

Technology & IP and Global Issues Forums: FCPA Compliance – Leading Practices, Tools and Techniques

Howard Scheck
David Cappellina
StoneTurn

Farzaneh Paslar
Honeywell

Joseph Terry
Samuel Davidoff
Williams & Connolly

Zoe Sharp
Optoro, Inc.

June 28, 2018



WILLIAMS &
CONNOLLY^{LLP}®

StoneTurn



Discussion Topics

1. Introduction
2. FCPA Overview
3. Risk Assessments
4. Prevention and Detection
5. Tools
6. Investigations
7. Resolution

Today's Panelists



Howard Scheck

Partner

StoneTurn



David Cappellina

Managing Director

StoneTurn



Farzaneh Paslar

General Counsel,
International Transactions
& Compliance

Honeywell



Joseph Terry

Partner

Williams & Connolly



Samuel Davidoff

Partner

Williams & Connolly

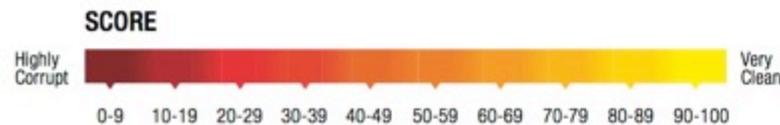
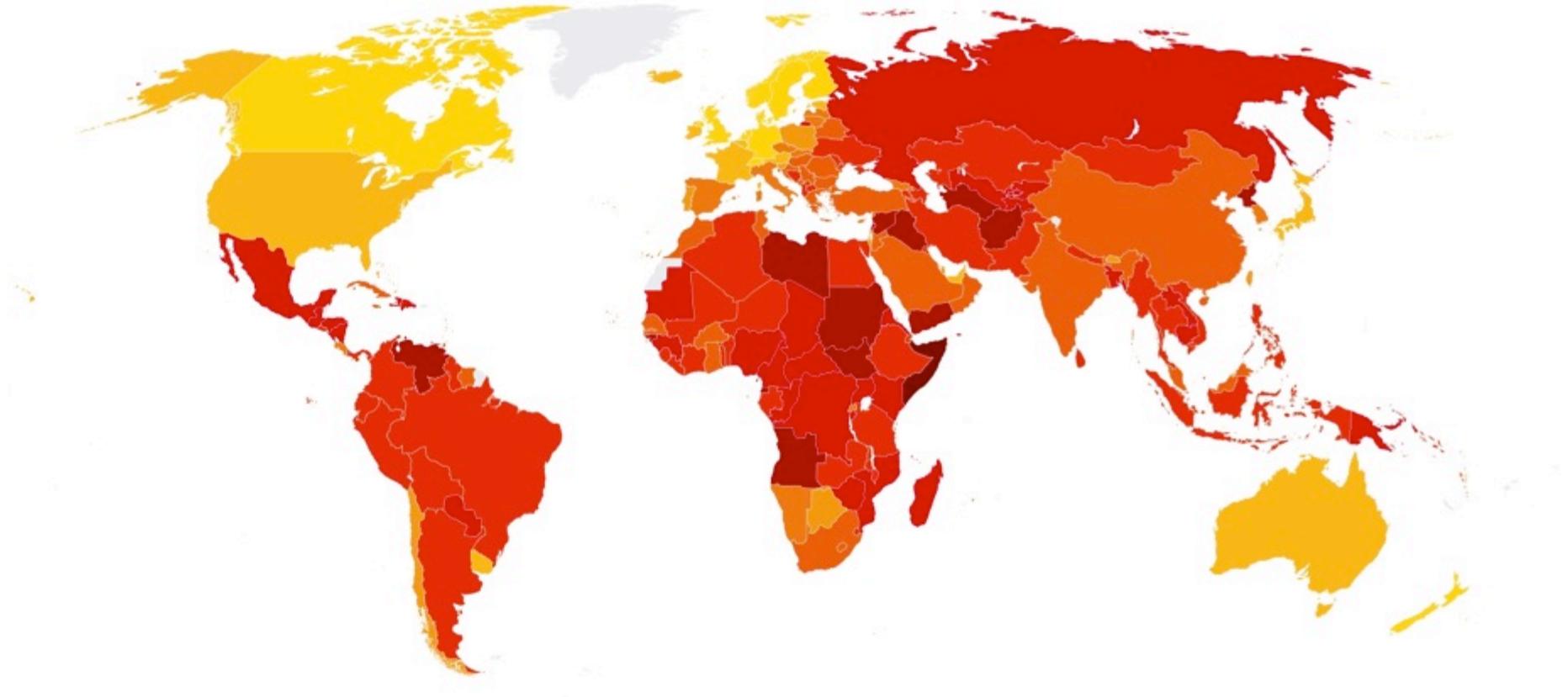


Zoe Sharp

(Moderator)
Deputy General Counsel

Optoro, Inc.

Global Corporations Face Corruption Challenges



#cpi2017

www.transparency.org/cpi

This work from Transparency International, 2018 is licensed under CC BY-ND 4.0

Overview: the U.S. Foreign Corrupt Practices Act (“FCPA”)

History

- Enacted in 1977 in response to the Watergate scandal. More than 400 U.S. companies admitted to paying over \$300 million in bribes to foreign officials.
- Three objectives:
 - (1) prevent and deter the payment of bribes to non-U.S. government officials;
 - (2) greater transparency in financial reporting; and
 - (3) create a level playing field for companies operating overseas.

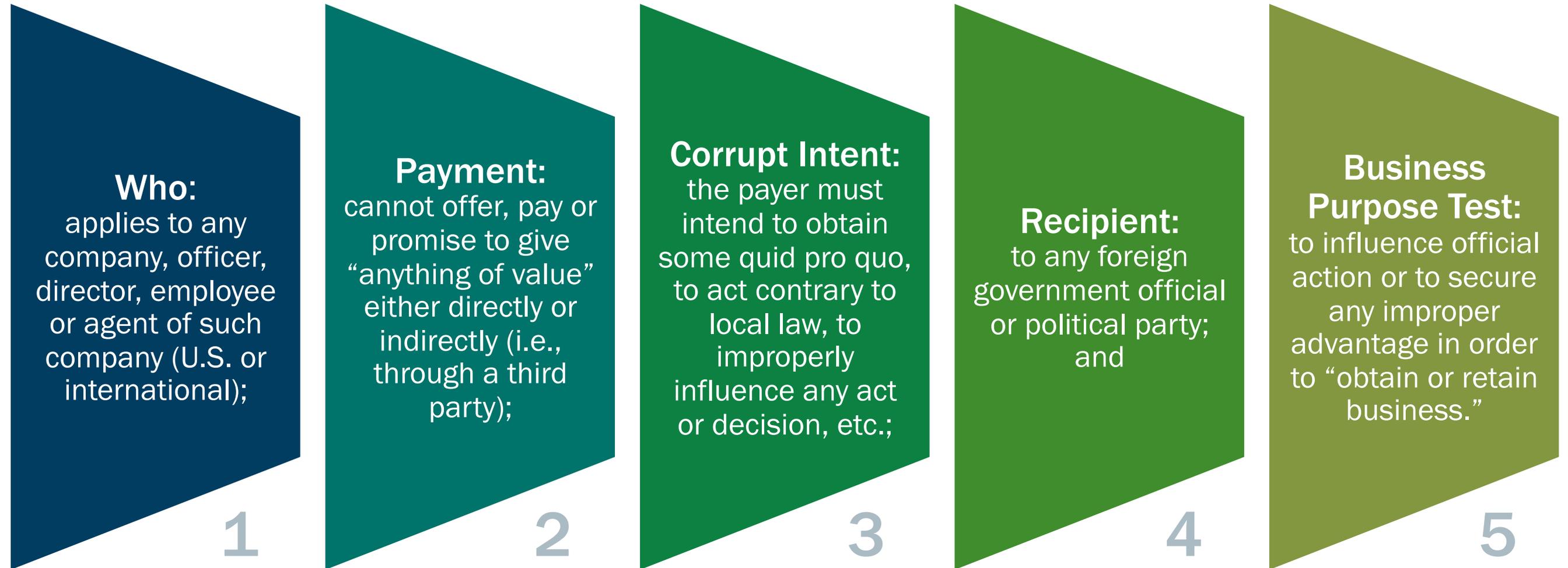
Anti-Bribery Provision

- Illegal to offer, promise, or make a corrupt payment to a foreign government official for the purpose of obtaining or retaining business.

Financial Reporting Provisions

- Books and Records Provisions
- Internal Control Provisions

Elements of the Anti-Bribery Provision



Prohibited Payments: it is unlawful to bribe foreign officials in order to obtain or retain business.

Financial Reporting Provisions

Who does the Books and Records Provision apply to?

- U.S. public companies registered with the U.S. Securities and Exchange Commission (“SEC”) and
- Foreign companies listed on U.S. stock exchanges.

What are the requirements of the Provision?

- Books and Records: maintain books, records and accounts, which in reasonable detail, accurately reflect transactions and dispositions of their assets.
- Internal Controls: devise and maintain a system of internal accounting controls to provide reasonable assurance that transactions are authorized by management and financial statements are in conformity with U.S. Generally Accepted Accounting Principles (“GAAP”).

**There is no
materiality
threshold
for the FCPA**

Risk Assessments

Importance

- Identify risks and gaps; areas to enhance policies, processes and internal controls (preventive and detective); and areas to focus monitoring and Anti-Corruption / FCPA-focused audits.
- Assist the Board and Management in determining the company's "risk appetite" and how tightly or loosely to design compliance control activities.

Performance

- Ownership: Risk and Compliance.
- Team: Compliance Professionals (typically attorneys, can include forensic accountants/ auditors), and internal audit.
- Process: surveys, walkthroughs, interviews, testing and workshops.
 - Risk matrices to rank / score (e.g., assessing legal / regulatory implications, financial impact, possibility of occurrence).
 - Tools: Corporate Intelligence, Data Analytics, Scoring Models, Dashboards.

Risk Assessments (cont'd).

Frequency

- Can vary based on industry, size of the company and nature of the risks.

U.S. Regulatory Expectations

- US Federal Sentencing Guidelines (one of the elements of an effective ethics and compliance program);
- Guidance
 - Evaluation of Corporate Compliance Programs, US Department of Justice – Criminal Division – Fraud Section:
<https://www.justice.gov/criminal-fraud/page/file/937501/download>
 - Anti-Corruption Ethics and Compliance Handbook for Business, OECD:
<https://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf>
 - A Resource Guide to the U.S. Foreign Corrupt Practices Act, By the Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission:
<https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf>

Other Countries

- Expectations and guidance country specific; we advise that your risk assessment consider country and local anti-corruption regulations and laws.

Prevention and Detection: Elements of an Anti-Corruption / FCPA Compliance Program

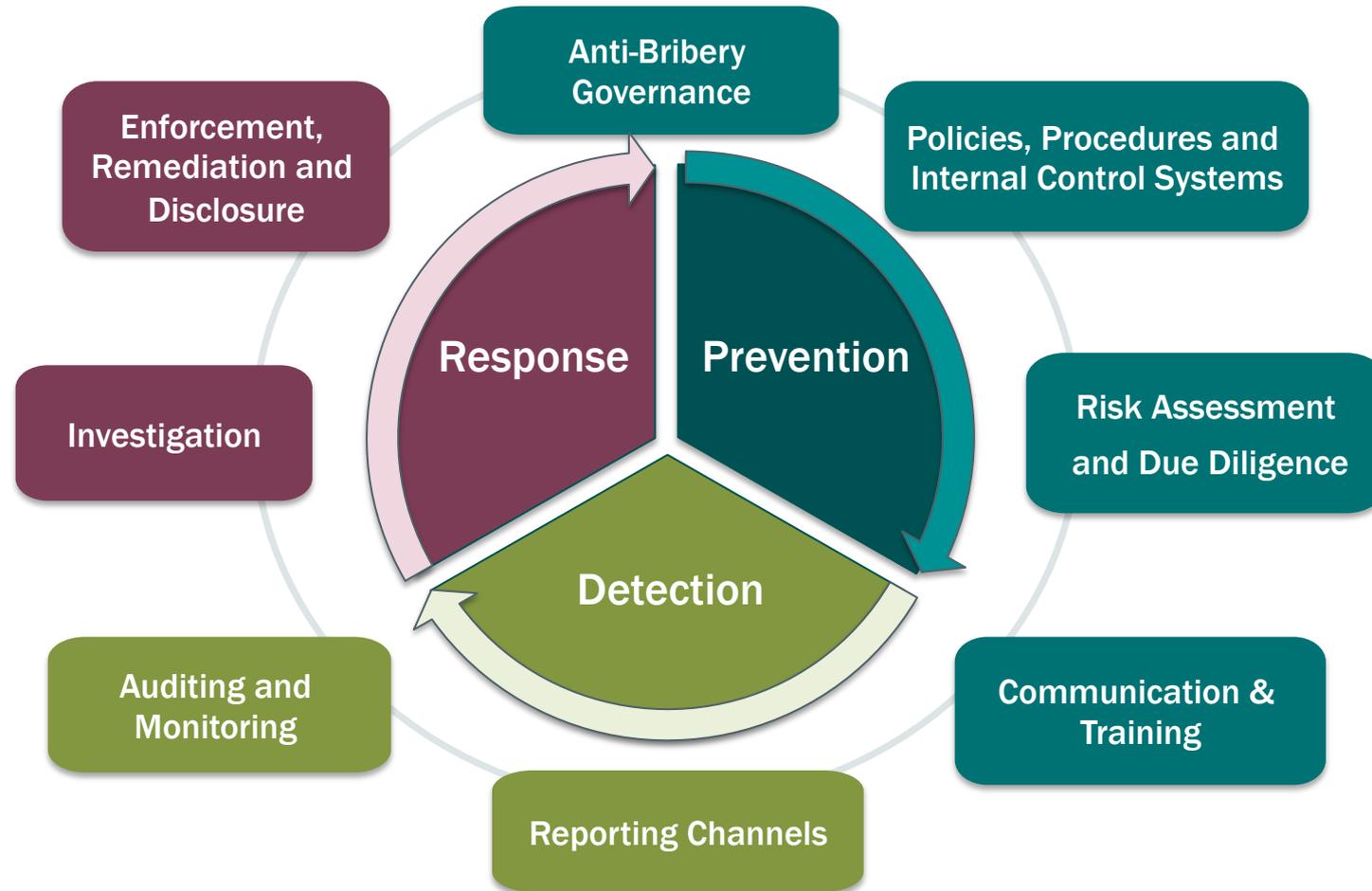
Effective compliance organization with autonomy from management and resources to affect sound anti-corruption controls.

Development and enforcement of policies and procedures including consistent application of disciplinary measures.

Incident response plan and policies to investigate alleged bribery or corruption.

Periodic activities to assess compliance with anti-corruption policies.

Mechanisms that allow for anonymous reporting of anti-corruption issues or concerns.



Policies, procedures and controls developed under the direction of the compliance officer and compliance committee with support from legal, operations and finance.

Ongoing assessment of internal and external corruption risks.

Anti-corruption policies and procedures are communicated to all impacted employees and business partners.

Prevention

- Board and Audit Committee Oversight
- Internal Audit, Compliance and Monitoring Functions
- Executive and Line Management Functions
- Bribery and Corruption Risk Assessment
- Code of Conduct
- Communication and Training
- Employee and Third Party Due Diligence
- Entity / Process Specific Controls

Includes:

- ✓ Setting proper “tone at the top”
- ✓ Establishing roles and responsibilities
- ✓ On-going assessment of internal and external risks
- ✓ Promoting a strong ethics program
- ✓ Designing, implementing and monitoring anti-corruption controls
- ✓ Training

Goals include preventing something “bad” from happening before its “too late”; stop activity that can lead to a violation of the FCPA.

Detection

- Hotlines and Whistleblower Mechanisms
- Vendor Due Diligence
- Compliance and Internal Audits
- Monitoring

Includes:

- ✓ Mechanisms that allow for anonymous reporting of issues or concerns.
- ✓ Management monitoring, self assessments
- ✓ Compliance program monitoring, testing
- ✓ Internal audit testing of controls
- ✓ Periodic activities to assess employees and third-party compliance.

According to the Association of Certified Fraud Examiners
“2018 Global Study of Occupational Fraud and Abuse”:

50% of Corruption Cases were detected by a tip!

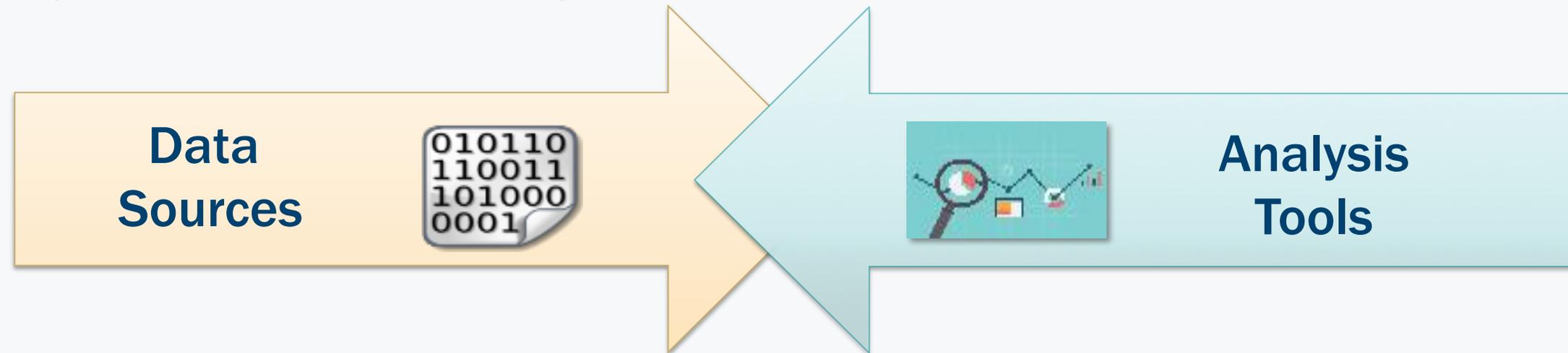
- Includes use of traditional whistleblower mechanism (e.g., email, telephone)
- Includes contacting directly (e.g., supervisor, executive, internal investigations or audit)

Goals include identifying potential improper payments or activities; investigate, remediate and resolve.

Tools: Data Analytics

What is “Data Analytics”?

- The process of inspecting, cleansing, transforming, and modeling data with the goal of discovering useful information, suggesting conclusions, and supporting decision-making.
- Employs a combination of statistics, mathematics, programming, and problem-solving to find patterns, trend and anomalies otherwise lost in a mass of information.
- Applying analysis tools and methodologies to available data sources.



Tools: Data Analytics

Anti-Corruption / FCPA

- Technology based approach to analyze relevant data that organizations routinely collect in the normal course of business, such as:
 - Cash disbursements, accounts payable, payroll, sales, commissions, travel and entertainment expenses, gifts, donations, vendor data.
- Analyzes 100% of data sets rather than using statistical sampling.
- Extracts additional value from these datasets by performing a series of comparisons, summaries, and aggregations, such as:
 - Identify irregularities and anomalies that may indicate patterns of anti-corruption/FCPA “red flags” and identify system and controls weaknesses.
- Analyzes, groups and prioritizes anomalies and “red flag” indicators for customers, vendors, and employees, including volume and magnitude.
- Can be utilized in compliance monitoring, during anti-corruption / FCPA audits, and in internal investigations.

Tools: Data Analytics Examples

Risks Identified	Data Sources	Example Data Analytic Routines
Third party vendors (including business partners) that interact with government entities and officials on behalf of the company.	Cash disbursements (including accounts payable and manual checks), consulting expenses, vendor master.	<ul style="list-style-type: none"> • Duplicate/split invoices/payments. • Multiple payments in a short period of time. • Payments to offshore accounts. • Payments to a bank account in the name of a different vendor. • Payments made near the date of contract termination.
Employee expense reimbursement used to make an improper payment to a government official.	Cash disbursements (including accounts payable and manual checks), travel and entertainment expenses, vendor master.	<ul style="list-style-type: none"> • Large reimbursements in relation to historical patterns. • Country visited or client entertained. • Multiple reports filed in a short period of time. • Ratio of expense to business/country area revenue not consistent with other businesses/countries.
Payments to politically exposed persons (“PEPs”), state owned enterprises (“SOEs”), person/entities on sanctions lists.	Third party PEP, SOE and sanctions lists, vendor master, cash disbursements, accounts payable.	<ul style="list-style-type: none"> • Key word searches. • Compare PEP, SOE and sanctioned entities and persons to vendor master and payee lists.
Transactions that present AC/FCPA risks improperly recorded in the “books and records”.	Higher risk expense accounts (e.g., consulting, miscellaneous), employee advances, manual checks, cash disbursements.	<ul style="list-style-type: none"> • Key word searches. • Frequency/trend analysis (e.g., one-time payment to vendor, payment outside normal range). • Payment methods (e.g., cash, manual checks, credit memos).

Challenges to Using Data Analytics Tools

■ Data Privacy

- Many countries have laws and regulations that impact the following:
 - Data you can collect and analyze (with emphasis on personally identifiable information);
 - Required disclosures to parties included in the data; and,
 - Movement of data being analyzed.
- Prior to planning any use of data analytics, consult with legal counsel to determine “the rules of the road”.
- General Data Protection Regulation (“GDPR”)
 - Recent EU law on data privacy that contains provisions and requirements pertaining to the processing of personally identifiable information of individuals inside the European Union.

■ Data Collection and Normalization

- Detail transaction data required for analysis (e.g., date, amount, payee, text fields, approvals, vendor detail) often resides in multiple accounting systems and sub ledgers “below” the main accounting system.
- The cost to map systems, identify relevant data, collect data and normalize data can be significant.
- Risk assessment results should be utilized to identify risk areas and associated data to consider for analytics.

Investigations

What are the first steps regarding a potential investigation?

- When do you notify, if necessary, regulatory bodies, law enforcement, and external auditors?
- What roles do the following play in an investigation?
 - Board, Management
 - General Counsel, Compliance, Internal Investigations, Internal Audit
 - Outside counsel
 - Forensic accountants
- What are the impacts of privacy and cross-border regulatory changes?

Investigations – First Steps

- Determine whether to handle in-house or retain outside counsel.
- Ensure relevant data is preserved, including through hold notices.
- Develop plan for review and identification of key documents.
- Develop a strategy for sequence of employee interviews.
- Identify a plan for addressing issues related to whistle-blowers and / or culpable employees.
- Consider whether there is an obligation or incentive to disclose early.
- Consider the existing controls and anticipate remediation that may be appropriate.

Disclosure and Notification Considerations

Disclosure Obligations

- ✓ Public companies
- ✓ Contracts
- ✓ Foreign laws

Disclosure Benefits

FCPA Corporate Enforcement Policy – U.S. Atty. Man. § 9.47.120

Presumption of declination, absent aggravating circumstances, when a company:

- ✓ Voluntarily self-discloses
- ✓ Fully Cooperates
- ✓ Timely and appropriately remediates
- ✓ Pays all disgorgement, forfeiture and/or restitution

Disclosure Risks

Company Roles

- Board of Directors/Committee Roles
- In House Counsel
 - Ensure proper and effective process
 - Maximize privilege protections (where available)
 - Maximize objectivity
 - Attorney / compliance officer / internal auditor, frequently with geographical proximity
- Other Team Members, Depending on Specifics
 - Business unit management?
 - Finance?
 - Communications?
 - Internal Audit?
 - HR?
 - Compliance?

The Role of the Outside Advisor

- Outside counsel
 - When to consider hiring outside counsel
 - Selecting appropriate outside counsel for the investigation
- Forensic accountants/investigators
- Other outside advisors
- Lines of reporting
- Who is hiring?

Cross-Border Privacy Considerations

European Union

- General Data Protection Regulation, effective May 25, 2018
- Data controller must have lawful basis for processing personal data or the data subject's express consent.
- GDPR can apply to collection and processing of data for an internal investigation if:
 - The data relates to the data controller's presence within the EU; OR
 - The data relates to data subjects who were physically within the EU at the time of the data collection and
 - The data controller provides goods or services within the EU; or
 - The data controller monitors the behavior of data subjects within the EU.
- Transfer of data to the United States may require additional safeguards
 - EU-U.S. Privacy Shield
 - Standard Contractual Clause
 - Binding corporate rules
 - Codes of conduct or certification mechanism

Cross-Border Privacy Considerations

China

- Cyber Security Law, effective June 1, 2017
- Draft Security Assessment measures, could be effective in coming months.
- Prohibits network operators from collecting personal information that is not relevant to the services they offer.
- Requires network operators to inform the data subject before collecting his or her data about the purpose, means, and scope of the collection.
- For data transfers, network operators must:
 - Notify data subject of type of information being transferred and to which country it will be transferred
 - Conduct internal security assessment
- It is not permissible to transfer data outside of China if doing so damages public and national interests, the security of national politics, the territory, military, economy, culture, society, technology, information, environment, resources or nuclear facilities, etc. of China.

Resolutions – DOJ / SEC

- Internal Changes
 - Controls
 - Third-party relationships
 - Employee discipline
- Declinations
- Settlement / NPA / DPA / Consent Decrees
 - Fines
 - Compliance / Remediation
 - Monitorship
- Litigation / Prosecution

Monitors

Role of Monitor

- Assess and monitor compliance with NPA or DPA
- Independent third party; not an employee or agent of the company or the Government

Scope and Duration

- Monitor's duties should no broader than necessary to address and reduce the risk of recurrence of misconduct.
 - Role is not to investigate historical misconduct.
- May be required to make periodic reports to the Government
 - Either the company or the Monitor must report to Government if company chooses not to adopt a Monitor's recommendation.
 - Monitor must report new or previously undisclosed conduct identified in the agreement.
 - Monitor should directly report certain types of misconduct to the Government (e.g., criminal activity or conduct that creates substantial risk of harm).
- Duration should be tailored to identified problems
 - DOJ policy advises that agreement should provide for extension at Government's discretion.

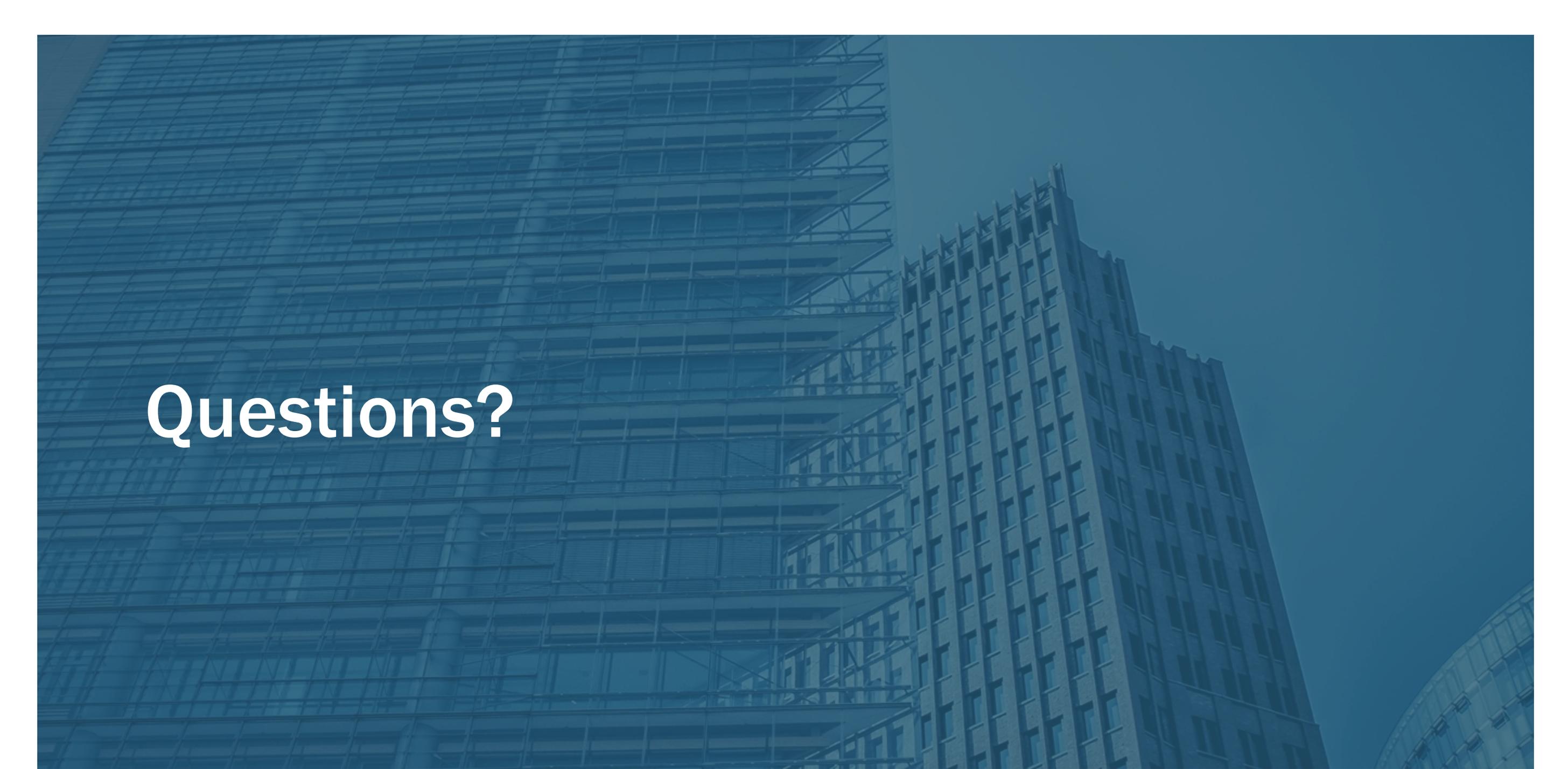
Monitors

Impact on Company

- Significant expense
- Practical effect of extending the investigation
- Potentially intrusive

Recent Developments

- Increased assignment of monitors in corporate settlements
- Interaction with Pilot Program / FCPA Corporate Enforcement Policy
 - In 2017, no company that self-reported FCPA violations to the DOJ was required to engage a corporate monitor.
- United States v. ZTE Corp. (N.D. Tex. 2017)
 - Court rejected DOJ / ZTE Corp. proposed plea agreement which set out terms for selecting a monitor.
 - Court appointed Monitor, similar to “special master”



Questions?

Disclaimer

The concepts and theories covered by this presentation are for discussion purposes only and are not intended to be all-inclusive on the topics.

Many of the concepts are illustrative only and do not necessarily represent the approaches or advice that StoneTurn, Williams & Connolly, ACC NCR, Honeywell or Optoro, Inc. would recommend in any particular case. Further, this presentation does not necessarily reflect the opinions of the presenters nor StoneTurn, Williams & Connolly, ACC NCR, Honeywell or Optoro, Inc. Finally, these materials may only be used by the recipient for educational purposes (including fair use) and may not be used for any other purpose including, but not limited to, litigation, deposition, or trial.

About StoneTurn

StoneTurn is a leading forensic accounting, corporate compliance and expert services firm. We “leave no stone unturned” when it comes to helping attorneys, corporations and government agencies solve high-stakes legal and compliance issues.

Learn more at [StoneTurn.com](https://www.stoneturn.com)

About Williams & Connolly

Williams & Connolly is widely recognized as one of the nation's premier litigation firms. Our lawyers routinely handle significant and complex civil, criminal, and administrative cases across the United States and around the globe. The firm maintains a strong tradition of hiring the best and the brightest and training and promoting its lawyers from within, producing a closely knit community of attorneys who work collaboratively to achieve successful outcomes for their clients.

Learn more at www.wc.com

Thank You!



Howard Scheck

StoneTurn

hscheck@stoneturn.com

+1 202 349 1131



David Cappellina

StoneTurn

dcappellina@stoneturn.com

+1 202 349 3809



Joseph Terry

Williams & Connolly

jterry@wc.com

+1 202 434 5320



Samuel Davidoff

Williams & Connolly

sdavidoff@wc.com

+1 202 434 5648



Farzaneh Paslar

Honeywell

farzenah.paslar@honeywell.com



Zoe Sharp

Optoro, Inc.

zsharp@optoro.com



Appendix

Risk Assessments: Process Steps Example

Inventory, Categorize and Rank

- Information gathering, e.g., document review, interviews, transaction testing and surveys.
- Analyze and inventory industry and organizational risks.
- Assess and rate the likelihood and significance of each risk identified.
 - Likelihood factors may include, among others:
 - Country of operations;
 - Known instances/allegations;
 - Previous history;
 - Pervasiveness of the risk across operations;
 - Complexity of the risk;
 - Results of employee and management interviews;
 - Criticisms by the media or NGOs;
 - Violations by other companies and industry peers; and
 - Government enforcement priorities and pronouncements.

Evaluate factors individually and in conjunction with one another, assigning a numerical value within a classification range. For example: Low (1-3), Moderate (4-6) and High (7-9).

Risk Assessments: Process Steps Example

Inventory, Categorize and Rank (cont.)

- Significance factors (qualitative and quantitative) may include, among others:
 - Criminal investigation;
 - Major class action litigation;
 - Major changes to corporate or business strategy;
 - Regulatory intervention/probation/sanction;
 - Resignation or dismissal of C-Level executives or business unit executives; and
 - National media attention.

Evaluate factors from a financial and non-financial impact standpoint, assigning a numerical value within a classification range. For example: Low (1-3), Moderate (4-6) and High (7-9).

- Determine risk rating considering likelihood and significance scores; rank risks.
- Use results to, for example:
 - Conduct a gap analysis to identify policies, procedures and controls that may require enhancements;
 - Identify business operations and transactions to monitor and audit; and
 - Revise training programs, content and delivery mechanisms.

Risk Assessments: a Tool to Enhance your Anti-Corruption/FCPA Compliance Program

Gap Analysis, Process Flow Walkthroughs,
Enhancement of Policies, Procedures and Controls

Risk Assessment

Rank	Risk Area	Risks Identified	Likelihood	Significance	Rating	Compliance Control Focus	Impacted Departments	Areas/Processes Requiring Policy/Control Enhancements
7	Licenses and Permits (operational)	LATAM Business Operations Use of Third Party consultants to make improper payments to government officials to obtain licenses and permits. Use of employees to make improper payments to government officials to obtain licenses and permits.	8	4	6	1. LATAM Business Unit (A) 2. Vendor screening (B) 3. Vendor contracting (C) 4. Vendor set-up/modifications (D) 5. Disbursements (E) 6. Expense reimbursement (F)	* Government Sales (A) * Compliance (B, D) * Legal (C, D) * Finance (D, E, F)	1. Training (A) 2. Procurement (A, B, C, D) 3. Accounts Payable, Petty Cash (E) 4. Travel and Entertainment (F) Reimbursements Advances

Policy and Control Enhancements (LATAM – Government Sales Dept.)

- Modify existing anti-corruption training to Government Sales management and the licenses and permits group by including practical scenarios.
- On the “Vendor/Supplier On-Boarding” form, include a definition of vendors/suppliers that require the application of due diligence procedures by Compliance.
- Add anti-corruption certification language to vendor contracts for those that interact with government officials on the company’s behalf.
- Add a financial control in the accounting system to block payments to vendors that are rejected by Compliance during the due diligence process; expand monitoring over payments made from petty cash or through manual checks.
- Add a policy that prohibits the use of cash advances.
- Add policies that clearly define supporting documents and approvals required by accounting before expense reimbursements are paid.

Anti-Corruption / FCPA Red Flags

General

- Operations in countries with:
 - high perceived risk for bribery and corruption challenges; and
 - historical bribery and corruption challenges.
- Operations in higher risk industries (e.g., defense, aircraft, energy, engineering, construction, IT, Pharma, Medical Device).
- Violations of local laws.
- Employee and / or intern related to foreign government official or royal family member.
- Unusual / abnormal increase in sales to state owned entities and / or government contract wins / revenue.
- General fraud and misconduct red flags.
- Lack of professional skepticism from Internal Audit, Finance and Operations.

Compliance Structure

- Insufficient “Tone at the Top”; complacent Board
- Lack of, or incomplete risk assessment.
- Policies and procedures not operationalized (e.g., policy says compliance authorizes payments of fines and penalties yet no processes or controls exist to enable this activity).
- Inadequate training program.
- Protocols regarding disciplinary procedures not followed consistently
- FCPA and other integrity certifications not executed by company, personnel, agents, joint venture partners, and/or other third parties
- Lack of segregation of duties.
- Failure to modify policies and procedures in response to past violations or regulatory changes.
- Reporting structure and authorization controls ignored or overridden, or not available.
- Limited oversight over foreign subsidiary or related parties.
- Lack or override of internal controls.
- Hotline calls not investigated.

Anti-Corruption / FCPA Red Flags (cont'd).

Third Party that Interacts with Foreign Government / Officials

(e.g., business partner, JV partner, sales agents, consultants, other)

- Family or business relationships with foreign government official or royal family member.
- Excessive fees, bonus and / or commissions; claims of special arrangements (e.g., “to get the business”).
- Payment through company expense reimbursement process
- Lump sum payments.
- Payments prior to executed contract or performance of work; vague or no contract.
- Payments to bank account in name of a different vendor; payments to bank account located in a country other than where the work is performed; and payment to offshore account.
- FCPA and other integrity certifications not executed by third party.
- Third party processing requests for payment to other third parties.

Books and Records

- Improper or missing authorizations.
- False invoices and / or other documents (e.g., duplicate invoice numbers, photocopies).
- Undocumented billings or disbursements.
- Incomplete invoices and / or supporting documentation.
- Supporting documents description of goods and services vague and / or is not consistent with the contract or statement of work.
- General ledger account description does not correlate with goods and services provided or supporting documentation.
- Unusual journal entries.
- Payments in cash, manual checks or to offshore accounts.
- Excessive fees and / or commissions; payments inconsistent with the going rates.
- Large payment recorded as several small payments, less than the threshold requiring additional levels of approval.
- Unusual bonuses paid to foreign operational managers.
- Transaction not recorded.
- Duplicate invoices.

Tools: Compliance Dashboards

- Some organizations use dashboards (or scorecards) as a shortcut to providing executives, board members and management information on their compliance program, identified risks, and program effectiveness.
- A significant challenge is determining what metrics to include. Metrics need to be specific and unique to your company, and risk based.
- Data and metrics can be derived from, for example, internal audit, compliance monitoring and management self assessment results.
- Effectiveness remains less a science and more an art. Creating the story around effectiveness requires an understanding of the data available, how to interpret the data, and how to design a report that communicates the status and effectiveness of your program to leadership, and if ever required, to enforcement authorities and industry regulators.

Example Compliance Dashboard

Compliance Dashboard: Anti-Corruption Program – China Lead Sheet						
Risk Areas	Last Assessment Completed	Last Assessment Score	Last Assessment Date	Compliance Monitoring		Comments
				Score	Period	
Sales Agents, Business Partners	Compliance Review A30		9/30/18		3 rd Qtr 2018	
Licenses, Permits, Fines and Penalties	Internal Audit Report 1205		6/30/18		3 rd Qtr 2018	Employee personal bank account used to pay health/safety fines – remediation action item due 10/23/18 (see Schedule A attached).
Donations	Internal Audit Report 1205		6/30/18		1 st Qtr 2018	
Gift Cards	Internal Audit Report 1205		6/30/18		1 st Qtr 2018	
Petty Cash	Internal Audit Report 1205		6/30/18		1 st Qtr 2018	
Travel and Entertainment	Internal Audit Report 1205		6/30/18		3 rd Qtr 2018	Sales managers not completing all required forms - remediation action item due 10/15/18 (see Schedule A attached).
Sales to State Owned Enterprises	Compliance Review A30		9/30/18		3 rd Qtr 2018	Insufficient supporting documentation – remediation action item due 10/15/18 (see Schedule A attached).

 Program operating as designed
  Area requiring reinforcement
  Area requiring improvement



Prevention: Methodologies and Approaches to Mitigate Risk

Area	Overview	Leading Practice
Board and Audit Committee Oversight	Board and Audit/Compliance Committee provide oversight over programs and controls to prevent, detect and respond to alleged violations of laws and regulations.	Cross-functional compliance committee includes a designate to provide oversight of AC/FCPA initiatives.
Internal Audit, Compliance and Monitoring Functions	Conduct periodic risk assessments; monitor compliance program (policies, procedures, controls); and test effectiveness of programs and controls.	Internal audit professionals that support the compliance function have AC/FCPA knowledge and experience.
Executive and Line Management Functions	Typically includes C-Level Officers and leaders of business units or country-level operations. Responsible for day-to-day implementation of AC/FCPA program.	Business, operating and strategic plans and reports will include information that illustrates consideration of AC/FCPA risks.
Bribery and Corruption Risk Assessment	Risk assessment provides information that enables the development of effective controls to prevent, detect and respond to risks.	Transaction testing is included in the risk assessment process to verify information obtained from interviews and document reviews.
Code of Conduct and Related Standards	Clarifies an organization's mission, values and principles, linking them with standards of professional conduct.	Code of Conduct includes specific guidance and AC/FCPA regulatory requirements.
Communication and Training	Risk based; customize approach that considers job title, business area and level of perceived anti-corruption risk.	In-person/instructor led training recommended for employees in higher-risk areas; computer based learning for others. Training conducted in local language by a natural born citizen is more effective.
Employee and Vendor Due Diligence	Prior to hiring an employee or on-boarding a vendor, HR and compliance due diligence procedures to identify potential AC / FCPA risks.	Vendors that will interact with government officials on a companies behalf are screened for AC/FCPA risks before on-boarding.
Entity and Process-Specific Anti-Corruption("AC")/FCPA Controls	Includes preventive, detective, manual, computer and management controls.	Job aides are developed to assist employees responsible for authorizing and reviewing AC/FCPA related transactions.

Detection: Methodologies and Approaches to Mitigate Risk

Area	Overview	Leading Practice
Hotlines and Whistleblower Mechanisms	Internal reporting system whereby employees and/or external parties can report suspected wrongdoing related to AC/FCPA matters.	Protocols and policy is developed to identify the nature of allegations that are escalated to the audit committee.
Vendor Due Diligence	Subsequent to on-boarding a vendor, compliance will conduct periodic due diligence procedures to identify potential anti-corruption/FCPA risks.	Vendors that interact with government officials on behalf of the company are periodically re-screened for AC/FCPA risks.
Compliance and Internal Audits	Audit procedures are in place to test AC/FCPA program elements, including testing the effectiveness of controls and identifying transactions that present AC/FCPA “red flags”.	Use of data analytics and related tools to perform testing.
Monitoring	Management is responsible for monitoring the quality and effectiveness of AC/FCPA programs and controls.	Utilize an AC/FCPA risk assessment to allocate resources to areas that present the highest risk to the company. Compliance group includes forensic accountants and auditors that can use audit testing procedures to monitor higher-risk transactions.

Data Analytics – Asset and Expense Accounts of Interest When Monitoring and Testing

- Advertising Expenses
- Business Development Expenses
- Cash
- Cash Advances
- Charitable Contributions/Donations
- Consulting Fees
- Customs Fees and Duties (including customs brokers and freight forwarders)
- Discounts
- Employee Advances
- Extraordinary Fees and Expenses
- Facilitating and Expediting Fees
- Gifts
- Fines and penalties
- Hospitality

- Licenses and Permits
- Lobbying
- Marketing Expense
- Miscellaneous
- Payroll
- Per Diem
- Petty Cash
- Political Contributions
- Professional Services
- Promotional and/or Conference Expenses
- Rebates
- Sponsorships
- Subcontractor payments
- Taxes
- Travel and Entertainment

Tools: Data Analytic Solutions

Analytics Tools

Most flexible, these analytics tools require analysts to program, code, or manipulate the data to perform ad-hoc analyses. Many of these tools are available for free.

- [Microsoft Excel](#)
- [SQL](#)
- [Python](#)
- [R](#)
- [VBA / .NET](#)

Vendor-Supplied Tools

Least flexible vendor supplied tools that are similar to BI Tools but often set-up with anti-corruption-focused default reports or analytics.

Sometimes customization is available, but may require vendor intervention or additional cost. Typically costs are a combination of set-up and monthly subscription fees.

- [CaseWare Analytics](#)
- [ACL](#)
- [Oversight Technologies](#)
- [MetricStream](#)
- [LogicGate](#)

Business Intelligence (“BI”) Tools

Less flexible than analytics tools, these programs allow for consistent presentation (visual or tabular) of large data sets.

BI tools allow for customization, but may require expertise in initial set-up or development. Many of these tools have free single-user licenses, but are more costly for enterprise installation.

- [Tableau](#)
- [Power BI](#)
- [QlikView](#)
- [ThoughtSpot](#)
- [Looker](#)

Resolution

What are the different types of resolutions with the DOJ and SEC?

DOJ

Criminal Complaints, Information, and Indictments

Plea Agreements

Deferred Prosecution Agreements

Non-Prosecution Agreements

Declinations

SEC

Civil Injunctive Actions and Remedies

Civil Administrative Actions and Remedies

Deferred Prosecution Agreements

Non-Prosecution Agreements

Termination Letters and Declinations

Source: A Resource Guide to the U.S. Foreign Corrupt Practices Act, By the Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission: <https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf>

FCPA Monitorships

What is a Compliance Monitor?

- A monitor is an independent third party who assesses and monitors a company's adherence to the compliance requirements of an agreement that was designed to reduce the risk of recurrence of the company's misconduct.

When is it Applied?

- Deferred and Non-Prosecutorial Agreements.

Factors DOJ and SEC consider when determining whether a compliance monitor is appropriate include:

- Seriousness of the offense.
- Duration of the misconduct.
- Pervasiveness of the misconduct, including whether the conduct cuts across geographic and/or product lines.
- Nature and size of the company.
- Quality of the company's compliance program at the time of the misconduct.
- Subsequent remediation efforts.

FCPA Monitorships

Monitor's Goals

Provide assurance to the government that:

- The company has a strong compliance program;
- There are sufficient controls/program in place to prevent similar conduct;
- If such conduct were to occur that the program would identify it whether it be independently or through a whistleblower; and
- That the conduct will be handled/remediated properly.

Challenges Companies May Face with a Monitor

- Monitors do not always employ business reasonableness; there is a cost/benefit to all decisions and sometimes the 'gold standard' is not reasonable (e.g., putting contracts in place with every single supplier, while ideal, is not always realistic particularly for small suppliers).
 - Companies should be prepared to offer alternative solutions based on its risk assessments.
- Monitors can “scare” employees and impact productivity. Your typical employee is not used to being questioned by attorneys or forensic accountants.
 - Companies should communicate the role of the monitor clearly and frequently to employees impacted by the monitorship.

FCPA Monitorships

Challenges Companies May Face with a Monitor (cont.)

- Scope has the potential to “get out of hand” as there is no 'template' for a work plan that monitors are required to follow. It is important for the compliance team to make sure the monitor stays within their defined scope without obstructing their work - it is a delicate balance.
 - Open communication with the monitor and regulators is advised when significant disputes arise.
- White collar crime attorneys that are monitors are used to conducting investigations; in such instances that require a monitor the conduct has already been uncovered but monitors tend to want to see if there is any additional conduct from a historical perspective which is not their role.
 - Open communication with the monitor and regulators is advised when significant disputes arise.

FCPA Monitorships

Benefits a Monitor May Provide

- An independent and unbiased assessment of a company's compliance program.
- Expertise on best practices to benchmark the company's compliance program against other programs.
- Establishes a 'focus' on compliance and can act as a 'hammer' for compliance teams (e.g. “the monitor says we need...”).
- Focuses upper management on compliance and helps to set an appropriate tone at the top (C-Suite and Board level).
- Companies tend to invest in compliance tools to strengthen their program which otherwise may not have been on the table had a monitor not been in place.