5 Essential Elements of Corporate Compliance: A Global Template

Paul McNulty, Partner
Stephen Martin, Managing Director

Institute for Enterprise Ethics
Daniels College of Business
University of Denver

September 10, 2012
The Current Enforcement Environment

– Over the past five years, the US Department of Justice and the Securities and Exchange Commission have engaged in unmistakably more vigorous anti-bribery enforcement actions.

– Whistleblowers have increased.

– No company or industry is immune: all companies, especially those with international operations in high-risk jurisdictions, must consider themselves open to scrutiny by authorities.

– A proactive approach is essential in this environment and will ultimately protect an organization’s bottom line. Directors and officers who commit resources to ethics and compliance programs as well as training, monitoring and swift remediation can ultimately save their company from exposure to enormous fines, legal and investigative fees and the steep costs of monitorship.
Why is this important? Risks.

- Significant fines.
- Personal liability (including jail, extradition, director disqualification and loss of employment) not only for those directly involved, but also management and board members.
- Third party damages (e.g., shareholder actions).
- Negative publicity, which can impact reputation and share price and also negatively affect customer base and revenues.
- Costs of investigation and remediation.
Top 20 FCPA Settlements (millions)

<table>
<thead>
<tr>
<th>Company</th>
<th>Settlement (millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siemens</td>
<td>$800</td>
</tr>
<tr>
<td>KBR/Halliburton</td>
<td>$579</td>
</tr>
<tr>
<td>BAE</td>
<td>$400</td>
</tr>
<tr>
<td>ENI S.p.A.</td>
<td>$365</td>
</tr>
<tr>
<td>Technip</td>
<td>$338</td>
</tr>
<tr>
<td>JGC Corporation</td>
<td>$219</td>
</tr>
<tr>
<td>Daimler</td>
<td>$185</td>
</tr>
<tr>
<td>Alcatel-Lucent</td>
<td>$137</td>
</tr>
<tr>
<td>Deutsch / Magyar Telekom</td>
<td>$95</td>
</tr>
<tr>
<td>Panalpina</td>
<td>$82</td>
</tr>
<tr>
<td>Johnson &amp; Johnson</td>
<td>$70</td>
</tr>
<tr>
<td>ABB</td>
<td>$58</td>
</tr>
<tr>
<td>Pride International</td>
<td>$56</td>
</tr>
<tr>
<td>Marubeni Corporation</td>
<td>$54</td>
</tr>
<tr>
<td>Baker Hughes</td>
<td>$44</td>
</tr>
<tr>
<td>Willbros</td>
<td>$32</td>
</tr>
<tr>
<td>Chevron</td>
<td>$30</td>
</tr>
<tr>
<td>Titan</td>
<td>$29</td>
</tr>
<tr>
<td>Bridgestone</td>
<td>$28</td>
</tr>
<tr>
<td>Vetco</td>
<td>$26</td>
</tr>
</tbody>
</table>
Why is this important? Benefits.

– Reduction of compliance violations and related risks.

– Mitigation of risk of enforcement (the “adequate procedures” defense under the UK Bribery Act).

– Reduction of fine levels (US Sentencing Guidelines).

– Fulfills fiduciary duty to stockholders and gives comfort to stakeholders such as customers, employees, as well as to regulators.

– Represents a core component of corporate and social responsibility (CSR) objectives.

– An ounce of prevention is worth a pound of cure. The costs of a compliance program will always be much less than the alternatives.
The Age of Corporate Compliance

– Compliance requirements are routinely inserted into FCPA settlement agreements.

– A company’s pre-existing compliance program is a key factor prosecutors consider when making enforcement decisions.

– General principles about business integrity are no longer enough.
Case Study: Morgan Stanley

- Provides the most recent, and powerful, evidence of the benefits of investing in compliance.
- Morgan Stanley’s pre-existing compliance program was highlighted in press releases and public comments as the biggest reason for the Government’s decision not to prosecute the bank.
- The decision not to prosecute was based on evidence of:
  - Rigorous internal controls
  - Regular training and reminders on FCPA policy and compliance
  - Internal policies addressing the corruption risks associated with the giving of gifts, business entertainment, travel, lodging, meals, charitable contributions and employment, that were updated regularly to reflect regulatory developments and specific risks
  - Compliance program monitoring and auditing
  - Extensive pre-retention due diligence on business partners and stringent controls on payments to business partners
The Essential Elements of Corporate Compliance

- Leadership
- Risk Assessment
- Standards and Controls
- Training and Communication
- Monitoring, Auditing and Response
# The Essential Elements of Corporate Compliance

<table>
<thead>
<tr>
<th>USSG’s 7 Elements of an Effective Compliance Program</th>
<th>13 Good Practices by the OECD on Internal Controls, Ethics, and Compliance</th>
<th>UK’s 6 Principles for “Adequate Procedures”</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Standards and procedures to prevent and detect criminal conduct</td>
<td>1. Risk assessment as basis for effective internal controls and compliance program</td>
<td>1. Proportionate procedures</td>
</tr>
<tr>
<td>2. Leaders understand / oversee the compliance program to verify effectiveness and adequacy of support; specific individuals vested with implementation authority / responsibility</td>
<td>2. Policy that clearly and visibly states bribery is prohibited</td>
<td>2. Top level commitment</td>
</tr>
<tr>
<td>3. Deny leadership positions to people who have engaged in misconduct</td>
<td>3. Training – periodic, documented</td>
<td>3. Risk assessment</td>
</tr>
<tr>
<td>4. Communicate standards and procedures of compliance program, and conduct effective training</td>
<td>4. Responsibility – individuals at all levels should be responsible for monitoring</td>
<td>4. Due diligence</td>
</tr>
<tr>
<td>5. Monitor and audit; maintain reporting mechanism</td>
<td>5. Support from senior management – strong, explicit and visible</td>
<td>5. Communication</td>
</tr>
<tr>
<td>6. Provide incentives; discipline misconduct</td>
<td>6. Oversight by senior corporate officers with sufficient resources, authority, and access to Board</td>
<td>6. Monitoring and review</td>
</tr>
<tr>
<td>7. Respond quickly to allegations and modify program</td>
<td>7. Specific risk areas – promulgation and implementation programs to address key issues</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> A general provision requires periodic assessment of risk of criminal conduct and appropriate steps to design, implement, or modify each element to reduce risk</td>
<td>8. Business partners due diligence</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. Accounting – effective internal controls for accurate books and records</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10. Guidance – provision of advice to ensure compliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11. Reporting violations confidentially with no retaliation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12. Discipline for violations of policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13. Re-assessment – regular review and necessary revisions</td>
<td></td>
</tr>
</tbody>
</table>
Meeting the Government’s Expectations

– Guidelines and statutes vary in length, tone and detail, depending on the jurisdiction and the enforcement agency.

– They all, however, describe concepts that can be boiled down to 5 Essential Elements:
  – Leadership
  – Risk Assessment
  – Standards & Controls
  – Training & Communication
  – Oversight
1 Leadership
Beyond “Tone at the Top”

- A successful compliance program must be built on a solid foundation of ethics that are fully and openly endorsed by senior management; otherwise, the program may amount to little more than a hollow set of internal rules and regulations. There should be an unambiguous, visible and active commitment to compliance.

- But compliance standards require even more than support or “tone” from the top. Companies must have high-ranking compliance officers with the authority and resources to manage the program on a day-to-day basis. And compliance officers must have the ear of those ultimately responsible for corporate conduct, including the board of directors.
Leadership: Roles and Responsibilities

Questions to ask:

– How is board oversight implemented? Is there an ethics or audit committee reporting to the full board?

– What is the role of the Chief Compliance Officer?

– Of the General Counsel?

– How do the legal and compliance departments interact?

– Does the CCO have “real power”? Is she or he treated as a second-class citizen?
Leadership: What Regulatory Guidelines Say

- USSG: Leaders understand and oversee the compliance program to verify its effectiveness; specific individuals have the authority and responsibility to carry out the program. The company denies leadership positions to people who have engaged in misconduct.

- OECD: Support from senior management is strong, explicit and visible. Program is overseen by senior corporate offices with sufficient resources, authority and access to the board.

- UK’s 6 Principles: Top-level commitment.
Board of Directors’ Governance Responsibilities

– Ensure compliance policies, systems and procedures in place.
– Monitor implementation and effectiveness of compliance program:
  – Be actively involved
  – Attend Board meetings
  – Review, consider and evaluate information provided
  – Inquire further when presented with questionable circumstances or potential issues
– Once Board knows of a potential compliance issue it must act.
– Regularly receive compliance briefings and training.
Structure of Compliance

- Chief compliance officer:
  - High ranking
  - Dedicated to compliance and responsible for day-to-day management and oversight of compliance program
  - Direct access to the Board or appropriate Board committee
  - Provided sufficient resources
- Compliance officers in high-risk markets.
- Global compliance committees or task forces.
- Regularly communicate with managers in the field.
Compliance Communications from Leadership

- Companies should have in place an active program to communicate the importance of compliance:
  - Annual meetings
  - Annual reports
  - Employee newsletters
  - Management conferences and retreats
  - Large employee gatherings or town halls
- Companies should also regularly assess the effectiveness of communications on the importance of compliance.
Recommendation I

Make sure central compliance is communicating with those in the field.

– Country managers are often the employees in the trenches and are responsible for overseeing sales people and third-party agents who are producing, selling and distributing the company’s products and services.

– Local managers are often in the best position to set the tone for compliance and to detect and address illegal or unethical practices before they become issues that put the company at risk.
Recommendation II

Place compliance officers in high-risk markets.

– A leadership structure that is too centralized will stifle efforts to foster a healthy compliance cultures across all geographies and minimize global risk.

– Critical to success is buy-in from local managers who have the training and experience to reinforce rules.

– Begin by building an active presence of trained compliance managers in markets with greatest bribery risk.
Recommendation III

Create a global compliance committee.

– Should be comprised of trained leadership from central compliance department, country managers and local compliance officers working in foreign offices.

– Hold regular (at least bi-monthly) conference calls to keep members aware of potential problems and what is being done to address them. Global communication on a consistent basis can foster a culture of compliance permeating the entire organization.
Risk assessment
Implementing an effective corporate compliance program is more than following accounting rules or providing FCPA training.

Compliance touches all aspects of your business. Within each category there are all kinds of issues a company must tackle to stay out of trouble with anti-corruption authorities. With so many pieces in the puzzle, how do you know which areas to focus on first? By providing a big-picture view of your compliance obligations, we help you identify your areas of vulnerability and prioritize those areas so you can tackle them first — using your resources most effectively to minimize risk.
Risk Environment

Compliance Risks

Data
- Child Protection
- Data Breach
- Data Collection/Transfer
- Data Integrity
- Data Protection/Privacy
- Records Management
- Security

Design & Production
- Domestic Commerce
- Environmental Export Controls
- Intellectual Property
- Product Safety
- Trade Sanctions
- Transfer Pricing
- Workplace Safety

Distribution
- Agents/Distributors
- Benches
- Corporate Practices
- Customs
- Export Controls
- Franchising
- Import Licensing
- Parallel Importing
- Trade Sanctions

Financial
- Corrupt Practices
- Emissions Trading
- Financial Controls
- Foreign Exchange
- Pricing
- Securities
- Tax

Governance & Structure
- Board of Directors
- Compliance Programs
- Corporate Structure
- CSR Policies
- Fiduciary Obligations
- Transactional Issues

People
- Compensation & Incentives
- Disability/Discrimination
- Data Protection/Privacy
- Employee Monitoring
- Harassment/Retaliation
- Labor Relations
- Mergers/Divestitures
- Pensions & Benefits
- Recruiting & Hiring
- Workplace Change

Sales & Marketing
- Advertising/Publication
- Antitrust/Competition
- Consumer Protection
- Corruption Practices
- Government Contracting
- Packaging
- Pricing
Potential Work Streams: Finance

**Accounting**
- Subsidiaries
- Joint Ventures
- Levels of Authority
- Regional Controls
- Reporting

**Sox Compliance**
- Internal Controls
- Disclosure Controls
- Auditor Independence

**Tax Planning & Compliance**
- State & Local Taxes (SALT)
- Federal Tax Filings
- Foreign Account Reporting
- Payroll Taxes
- Transfer Pricing
- Tax Planning & Transactions
- VAT/Sales & Use

**Contract Management**
- Customer Contracts
- Supplier Contracts
- Terms & Conditions Oversight

**Standards and Controls**
- Control of Assets
- Systems
- Property/Inventory Management

**Treasury**
- Cash Management
- Bank Accounts/Authority
- Hedging/Derivatives
- Credit Arrangements
- Disbursements & Collections
- Investing & Asset Management
- Capital Formation
Potential Work Streams: Corporate Governance

**Audit**
- Audit Committee & Scope
- Functions and Reporting
- Resources

**Board Practices**
- Auditor Interaction
- Board Committee Charters
- By-laws and Articles
- Capital Structure
- Conflicts of Interest
- Director Responsibility
- Fiduciary Activities
- Management Structure and Oversight
- Processes/Reporting
- Succession Planning
- Special Committees
- Standing Committees
- Subsidiary Oversight

**Ethics & Compliance Program**
- Policies
- Compliance (Code of Conduct, Investigations, Reporting)
- Periodic Compliance Program Review
- Risk Assessments
- Regulatory Environment Review
- Training Programs

**Information Technology**
- Internal Systems Licensing
- System Integrity
- Reporting

**Investor Relations**
- Business Reporting & Disclosures
- Annual Filings
- Corporate Communications
- Crisis Management

**Legal Department**
- Organizational Structure
- Scope of Authority
- Litigation

**International Governance Structures**

**Public Company Requirements**
- Corporate Structure
- Disclosure Controls
- Insider Trading Policy
- Related Party Transaction Policy
- Section 16 Reporting Process
- Tax Planning & Compliance

**Risk Management**
- Board Role
- Senior Management Role
- Subsidiary Program Management
- Document Retention Program
- Environmental/Corporate Social Responsibility
- Health & Safety
- Insurance
- Privacy
- Records Management
- Corporate Security
Potential Work Streams: People

Benefits & Pensions
- Health, Life, Disability
- Retirement
- Pensions
- ERISA
- Social Security
- Plan Administration

Immigration
- Visa and Work Permits
- Executive Transfer
- Expatriate Assignments

Compensation & Incentives
- Executive Compensation
- Incentive Plans
- Deferred Compensation
- Change in Control Agreements
- Global Equity Plans
- Sales and Commission Structures

Labor Relations
- Labor (Strategy, Union Elections, Collective Bargaining)
- Works Councils
- Work Rules Compliance
- Grievances
- Notification and Consulting
- Wage & Hour

Human Resources Department
- Organizational Structure
- Resources
- Oversight of Subsidiary Operations
- Workplace Change

Policies and Procedures
- Employee Handbook
- Transfers
- Leave Policies & Rights
- Employee Screening
- Employee Loyalty
- Consulting Agreements
- Due Diligence

Phase 1
Phase 2
Phase 3
Phase 4
## Potential Work Streams: Commercial Operations

### Anti-trust
- Abuse of Dominance
- Territorial Restrictions
- Resale Price Maintenance
- Price Fixing/Bid Rigging
- Market Allocation
- Predatory Pricing
- Trade Group Activity
- Competitor Communication

### Intellectual Property
- Licensing
- Infringement
- Patents
- Trademarks
- Trade Secrets

### M&A
- Due Diligence
- Integration

### Sales & Marketing
- Advertising/Promotion
- Branding
- Channel Management
- Customer Service
- Pricing
- Product Liability/Warranty
- Sales Management
- E-Marketing/Telemarketing

### Joint Ventures
- Due Diligence
- Controls
- Accounting/Reporting
- Systems
- Compliance Programs
- Auditing/Certification

### Supply Chain
- Production Distribution
- Research & Development
- Purchasing
- Manufacturing/Service
- Quality
- Auditing/Certification

### Third Party Agents
- Due Diligence
- Compensation Processing
- Training
- Auditing/Certification

### FCPA/Anti-corruption
- Anti-Money Laundering

### Intellectual Property
- Licensing
- Infringement
- Patents
- Trademarks
- Trade Secrets

### M&A
- Due Diligence
- Integration

### Sales & Marketing
- Advertising/Promotion
- Branding
- Channel Management
- Customer Service
- Pricing
- Product Liability/Warranty
- Sales Management
- E-Marketing/Telemarketing

### Joint Ventures
- Due Diligence
- Controls
- Accounting/Reporting
- Systems
- Compliance Programs
- Auditing/Certification

### Supply Chain
- Production Distribution
- Research & Development
- Purchasing
- Manufacturing/Service
- Quality
- Auditing/Certification

### Third Party Agents
- Due Diligence
- Compensation Processing
- Training
- Auditing/Certification

### Governmental Relationships
- Government Contracting
- Lobbying
- Political Contributions

### Trade Compliance
- Customs
- Import/Export
- OFAC
What are the risk factors your company faces?

**Country Risk**
- Correlation between growth markets and corruption risk
- Perceived level of corruption

**Sectoral Risk**
- Has government publicly stated industry is under scrutiny or already conducted investigations in sector?
- Are there corruption risks particular to the industry?

**Business Opportunity Risk**
- High value projects
- Multiple contractors or intermediaries
What are the risk factors your company faces?

Business Partnership Risk
- Government relationships
- Reliance on third parties

Transaction Risk
- Political/charitable contributions
- Licenses and permits
The Role of Globalization

– In 1991, the US Sentencing Commission did not specifically identify the completion of a formal risk assessment as essential to compliance. Today, however, government officials routine identify risk assessments as a cornerstone of an effective program.

– Why? As multinationals have grown more dependent on supply chain, knowing and understanding the nature of business risks has become a critical first step in developing compliance plans.

– Enforcement authorities increasingly expect companies to have formal processes for periodic assessment of compliance risks everywhere they do business.
Risk Assessment: What Regulatory Guidelines Say

- USSG: Companies must conduct periodic assessments of risk of criminal conduct and take appropriate steps to design, implement or modify each element to reduce risk.

- OECD: Risk assessment should be the basis for effective internal controls and the compliance program.

- UK’s 6 Principles: Broad categories of risk must be carefully examined, including country, sectoral, transaction, business opportunity and partnerships. Program priorities, resources and controls should be determined based on results of risk assessment.
Recommendation I

Conduct annual risk assessments.

– Strong preventive measure if done before something goes wrong.

– Enforcement trends and government priorities change rapidly. It’s vital to stay up to date and conduct regular assessments.

– Avoid a “wait and see” approach.
Recommendation II

Build this annual risk assessment into your company’s compliance program.

– Risk assessments should be a regular, systemic part of compliance efforts rather than an occasional, ad hoc exercise cobbled together when convenient or after a crisis.

– Conduct risk assessments at the same time every year and deputize a consistent group, such as your internal audit department or enterprise risk management team, to conduct the annual review.

– Understand the array of compliance risk faced by the company and undertake a comprehensive review.
Recommendation III

Scrutinize new business partners and third-party agents.

– Today, the majority of FCPA/anti-corruption investigations and enforcement actions involve some use of third parties, including consultants, distributors, contractors and sales agents.

– Conducting a formal risk assessment each year provides an opportunity to take a closer look at recently-established business relationships to make sure partners and third parties do not have improper connections to government officials or some involvement in unethical or illegal conduct.

– Proactively address and remediate any risks that are uncovered.
Recommendation IV

Update policies and procedures based on enforcement trends.

- Paying attention to the types of enforcement actions the government is targeting can tell a lot about what your compliance program needs to focus on to avoid government scrutiny.
Recommendation V

Memorialize risk assessment findings in an internal annual reporting process.

– While an initial formal risk assessment will likely take longer, when conducted every year, subsequent risk assessments may require only three to four weeks to complete, depending on the size of the company, its available compliance resources, and related factors.

– Once the assessment is complete, the compliance or audit team should carefully compile its findings and recommendations in a comprehensive report to be presented to the chief compliance officer and board of directors for review and consideration of appropriate program enhancement actions.
Risk Assessments: Methodology

- Questionnaires
- Interviews
- Use of existing internal resources, for example internal audit reports
- Review of existing systems and controls
- Responsibility for assessment: internal vs. external; business, legal, compliance, internal audit, finance
- Using lawyers as it is privileged
Risk Assessments: Output

– Consider carefully the addressees of full risk assessment

– Use of a summary report for other stakeholders, including the board and senior management

– Outline your methodology and be clear on scope and limits of assessment

– Use risk matrices to grade risks into categories

– Identify areas of uncertainty and those requiring further assessment

– Put together timetable for updating risk assessments
12 Common Pitfalls

- Expectations (unclear, undefined, unrealistic)
- Unrealistic deadlines
- Lack of resources
- Ownership
- Coordination
- Lack of objectivity, credibility
- Qualitative skew
- Narrow and deep vs. shallow and wide
- Document availability (e.g., policies)
- Too much focus on the perceived “priority” risks
- Lack of follow through
- One-time event
9 Tips for Success...and to Stay Sane!

- Don’t rush into it – “lite” may be possible first
- Use outcomes to improve program structure and focus
- Use it to prove program efficiency, not vice-versa
- Strive for objectivity - open-ended questions (3x rule)
- Document structure is key
- Know what the measures will be
- Message clear, concise and unique from Internal Audit
- Cross-pollinate non-compliance ideas and feedback – you are in a unique facilitating position
- Be prepared to deal with what you find – and steer leadership accordingly in ADVANCE
# Recommended Compliance Initiatives

<table>
<thead>
<tr>
<th>Compliance Area</th>
<th>Proposed initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 PCI Compliance/Network Security</td>
<td>- 1a. PCI Compliance</td>
</tr>
<tr>
<td></td>
<td>- 1b. Network Security Controls</td>
</tr>
<tr>
<td>2 Disaster Recovery/Business Continuity</td>
<td>- 2. System Integrity Review/Assurance</td>
</tr>
<tr>
<td>3 Fraud Prevention</td>
<td>- 3. Fraud Prevention Controls</td>
</tr>
<tr>
<td>4 Data Protection/Privacy</td>
<td>- 4. In-Depth Data Protection/Privacy Review</td>
</tr>
<tr>
<td>5 Code of Conduct</td>
<td>- 5a. Update &amp; Revise Code</td>
</tr>
<tr>
<td></td>
<td>- 5b. Expand Code Topics/Risk Areas</td>
</tr>
<tr>
<td>6 Corporate Compliance Policies/Procedures</td>
<td>- 6. Update &amp; Revise Policies</td>
</tr>
<tr>
<td>7 FCPA/Anti-Bribery/Competition/OFAC/Customs</td>
<td>- 7. Compliance Risk</td>
</tr>
<tr>
<td></td>
<td>International/Regional Review</td>
</tr>
<tr>
<td>8 Compliance Training</td>
<td>- 8a. Code Training &amp; Certification</td>
</tr>
<tr>
<td></td>
<td>- 8b. Targeted Compliance Training (including FCPA/Anti-Bribery &amp; Competition Training)</td>
</tr>
<tr>
<td>9 Supplier/Vendor Compliance Program</td>
<td>- 9a. Supplier/Vendor Code of Conduct</td>
</tr>
<tr>
<td></td>
<td>- 9b. Vendor Screening &amp; On-Boarding</td>
</tr>
<tr>
<td>10 Corporate Compliance Program Plan</td>
<td>- 10a. Compliance Program Plan</td>
</tr>
<tr>
<td></td>
<td>- 10b. “Whistleblower” Policy &amp; Hotline</td>
</tr>
<tr>
<td>11 Record Retention</td>
<td>- 11. Record Retention</td>
</tr>
<tr>
<td>12 Risk Assessment</td>
<td>- 12. Risk Assessment Review</td>
</tr>
</tbody>
</table>
## Initiative Scoring: Implementation versus Impact

<table>
<thead>
<tr>
<th>Difficult to implement</th>
<th>Medium</th>
<th>Easy to implement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High impact</strong></td>
<td><strong>Medium</strong></td>
<td><strong>Low impact</strong></td>
</tr>
<tr>
<td>1a. PCI Compliance</td>
<td>9c. Audit/Monitor High Risk Vendors</td>
<td>8c. Compliance Training Log</td>
</tr>
<tr>
<td>1b. Network Security Controls</td>
<td>11. Record Retention</td>
<td></td>
</tr>
<tr>
<td>3. Fraud Prevention</td>
<td>7. Compliance Risk Int’l/Regional Review</td>
<td></td>
</tr>
<tr>
<td>5b. Expand Code Topics/Risk Areas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8b. Targeted Compliance Training</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9a. Supplier/Vendor Code of Conduct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9b. Vendor Screening &amp; On-Boarding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10b. “Whistleblower” Policy &amp; Hotline</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Impact:**
- High impact
- Medium
- Low impact

**Difficult to implement:**
- Easy to implement
## Compliance Initiatives: Prioritized Based on Risk

<table>
<thead>
<tr>
<th>GOAL</th>
<th>RELEVANT INITIATIVES</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target high risk areas</strong></td>
<td>1a. PCI Compliance; 1b. Network Security Controls; 2. Disaster Recovery/Business Continuity Review; 3. Fraud Prevention Controls</td>
<td>Implement recommendations in PCI DSS Preliminary Assessment for all environments that process card data — Conduct broader review of information security protections for non-PCI categories of sensitive personal data — Ensure effectiveness of network security and disaster recovery/business continuity controls — Complete implementation of fraud prevention recommendations and conduct updated review</td>
</tr>
<tr>
<td><strong>Confirm compliance</strong></td>
<td>4. Data Protection/Privacy Review</td>
<td>Conduct in-depth review of data protection/privacy controls to: confirm compliance with Safe Harbor obligations and that compliance can be substantiated to the FTC through policies, procedures and vendor agreements; confirm advances into digital marketing are in compliance with domestic and international privacy requirements; check ABC BU and ABC Co website privacy policies against Safe Harbor and high risk jurisdictions; address international privacy restrictions on processing of internal human resources data, including registrations with data protection authorities</td>
</tr>
<tr>
<td><strong>Acknowledge international expansion</strong></td>
<td>5a. Update &amp; Revise Code; 5b. Expand Code Topics/Risk Areas; 6. Update &amp; Revise Policies; 7. Compliance Risk Int’l/Regional Review</td>
<td>Update breach guide to reflect international notification requirements and ABC Co practices — Update and expand Code topics/risk areas to reflect new international operations — Edit and revise policies and training to ensure consistency in documents across compliance program — Conduct high-level, regional review of target risk areas to ensure current compliance</td>
</tr>
<tr>
<td><strong>Target &amp; track</strong></td>
<td>8a. Code Training &amp; Certification; 8b. Targeted Compliance Training; 8c. Compliance Training Log;</td>
<td>Establish annual Code training, certification and tracking — Enhance plan for targeted training (including updating anti-corruption and competition training for 2012-13) — Link Training Log with training documents/attendance by employees</td>
</tr>
<tr>
<td><strong>Develop and document new programs</strong></td>
<td>9a. Supplier/Vendor Code of Conduct; 9b. Vendor Screening &amp; On-Boarding; 9c. Audit/Monitor High Risk Vendors</td>
<td>Consider creating supplier/vendor code of conduct with certification — Organize and fully document vendor on-boarding and screening program/documents across all regions — Create auditing/monitoring plan for high risk areas/vendors</td>
</tr>
<tr>
<td><strong>Redefine &amp; update existing programs</strong></td>
<td>10a. Compliance Program Plan; 10b. “Whistleblower” Policy &amp; Hotline</td>
<td>Create 1-3 year plan for proactive next steps in compliance program work done by Company — Enhance “whistleblower” policy and hotline for international expansion</td>
</tr>
<tr>
<td><strong>Comprehensive program review</strong></td>
<td>11. Record Retention; 12. Risk Assessment Review</td>
<td>Validate record storage retention policy against regulatory requirements — Conduct Compliance Risk Assessment Review in 2013; Consider 3rd party review in combination with Internal Audit due to resource constraints</td>
</tr>
</tbody>
</table>
3 Standards and controls
Three Layers of Standards and Controls

- Every company should have a Code of Conduct, but this is not enough.

- Companies should also have standards in place that build upon the foundation of the Code and articulate Code-based policies.

- Companies should then ensure procedures are implemented to put these policies into effect.
Beyond a Code of Conduct

– Besides a flagship code of conduct, today’s corporations should employ detailed written policies covering issues such as bribery, corruption and accounting practices, as well as clear procedures and protocols for making sure those policies are followed and enforced.

– Best practices now require companies to have additional standards and controls, including, for example, detailed due diligence protocols for screening third-party business partners for criminal backgrounds, financial stability and improper associations with government agencies.

– Ultimately, the purpose of establishing effective standards and controls is to demonstrate that your compliance program is more than just words on a piece of paper.
Standards & Controls: What Regulatory Guidelines Say

**USSG:** Companies should have standards and procedures to prevent and detect criminal conduct. They should provide incentives and discipline misconduct.

**OECD:** Company policy should clearly and visibly state that bribery is prohibited. Compliance programs should address key risk areas. Companies should conduct due diligence on business partners and implement effective internal controls for accurate books and records. Employees should be able to report violations confidentially without fear of retaliation.

**UK’s 6 Principles:** Policies and procedures should be clear, practical and accessible. Companies should have due diligence protocols for screening third-party intermediaries.
Code of Conduct

- Top-line expression of a company’s core values and business ethics.

- A binding set of principles that applies to several components of a company’s business practices including for example:
  - Employees
  - Business partners
  - Customers
  - Regulators
Suggested Compliance Policies

- Anti-bribery: public officials (corruption); private parties (commercial bribery); gifts, entertainment & hospitality
- Accounting, tax
- Anti-money laundering
- Trade/export limitations
- Insider trading
- Ethics/conflicts of interest
- Anti-discrimination (human resources & employment)
- Whistleblower protections, hotlines
- Immigration
- Environment, health and workplace safety
- Data and personal privacy
- Political, charitable contributions
Recommended Procedures

- Example: Anti-bribery and corruption:
  - Screening of suppliers, agents and other business partners
    - Questionnaires, publicly available data
    - Compliance covenants and certifications; right to audit
  - Pre-acquisition due diligence
  - Post-closing due diligence; integration and training
  - Oversight of gifts, entertainment and hospitality
  - Accounting: accurate books and records (FCPA)
  - Whistle-blowing/escalation procedures
  - Investigation procedures, including dawn raids
Recommendation I

Establish stringent protocols for screening business partners and third parties.

– Some companies still give their business partners only a cursory look — a considerable oversight considering that most government investigations involve allegations of impropriety by a company’s third-party agents.

– To conduct proper due diligence, companies must require third parties and other business partners to complete background questionnaires detailing, among other things, their financial stability, foreign government ties and any history of investigations.

– Third parties should declare their commitment to robust corporate compliance in a signed certification form. To increase accountability we also recommend using business sponsor forms.
A Checklist for Third Party Screening

Necessity: Do we need the third party?

Qualification: Is the third party qualified? Competent/experienced?

Reasonableness of Compensation: How is the compensation commensurate with services provided? How does it compare to other benchmarks, such as industry practice or our practice in comparable situations?

Integrity: Who is the third party? What does the third party request?
Recommendation II

Conduct background checks on important business partners in high-risk markets.

- This can be expensive but it is important to ensure key business partners have represented themselves accurately in paperwork.

- When necessary, consider hiring trained, local investigators to get a clear picture of whether a potential business partner might be a compliance liability.
Recommendation III

Include strict compliance covenants in third-party agreements.

– At a minimum, compliance covenants should cover three core concerns: adherence to the FCPA and other international anti-corruption laws, audit rights, and contract termination rights.

– More specifically, these provisions should require the business partner to agree not to violate the FCPA and other anticorruption laws, to give the company the right to review the partner’s books and records, and to enable the company to terminate the contract if it later determines the partner is engaged in misconduct, unethical behavior or illegal activity.
Recommendation IV

Establish internal controls to ensure accounting records are accurate.

- The FCPA requires companies to book transactions correctly by securing receipts and accurately recording the date and amount of the payment.

- Reconcile bank accounts with outgoing and incoming payments every month and inquire into any suspicious payments and missing funds that could indicate misappropriation or off-the-books transactions.

- Pay particular attention to transactions with consultants and business development agents, customs payments, charitable giving arrangements, and gifts and hospitality involving government officials.
Recommendation V

Provide clear guidelines for gift-giving and hospitality.

- Differences in culture and economic prosperity can make it difficult for companies to establish standard “one size fits all” gift-giving and hospitality guidelines for the countries where they conduct business.

- Tailor hospitality policies to individual countries. Companies can do this in any number of ways, including the creation of a thresholds table of allowable hospitality amounts in the countries where they operate, and is based on local laws and regulations in each country plus advice from experienced local counsel.
Training
Training: Is Your Message Getting Through?

- Another pillar of a strong compliance program is properly training company officers, employees and third parties on relevant laws, regulations, corporate policies and prohibited conduct.

- Simply conducting training usually isn’t enough. Enforcement officials want to be certain the messages in the training actually get through to employees.

- The government’s expectations of effectiveness are measured by who a company trains, how the training is conducted and how often training occurs.
Training: What the Regulatory Guidelines Say

**USSG:** Companies must communicate the standards and procedures of its compliance program and conduct effective training.

**OECD:** Training should be periodic, consistent, and documented.

**UK’s 6 Principles:** Effective implementation of compliance program policies and procedures through adequate training.
Recommendation I

Train the right people.

- Prioritize which audience to educate.

- Start your training program in higher risk markets and focus on directors, officers and sales employees who may have direct contact with government officials or deal with state-owned entities.

- Again, focus initially on training country managers in your company's high-risk markets, then expand geographically and through the ranks of employees.
Recommendation II

Conduct live, annual training in high-risk markets.

- Enforcement officials have made it clear that live, in-person training is the preferred method in high-risk markets and also that it should be regular and frequent.

- Another benefit of live training is the immediate feedback from employees that would be much less likely to occur during a webinar or other remote training.

- Furthermore, during live training, employees are more likely to make casual mention of a potentially risky practice, giving you the opportunity to address it before it becomes a larger problem.
Recommendation III
Tailor your training to each country.

– Employing a generic script for compliance training is a mistake.

– To be effective, training programs should be customized by region, country, industry, areas of compliance and types of employee.

– In addition to FCPA, UK Bribery Act, and OECD guidelines, focus on compliance risks in the country where the employees being trained are working.

– For example: In China, address the many corruption risks involved in dealing with state-owned entities.
Recommendation IV

Update your training regularly.

- Government officials are increasingly collaborating across borders to conduct large scale investigations, and enforcement trends and anti-corruption laws change rapidly.

- Monitor what’s happening around the world and incorporate those developments into training. *Compliance is a global issue that requires corporate vigilance and constant attention.*

- Effective implementation of training—and detailed documentation of your efforts company-wide—is critical to demonstrating your organization’s commitment to corporate compliance.
Oversight
(Monitoring, Auditing, and Response)
Oversight: Are Employees Staying with the Program?

- Even after all the important ethical messages from management have been communicated to the appropriate audiences and key standards and controls are in place, there should still be a question of whether the workforce is adhering to the compliance program.

- Two of the seven compliance elements in the US Sentencing Guidelines call for companies to monitor, audit and respond quickly to allegations of misconduct.

- These three highlighted activities are key components enforcement officials look for when determining whether companies maintain adequate oversight of their compliance programs.
Monitoring vs. Auditing

– Many companies fall short on effective monitoring. This can sometimes be attributed to confusion about the differences between monitoring and auditing.

– **Monitoring** is a commitment to reviewing and detecting compliance programs in real time and then reacting quickly to remediate them. A primary goal of monitoring is to identify and address gaps in your program on a regular and consistent basis.

– **Auditing** is a more limited review that targets a specific business component, region or market sector during a particular timeframe in order to uncover and/or evaluate certain risks, particularly as seen in financial records.
Compliance “Cousins”

- *Don’t assume that because your company conducts audits that it’s effectively monitoring.* A robust program should include separate functions for auditing and monitoring.

- While unique in protocol, however, the two functions are related and can operate in tandem.

- Monitoring activities can sometimes lead to audits. For example, if you notice a trend of suspicious payments in recent monitoring reports from Indonesia, it may be time to conduct an audit of those operations to further investigate the issue.
Oversight: What the Regulatory Guidelines Say

**USSG:** Companies should monitor and audit their compliance programs and maintain reporting mechanisms. They should respond quickly to allegations and modify their programs as needed.

**OECD:** Individuals at all levels of the company should be responsible for monitoring. Companies should discipline employees for violations of the policy. Companies should regularly review their compliance programs and make necessary revisions.

**UK’s 6 Principles:** Companies must monitor and review their compliance programs.
Recommendation I

Establish a regular monitoring system to spot problems and address them.

– Effective monitoring means applying a consistent set of protocols, checks and controls tailored to your company’s risks to detect and remediate compliance problems on an ongoing basis. For example, your compliance team should be checking in routinely with local finance departments in your foreign offices to ask if they’ve noticed recent accounting irregularities.

– Regional directors should be required to keep tabs on potential improper activity in the countries they manage. And the global compliance committee should meet or communicate as often as every month to discuss issues as they arise.

– These ongoing efforts demonstrate your company is serious about compliance.
Recommendation II

Pay attention to what employees say during training.

- Training can alert you to potential problems based on the type of questions employees ask and their level of receptiveness to certain concepts.

- For example, during training employees might ask specific questions about important compliance considerations such as their interactions with government officials or gift-giving practices. Such questions can raise red flags and uncover issues that should be reviewed and addressed quickly.
Recommendation III

Establish protocols for internal investigations and disciplinary action.

- A swift and effective response to compliance issues will sometimes require a company to conduct an internal investigation.

- Prior to such an investigation, however, the company should have procedures—including document preservation protocols, data privacy policies, and communication systems designed to manage and deliver information efficiently—in place to make sure every investigation is thorough and authentic.
Recommendation IV

Remediate problems quickly.

- A key concept behind the oversight element of compliance is that if companies are policing themselves on compliance-related issues, the government won’t have to do it for them. Remediation, then, is an important component of oversight.

- For example, if your company’s sales force in Thailand is engaged in potentially improper activity due to a lack of adequate training, remediate the deficiency and schedule that training now.

- In the end, it’s not enough to just gather information and identify compliance problems through monitoring and auditing. To fulfill this essential element of compliance, you also have to respond and fix the problems.
The benefits of our experience: Clear direction. Real-time answers.

Our experience goes beyond representing big-name clients in high-stakes investigations. It’s what we’ve learned in the process and how we apply those lessons to help companies around the world reduce compliance risk and minimize damages. Time and again clients ask us, “How do we measure up to our competitors? What’s the industry standard? What does the government expect from us?”

For more than 30 years we’ve tracked the evolution of compliance standards, worked closely with enforcement authorities and advised clients across a wide range of industries. That’s enabled us to guide clients in maintaining effective compliance programs, provide clear direction on the government’s stance on various business practices and develop benchmarks to help clients know where they stand.

We also have a unique approach to internal investigations. Our experience has taught us that clients want to do whatever’s necessary with as little disruption and cost as possible. We also know the government expects a thorough, credible investigation. Balancing those interests takes informed judgment. After handling hundreds of investigations with candor and transparency, we’ve earned the trust of government authorities and developed best practices to ensure we do no more and no less than what is necessary to reach a successful resolution.