

FRAUD, BRIBERY, AND ANTI-CORRUPTION

STEVEN KUZMA
Senior Managing Director,
Forensic Investigation and Litigation Services

ROBERT MROZ
Managing Director,
Forensic Investigation and Litigation Services

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.



1

With You Today



Steven Kuzma
CPA, CFE, CFF, ASA, ABV, CCEP
Senior Managing Director,
Forensic Investigation and
Litigation Services

404-942-2914
skuzma@bdo.com

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 Mroz
ASA, CBA, CVA, MBA
Managing Director,
Forensic Investigation and
Litigation Services

602-293-2368
rmroz@bdo.com

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.



2

FRAUD, BRIBERY, AND ANTI-CORRUPTION

2

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



3

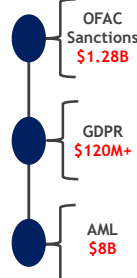
FRAUD, BRIBERY, AND ANTI-CORRUPTION

3

Recent Enforcement Actions - Compliance Failures

	AIRBUS	ERICSSON
Year	2020	2019
Violation	Anti-bribery and Corruption, Arms Export Control Act and International Traffic in Arms Regulations	Anti-bribery and Corruption
Countries	Various (e.g., China, Japan, Russia, Ghana, Indonesia, Vietnam, Austria, Mexico, Malaysia, Taiwan, Sri Lanka)	Djibouti, China, Egypt, Vietnam, Indonesia, and Kuwait
Schemes	<ul style="list-style-type: none"> ► Irregularities in payments made to third-party consultants ► Establishment of a purported "educational" fund that was used to host social events for government officials ► Payments to relatives of government officials ► Lavish gifts/entertainment 	<ul style="list-style-type: none"> ► Payments to agents, consultants, and service providers through sham contracts ► Payment of phony invoices to create off-book slush funds ► Bribes for insider tender info ► Improper travel and entertainment for government officials
Bribe Recipient(s)	Employees of state-owned and state-controlled airlines; Other government officials	Employees of state-owned and state-controlled technology companies
Compliance Program Failures	<ul style="list-style-type: none"> ► Lack of third-party oversight ► Failure in due diligence controls 	<ul style="list-style-type: none"> ► Lack of third-party oversight ► Failure in due diligence controls ► Failure in internal accounting controls
Method Uncovered	Whistleblower; led to an internal investigation	From a "voluntary request" for information from U.S. authorities
Government Penalties	\$4B	\$1B Compliance Monitor

Fines for other compliance risk failures (2019)



4

FRAUD, BRIBERY, AND ANTI-CORRUPTION

4

Fraud and Corruption - Impact

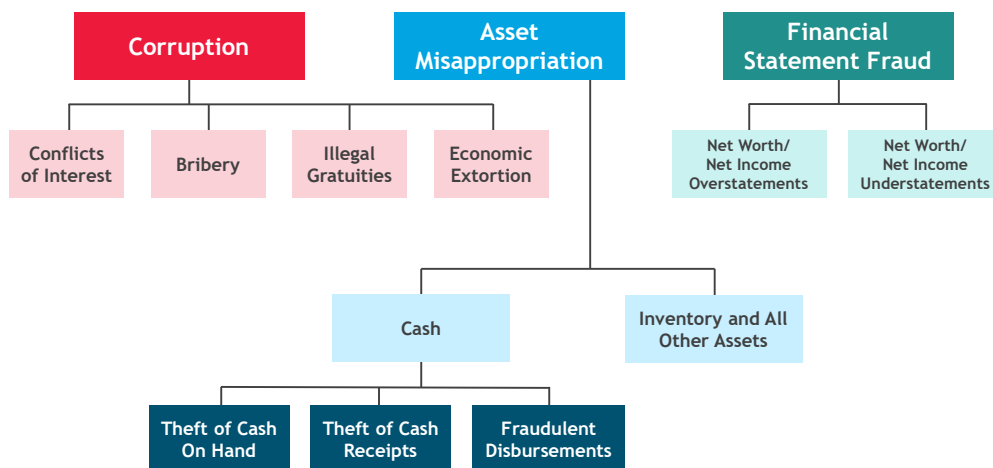
ACFE and BDO Insights

- ▶ 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



Why Is This Important?

ACFE Fraud Profile

	Corruption	Asset Misappropriation	Financial Statement Fraud
Median Loss:	\$250,000	\$114,000	\$800,000
% of Cases:	38%	89%	10%
Risk by Industry:	<ol style="list-style-type: none"> 1. Energy 2. Manufacturing 3. Government 4. Transportation 5. Insurance 	<ol style="list-style-type: none"> 1. Charitable (Billing) 2. Professional Services (T&E) 3. Construction (Billing) 4. Arts/Entertainment (Cash) 5. Retail (Noncash) 	<ol style="list-style-type: none"> 1. Technology 2. Construction 3. Professional Services 4. Retail 5. Hospitality
Risk by Department:	<ol style="list-style-type: none"> 1. Purchasing 2. Upper Management 3. Finance / Operations 	<ol style="list-style-type: none"> 1. Upper Management 2. Administrative Support 3. Accounting 	<ol style="list-style-type: none"> 1. Upper Management 2. Finance 3. Accounting
Other Considerations:	<ul style="list-style-type: none"> ▶ 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 	<ul style="list-style-type: none"> ▶ Most common and least costly fraud category ▶ 38% of cases detected by tip ▶ Small companies (<100 employees) are at a higher risk 	<ul style="list-style-type: none"> ▶ 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**.

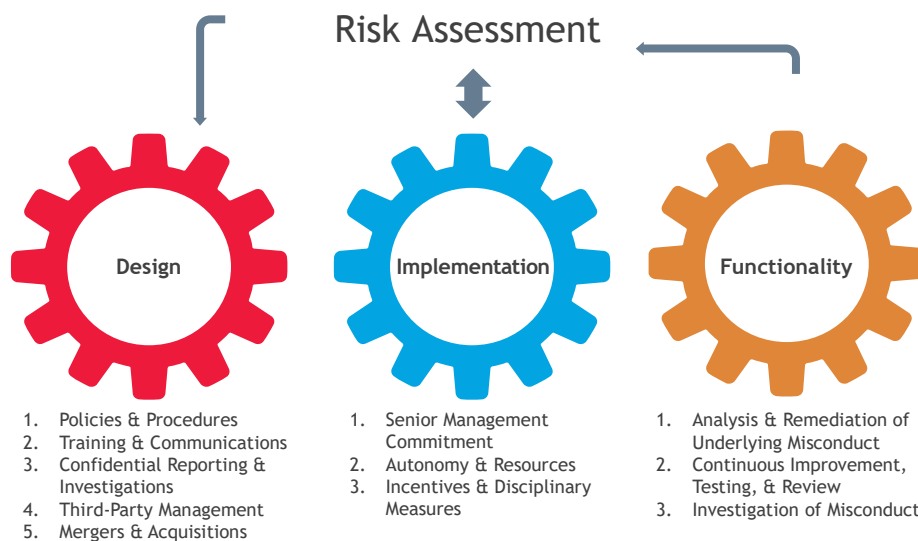


“Assessment of risk is fundamental to developing a strong compliance program, and is another factor DOJ and SEC evaluate when assessing a company’s compliance program.”

*DOJ and SEC -
A Resource Guide
to the FCPA*

Risk Assessment

Supporting the Compliance Program Design



Risk Assessment

Understanding the Risk Universe

Types of Risk		Risk Factors (examples)	Risk Evaluation
Legal & Regulatory	Business Requirements	Geography Third Parties Business Industry Customer Network Employee Network Go-To-Market Strategy Product Raw Materials Licenses/Permits Government Oversight Regulatory Environment	Likelihood Priority Impact Pervasiveness
Fraud Bribery & Corruption Anti-Trust Anti-Money Laundering International Trade Data Privacy Corporate Governance Government Contracts Labor & Employment Environmental	Ethics & Integrity Corporate Social Responsibilities Contractual Obligations Vendor Management Public Commitments Voluntary Standards Emerging Issues		

11

FRAUD, BRIBERY, AND ANTI-CORRUPTION



11

Risk Assessment

Methodology

STEP 1	STEP 2	STEP 3	STEP 4
Define Objectives & Develop a Plan	Information Gathering	Assess & Evaluate Risk	Risk Response Plan

12

FRAUD, BRIBERY, AND ANTI-CORRUPTION



12

Risk Assessment

Methodology

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	
Define Objectives	Develop a Plan
<ul style="list-style-type: none"> ▶ Identify Risks to be Assessed and Evaluated ▶ Determine End Goals of the Risk Assessment 	<ul style="list-style-type: none"> ▶ Develop a Process for Analyzing Risks ▶ Create a Timeline ▶ Establish a Project Team ▶ Determine Key Stakeholders ▶ Identify Roadblocks / Barriers to Success

Risk Assessment

Methodology

STEP 2 - INFORMATION GATHERING

Employee Feedback		Document Review		Industry / Business Environment		
<ul style="list-style-type: none"> ▶ Risk Survey ▶ Interviews 		<ul style="list-style-type: none"> ▶ Policies ▶ Prior Audits ▶ Organization Charts 		<ul style="list-style-type: none"> ▶ Recent News and Events ▶ Enforcement Actions ▶ Competitive Environment 		
Legal / Compliance	Leadership	Accounting / Finance	Sales	Marketing	HR	Operations
Known compliance issues, whistleblower allegations	Tone at the Top, knowledge of company policies and procedures	Process walkthroughs of internal financial controls	Client entertainment, route to market, and competitive market	Rebates, discounts, promotions, and samples	Compensation and bonuses, hiring/promotion procedures, and internships	Licenses, permits, inspections, and customs

Risk Assessment

Methodology

STEP 3 - ASSESS & EVALUATE RISK

Data Analytics/ Risk Mapping	<ul style="list-style-type: none">▶ Data Analytics▶ High-risk Accounts▶ Red Flags & Anomalies
Transaction Testing	<ul style="list-style-type: none">▶ Review of Supporting Documentation▶ Transaction Walkthroughs
Follow-up Interviews	<ul style="list-style-type: none">▶ Interviews of Process Owners

Interviews and transaction testing often inform one another



Risk Assessment

Methodology

STEP 4 - RISK RESPONSE PLAN

Evaluating Effectiveness

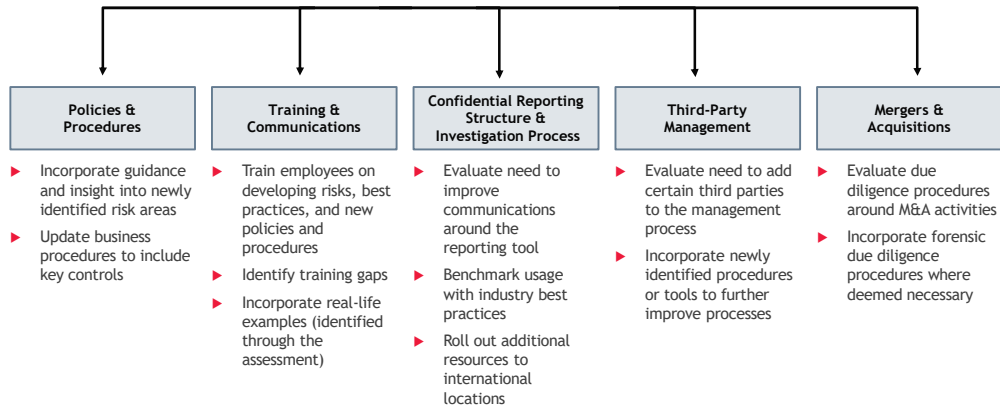
- ✓ How often are risk assessments performed?
- ✓ Are risk assessments performed when there are changes to the business, industry, or regulatory landscape?
- ✓ Do the results of the risk assessments trigger changes to the key elements of your compliance program?

Risk Assessment

Leverage Results To Customize Compliance Program Elements

Risk Assessment

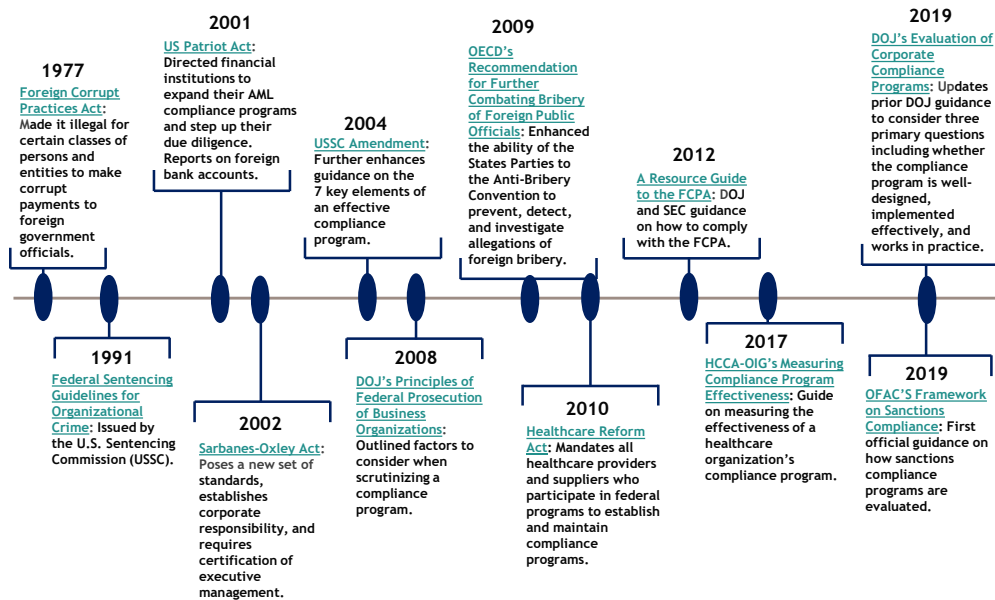
Input from the Risk Assessment helps drive improvements across the key elements of the compliance program



Effective Compliance Programs

REGULATORY GUIDANCE AND BEST PRACTICES

History Of Compliance Program Guidance



19

FRAUD, BRIBERY, AND ANTI-CORRUPTION

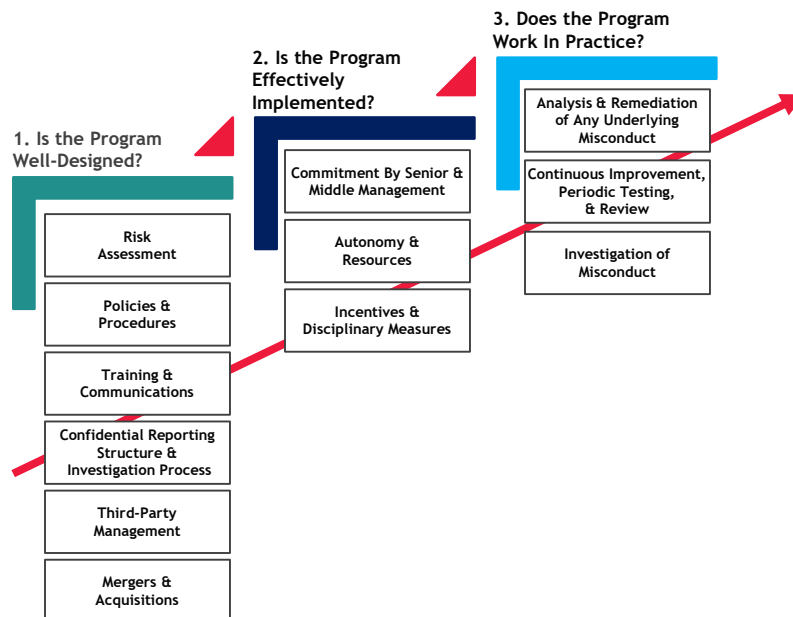
* Timeline is not intended to be exhaustive.



19

Effective Compliance Programs

DOJ Guidance 2019



20

FRAUD, BRIBERY, AND ANTI-CORRUPTION



20

Evolution of DOJ Guidance

"Seven Elements"	2017 Guidance	2019 Guidance	
Compliance officer / Compliance committee	Risk assessment	Risk assessment	Is the Program Well-Designed?
Standards, policies, & procedures	Policies & procedures	Policies and procedures	
Training & education	Training & communications	Training & communications	
Effective lines of communication	Confidential reporting structure & investigation process	Confidential reporting structure & investigation process	
Internal auditing & monitoring	Third-party management	Third-party management	
Investigations & disciplinary guidelines	Mergers & acquisitions	Mergers and acquisitions	Is the Program Effectively Implemented?
Corrective action	Commitment by senior & middle management	Commitment by senior & middle management	
	Autonomy & resources	Autonomy & resources	
	Incentives & disciplinary measures	Incentives & disciplinary measures	Does the Program Work In Practice?
	Analysis & remediation of any underlying misconduct	Analysis & remediation of any underlying misconduct	
	Continuous improvement, periodic testing, & review	Continuous improvement, periodic testing, & review	
		Investigation of misconduct	

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

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.

Effective Compliance Programs

DOJ Guidance 2019

3. Does the Program Work In Practice?

Analysis & Remediation
of Any Underlying
Misconduct

Continuous Improvement,
Periodic Testing,
& Review

Investigation of
Misconduct

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



25

General Data Protection Regulation Impact On Fraud, Bribery, and Anti-Corruption

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

1 Non-Criminal Personal Data

“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.”

GDPR Article 6

2 Special Category Data

“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.**”

GDPR Article 9

3 Criminal Convictions and Offenses

“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.”

GDPR Article 10

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.



26

FRAUD, BRIBERY, AND ANTI-CORRUPTION

26

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?

CHECK AUTHORIZATION

- ▶ Check local EU Member State anti-bribery and anti-corruption laws and regulations for processing authorization
- ▶ GDPR considers various instances when processing personal data is allowable including when “processing is necessary for compliance with a legal obligation...”

DOCUMENT BALANCING TEST

- ▶ Document how the legitimate interest of the company is balanced against an individual’s rights and freedoms
- ▶ Explain why the collection and processing of personal data is necessary to fulfill legal obligations

DO NOT COLLECT SPECIAL CATEGORY DATA

- ▶ Ensure data collection in no way includes special categories of personal data

ADDITIONAL SAFEGUARDS

- ▶ Meet your data processing obligations of data minimization, use limitation, storage limitation, security, accuracy, etc.
- ▶ Establish approved mechanism(s) to authorize intra-company international data transfers
- ▶ Establish processes and controls to meet breach notification, rights request, and other GDPR obligations
- ▶ Establish controller-processor agreements

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

