FRAUD, BRIBERY, AND ANTI-CORRUPTION

STEVEN KUZMA
Senior Managing Director,
Forensic Investigation and Litigation Services

ROBERT MROZ
Managing Director,
Forensic Investigation and Litigation Services
Steve is a Senior Managing Director in BDO’s Forensic Investigation and Litigation Services (FILS) Advisory practice in Atlanta, Georgia. He has more than 40 years of experience providing Fortune 1000 company senior management teams, corporate boards, audit committees, and large law firms with assistance on complex issues in the areas of corporate compliance, commercial disputes, fraud and forensic investigations, lost profits, bankruptcy and insolvency, insurance claim/business interruption, franchise and dealership disputes, economic valuation, and damages analysis. He has testified in deposition, arbitration and in federal and state courts throughout the United States.

Robert is a Managing Director in BDO’s Forensic Investigations and Litigation Services (FILS) Advisory practice and the West Region Practice Leader for FILS. He has over 30 years of experience in helping counsel and clients resolve complex business issues, providing dispute advisory services in litigation, forensic accounting and valuation matters, as well as bankruptcy and receivership matters. Robert is responsible for the design and implementation of projects and has provided support to clients in many industries, ranging from manufacturing, distribution, mining, insurance, oil and gas, and coal concerns to fast food franchises, construction, and real estate entities.
Today’s Agenda

- Fraud and Corruption (Overview and Impact)
- Risk Assessments
- Effective Compliance Programs
  - Elements of a Corporate Compliance Program (2019 DOJ Guidance)
- General Data Protection Regulation (GDPR) Impact on Fraud, Bribery, and Anti-Corruption
Recent Enforcement Actions - Compliance Failures

<table>
<thead>
<tr>
<th></th>
<th>AIRBUS</th>
<th>ERICSSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>2020</td>
<td>2019</td>
</tr>
<tr>
<td>Violation</td>
<td>Anti-bribery and Corruption, Arms Export Control Act and International</td>
<td>Anti-bribery and Corruption</td>
</tr>
<tr>
<td></td>
<td>Traffic in Arms Regulations</td>
<td></td>
</tr>
<tr>
<td>Countries</td>
<td>Various (e.g., China, Japan, Russia, Ghana, Indonesia, Vietnam, Austria,</td>
<td>Djibouti, China, Egypt, Vietnam, Indonesia, and Kuwait</td>
</tr>
<tr>
<td></td>
<td>Mexico, Malaysia, Taiwan, Sri Lanka)</td>
<td></td>
</tr>
<tr>
<td>Schemes</td>
<td>▶ Irregularities in payments made to third-party consultants</td>
<td>▶ Payments to agents, consultants, and service providers through sham</td>
</tr>
<tr>
<td></td>
<td>▶ Establishment of a purported “educational” fund that was used to</td>
<td>contracts</td>
</tr>
<tr>
<td></td>
<td>host social events for government officials</td>
<td>▶ Payment of phony invoices to create off-book slush funds</td>
</tr>
<tr>
<td></td>
<td>▶ Payments to relatives of government officials</td>
<td>▶ Bribes for insider tender info</td>
</tr>
<tr>
<td></td>
<td>▶ Lavish gifts/entertainment</td>
<td>▶ Improper travel and entertainment for government officials</td>
</tr>
<tr>
<td>Bribe</td>
<td>Employees of state-owned and state-controlled airlines; Other</td>
<td>Employees of state-owned and state-controlled technology companies</td>
</tr>
<tr>
<td>Recipient(s)</td>
<td>government officials</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td>▶ Lack of third-party oversight</td>
<td>▶ Lack of third-party oversight</td>
</tr>
<tr>
<td>Program</td>
<td>▶ Failure in due diligence controls</td>
<td>▶ Failure in due diligence controls</td>
</tr>
<tr>
<td>Failures</td>
<td></td>
<td>▶ Failure in internal accounting controls</td>
</tr>
<tr>
<td>Method</td>
<td>Whistleblower; led to an internal investigation</td>
<td>From a “voluntary request” for information from U.S. authorities</td>
</tr>
<tr>
<td>Uncovered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government</td>
<td>$4B</td>
<td>$1B Compliance Monitor</td>
</tr>
<tr>
<td>Penalties</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fraud and Corruption - Impact
ACFE and BDO Insights

► ACFE reports 5% of annual revenue is lost to fraud.

► BDO’s 2020 survey showed a majority of CFOs identify Fraud, Data Privacy Breaches, Regulatory Uncertainty, and/or Reputational Damage as their greatest business threats in 2020.

► BDO’s 2020 survey noted CFOs' biggest regulatory compliance challenges include Data Privacy, Anti-Bribery and Corruption, and Anti-Trust.

► BDO’s 2020 survey illustrated that CFOs view “Keeping up with Regulatory Changes” as their biggest challenge.

Sources: ACFE’s 2018 Report To The Nations On Occupational Fraud and Abuse; 2020 BDO CFO Survey Risk Management Findings
Copyright 2018 by the Association of Certified Fraud Examiners, Inc.
ACFE’s Fraud Classification

- Corruption
  - Conflicts of Interest
  - Bribery
  - Illegal Gratuities
  - Economic Extortion

- Asset Misappropriation
  - Cash
    - Theft of Cash On Hand
    - Theft of Cash Receipts
    - Fraudulent Disbursements
  - Inventory and All Other Assets

- Financial Statement Fraud
  - Net Worth/Net Income Overstatements
  - Net Worth/Net Income Understatements
### Why Is This Important?

**ACFE Fraud Profile**

<table>
<thead>
<tr>
<th>Risk by Industry:</th>
<th>Corruption</th>
<th>Asset Misappropriation</th>
<th>Financial Statement Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Energy</td>
<td>$250,000</td>
<td>$114,000</td>
<td>$800,000</td>
</tr>
<tr>
<td>2. Manufacturing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Government</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Transportation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Insurance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% of Cases:</td>
<td>38%</td>
<td>89%</td>
<td>10%</td>
</tr>
</tbody>
</table>

### Other Considerations:
- Regulatory fines and penalties as well as remediation costs can be extremely large
- Highest risk regions include Asia Pacific, EMEA, and South America
- 50% of cases detected by tip

### Other Considerations:
- Most common and least costly fraud category
- 38% of cases detected by tip
- Small companies (<100 employees) are at a higher risk

### Other Considerations:
- Although uncommon, financial statement fraud can have a large impact on companies
- 38% of cases detected by tip

Source: ACFE’s 2018 Report To The Nations On Occupational Fraud and Abuse
Copyright 2018 by the Association of Certified Fraud Examiners, Inc.
Evaluating Your Company’s Risks

RISK ASSESSMENT
Risk Assessment
Overview, Considerations, and Best Practices

- A risk assessment is the starting point for building an effective compliance program and understanding the company’s risk environment.
- Risk assessments can include a variety of risk areas including fraud, corruption, money laundering, sanctions, data privacy, employment, contract terms, health, safety, etc.
- Without an effective risk assessment, it is highly unlikely the compliance program or remediation efforts will be effective.
- One-size-fits-all compliance programs are generally ineffective.
- Focusing on minor infractions (e.g., T&E expenditures) can drive program inefficiencies.
- Risk assessment approach and related compliance efforts should be risk-based.

“Assessment of risk is fundamental to developing a strong compliance program, and is another factor DOJ and SEC evaluate when assessing a company’s compliance program.”

DOJ and SEC - A Resource Guide to the FCPA
Risk Assessment
Supporting the Compliance Program Design

1. Policies & Procedures
2. Training & Communications
3. Confidential Reporting & Investigations
4. Third-Party Management
5. Mergers & Acquisitions

1. Senior Management Commitment
2. Autonomy & Resources
3. Incentives & Disciplinary Measures

1. Analysis & Remediation of Underlying Misconduct
2. Continuous Improvement, Testing, & Review
3. Investigation of Misconduct
### Risk Assessment
Understanding the Risk Universe

#### Types of Risk

<table>
<thead>
<tr>
<th>Legal &amp; Regulatory</th>
<th>Business Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud</td>
<td>Ethics &amp; Integrity</td>
</tr>
<tr>
<td>Bribery &amp; Corruption</td>
<td>Corporate Social Responsibilities</td>
</tr>
<tr>
<td>Anti-Trust</td>
<td>Contractual Obligations</td>
</tr>
<tr>
<td>Anti-Money Laundering</td>
<td>Vendor Management</td>
</tr>
<tr>
<td>International Trade</td>
<td>Public Commitments</td>
</tr>
<tr>
<td>Data Privacy</td>
<td>Voluntary Standards</td>
</tr>
<tr>
<td>Corporate Governance</td>
<td>Emerging Issues</td>
</tr>
<tr>
<td>Government Contracts</td>
<td></td>
</tr>
<tr>
<td>Labor &amp; Employment</td>
<td></td>
</tr>
<tr>
<td>Environmental</td>
<td></td>
</tr>
</tbody>
</table>

#### Risk Factors (examples)

- Geography
- Third Parties
- Business Industry
- Customer Network
- Employee Network
- Go-To-Market Strategy
- Product
- Raw Materials
- Licenses/Permits
- Government Oversight
- Regulatory Environment

#### Risk Evaluation

- Likelihood
- Priority
- Impact
- Pervasiveness
Risk Assessment
Methodology

<table>
<thead>
<tr>
<th>STEP 1</th>
<th>STEP 2</th>
<th>STEP 3</th>
<th>STEP 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define Objectives &amp; Develop a Plan</td>
<td>Information Gathering</td>
<td>Assess &amp; Evaluate Risk</td>
<td>Risk Response Plan</td>
</tr>
</tbody>
</table>
STEP 1 - DEFINE OBJECTIVES & DEVELOP A PLAN
What should be accomplished?

Goals and objectives should be defined in the context of the organization’s business strategy

<table>
<thead>
<tr>
<th>Define Objectives</th>
<th>Develop a Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Identify Risks to be Assessed and Evaluated</td>
<td>► Develop a Process for Analyzing Risks</td>
</tr>
<tr>
<td>► Determine End Goals of the Risk Assessment</td>
<td>► Create a Timeline</td>
</tr>
<tr>
<td></td>
<td>► Establish a Project Team</td>
</tr>
<tr>
<td></td>
<td>► Determine Key Stakeholders</td>
</tr>
<tr>
<td></td>
<td>► Identify Roadblocks / Barriers to Success</td>
</tr>
</tbody>
</table>
Risk Assessment
Methodology

STEP 2 - INFORMATION GATHERING

<table>
<thead>
<tr>
<th>Employee Feedback</th>
<th>Document Review</th>
<th>Industry / Business Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Survey</td>
<td>Policies</td>
<td>Recent News and Events</td>
</tr>
<tr>
<td>Interviews</td>
<td>Prior Audits</td>
<td>Enforcement Actions</td>
</tr>
</tbody>
</table>

- **Legal / Compliance**
  - Known compliance issues, whistleblower allegations
  - Tone at the Top, knowledge of company policies and procedures

- **Leadership**

- **Accounting / Finance**
  - Process walkthroughs of internal financial controls

- **Sales**
  - Client entertainment, route to market, and competitive market

- **Marketing**
  - Rebates, discounts, promotions, and samples

- **HR**
  - Compensation and bonuses, hiring/promotion procedures, and internships

- **Operations**
  - Licenses, permits, inspections, and customs
Risk Assessment
Methodology

STEP 3 - ASSESS & EVALUATE RISK

| Data Analytics/ Risk Mapping | ► Data Analytics   
|                             | ► High-risk Accounts   
|                             | ► Red Flags & Anomalies |

| Transaction Testing         | ► Review of Supporting Documentation   
|                             | ► Transaction Walkthroughs |

| Follow-up Interviews        | ► Interviews of Process Owners |

Interviews and transaction testing often inform one another
STEP 4 - RISK RESPONSE PLAN

Evaluating Effectiveness

- How often are risk assessments performed?
- Are risk assessments performed when there are changes to the business, industry, or regulatory landscape?
- Do the results of the risk assessments trigger changes to the key elements of your compliance program?
Input from the Risk Assessment helps drive improvements across the key elements of the compliance program:

- **Policies & Procedures**
  - Incorporate guidance and insight into newly identified risk areas
  - Update business procedures to include key controls

- **Training & Communications**
  - Train employees on developing risks, best practices, and new policies and procedures
  - Identify training gaps
  - Incorporate real-life examples (identified through the assessment)

- **Confidential Reporting Structure & Investigation Process**
  - Evaluate need to improve communications around the reporting tool
  - Benchmark usage with industry best practices
  - Roll out additional resources to international locations

- **Third-Party Management**
  - Evaluate need to add certain third parties to the management process
  - Incorporate newly identified procedures or tools to further improve processes

- **Mergers & Acquisitions**
  - Evaluate due diligence procedures around M&A activities
  - Incorporate forensic due diligence procedures where deemed necessary
**History Of Compliance Program Guidance**

1977
- **Foreign Corrupt Practices Act**: Made it illegal for certain classes of persons and entities to make corrupt payments to foreign government officials.

1991
- **Federal Sentencing Guidelines for Organizational Crime**: Issued by the U.S. Sentencing Commission (USSC).

2001
- **US Patriot Act**: Directed financial institutions to expand their AML compliance programs and step up their due diligence. Reports on foreign bank accounts.

2002
- **Sarbanes-Oxley Act**: Poses a new set of standards, establishes corporate responsibility, and requires certification of executive management.

2004
- **USSC Amendment**: Further enhances guidance on the 7 key elements of an effective compliance program.

2008
- **DOJ’s Principles of Federal Prosecution of Business Organizations**: Outlined factors to consider when scrutinizing a compliance program.

2009
- **OECD’s Recommendation for Further Combating Bribery of Foreign Public Officials**: Enhanced the ability of the States Parties to the Anti-Bribery Convention to prevent, detect, and investigate allegations of foreign bribery.

2010
- **Healthcare Reform Act**:mandates all healthcare providers and suppliers who participate in federal programs to establish and maintain compliance programs.

2012
- **A Resource Guide to the FCPA**: DOJ and SEC guidance on how to comply with the FCPA.

2017
- **HCCA-OIG’s Measuring Compliance Program Effectiveness**: Guide on measuring the effectiveness of a healthcare organization’s compliance program.

2019
- **DOJ's Evaluation of Corporate Compliance Programs**: Updates prior DOJ guidance to consider three primary questions including whether the compliance program is well-designed, implemented effectively, and works in practice.

2019
- **OFAC’s Framework on Sanctions Compliance**: First official guidance on how sanctions compliance programs are evaluated.

---

*Timeline is not intended to be exhaustive.*
Effective Compliance Programs
DOJ Guidance 2019

1. Is the Program Well-Designed?
   - Risk Assessment
   - Policies & Procedures
   - Training & Communications
   - Confidential Reporting Structure & Investigation Process
   - Third-Party Management
   - Mergers & Acquisitions

2. Is the Program Effectively Implemented?
   - Commitment By Senior & Middle Management
   - Autonomy & Resources
   - Incentives & Disciplinary Measures

3. Does the Program Work In Practice?
   - Analysis & Remediation of Any Underlying Misconduct
   - Continuous Improvement, Periodic Testing, & Review
   - Investigation of Misconduct

Analysis & Remediation of Any Underlying Misconduct
Continuous Improvement, Periodic Testing, & Review
Investigation of Misconduct

1. Is the Program Well-Designed?
2. Is the Program Effectively Implemented?
3. Does the Program Work In Practice?
## Evolution of DOJ Guidance

<table>
<thead>
<tr>
<th>“Seven Elements”</th>
<th>2017 Guidance</th>
<th>2019 Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance officer / Compliance committee</td>
<td>Risk assessment</td>
<td>Risk assessment</td>
</tr>
<tr>
<td>Standards, policies, &amp; procedures</td>
<td>Policies &amp; procedures</td>
<td>Policies and procedures</td>
</tr>
<tr>
<td>Training &amp; education</td>
<td>Training &amp; communications</td>
<td>Training &amp; communications</td>
</tr>
<tr>
<td>Effective lines of communication</td>
<td>Confidential reporting structure &amp; investigation process</td>
<td>Confidential reporting structure &amp; investigation process</td>
</tr>
<tr>
<td>Internal auditing &amp; monitoring</td>
<td>Third-party management</td>
<td>Third-party management</td>
</tr>
<tr>
<td>Investigations &amp; disciplinary guidelines</td>
<td>Mergers &amp; acquisitions</td>
<td>Mergers and acquisitions</td>
</tr>
<tr>
<td>Corrective action</td>
<td>Commitment by senior &amp; middle management</td>
<td>Commitment by senior &amp; middle management</td>
</tr>
<tr>
<td></td>
<td>Autonomy &amp; resources</td>
<td>Autonomy &amp; resources</td>
</tr>
<tr>
<td></td>
<td>Incentives &amp; disciplinary measures</td>
<td>Incentives &amp; disciplinary measures</td>
</tr>
<tr>
<td></td>
<td>Analysis &amp; remediation of any underlying misconduct</td>
<td>Analysis &amp; remediation of any underlying misconduct</td>
</tr>
<tr>
<td></td>
<td>Continuous improvement, periodic testing, &amp; review</td>
<td>Continuous improvement, periodic testing, &amp; review</td>
</tr>
<tr>
<td></td>
<td>Investigation of misconduct</td>
<td>Investigation of misconduct</td>
</tr>
</tbody>
</table>

- **Is the Program Well-Designed?**
- **Is the Program Effectively Implemented?**
- **Does the Program Work In Practice?**
Critical factors in evaluating a compliance program include whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees, is enforced by management, and is well-integrated into the company’s operations and workforce.
Effective Compliance Programs
DOJ Guidance 2019

2. Is the Program Effectively Implemented?

- Commitment By Senior & Middle Management
- Autonomy & Resources
- Incentives & Disciplinary Measures

The program must be more than a “paper program” and should be actively implemented, reviewed, and revised, as appropriate, with enough staff and clear management support.
An assessment of whether a program is effective in the event of misconduct should consider if and how the misconduct was detected, what resources were in place to investigate, and the nature and thoroughness of remedial efforts. The effectiveness of the program should be assessed over time, including whether the program is evolving to address existing and changing compliance risks.
GENERAL DATA PROTECTION REGULATION (GDPR) IMPACT ON FRAUD, BRIBERY, AND ANTI-CORRUPTION
General Data Protection Regulation
Impact On Fraud, Bribery, and Anti-Corruption

Do GDPR requirements limit the effectiveness of anti-bribery due diligence best practices?

<table>
<thead>
<tr>
<th></th>
<th>Non-Criminal Personal Data</th>
<th>Special Category Data</th>
<th>Criminal Convictions and Offenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>“There is currently no clear reliable legal basis under the GDPR that could unquestionably legitimize the processing of any—even of non-criminal nature—personal data as part of anti-bribery due diligence.”</td>
<td>“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.”</td>
<td>“Processing of personal data relating to criminal convictions and offenses” can only be carried out under the control of government authorities or when authorized by an EU or an EU Member State law that provides “appropriate safeguards for the rights and freedoms of data subjects.”</td>
</tr>
<tr>
<td></td>
<td>GDPR Article 6</td>
<td>GDPR Article 9</td>
<td>GDPR Article 10</td>
</tr>
</tbody>
</table>

In response, a few of EU Member States (including Ireland, Austria, Denmark, France, and a few others) recently adopted regulations to allow personal data processing for due diligence. Most countries do not have such laws yet.
## General Data Protection Regulation
### Impact On Fraud, Bribery, and Anti-Corruption

**How do you manage GDPR requirements and best practices? How do you operate with these restrictions?**

<table>
<thead>
<tr>
<th><strong>CHECK AUTHORIZATION</strong></th>
<th><strong>DOCUMENT BALANCING TEST</strong></th>
<th><strong>DO NOT COLLECT SPECIAL CATEGORY DATA</strong></th>
<th><strong>ADDITIONAL SAFEGUARDS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ Check local EU Member State anti-bribery and anti-corruption laws and regulations for processing authorization</td>
<td>▶ Document how the legitimate interest of the company is balanced against an individual’s rights and freedoms</td>
<td>▶ Ensure data collection in no way includes special categories of personal data</td>
<td>▶ Meet your data processing obligations of data minimization, use limitation, storage limitation, security, accuracy, etc.</td>
</tr>
<tr>
<td>▶ GDPR considers various instances when processing personal data is allowable including when “processing is necessary for compliance with a legal obligation…”</td>
<td>▶ Explain why the collection and processing of personal data is necessary to fulfill legal obligations</td>
<td></td>
<td>▶ Establish approved mechanism(s) to authorize intra-company international data transfers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▶ Establish processes and controls to meet breach notification, rights request, and other GDPR obligations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▶ Establish controller-processor agreements</td>
</tr>
</tbody>
</table>
WHAT CAN WE CLARIFY?
BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 65 offices and over 700 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 88,000 people working out of more than 1,600 offices across 167 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.

For more information please visit: www.bdo.com.