to establish full and actual participation by attendees
- Certification requirements may be helpful to establish employee knowledge of requirements in case of a violation, and also to reinforce employee acceptance of the rules
- Use recordings as part of training both for variety and also to leverage for subsequent distribution
Building Blocks of an Effective Ethics & Compliance Program

• Incentives, Investigations and Discipline
US Sentencing Guidelines
Investigations

“After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct. . .”

➢ Investigation of the facts is considered to be the first step in responding appropriately
Who Conducts an Internal Investigation?

➢ There are multiple options:
  − Ethics & Compliance
  − Human Resources
  − Internal Law Department
  − Outside Counsel
  − Specialist Consultant
  − Audit Committee

➢ The best option depends on the circumstances and there is no one right answer:
  − Confidentiality
  − Privilege
  − Independence
  − Language and location
  − Technical needs
Phases of an Internal Investigation

Phase 1: Preliminary Considerations
Phase 2: Planning
Phase 3: Gathering Information
Phase 4: Analysis
Phase 5: Reporting
Phase 6: Closure
Phase 1—Preliminary Considerations

- Who should be involved within the organization?
- Who will require communication or reports?
- Examination of documentation
- Third party involvement
- Policy and procedures
- Rules and regulations
- Privilege
Phase 2—Planning

➢ Are there timing issues?
➢ Document the work plan including:
  - objectives, and
  - scope
➢ Document known facts
➢ Identify witnesses and the order in which they should be interviewed
➢ Clarify responsibilities of each investigative team member
➢ Assure a common understanding of issues to be investigated
Investigations – Phase 3

➢ Discovery process
  – Interviews (including note taking)
  – Email and electronic data review
  – Financial analysis

➢ Documents to consider
  – Public
  – Company

➢ Document control

➢ Digital evidence

➢ Be very cognizant of what you document or write, it should be only the facts without judgement or conclusions
Investigations – Phase 3

- Interviews
  - Understand
  - Substantiate
  - Document
  - Develop leads
  - Corroborate or refute allegations, issues or concerns

- Start with peripheral witnesses and move to target
- Interview in twos, never go alone
- Notes taker should complete draft of notes the same day
- Interviews are not interrogations!
Investigations – Phase 4

➢ Financial analysis
➢ Non-financial analysis
➢ Collaboration and comparison of information
➢ Internal records are used to:
  - Build databases or extract details of financial transactions
  - Build timelines
  - Trace assets, funds and non-monetary transactions
  - Reconstruct books and records
  - Search electronic data for key facts and information
Investigations – Phase 5

➢ Select the requirements for the report
➢ Verbal reports are sometimes sufficient
➢ Written reports are often required
  – Introduction
  – Objective and scope
  – Approach and Analysis
  – Findings and Observations
➢ Always keep in mind that documentation and report could end up in court or disclosed to regulators – limit it to facts only
Investigations – Phase 6

➢ Document Management
  – Storing documentation
  – Evidence retention

➢ Investigation debrief
  – Investigation team
  – Stakeholders
“The organization’s compliance and ethics program shall be promoted and enforced consistently through the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.”

“Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline will be case specific”
Rewards? Discipline? Both?

➢ To build a culture of compliance in an organization you must influence behavior

➢ Rewards and discipline (and their absence) are proven methods to influence behavior

➢ Enforcement of the requirements of your code of conduct and policies is essential

➢ Is it necessary or appropriate to reward an employee for ethical behavior, or is being ethical and following the code of conduct just an expected part of their job?

➢ The DOJ and SEC have been very public that they believe incentives are as important as discipline
Reward and Discipline Best Practices

➢ Be consistent!!
➢ Scrutinize business goals and compensation systems to assure they are not incentivizing unethical or criminal conduct
➢ Coordinate with HR to assure compliance rewards and discipline practices are consistent with other performance issue metrics
➢ Be fair and impartial in all cases at all employee levels
➢ Allow accused employees notice and an opportunity to discuss or explain their actions
➢ Consider if compliance failures by employees are also compliance failures by their manager(s) and act accordingly
➢ Document, track and be prepared to report on disciplinary and reward systems
➢ Communicate, within the limits of privacy, decisions regarding both discipline and rewards
Building Blocks of an Effective Ethics & Compliance Program

- Board Oversight
- Responsibility
- Risk Assessment
- Policies & Procedures
- Training & Communications
- Incentives, Investigations, Discipline
- Employee Screening, Selection, Evaluation
- Monitoring, Audit, Modification
“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 criminal conduct;

(B) to evaluate periodically the effectiveness of the organization’s compliance and ethics program; and

(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 criminal conduct without fear of retaliation.”

“After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization’s compliance and ethics program.”
How the Other Standards Address Mitigation, Audits and Monitoring

➢ The COSO Framework regarding “Monitoring” requires that the organization evaluate and communicate internal control deficiencies in a timely manner to those parties responsible for taking corrective action.


➢ Recent DOJ Guidance on evaluating effective corporate compliance programs lists questions relating to “Analysis and Remediation of Underlying Misconduct” as its first topic. It also lists questions relating to “Continuous Improvement, Periodic Testing and Review” as necessary parts of the evaluation.
Best Practices for Reporting Hot Lines

➢ It is common for several different systems to be provided for employees and agents to make reports, by phone, email, website and other methods

➢ Provide mechanisms to allow employees and agents to make reports in their native language

➢ Retaliation against a “whistleblower” is a serious violation of law in the US for any public company and its worldwide subsidiaries

➢ Reports that are intentionally false or made in bad faith can be punished

➢ Confidentiality and anonymity protection for employee and agent reports are also required by law for publicly traded companies in the US

➢ Timely response to reports received is critical

➢ It is important to track reports received and the organization’s response

➢ Reports are a good source of information for risk assessment and identifying program gaps – you want to receive reports
Dodd-Frank Whistleblowers

- Bounty program administered by the US SEC
- Over US $100 million in bounties has been paid
- To claim bounty whistleblowers must be individuals or groups not convicted of a criminal violation related to the conduct reported
- Protection from retaliation is not extra-territorial, but a bounty can be claimed by non-US whistleblowers who provide qualifying information
- The SEC “shall” pay the reward to a whistleblower if the conditions are met; it is not discretionary
- The amount of the award will be 10 to 30% of fines etc. over US $1 million at SEC discretion based upon stated factors, including cooperation
- Whistleblower remains anonymous until payment if represented by counsel
- Whistleblowers do not have to be employees to qualify for bounty payment
- In fiscal year 2016, the SEC received 4219 whistleblower tips from all 50 states and all its territories as well as 67 foreign nations
Best Practices for Continuous Improvement

- Your compliance program must fit your business to be effective; involve various aspects of the business in your reviews as appropriate
- Assure independence and impartiality in periodic reviews
- Protect results under privilege when feasible and appropriate
- Benchmark program elements against those of similar sized companies in similar industries to the extent possible
- Identify weaknesses *before* they become failures
- Promptly take action to remediate/mitigate weaknesses when they are discovered
- The DOJ/SEC Resource Guide states “a good compliance program should constantly evolve... [T]he idea behind such efforts is... continuous improvement and sustainability”
International Compliance

This presentation relies for both organization and content on *The Ethics and Compliance Handbook*, published by the Ethics and Compliance Officer Association, Copyright © 2008

Questions or Comments?