OVERVIEW OF FOREIGN CORRUPT PRACTICES ACT & DODD-FRANK, UK BRIBERY ACT

FOREIGN CORRUPT PRACTICES ACT
FOREIGN CORRUPT PRACTICES ACT
Overview

- FCPA is a U.S. federal law enforced by the Securities and Exchange Commission (SEC) and the Department of Justice (DOJ)
- Enacted in 1977 by U.S. Congress in response to SEC investigations in the 1970s
  - FCPA prohibits corrupt payments to foreign officials for the purpose of obtaining or retaining business
  - Anti-bribery
  - Books and records

FOREIGN CORRUPT PRACTICES ACT
Anti-Bribery Provision

- Issuers, domestic concerns and any person
- Making use of interstate commerce
- Corruptly
- Furthering offer or payment of anything of value
- To foreign official, political party, or candidate for political office
- Influence official act of that foreign official in violation of the duty of that official, or to secure any improper advantage in order to obtain or retain business
FOREIGN CORRUPT PRACTICES ACT
Books & Records Provision

1) Books, records and accounts are kept in reasonable
detail to accurately and fairly reflect transactions and
dispositions of assets

2) System of internal accounting controls is devised

FOREIGN CORRUPT PRACTICES ACT
Liability

- Prosecution does not have to prove actual knowledge
- Company will be liable if it had reason to know that a
corrupt payment has been made
- Companies are responsible for ensuring that employees and
  intermediaries
  • Comply with applicable laws
  • Adhere to standards of business conduct consistent with
    company’s conduct guidelines

IBDO
FOREIGN CORRUPT PRACTICES ACT
Penalties for Individuals

- Up to $5 million per record-keeping violation + up to 20 years in prison (applies to accounting/finance professionals)
- Up to $250,000 per anti-bribery violation + up to 5 years in prison per violation (applies to business developers/marketing professionals)
- Company is prohibited from paying employee fines

FOREIGN CORRUPT PRACTICES ACT
Penalties for Companies

- Up to $25 million per record-keeping violation
- Up to $2 million per anti-bribery violation
- Twice the pecuniary gain (or losses) from illegal activities
- Disgorgement of gross profits obtained from tainted business
- Post-enforcement monitoring
- Loss of State Department export licenses
- Disbarment from government contracts
- Disbarment from World Bank, OPIC and the CFTC
FOREIGN CORRUPT PRACTICES ACT
Enforcement Trends

FCPA Enforcement Action Brought By DoJ and SEC By Year:

<table>
<thead>
<tr>
<th>Year</th>
<th>Company</th>
<th>Country</th>
<th>Penalty Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>Siemens</td>
<td>Germany</td>
<td>$800 mm</td>
</tr>
<tr>
<td>2009</td>
<td>KBR/Halliburton</td>
<td>United States</td>
<td>$579 mm</td>
</tr>
<tr>
<td>2010</td>
<td>BAE</td>
<td>United Kingdom</td>
<td>$400 mm</td>
</tr>
<tr>
<td>2010</td>
<td>Snamprogetti Netherlands B.V./ENI S.p.A.</td>
<td>Holland/Italy</td>
<td>$365 mm</td>
</tr>
<tr>
<td>2010</td>
<td>Technip S.A.</td>
<td>France</td>
<td>$338 mm</td>
</tr>
<tr>
<td>2011</td>
<td>JGC Corporation</td>
<td>Japan</td>
<td>$218.8 mm</td>
</tr>
<tr>
<td>2010</td>
<td>Daimler AG</td>
<td>Germany</td>
<td>$185 mm</td>
</tr>
<tr>
<td>2010</td>
<td>Alcatel-Lucent</td>
<td>France</td>
<td>$137 mm</td>
</tr>
<tr>
<td>2010</td>
<td>Panalpina</td>
<td>Switzerland</td>
<td>$81.8 mm</td>
</tr>
<tr>
<td>2011</td>
<td>Johnson &amp; Johnson</td>
<td>United States</td>
<td>$70 mm</td>
</tr>
</tbody>
</table>
Importance of FCPA Corruption Compliance

Morgan Stanley Case

- Morgan Stanley maintained a system of internal controls meant to ensure accountability for its assets and to prevent employees from offering, promising or paying anything of value to foreign government officials.

- Morgan Stanley’s internal policies, which were updated regularly to reflect regulatory developments and specific risks, prohibited bribery and addressed corruption risks associated with the giving of gifts, business entertainment, travel, lodging, meals, charitable contributions and employment.

FOREIGN CORRUPT PRACTICES ACT

Components of FCPA Compliance

- Provisions of plea and deferred prosecution agreements companies enter into with government provide compliance guidance
  - Panalpina (2010)
  - Johnson & Johnson (2011)
  - Bridgestone (2011)
  - Pfizer (2012)
FOREIGN CORRUPT PRACTICES ACT
Components of FCPA Compliance

1) Clearly articulated and “visible” corporate policy against violations of the FCPA and other anti-corruption laws
2) Strong, explicit and visible support from senior management
3) Assessment of the company’s corruption risks
4) Development and promulgation of compliance standard and procedures designed to reduce the prospect of violations of anticorruption laws, including provisions
5) Designation of one or more senior executives who are responsible for anti-corruption compliance

6) Mechanism for effective communication of policies, standards and procedures to directors, officers, employees and (where appropriate) agents and business partners
7) Establish and maintain effective system
8) Due diligence for retention and oversight of agents and business partners (periodic reviews)
9) Standard provisions in agreements, contracts and renewals with agents and business partners
10) Periodic testing of compliance code, standards and procedures, updating based on evolving standards and changes in corporate corruption risk profile
DODD-FRANK WALL STREET REFORM AND CONSUMER PROTECTION ACT

DODD-FRANK ACT

Key Components

- Signed into law on July 21, 2010; after comment period, the SEC issued rules relating to its bounty program. Those rules went into effect on August 12, 2011
- Contains whistleblower provisions designed to incentivize and protect individuals who voluntarily provide “original information” to the SEC
- Significantly expands the scope of Sarbanes-Oxley whistleblower provisions and entities covered
DODD-FRANK ACT

Key Components

Expanded scope of claims and applicable entities:

- Relates to any potential violation of securities laws, including FCPA
- Applicable to both public and some private companies

SEC Whistleblower Program

An individual (“natural person”) who, alone or jointly with others, voluntarily provides original information to the SEC or CFTC relating to a possible violation of the federal securities laws that has occurred, is ongoing, or is about to occur

- A company or other business entity cannot qualify as a whistleblower
- The reported information must relate to a violation of federal securities laws. Individuals providing information relating to violations of state or foreign laws will not qualify for the Whistleblower Bounty under Dodd-Frank Act
SEC WHISTLEBLOWER RULES
Individuals Ineligible to be Whistleblowers

- An officer, director, trustee, or partner of a company who receives information about the alleged misconduct from a company employee or from the company's internal compliance process

- Attorneys and non-attorneys who obtain information through a communication which is subject to the attorney-client privilege or in the course of representing a whistleblower or whistleblower’s employer, unless disclosure is allowed under applicable state attorney conduct rules

- Certain personnel with compliance-related responsibilities

- Public accountants working on engagements required under the federal securities laws if the information relates to violations by the client or the client’s directors, officers or other employees

- Persons who obtain information as a result of an audit of a company’s financial statements if submission of such information to the SEC would be contrary to the reporting requirements of Section 10A of the Securities Exchange Act of 1934, as amended
SEC WHISTLEBLOWER RULES
Individuals Ineligible to be Whistleblowers

- Persons who obtain information in a way that is determined by a domestic court to violate applicable federal or state criminal law
- Anyone who obtains information from persons subject to the above exclusions, subject to certain exceptions

SEC WHISTLEBLOWER RULES
Reasonable Basis Exception

- Principals, compliance or internal audit personnel, individuals employed by or otherwise associated with a firm retained to conduct an inquiry or investigation into possible violations of law, and independent public accountants can be eligible for an award under limited circumstances
SEC WHISTLEBLOWER RULES
Definition of “Original Information”

- Provided for the first time to the SEC after July 21, 2010, the date that the statute was enacted
- Derived from the whistleblower’s “independent knowledge” or “independent analysis”
- Not already known to the SEC from any other source
- Not exclusively derived from an allegation made in a judicial or administrative hearing, in a governmental report, hearing, audit, or investigation, or from the news media, unless the whistleblower is the source of the information

SEC WHISTLEBLOWER RULES
Definition of “Voluntary”

Information is provided voluntarily if the information is provided before a request, inquiry, or demand was directed to the whistleblower personally or to his or her representative by the Commission, the Public Company Accounting Oversight Board or any self-regulatory organization, Congress, any other authority of the federal government, or a state Attorney General or another securities regulatory authority.
SEC WHISTLEBLOWER RULES
Definition of “Not Voluntary”

A submission of information is not voluntary if the whistleblower is required under a pre-existing legal or contractual duty owed to the SEC or one of the above-listed authorities to report such information to the SEC.

SEC WHISTLEBLOWER RULES
No Internal Reporting Requirement

Whistleblower reports through corporate compliance procedure and company reports same and additional information to SEC within 120 days, whistleblower deemed to have reported to the SEC on the date he/she originally reported the violation internally, and given credit for both original and additional information self-reported by the company.

SEC has discretion to increase the award amount if a whistleblower voluntarily reports to, and cooperates with internal compliance systems, and to decrease the award amount if whistleblower delays reporting, or interferes with internal compliance systems.
SEC WHISTLEBLOWER RULES

Amount of Monetary Award

SEC discretion to pay whistleblower(s) who qualify for an award **between 10 and 30 percent** of the monetary sanctions collected by the SEC based upon the information provided by the whistleblower.

Whistleblower may also collect an award based on monetary sanctions that are collected from a related action (if the whistleblower’s original information led the SEC to obtain monetary sanctions exceeding $1 million).

Factors that Increase Amount of Monetary Award

1) The significance of the information provided by a whistleblower to the success of the Commission action or related action.

2) The degree of assistance provided by the whistleblower and any legal representatives of the whistleblower in the Commission action or related action(s), including timeliness, resources conserved, efforts undertaken by the whistleblower to mitigate harm, and any undue hardship suffered by the whistleblower.

3) The SEC’s interest in deterring violations of the securities laws by making awards to whistleblowers who provide information that leads to successful enforcement actions.

4) Whether the whistleblower participated in internal compliance systems and reported any violation internally, or assisted in any internal investigation.
DODD-FRANK ACT
Anti-Retaliation Protections

- Dodd-Frank prohibits retaliation against whistleblower who:
  - Provide information to the SEC or CFTC;
  - Assist in any investigation or legal action of the SEC or CFTC related to such information; or
  - Engage in other protected activity under SOX.

DODD-FRANK ACT
Anti-Retaliation Protections

For the purpose of the anti-retaliation provisions, an individual is a whistleblower if that individual possesses a reasonable belief that the information he or she is providing relates to a possible securities law violation that has occurred, is ongoing, or is about to occur, and he or she reports that information in accordance with the procedures delineated in the rules.
DODD-FRANK ACT
Anti-Retaliation Protections

Originally, under SOX, whistleblowers had 90 days after the date of the alleged retaliatory conduct or after the individual became aware of the alleged retaliatory conduct to bring a complaint. Dodd-Frank increased that time period to 180 days.

Whistleblower claiming retaliation can bring an action directly in federal court (SOX had required first filing a complaint with OSHA).

Expansive Statute of Limitations:

- For SEC-related retaliation Claims:
  - No more than six years after the violation, or
  - Three years after facts to the right of action are known or should have been known by the employee (this can be up to ten years after the violation)

- For CTFC retaliation claims, up to a maximum of two years.
UK BRIBERY ACT

Introduction

- Enacted in April, 2010; effective on July 1, 2011
- Previous legislation - collection of laws dating as far back as 1889
- Wider in scope than the US Foreign Corrupt Practices Act
- Severe penalties for individuals (up to 10 years imprisonment, unlimited fines) and corporations (criminal conviction, unlimited fines)
- Intended to target “mavericks” rather than burden “law abiding firms”
UK BRIBERY ACT
Summary of Offenses

Section 1: Paying bribes

Section 2: Receiving bribes

Section 6: Active offense of bribing a foreign public official

Section 7: Strict liability offense where “relevant commercial organization” fails to prevent bribery by an “associate person”

UK BRIBERY ACT
Guidance

- Draft guidance published for comment in September, 2010
- Final guidance published in March, 2011
- Not prescriptive
- No direct obligations
- Emphasizes a risk-based approach to managing corruption risk and for “proportionate” procedures
- “Thematic Review into ABC Controls at Investment Banks” in March, 2012
UK BRIBERY ACT
Jurisdiction

- Sections 1, 2 and 6 (giving or receiving a bribe) apply to:
  - Conduct where an act or omissions which forms part of the offense takes place in the UK (including conduct of companies incorporated in the UK)
  - Conduct of individuals who are UK citizens or ordinarily resident in the UK, even if conduct occurs outside the UK

Section 7 (failure to prevent bribery) applies to a “relevant commercial organization”:

- Companies incorporated in the UK; and
- Companies that “carry on a business or part of a business in the UK”

1) Common sense approach so that non-UK organizations that do not have a “demonstrable business presence” in the UK would not be covered (trading on London Stock Exchange, operating a subsidiary)

2) SFO warns against “over-technical” interpretations

3) UK courts final arbiter on determining jurisdiction
UK BRIBERY ACT

Associated Persons

- Commercial organization strictly liable for Section 7 offense by acts of an associated person
  - Includes any person or legal entity that “performs services for or on behalf of the commercial organization”
  - No limits regarding capacity or nature of the relationship
  - Employees, agents, subsidiaries, joint venture partners

UK BRIBERY ACT

Corporate Hospitality

- No safe harbor for “promotion and demonstration of products and services”
- Emphasis on “reasonable and proportionate”
- Hospitality and other promotional activities can be used a bribe
- No prescriptive advice

Factors to consider

- Intent or business purpose
- Amounts involved
- Client’s influence
- Frequency
- Industry standards
- Location (country guidance for government officials)
- Transparency
UK BRIBERY ACT
Facilitation Payments

- Small bribes paid to facilitate routine Government action
- Guidance acknowledges that this is a “long-term objective”
- Policy, pattern, practice

UK BRIBERY ACT
Adequate Procedures

1. Proportionate procedures
2. Top level commitment
3. Risk assessment
4. Due diligence
5. Communication
6. Monitoring and review
UK BRIBERY ACT
Enforcement

“There will always be companies, whether based here or overseas, that have no intention of playing by the rules and want to use corruption to undercut ethical companies. It’s in the UK public interest to get them into the criminal courts because they are damaging everybody else. Those are the people I want to investigate and prosecute—not the well meaning businessperson who happens to have stumbled into a problem.”

Richard Alderman
Director, Serious Fraud Office
June, 2011
## Principle 1 - Proportionate Procedures

Procedures for compliance with the UK Bribery Act should be proportionate to the bribery risks your Corporation(s) face and to the nature, scale and complexity of your business activities. The procedures you have should also be clear, practical, accessible, effectively implemented and enforced.

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Unclear</th>
<th>Plan date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>An initial assessment of risk across all of the organisation globally has been carried out to identify potentially risk areas.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>An initial assessment of the risk of bribery on the part of associated persons external to the organisation has been carried out.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policies and procedures that need to be implemented are identified and proportional to the bribery risks that the organisation faces globally.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The policies and procedures seek to ensure that there is a practical and realistic means of achieving the organisation’s anti-bribery policy objectives globally across all of the organisation’s functions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

## Principle 2 - Top-Level Commitment

The top-level of management in the organisation should be committed to preventing bribery by persons associated with it. Management should foster a culture within the organisation in which bribery is never acceptable.

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Unclear</th>
<th>Plan date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top-level management is engaged in:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. The development and determination of bribery prevention procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Any key decision making relating to bribery risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Communication of the organisation’s anti-bribery stance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal and external communication includes:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. A commitment to carry out business fairly, honestly and openly</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. A commitment to zero tolerance towards bribery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. The consequences of breaching the policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. The bribery prevention procedures in place, including any protection and procedures for confidential reporting of bribery (whistle-blowing)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. For other associated persons the consequences of breaching contractual provisions relating to bribery prevention</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. The business benefits of rejecting bribery (reputational, customer, business partner and share holder confidence)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g. Who is involved in development and implementation of the bribery prevention procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Appendix

**UKBA: Form Adequate Procedures Checklist**

#### Principle 3 - Risk Assessment

The organisation should assess the global nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment should be periodic, informed and documented and communicated to top management including the audit committee.

<table>
<thead>
<tr>
<th>Sufficient oversight exists of the risk assessment by top level management and audit committee</th>
<th>Yes</th>
<th>No</th>
<th>Unclear</th>
<th>Plan date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriate resourcing is available to carry out effective risk assessments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal and external information sources that will enable risk to be assessed and reviewed have been identified</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Due diligence enquiries are conducted (see Principle 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accurate and appropriate documentation is maintained of the global risk assessment and its conclusions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk assessments are carried out as the business evolves and new markets are entered</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk assessments include assessing the following risks where appropriate: Country risk, Sector risk, Transaction risk, Business Opportunity risk and Business Partnership risk, including Mergers &amp; Acquisitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk assessments include a review of deficiencies in: employee training; skills and knowledge; bonus culture that rewards excessive risk taking; lack of clarity in the organisation’s policies and procedures for hospitality; promotional expenditure, and political or charitable contributions; lack of clear financial controls (manual and automated); lack of a clear anti-bribery message from top management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Principle 4 - Due Diligence

The organisation should apply due diligence procedures, taking a proportionate and risk based approach, in respect of persons who perform or will perform services, in order to mitigate identified bribery risks.

<table>
<thead>
<tr>
<th>Due diligence procedures are proportionate to the identified risk</th>
<th>Yes</th>
<th>No</th>
<th>Unclear</th>
<th>Plan date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensive due diligence is conducted, prior to any commitment being given, when entering into business relationships where it may be difficult to extricate from the relationship once established, including Mergers and Acquisitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Due diligence is be conducted using a risk-based approach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proportionate due diligence is incorporated in recruitment - employee background checks and human resources procedures to mitigate the risks of bribery being undertaken by employees</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In higher risk situations, due diligence include conducting direct interrogative enquiries, indirect investigations, or general research on proposed associated persons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appraisal and continued monitoring (manual and automated) of recruited or engaged associated persons, is conducted proportionate to the identified risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Due diligence on individuals involves proportionate requests for details on the background, expertise and business experience. Information received is verified through research and the following up of references</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Anti-Corruption Workshop
Page 47
Appendix
UKBA: Form Adequate Procedures Checklist

Principle 5 - Communication (including training)
Organization(s) should seek to ensure that bribery prevention policies and procedures are embedded and understood throughout the entity through internal and external multi-language communication, including training that is proportionate to the risks faced.

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Unclear</th>
<th>Plan date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Internal communications convey top level involvement; focus on the implementation of the organization’s policies and procedures; make clear the implications for employees
- Communications include policies on the following areas: decision making; financial control; hospitality and promotional expenditure; facilitation payments; multi-language training; charitable and political donations; penalties for breach of rules; the establishment of a secure, confidential and accessible means to raise concerns about bribery; the process to provide suggestions for improvement of bribery prevention procedures and controls and for requesting advice
- External communication of bribery prevention policies is communicated (in multi-languages where necessary) to reassure existing and prospective associated persons and to deter those intending to bribe on the organization’s behalf
- Basic training in multi-language is offered
- More advanced training offered is proportionate to risk
- Training is mandatory for new employees or for agents as part of an induction process
- Training is continuous, and regularly monitored and evaluated

---

Appendix
UKBA: Form Adequate Procedures Checklist

Principle 6 - Monitoring and Review
The organization should monitor and review procedures designed to prevent bribery by persons associated with it and makes improvements where necessary.

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Unclear</th>
<th>Plan date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- There is a process to monitor (manual and automated) and evaluate the effectiveness of the bribery prevention procedures
- In addition to regular monitoring (manual and automated) there is a system to review processes when the nature and scale of the organization’s activities change and in response to other stimuli
- There are formal periodic reviews and reports for top-level management and audit committee
- Systems such as internal financial control mechanisms (manual and automated) are set up to deter, detect and investigate bribery, and monitor the ethical quality of transactions
- Multi-language staff surveys, questionnaires and feedback from training is used to provide information on policy and process effectiveness
- Information is drawn on best practice from other organisations, relevant trade bodies or regulators
Insanity is Doing the Same Thing Over and Over

- There is a need for a Game Change Approach to FCPA Compliance.
- Most of the major recent FCPA, AML and Sanction scandals were not the result of compliance failures in the ordinary sense.
- Game Changer: How the NYPD Reduced Crime & Revolutionized Public Management – CompStat and Common Sense.
- Continuous Accounting (CA) and Continuous Controls Monitoring (CCM) are concepts already being applied in the compliance context.
- We need to focus on the most significant and damaging corruption risks and we need to develop the tools and strategies needed to prevent, detect and expose such corruption before it is too late.
- Matched to a CompStat-like focus on internal risk, an integrated CA and CCM process can demonstrably limit such risks and improve business performance.
Look at the Cases: Would Your Program have Prevented or Detected This Misconduct?

- The customary FCPA compliance approach may not be adequate to protect your firm against the sort of major violations.
- Genuine management buy-in requires a great deal more than is typically provided.
- Standard controls and audits may be missing a very significant spectrum of risk.
- Corporate audit programs can miss the forest of risk while counting the trees.
- The solution will require the sustained involvement of management and senior business staff, especially those in high risk jurisdictions and projects.

Consider the TSKJ Case

- Four major engineering firms, from four different nations conspired to make massive bribes to Nigerian public officials to obtain more than $6 billion in EPC contracts between 1995 and 2004.
- They formed a joint venture for this purpose and each contributes tens of millions of dollars in corporate funds to establish a slush fund totaling at least $183 million.
- The CEO of one of the companies obtained a kickback of at least $10.8 million for himself.
- The key bribery agent, a U.K. solicitor, forfeited $149 million upon conviction for his role in the scheme. (Ask yourself, he had this money available to forfeit to the DOJ, how much in bribes did he actually pass along to corrupt Nigerian officials?)
- How did this massive bribery scheme come to the attention of the authorities?
- Is anyone confident that similar schemes are not being plotted or already in existence at other major corporations? (A trick question as several have already been exposed.)
Before CompStat, the NYPD Mission Assumed Failure Was Inevitable

■ False Assumptions:
  – Crime is caused by economic and societal conditions beyond the control of a police force;
  – Crime rates climb because of poverty and despair;
  – Since the police can not stem the rising tide of crime, limited police resources should be reserved for serious (“high risk”) violent crimes
  – Because narcotics trafficking can corrupt cops, ordinary patrol officers should merely report evidence of drug dealing and allow specialist drug units to address the problem

■ Wrong crime fighting strategies:
  – Ignore minor crimes = encourage a poor regard for law and order
  – Assign promising young officers to “safe” precincts; poorly regarded officers to dangerous and risky precincts = poorest managers responsible for high crime precincts
  – Ignore intelligence regarding serious crimes = police know less about where guns and dangerous drugs are being sold than ordinary neighborhood residents
  – Shield police from encounters with the public = poor community relations, little cooperation, lower clearance rates

The New Strategy Produced Astonishing Results

■ Headline: since 1993, unparalleled reductions in crime: Murder down 78.7%, Rape down 54.8%, Robbery down 77%; Burglary down 82%; Grand Larceny down 51.6%; GLA (auto theft) down 92.9%.

■ Your chance of being murdered, rape, robbed, car jacked or burgled in London today is significantly higher than in New York City. I finished a 26 year law enforcement career in New York and no one I knew during that career would have imagined that such a statement could ever be true.

■ Common sense strategies that were never tried before are now routine:
  – Intelligence about where crime is occurring and who is responsible is carefully collected, analyzed and enforcement strategies determined by it.
  – Through the dynamics of the CompStat meeting, police commanders are regularly challenged to address local crime problems and provided with the resources for doing so.
  – The controversial but statistically proven policy of “stop and frisk” hundreds of weapons are seized every year but more importantly, criminals report they are afraid to carry their weapons with them for fear of being frisked and arrested.
Success of CompStat Has Been Replicated in Other City Agencies & Other Police Departments

- The CompStat process was extended to every major City agencies and helped those agencies achieve significant cost savings and service improvements. Since 1996, it has been copied by at least seven major U.S. police departments as well as numerous major European cities and the fact that it is still used by almost every one of those agencies is a testament to its effectiveness.

- CompStat is not a computer system (although the name emerged from the computer maps showing were crimes are being committed that are a major control point and measurement for the command meetings). It is a management and accountability process that requires managers to rigorously review, react and assess their efforts to achieve stated goals. It has been compared to the Six Sigma and TQM management strategies.

- CompStat is not a panacea. Several police departments and other organizations have embraced it and yet not achieved anything near the results enjoyed by the NYPD. Recently, there have been public reports of instances in which police commanders have allegedly manipulated their crime figures to meet certain goals. Such risk is inherent in any management system and particularly where the approach holding managers strictly accountable for results.

Continuous Auditing

- Continuous auditing is the independent application of automated tools to provide assurance on financial, compliance, strategic and operational data within a company. Continuous auditing uses a set of tools to assure the internal control system is functioning to prevent fraud, errors and waste. The "continuous" aspect of continuous auditing and reporting refers to the near real-time capability for financial information to be checked and shared. Not only does it indicate that the integrity of information can be evaluated at any given point of time, it also means that the information is verified constantly for errors, fraud and inefficiencies.

- Each instance of continuous auditing has its own pulse. The internal management chooses for evaluation depends on the frequency of updates within the accounting information systems. Analysis of the data may be performed hourly, daily, weekly, monthly, etc. depending on the application.

- Non-financial aspects of continuous auditing might encompass an ongoing assessment program to determine the state of security control effectiveness as a result of changes in an organization’s information systems or its environment of operation. Large changes to an organization’s security and network infrastructure profile should trigger near real-time monitored events.
Continuous Control Monitoring

- Continuous Control Monitoring has been defined as “... a process that management puts in place to ensure that its policies, procedures, and business processes are operating effectively.” (See IIA’s Global Technology Guide on Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment.)

- It is not a new concept. Companies have been performing continuous monitoring for operational risks, controls, and activities for decades. There are a number of consulting firms that offer such solutions.

- Continuous Controls Monitoring (CCM) applications automatically identify exceptions and control breakdowns at the time they occur.

- By finding and correcting errors immediately CCM helps reduce risk, automate compliance obligations, elevate red flags and eliminate waste.

CA plus CCM = Continuous Assurance

- Continuous Auditing
  - Method used to perform audit-related activities on a continuous basis, including control and risk assessment.

- Continuous Controls Monitoring
  - Automated Processes to ensure policies/procedures are operating effectively and to assess the adequacy & effectiveness of controls
  - Performed by management and key business staff and audited independently to evaluate the effectiveness of the process.

- Continuous Assurance
  - The combination of continuous auditing and audit oversight of continuous monitoring has been successfully applied to functions such as fraud, so why not FCPA compliance?
An Integrated Approach

- The challenge is to integrate the discipline of the CompStat process with CA and CCM.
- Continuous auditing basically means auditing transactions and other risk relevant events on a continuous basis.
- Continuous monitoring means ensuring that compliance procedures are operating as required and that controls are producing adequate results.
- Independently test all critical transactions or events for compliance with FCPA controls at, or soon after, the point at which they occur.
- Results support the CompStat process and are regularly reviewed by management, business staff, legal and compliance.
- The ideal result is Continuous Assurance.

Management Retains Responsibility

- The key to success is management’s engagement with and responsibility for the continuous monitoring of controls.
- Effective management of controls is best achieved through an integrated approach. Just having senior management involvement in the ongoing review process and the assessment of the results is a game changer. They may not like it at first but the organization will be better served by their true commitment to this process.
- And with Audit’s independent assessment of the FCPA controls function through the CompStat process is the best way to achieve genuine continuous assurance.
Limitations of Traditional Audit Approach

- Retrospective view:
  - Audit or analysis frequently occurs long after a transaction has taken place;
  - Often too late for action;
  - Often lacks a critical view of the risks and the red flags.
- Lack of timely visibility into control risks and deficiencies.
- Problems escalate, increasing compliance and business risk.
- As several enforcement actions have dramatically demonstrated, periodic audits can be defeated by a variety of simple off-balance sheet movements or through the establishment of shell companies (e.g. TSKJ et al., Siemens and others.)

The Hard Part: Defining Controls and Maintaining a Balanced Approach

- The right controls are the key to ensuring integrity while maintaining the right efficiency and economy.
- No system is fool-proof; we are in a risk business and perfection is not achievable.
- Which transactions and “approvals” or “authorizations” should be subject to controls?
- What controls are necessary to flag efforts to illegally divert corporate assets into a slush fund or to make direct bribe payments?
- Who from management and business should manage these controls?
- How can the effectiveness of these controls be measured and assurance determined?
- Transactions and permissions should be the focus.
- The goal is to establish that “game changer.”
THANK YOU

Contact: Kevin J. Ford, Managing Director
Strategic Advisory Solutions
kford@rdc.com
917-817-4930

Lean Six Sigma in Compliance

PREAM4 Anti-Corruption Workshop
October 14, 2012
9.00am to 12 noon

Sulaiman Afzal
US Data Solutions
Disclaimer

- US Data Solutions is not, by means of this presentation, rendering business, accounting, legal, information technology, or other professional advice or services.

- This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect local and international business. Before making any decision or taking any action that may affect local and international business, qualified professionals should be consulted.

- US Data Solutions, and related entities shall not be responsible for any loss sustained by any person or entity that relies on this presentation.

- US Data Solutions endeavors to give attribution to materials used by other professionals and their respective organizations.
Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework

COSO Framework - Definition

COSO says internal control consists of five interrelated components that are derived from the way management runs a business and are integrated into the management process.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control environment</td>
<td>The tone of the organization influences the control consciousness of its employees. Examples include the integrity, ethical values and competence of employees, management’s philosophy, and input provided by the board of directors.</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Identification and analysis of risks relevant to achieving corporate goals, determination of how such risks should be managed and implementation of a process to address risks associated with change.</td>
</tr>
<tr>
<td>Control activities</td>
<td>Policies, procedures and processes that help ensure a company carries out management directives. Examples include approvals, verifications, reconciliations, review of operating performance, security of assets and segregation of duties.</td>
</tr>
<tr>
<td>Information and communication</td>
<td>Communication within the company and with external parties such as customers, agents, suppliers, regulators and shareholders. For example, reports that contain operational, compliance or financial data or that share ideas or events across lines of business are generated from a company’s information systems.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Assessing the quality of a company’s internal control systems. This is done through ongoing monitoring (manual and automated) of activities within the business unit and an independent evaluation of existing controls by internal/external auditors and/or compliance personnel.</td>
</tr>
</tbody>
</table>
Lean Six Sigma and Automated Controls

Lean, Six Sigma and Automated Controls - Definitions

“Lean”, applied in the context of compliance, is the elimination of waste, where waste is work that adds no value to a compliance process or control.

“Six Sigma” relates to the number of mathematical deviations in a compliance process. Six Sigma practitioners focus on systematically eliminating the deviations to get as close to “zero deviations” as possible. Done properly, Six Sigma ensures that compliance processes are running at optimum efficiency with regard to qualities such as speed, quality, accuracy, and latency of data.

People trained on Six Sigma will recognize DMAIC as a phased methodology with which to improve existing compliance processes:

- Define – the problem, the voice of the internal or external compliance monitor, and the compliance goals, specifically
- Measure – key aspects of the current compliance process and collect relevant data
- Analyze – the data to investigate and verify cause-and-effect relationships. Determine what the relationships are, and attempt to ensure that all factors have been considered. Seek out root cause of the non-compliance under investigation
- Improve – or optimize the compliance process based upon data analysis techniques
- Control – the future state compliance process to ensure that any deviations from policies and procedures are corrected before they result in non-compliance

“Automated Controls” extend the reach of Six Sigma efforts:

- Increase the accuracy of the compliance process measurements.
- Improve the design and decision of compliance professionals.
- Shred cumbersome, manual, inconsistent, and error-prone manual efforts.
Six Sigma Leader Roles for DMAIC

- Establish project selection criteria
- Approve projects – ensure linkage to strategy and key needs
- Select Project Champions
- Provide needed resources and training
- Review Black Belt and Green Belt projects monthly
- Be accountable for the success of the effort

Six Sigma Leader Roles for DMAIC

- Establish and use communication process
- Review the entire process every 3-6 months
- Establish reward and recognition structure
- Link rewards to performance
- Be accountable for the success of the effort

Six Sigma and Champions - Definitions

Business Leaders sponsoring Six Sigma compliance projects are called “Champions.” Champions are responsible for supporting, aligning, and integrating the Six Sigma Compliance Launch into their organization. Champions are trained in the essentials of the Six Sigma Methodology, especially focusing on how to select compliance projects that are aligned with business goals. Champions in turn select and mentor Six Sigma project leaders who are called “Belts” and ensure the Belts have the training and resources they need to successfully lead Six Sigma projects.

Lean Six Sigma - Evaluate and Understand Compliance Gaps

Resources should be applied according to the biggest benefit, or in case of compliance processes, the largest risk. In order to prioritize where Lean Six Sigma process efforts are necessary, the company should gain an understanding of where the biggest risks and gaps exist.

Case Study:
Experience tells us that most master vendor files contain large numbers of entries that are no longer active, or are duplicates, or otherwise aren’t worth the trouble. At the same time that you develop your relationship types and apply some form of risk scoring, it would be prudent to de-dupe your master vendor files and combine any duplicates into single entries. Any inactive entities with which your organization hasn’t transacted in two years or more should be deactivated on the system.

Subsequent to risk scoring, a second round of thinning out the third party ranks may well be in order. Any third party that has been designated as high risk but isn’t worth the trouble and is either redundant or easily replaced with a less risky alternative should likewise be deactivated. And, if after due diligence investigations are performed, serious red flags are raised that cannot be resolved to your satisfaction, it may be prudent to exit some of those relationships as well.

Figure 1 shows a high-level process diagram with Potential Risks and Control Gaps for a third party risk.
Lean Six Sigma – **Pareto Chart** to Identify Risks

Lean Six Sigma tool that can be used to focus in on the highest areas of compliance risks is the **Pareto chart**. Figures 2 is an example from that revolves around the reporting of key issues and challenges in a compliance project.

**Case Study**

The **Pareto Chart** in Figure 2 helped the company prioritize where (in which business units) the most exceptions or control failures were occurring. This was then helpful in prioritizing where process improvement efforts should be focused. In this case, the company quickly identified three focus areas for further analysis.

![Pareto Chart](image)

**Case Study**

- **Step 1**: Identify the Problem
- **Step 2**: Work Out the Major Factors Involved
- **Step 3**: Identify Possible Causes
- **Step 4**: Analyze Your Diagram

Fishbone shape, showing factors of:
- Equipment
- Process
- People
- Materials
- Environment
- Management

All affecting the overall problem. Smaller arrows connect the sub-causes to major causes.

Lean Six Sigma – **Cause and Effect** to Identify Risks

Another Lean Six Sigma tool that can be used to focus on compliance risks is the “**cause-and-effect**” diagram. When you have a compliance problem, it’s important to explore the cause, before identifying a solution. **Cause and Effect Analysis** gives you a useful way of doing this. This diagram-based technique, which combines **Brandingstorming** with a type of **Mind Map**, pushes one to consider all possible causes of a problem, rather than just the ones that are most obvious.

**Case Study**

- **Step 1**: Identify the Problem
- **Step 2**: Work Out the Major Factors Involved
- **Step 3**: Identify Possible Causes
- **Step 4**: Analyze Your Diagram

![Cause-and-Effect Diagram](image)
Lean Six Sigma - Process Map Analysis to Find Waste

Another tool to increase understanding of key compliance risks is “Process Map Analysis”, one of the foundational tools of Lean Six Sigma. “Process Map Analysis”, in various forms – including value stream mapping, swim lane, deployment, etc. – can help companies determine what parts of which process are necessary to accomplish their purpose, and which add cost and time but no value.

Figure 1 is a SIPOC (Supplier, Inputs, Process, Outputs, Customer) Diagram.

Figure 2 shows Unified Modeling Language (UML).

Case Study: Figure 3, for example, shows a schematic of a process looking at how to most efficiently handle cash funding to clients, which is subject to certain approval and controllership regulatory requirements. The team created the map and then looked for “over-processing”, non-value-added processes, or in Lean terms, waste, including unnecessary handoffs and approvals, communication gaps, delays or wait time, and rework.

Lean Six Sigma Separating Value-Added Time from Non-Value-Added Time in Compliance

Another compliance process analysis approach is to measure and analyze how time is spent in a process, focusing on the time spent on “Value-Added” (VA) versus “Non-Value-Added” (NVA) activities.

Case Study: Figure 5 shows a picture of analysis method used by the compliance team. The method correlates compliance process steps with a table that summarizes the time for each step, separating VA from NVA time.

When looking at activities in a compliance process, we must determine if the activity is effective and efficient. We must also determine if the activity can be improved to provide a better result for compliance e.g.:

• Assessing country, industry, people and relationship risks
• Using knowledge of local culture and local business environment
• Recognizing that inherent risk cannot be eliminated
• Mitigating inherent risk and cost benefit analyses

Figure 5: Separating Value-Added Time from Non-Value-Added Time
Siemens FCPA Remediation Efforts – Case Study

• “Siemens also overhauled and greatly expanded its compliance organization, which now totals more than 500 full time compliance personnel worldwide. Control and accountability for all compliance matters is vested in a Chief Compliance Officer, who, in turn, reports directly to the General Counsel and the Chief Executive Officer.

• Siemens has also reorganized its Audit Department, which is headed by a newly appointed Chief Audit Officer who reports directly to Siemens’ Audit Committee. To ensure that auditing personnel throughout the company are competent, the Chief Audit Officer required that every member of his 450 person staff reapply for their jobs.

• Siemens also has enacted a series of new anti-corruption compliance policies, including a new anti-corruption handbook, sophisticated web-based tools for due diligence and compliance matters, a confidential communications channel for employees to report irregular business practices, and a corporate disciplinary committee to impose appropriate disciplinary measures for substantiated misconduct”.

Siemens FCPA Remediation Efforts  Case Study (Contd.)

• “Siemens has organized a working group devoted to fully implementing the new compliance initiatives, which consists of employees from Siemens’ Corporate Finance and Corporate Compliance departments, and professionals from PricewaterhouseCoopers (“PwC”). This working group developed a step-by-step guide on the new compliance program and improved financial controls known as the “Anti-Corruption Toolkit.”

• The Anti-Corruption Toolkit and its accompanying guide contain clear steps and timelier requirements of local management in the various Siemens entities to ensure full implementation of the global anti-corruption program and enhanced controls. Over 150 people, including 75 PwC professionals, provided support in implementing the Anti-Corruption Toolkit at 162 Siemens entities, and dedicated support teams spent six weeks on the ground at 56 of those entities deemed to be “higher risk,” assisting management in those locations with all aspects of the implementation.

• The total external cost to Siemens for the PwC remediation efforts has exceeded $150 million.”
Value Based Compliance

Multi-Disciplinary Team and Automated Controls in Compliance

Multi-disciplinary team provides "value" by offering access to a wide range of resources.

Utilize a multi-disciplinary team of specialists (lawyers, compliance officers, accountants and IT personnel) with experience in addressing issues relating to Compliance and Automated Controls.

Information driven decisions empower a multi-disciplinary team to improve processes and quality.

Automated controls further enhance the compliance model by increasing the span, timeliness, and accuracy of information – while also driving down the cost to assure this confidence.

By combining multi-disciplinary team (in-house and co-sourcing model) and Automated Controls, companies work towards "Value Creation" in compliance.
Objectives

• The rational and practical integration and application of these elements can result in Organizational Excellence that is compliant with management system.

• More importantly, when focus on "Value Creation" is implemented properly, the resulting management system will provide:
  o rationalized processes and procedures,
  o improved and consistent departmental interaction,
  o unfettered material and information flow,
  o optimized value streams,
  o the ability to identify and solve systemic process and product problems,
  o improved internal/external customer satisfaction and loyalty,
  o assured regulatory compliance, and
  o the platform for continual improvement and evolution of technology and business operating system.

Three Sub-Phased Value Creation Approach

Define Future Strategy
Develop Implementation Roadmap
Assess Current State

"Value Based" Compliance Framework

Multi-Disciplinary Compliance Team

<table>
<thead>
<tr>
<th>Multi-Disciplinary Team (Lawyers, Accountants and IT personnel)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Incorporate in Business Strategy</td>
</tr>
<tr>
<td>• Top-Level Support*</td>
</tr>
<tr>
<td>• Business and Compliance Team Relationship*</td>
</tr>
<tr>
<td>• Usability and Technology Adoption*</td>
</tr>
<tr>
<td>• Current Controls Portfolio</td>
</tr>
<tr>
<td>• Projected Controls Portfolio</td>
</tr>
<tr>
<td>• Business/Compliance Service Levels*</td>
</tr>
</tbody>
</table>

Automated Controls

Challenges and opportunities in Automated Controls

| • Lack of real-time operational reporting                     |
| • Lack of visibility into process level information           |
| • Disparate systems and platforms*                           |
| • Product-centric information silos*                         |
| • Multiple manual steps/semi-automated controls*             |

Co-Sourcing Compliance

Co-sourcing Compliance resources and operations to ensure efficient support of business and financial goals

<table>
<thead>
<tr>
<th>Finance and Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Vendors and Partners*</td>
</tr>
<tr>
<td>• Internal Communications</td>
</tr>
<tr>
<td>• Chief Compliance Officer Involvement</td>
</tr>
<tr>
<td>• Internal Audit coordination</td>
</tr>
<tr>
<td>• Controls Processes</td>
</tr>
<tr>
<td>• International Operations Support*</td>
</tr>
</tbody>
</table>

Technology

Technology products, underlying controls and processes for the long-term support of compliance capabilities

| • Preventive/detector testing of key transactions*           |
| • Identifying, track and route suspicious activity          |
| • Prioritize higher risk potential violations               |
| • Route to correct stakeholders                            |
| • Remediate and monitor potential violations*               |
| • Proof of compliance and remediation steps*               |
| • Certifying proper approvals (Suspicious Activity Reports (SAR)) |

Note: "Emphasis Indicator" is based on direction during investigation discussions – to be agreed upon.
Third Party Risk in Compliance

How to manage Third Party Risk in the Context of Compliance?

Global organizations maintain substantial commercial relationships with businesses and individuals that represent widely divergent risk. FCPA due diligence requires review of third-party agents for corruption risks or potential acquisitions or joint venture partners for corruption risks.

In the majority of FCPA enforcement actions reported, the improper payments are made indirectly through one or more third parties.

U.S. Department of Justice (DOJ), Securities and Exchange Commission (SEC) and international law enforcement and regulatory bodies are paying close attention to what companies are doing to identify high risk third parties and the heightened standard of care to which these riskier relationships are being held. To properly mitigate the risks associated with third parties requires an enterprise-wide, risk-based approach.
Third Party Risk—In context of Compliance

Business Relationship Types

A broad range of third parties should be assessed, across each country of operation.

Some examples
1. Accountants/Accounting Firms
2. Agents/Distributors
3. Authorized Dealers
4. Charitable Organizations
5. Commercial Consultants
6. Construction Firms/Sub-Contractors
7. Consultants
8. Customs Agents/Brokers
9. Distributors
10. Environmental Consultants
11. Freight Forwarding Agents/Brokers
12. Tax Agents Specialists
13. Marketing/Advertising
14. Pure Resellers
15. Real Estate Agents/Brokers
16. Sales Representatives
17. Lawyers/Law Firms
18. Lobbyists
19. Trade Associations
20. General Contractors
21. Engineering, Procurement
22. Joint Venture Partners

Suggested Process for Third-Party Management

Accountability at every stage
Business sponsorship and data collection
Risk assessment
Business justification
Investigative due diligence
FCPA certification
Documentation
Training
Third-party program controls
Third-party qualification requirements
Governance structure
FCPA compliance terms and conditions embedded in the relevant contract
Third Party Risk— In context of Compliance (Contd.)

How to manage Third Party Risk in the Context of Compliance?

- Companies spend a lot of time and effort on compliance around corporate hospitality and facilitation payments, and not enough on the issue of third-party due diligence – what agents, intermediaries, introducers and joint-venture partners are doing in their name.

- Third-party risk, is constant and ongoing. You can’t prevent other people breaking the law, but you are liable if they do.

Recommendations:
1. Undertake audits of third parties by using in-house/co-sourcing resources.
2. **Apply Value Add (VA)** Lean Six Sigma techniques in third party “due diligence”.

Watchdog Vs. Bloodhound
Watchdog Vs. Bloodhound

In the famous case Re: Kingston Cotton Mills Co. (1896), Lord Justice Lopes (UK) defined an auditor's duty of care as follows:

QUOTE
"It is the duty of an auditor to bring to bear on the work he has to perform that skill, care and caution which a reasonably careful, cautious auditor would use. What is reasonable skill, care and caution must depend on the particular circumstances of each case. An auditor is not bound to be a detective, or, as was said to approach his work with suspicion, or with a forgotten conclusion that there is something wrong. He is a watchdog, not a bloodhound. He is justified in believing tried servants of the company in whom confidence is placed by the company. He is entitled to assume that they are honest and rely upon their representations, provided he takes reasonable care."

UNQUOTE

Should the modern day auditor/compliance official be a watchdog or a bloodhound?

Summary
Value Creation in Compliance – Summary

Value Creation compliance systems are no different than any other business processes:
- They are made up of process steps and standards and people executing them.
- Appropriate Use of Lean Six Sigma Can Help Create Value

- Policies & Procedures
- Board of Director Role in Compliance
- Training & Communication
- External Audits of Third Parties
- Internal Audits of Compliance Policy
- Risk Assessment for Each Jurisdiction
- Accuracy of Books & Records
- Continuous Monitoring of Disbursements (Manual and Automated)

Further Information......
Sulaiman Afzal is a fellow of the Institute of Chartered Accountants in England & Wales (ICAEW) and a fellow of ICAP. He has over twenty years of international experience ranging from automotive industry (Visteon), public accounting (Ernst & Young), Commercial and Investment Banking (The National Commercial Bank and Morgan Stanley). Mr. Afzal is currently based in the United States.

Mr. Afzal has been involved in US publically-owned corporations which are subject to the auditing and reporting requirements of the US Sarbanes Oxley Law, US Foreign Corrupt Practices Act (FCPA) and Supply Chain risk management process.

Mr. Afzal’s research has recognized that controls are designed to manage risks, detect and prevent errors, and ensure compliance. His research shows that the existing internal control systems are costly due to reliance on manual controls and nonstandard automated controls. Mr. Afzal focuses on helping multi-national corporations implement automated controls which are 24/7 for global anti-corruption and anti-bribery in supply chain management by applying Continuous Controls Monitoring (CCM). This eliminates “waste” and builds a “value-based” compliance framework. Mr. Afzal is certified Green Belt for Lean Six Sigma.

Questions......

Contact Information:
Sulaiman Afzal
Cell: 734-474-3475
E-mail: sulaiman_afzal@comcast.net