Corporate Integrity™

2011-08

Prepared By:

Michael Rasmussen
J.D., OCEG Fellow, CCEP
Business Ethics & Compliance Lecturer, Author, & Advisor

ANTI-CORRUPTION: *EFFICIENT AND EFFECTIVE COMPLIANCE WITH U.K. BRIBERY ACT, U.S. FCPA, AND OECD GOOD PRACTICES*

"The best offense in anti-corruption is a good defense. Organizations must be prepared to show that they have a strong compliance program in place to mitigate or avoid exposure to penalties. In today's complex business environment, incidents do happen — the organization defends itself by demonstrating it has implemented appropriate compliance measures to prevent and detect issues of corruption and noncompliance."

Executive Summary

The distributed and dynamic nature of business makes ethics and compliance a challenge. How does an organization validate it is current with legal, regulatory, and other obligations within an ever-changing business environment? Global compliance in the context of a complex and dynamic business environment is particularly challenging as organizations face broadening anti-corruption laws and regulations. Ultimately, the best offense is a good defense. Organizations must be prepared to show they have a strong compliance program in place to mitigate or avoid exposure to penalties.

While anti-corruption laws vary around the world, the common compliance requirements of these laws are the backbone of any good compliance program. To effectively prevent and detect issues of corruption, bribery, and fraud in international business, compliance has to be an active part of the organization and culture. It is a continuous and ongoing process that must be monitored, maintained, and nurtured. This requires a new paradigm of activity that moves away from reactive fire-fighting to managing, monitoring for, preventing, and detecting corruption and compliance risks.

There are two primary models to manage compliance to anti-corruption obligations: One approach is build-your-own, ad hoc and ultimately labor-intensive, and produces significant manual processes and piles of documents. A more economical approach focuses on software designed to manage the complex and diverse needs of anti-corruption compliance.

Table of Contents

Executive Summary 1
Managing Compliance with Anti-Corruption Legislation Is Increasingly Burdensome 2
First There Was the U.S. FCPA . . . Now Enters the U.K. Bribery Act 2
Dodd-Frank Whistleblower Provisions Makes Matters Worse 3
Meeting Anti-corruption Obligations 3
The Role of Technology in Managing Anti-corruption 5
QUMAS Delivers an Anti-Corruption Compliance Management Platform 6
About this Paper 9
About Michael Rasmussen 9

www.**Corp-Integrity**.com
research@**Corp-Integrity**.com
+1.888.365.4560

Growing liability . . .[1]

- The court found Frederic Bourke, Jr. was willfully blind, and that as an investor he should have done more due diligence and should have known that the energy company he invested in bribed foreign officials.
- The government told Nature's Sunshine's CFO and COO they should have had better controls over financial reporting, even though the SEC never stated they specifically knew of the bribery happening within the corporation.

Fines are skyrocketing . . .

- The U.S. Department of Justice assessed nearly $2 billion in fines in 2010
- Eight of the top 10 FCPA settlements occurred in 2010
- BAE Systems was the third largest fine at $500 million
- Daimler AG had $185 million in fines and disgorgements
- Snamprogetti had $365 million in fines (fourth-largest)
- The average cost of an FCPA settlement is $50 million plus the expense for an external monitor to validate a compliance program is in place for the next 10 to 20 years. This does not include investigation expenses.

Executives can go to jail . . .

- Charles Jumet, former VP of Ports Engineering Consulting Corporation, was sentenced to 87 months in prison after pleading guilty of conspiracy to bribery by making bribes to government officials in Panama and giving false statements to the FBI.

Investigation costs are significant . . .

- Siemens spent $850 million in fees and expenses to investigate anti-corruption
- Daimler had a five-year investigation that cost over $500 million

Harsh collateral sanctions, in which the government can also . . .

- Terminate government licenses
- Disbar the organization from government contracting
- Disgorge company profits on contracts secured by improper payments

1 These statistics and others can be found at: http://www.foreign-corrupt-practices-act.org/foreign-corrupt-practices-act-news/5-siemens-ag-pays-450-million-to-settle-fcpa-bribery-charges.html

Managing Compliance with Anti-Corruption Legislation Is Increasingly Burdensome

Organizations across industries have global clients, partners, and operations. The larger the organization is, the more complex its interactions with external entities (e.g., government, regulators, contractors, vendors, and other third-parties) around the world.

Adding to the complexity and distribution of global business is a constantly changing business environment. In the brief moment spent reading this paper, your business has probably changed: New employees are hired, others change roles, and some leave. New business partner relationships are established — others terminated or changed. Business executes on strategy and enters new markets, opens up new facilities around the world, contracts with agents, or introduces new products and services. New laws are introduced that impact the organization, regulations change, and the environment around business changes, introducing risk (e.g., economic, geopolitical, operational) and impacting how business is conducted.

Global compliance in the context of a complex and dynamic business environment is particularly challenging as organizations face greater exposure to anti-corruption laws and regulations. How does an organization validate that it is current with legal, regulatory, and other obligations in the face of an ever-changing business environment?

First There Was the U.S. FCPA . . . Now Enters the U.K. Bribery Act

Laws such as the Foreign Corrupt Practices Act (FCPA) have been in place in the U.S. for nearly 35 years.[1] Despite this length of time, each year shows increasing noncompliance and growing fines and penalties by the US Department of Justice.[2] In 2010, the number of enforcement actions were double any previous year.[3]

1 http://www.justice.gov/criminal/fraud/fcpa/

2 FCPA Penalty structure: Violation — $250,000 and/or five years in prison for individuals, $2 million in fines for corporations. Violation of accounting provisions — $500,000 and/or twenty years in prison for individuals, $5 million for corporations. Willful violation of the books and records and internal control provisions — $25 million for the company, $5 million for an individual and up to 20 years in prison.

3 http://www.justice.gov/criminal/fraud/fcpa/cases/2011.html

If the FCPA was not enough, the United Kingdom approved the U.K. Bribery Act (UKBA) legislation in 2010, which went into force in July 2011. This anti-corruption law brings broader scope and implications to anti-corruption compliance. Both the FCPA and the UKBA are country-specific initiatives in support of the Organization for Economic Cooperation and Development's (OECD) anti-corruption initiatives in 34 democratic countries around the world. The OECD has released Good Practice Guidance on Internal Controls, Ethics, and Compliance to combat anti-corruption around the world.

The U.K. Bribery Act establishes four criminal offenses for corporations:[1]

1. Offering or paying a bribe
2. Requesting or receiving a bribe
3. Bribing a foreign public official
4. Failing to prevent bribery

1 http://www.natlawreview.com/article/uk-bribery-act-2010-corporate-hospitality-or-when-beer-bribe

The UKBA makes it illegal for a company operating or listed in the U.K. to make unofficial payments to public officials to secure or expedite performance of routine or necessary business transactions. The scope of the UKBA includes anyone with business operations in the U.K. and covers acts and omissions anywhere in the world. Organizations need to be prepared to defend themselves — UKBA has a rebuttable position that an employee is acting on behalf of the organization. This requires that the organization is able to demonstrate it has an appropriate compliance program in place to overcome this burden of proof.

Dodd-Frank Whistleblower Provisions Makes Matters Worse

In the U.S., anti-corruption has become much more complex: The U.S. Federal Government whistleblowing provisions in the Dodd-Frank Act entice employees to report ethical violations, such as bribery and corruption, to the government. It gives the SEC powers of enforcement of a whistleblower bounty program and whistleblowers a bounty from fines and penalties resulting from the investigation should the organization be culpable.[4] The scope includes areas of fraud, antitrust, insider trading, corruption, and bribery. Corporate whistleblowers who provide information which leads to a successful SEC enforcement receive 10 percent to 30 percent of the monetary sanctions over $1 million. In an era of increased scrutiny and judgments for anti-corruption, this is a significant concern keeping executives, the board, legal, and compliance professionals up at night.[5]

How you respond has impact . . .

Consider Johnson & Johnson, which responded quickly to the discovery of corruption and demonstrated initiative by working with the Department of Justice. As a result they significantly reduced the penalties imposed on them in the deferred prosecution agreement it reached with the DOJ.[1] The government agreed to a 25 percent reduction in the fine, to $21.4 million. This shows that a quick response by reporting and working with authorities offers a substantial reduction in penalties.

1 http://www.scribd.com/full/52602637?access_key=key-25vqtahmgo6iv6i0jxxx

Meeting Anti-corruption Obligations

With increased exposure to anti-corruption laws and investigations, how does an organization respond to anti-corruption compliance obligations?

The best offense in anti-corruption is a good defense. Organizations must be prepared to show that they have a strong compliance program in place to mitigate or avoid exposure to penalties. In today's complex business environment, incidents do happen — the organization defends itself by demonstrating it has implemented appropriate compliance measures to

4 Based upon the success of a similar program established by the IRS in 2006

5 http://www.sec.gov/rules/final/2011/34-64545.pdf

prevent and detect issues of corruption and noncompliance. The goal is to have preventive measures in place to avoid corruption issues, while at the same time having detective measures to monitor for instances of corruption and respond quickly and efficiently. This includes reporting and cooperating with authorities in investigations.

While there are different laws around the world aimed at anti-corruption, the compliance aspects to these laws are based on common requirements that are the backbone of any good compliance program. From a U.S. perspective, the best defense is to show that the organization has met the elements of an effective compliance program as established by the United States Sentencing Commission Organizational Guidelines.[6] The U.S. guidelines compliment and coordinate well with the U.K.'s guidance requiring a company to demonstrate adequate procedures to prevent bribery. It is a full defense in the U.K. Bribery Act when an organization proves that despite a particular incident of bribery it nevertheless has proper compliance practices in place to prevent corruption and bribery. Both the U.S. and U.K. guidance aligns with and supports OECD Good Practice on Internal Controls, Ethics, and Compliance. [7]

It is a full defense in the U.K. Bribery Act when an organization proves that despite a particular incident of bribery it nevertheless has proper compliance practices in place to prevent corruption and bribery.

An integrated view of the U.S., U.K., and OECD guidance requires that an organization have the following compliance elements in place:

- **Understand your risk:** An organization must have a risk-based approach to managing anti-corruption. This includes periodic assessment (e.g., annual) of the exposure to the organization for corruption and unethical conduct. However, the risk-assessment process should also be dynamic — completed each time there is a significant business change that could lead to exposure (e.g., mergers and acquisitions, new strategies, and new markets). Risk assessments should cover exposure to corruption in specific markets, business partners, and geographies.

- **Approach compliance in proportion to risk:** How an organization implements compliance procedures and controls is based on the proportion of risk it faces. If a certain area of the world or business partner carries a higher risk for corruption, the organization must respond with stronger compliance procedures and controls. Proportionality of risk also applies to the size of the business — smaller organizations are not expected to have the same measures as large enterprises.

- **Tone at the top:** The compliance program must be fully supported by the board of directors and executives. Communication to and from top-level management must be bidirectional. Management must communicate that they support the anti-corruption compliance program and will not tolerate corruption in any form. At the same time, they must be well-informed about the effectiveness and strategies for compliance and anti-corruption initiatives.

- **Know who you do business with:** It is critical to establish a risk-monitoring framework that catalogs third-party relationships, markets, and geographies. Due diligence efforts must be in place to make sure the organization is contracting with ethical entities. If there is a high degree of corruption risk in a relationship, additional preventive and detective controls must be established in response. This includes knowing your own employees and conducting background checks to understand if they are susceptible to corruption and unethical conduct.

- **Keep information current:** Due diligence and risk assessment efforts need to be kept current. These are not point-in-time efforts that happen once; they need to be done on a regular basis or when the business becomes aware of conditions that point to increased risk of corruption.

6 http://www.ussc.gov/Guidelines/Organizational_Guidelines/guidelines_chapter_8.htm

7 http://www.oecd.org/dataoecd/5/51/44884389.pdf

- **Compliance oversight:** The organization needs someone who is responsible for the oversight of anti-corruption compliance processes and activities. This person should have the authority to report to independent monitoring bodies, such as the audit committees of the board, to report issues of corruption.

- **Established policies and procedures:** Organizations must have documented and up-to-date policies and procedures that address corruption. The code of conduct is the governing policy that filters down to other policies that address anti-corruption, gifts, hospitality, entertainment and expenses, customer travel, political contributions, charitable donations and sponsorships, facilitation payments, and solicitation and extortion. Compliance requirements and processes must be clearly documented and adhered to.

- **Effective training and communication:** Written policies are not enough — individuals need to know what is expected of them. Organizations must implement anti-corruption training programs to educate employees and business partners at risk of exposure to bribery, corruption, and fraud. This includes getting acknowledgements from employees and business partners to affirm their understanding, and attestation of their commitment to behave according to established policies and procedures.

- **Implement communication and reporting processes:** The organization must have channels of communication where employees can get answers on policies and procedures. This could take the form of a help line that allows an individual to ask questions, or a FAQ database, or via form processing for approval on activities and requests. The organization must also have a hotline reporting system for individuals to report misconduct — in the U.S. this is called a whistleblower system, and in the U.K. it is referred to as a speak-up line.

- **Assessment and monitoring:** In addition to periodic risk assessment, the organization must also have regular compliance assessment and monitoring activities to ensure that policies, procedures and controls to prevent corruption and bribery are in place and working.

- **Investigations:** Even in the best organization, things go wrong. Investigation processes (hotlines, surveys, management reports, and exit interviews) must be in place to quickly identify potential incidents of corruption, and quickly and effectively investigate and resolve issues. This includes reporting and working with outside law enforcement and authorities.

- **Internal accounting controls:** Organizations must keep detailed books, records and accounts that fairly and accurately reflect transactions and disposition of assets that could be implicated in corruption issues. This includes contract-pricing review, due diligence and verification of foreign business representatives, accounts payable payments, financial account reconciliation, and commission payments.

- **Manage business change:** The organization must monitor the business environment for changes that introduce greater risk of corruption. The organization must document changes required to business practices as a result of observations and investigations, and address deficiencies through a careful program of change management. This requires that business change be monitored by compliance personnel to proactively prevent corruption.

The Role of Technology in Managing Anti-corruption

WARNING: The previous list of anti-corruption practices may appear to be a checklist of tasks to receive a "get out of jail free" card: This mentality must be avoided. Compliance needs to be an active part of the organization and culture to prevent and detect corruption, bribery, and fraud. This continuous and ongoing process must be monitored, maintained, and nurtured. The challenge is establishing corruption prevention and detection activities that move the organization from a reactive fire-fighting mode to one that actively manages, monitors, prevents, and detects risk. This requires the organization to implement technology to manage anti-corruption compliance.

Technology can help organizations manage and monitor anti-corruption compliance by enabling and automating:

- **Compliance program management:** The organization needs a 360-degree view of compliance activities and reporting. This requires an end-to-end system for managing compliance activities, metrics, and reports. From this system the organization should be able to produce reports and metrics relevant to the board of directors and executives, to assure them they are meeting fiduciary obligations to have a compliance program for anti-corruption in place. All compliance management personnel and employees should be able to access the system and see contextually relevant tasks and items.

- **Regulatory intelligence and change management:** The integration of regulatory content feeds and technology enables the compliance program to monitor changes in anti-corruption laws, requirements, and cases to determine how new developments impact the business. The organizations must use technology to take in legal and regulatory feeds and route them to the correct subject matter expert for review and business impact analysis.

- **Compliance risk assessment:** Risk assessments are mandatory for compliance initiatives. The organization needs a technology platform to manage risk surveys, assessments, and related risk information and report, analyze and model risk.

- **Policy and procedure management:** A core process of a compliance program is the ability to document policies and procedures to maintain a state of compliance. All relevant policies related to anti-corruption should be documented, maintained, communicated, and attested to within a technology platform with a robust audit trail and content management capability. This includes code of conduct, anti-corruption, and other related policies.

- **Training and communication:** It is not enough to make written policies available — the organization also needs to train individuals on policies. Organizations are increasingly using the economies of online training to deliver courses on anti-corruption, and to test employee understanding of policies and requirements.

- **Third-party management:** Central to an anti-corruption compliance program is the ability to manage the risk of third-party entities you interact and do business with. Technology, and the integration of content feeds, enables the ongoing due diligence effort to monitor and score vendor/third-party risk, communicate policies to vendors, track attestations, and deliver surveys and assessments.

- **Forms processing and automation:** A critical component of an anti-corruption program is the ability to process and automate forms related to compliance policies and procedures. Interactions for contributions, gift, entertainment, and facilitated payments should be managed through online forms and workflow for approval or disapproval.

- **Investigations management:** Technology enables the organization to manage and monitor issues and incidents, and collaborate and document investigations. This includes the ability to record the range of issues reported from hotlines and other mechanisms, what actions were taken, and the results of the investigation.

QUMAS Delivers an Anti-Corruption Compliance Management Platform

There are two primary models to manage compliance to anti-corruption obligations: One approach is build-your-own, ad hoc and ultimately labor-intensive, and produces significant manual processes and piles of documents. A more economical approach focuses on software designed to manage the complex and diverse needs of anti-corruption compliance.

QUMAS is a solution provider in the GRC market that Corporate Integrity has researched and evaluated. Through a purpose-built compliance management platform, QUMAS eases the anti-corruption compliance burden by delivering operational effectiveness, human and financial efficiency, and agility to compliance processes. QUMAS enables an anti-corruption compliance program that delivers:

- **Compliance program management:** QUMAS delivers a fully functional compliance program on a single compliance management platform to manage all anti-corruption activities. This gives the compliance officer one source for all compliance metrics and reporting, eliminating the need for resource- and time-intensive reporting projects and teams, which historically focus on building reports from a variety of disparate sources. The intensive effort of compiling and dashboarding information is taken away — compliance program information is now compiled automatically, and is controlled based on roles and permissions.

- **Regulatory intelligence and change management:** By integrating legal and regulatory intelligence into the compliance workflow, all relevant statutes, regulations, analysis, news, and other information needed to develop and maintain compliance policies can be searched. Alerts can be set to track and assess the impact of change, and results can be routed into a compliance workflow. Robust collections of compliance resources ensure research is comprehensive, reducing the effort of manually researching and tracking regulatory intelligence and change.

- **Compliance risk assessment:** The compliance platform enables integration with existing or new corporate risk systems, ensuring continuity of country, product, and counter-party assessments. All risk surveys, assessments and information can be reported on and analyzed through the compliance platform, ensuring action and monitoring is done actively to predict, avoid, or mitigate loss.

- **Policy and procedure management:** Content management is the cornerstone of the QUMAS Compliance Platform. This includes policies and procedures from creation through distribution and training for all users, including authors, reviewers, editors, approvers, trainers, and consumers. Key to ensuring compliance across all content and policy areas are:

    - Document templates (mandatory or elective)
    - Collaborative authoring and review
    - Automated workflows for content based on type
    - Document comparison for ease of review
    - Automated PDF rendering and version control
    - Read-and-understood notifications and training
    - Advanced search and retrieval
    - Controlled printing and watermarking
    - Hardcopy management and destruction
    - Built-in best practices for regulatory compliance

- **Training and communication:** Learning management is provided for e-learning modules, instructor-led training, and for approved policies and procedures along with related regulatory content. All of these modules can be easily browsed and converted into effective and measurable training. Industry standard SCORM-compliant content can be launched and tracked within the application, dramatically reducing the time needed to create and deliver critical training.

- **Third-party management:** Vendor and third-party auditing is a core element of the compliance platform, ensuring entities you deal with outside of your organization adhere to the same regulatory standards. Initial audit/due diligence and approval, along with ongoing monitoring of third parties, is key to achieving compliance. The compliance platform ensures all relevant policies are communicated in real time to vendors and that their attestations are tracked (with electronic signatures). Third parties can be given access to the systems, and included in any compliance program initiatives including training, monitoring, remediation, and reporting.

- **Forms processing and automation:** Process and forms management is a critical element of a compliance platform, particularly for mandated controls around gift, entertainment, and facilitated payments. QUMAS ensures all forms are routed and approved/rejected in real time and full traceability and accountability is audited, with any incidents or breaches escalated as required.

- **Investigations management:** Proving you have acknowledged, recorded, investigated, and remediated incidents is a core element of proving regulatory compliance, whether incidents are customer complaints, third-party issues, or inappropriate gifting episodes. QUMAS ensures incident management and remediation is logged and handled in a manner laid out by corporate procedures, and that accountability and escalation is built-in.

All of these core compliance capabilities across the QUMAS Compliance Platform are accessed in one interface: MyQUMAS. This allows users to easily connect and collaborate on compliance content, processes, tasks, training and reporting from one central location. It provides a unified interface into all compliance management initiatives, uniquely combining views and tasks related to documents, processes, training and reporting in a single view.

About this Paper . . .

This white paper is brought to you by QUMAS.

QUMAS delivers a closed-loop compliance model that standardizes and integrates the common elements of compliance tasks across the organization. Enterprises are able to effectively converge all of their compliance programs onto a single platform, radically reducing the cost of compliance and creating competitive advantage. With its proven track record in two of the of the most stringently regulated industries - financial services and life sciences - QUMAS has proven that it is best positioned to provide centralized compliance for any company, regardless of industry. Its solutions ensure corporate compliance with the full spectrum of global regulations.

Focused initially on the life sciences and financial services industries, QUMAS compliance solutions are used globally.

The "Big Three" financial titans in asset management, wealth management, and investment banking, rely on QUMAS to operationalize policies and procedures and automate regulatory processes.

QUMAS is a proven compliance standard across life sciences, with over 250 global deployments, scaling from SaaS clients with 20 users up to 120,000 users in enterprise implementations.

About Corporate Integrity . . .

Corporate Integrity, LLC is a GRC strategy advisory firm providing leadership in education, research, analysis, and advisory services by monitoring the challenges and trends in business for corporate governance, risk management, and compliance (GRC).

Through ongoing research, interactions, and analytics, Corporate Integrity is the authority in understanding how organizations can foster a culture that "walks the talk," where integrity is central to GRC practices. Corporate Integrity educates organizations — and GRC professionals within those organizations — on achieving sustainability, consistency, efficiency, and transparency in their corporate GRC practices to maintain a position of integrity aligned with corporate values and business performance.

About Michael Rasmussen . . .

J.D., CCEP, OCEG Fellow: Business Ethics & Compliance Lecturer, Author, & Advisor

Michael Rasmussen is an internationally recognized pundit on the topics of business ethics, corporate culture, policy management, and compliance. With more than 18 years of experience, Michael helps organizations understand their culture and improve related governance, risk, and compliance (GRC) strategies, processes, and technologies that deliver business agility, efficiency, and effectiveness. He is a sought-after keynote speaker, author, and advisor on compliance and risk management strategies. He is noted for being one of the earliest advocates for a collaborative and integrated approach to GRC.