

The End of Check the Box  
Anti-Corruption Compliance:

# Examining ISO and DOJ Guidance

**ISO 37001 IS A GLOBAL STANDARD**

Released in September 2016, ISO 37001 serves as a key consideration for private and government entities regardless of jurisdiction. It provides a global management standard for organizations to establish anti-bribery controls.

Over the past year, the release of ISO 37001 and the U.S. DOJ's Evaluation of Corporate Compliance Programs have highlighted to companies the need to develop and maintain a substantive program for identifying, evaluating and addressing bribery risk.

ISO 37001 is a global standard released in September 2016 and serves as a key consideration for private and government entities regardless of jurisdiction. It provides a global management standard for organizations to establish anti-bribery controls. Like an FCPA compliance program, the system can be stand-alone or integrated into an overall management system. Both Wal-Mart and Microsoft recently announced their intentions to obtain the ISO certification, which likely will lead to a requirement that their vendors, partners and other third parties around the world follow suit.

Released in February 2017, the U.S. DOJ's Evaluation of Corporate Compliance Programs lists factors that a United States Attorney's Office (USAO) should consider when assessing the effectiveness of a corporate compliance program. In turn, the viability of that program has a bearing on an Assistant U.S. Attorney's (AUSA) decision to launch a criminal (DOJ) or civil (SEC) investigation, seek an indictment or decline charges, or negotiate a non-prosecution agreement or a deferred prosecution agreement. While the evaluation can be applied to several types of compliance, this assessment will focus on its application to the U.S. Foreign Corrupt Practices Act (FCPA).

**COMPARE AND CONTRAST**

Although the DOJ evaluation and the ISO guidelines tend to cover several overlapping areas, the ISO 37001 document is much more detailed and prescriptive. Any anti-corruption program can use ISO as a general framework while tailoring its processes to account for coverage of any jurisdiction-specific requirements. In addition to the FCPA, other anti-bribery legislation such as the U.K. Bribery Act or the Brazil Clean Company Act can be taken into consideration depending on a company's regulatory exposure.

The DOJ evaluation and ISO guidelines have several similar requirements for the compliance function, which include:

- Establishing an anti-bribery program.
- Identifying the role of leadership and management in communicating and enforcing the compliance program.
- Outlining the roles and responsibilities of key stakeholders in the compliance function throughout multiple departments across the organization.
- Requiring operational integration of processes around anti-bribery.
- Monitoring the compliance program and investigating any type of misconduct.

Unlike the ISO Standard, however, the DOJ evaluation also recommends specific safeguards around the mergers and acquisitions process. These include mechanisms to detect and address bribery before and after the transaction.

- Conducting a risk assessment and requiring due diligence commensurate with the findings of that assessment.
- Enacting a set of incentives and penalties to foster ethical employee and third party conduct.
- Tracking and analyzing the effectiveness of any outsourced compliance functions.
- Highlighting the importance for enacting the program across business segments and subsidiaries.
- Conducting due diligence on channel partners, agents and third parties before onboarding and periodically thereafter.

#### RECENT DOJ AND SEC ENFORCEMENT ACTIONS

Observing the ISO and DOJ evaluation guidelines may have avoided investigations, fines or penalties for companies involved in several recent FCPA-related enforcement actions. Two of note include Zimmer Biomet Holdings and Mondelēz International.

In a January 2017 SEC administrative settlement, Mondelēz International, Inc. (FKA Kraft Foods, Inc.) paid a \$13 million civil penalty for failing to monitor and conduct due diligence on an overseas agent. The agent was tasked with obtaining licenses for a subsidiary in India. The settlement terms appear to have been more favorable due to the company's efforts to cooperate and put in place remedial measures to prevent the issue from reoccurring.

Also in January 2017 Zimmer Biomet Holdings, Inc., a medical device manufacturer, consented to pay \$30 million, retain a compliance monitor and agreed to other serious restrictions by the SEC and DOJ after it continued to use a distributor who was entangled in a 2012 bribery-related settlement with its predecessor, Biomet, Inc. The company also allegedly failed to conduct proper due diligence and put in place accounting controls with respect to its third parties in Latin America. Additionally, a subsidiary pled guilty to violating the FCPA's books-and-records provision.

## SUMMARY

Both ISO and DOJ guidance contain specific provisions that could help a company avoid the issues faced by Mondelēz and Zimmer Biomet. ISO 37001 requires a risk assessment, which under Section 8.2 “shall include any due diligence necessary to obtain sufficient information to assess the bribery risk. The due diligence shall be updated at a defined frequency, so that changes and new information can be properly taken into account.” Under Section 10 of the DOJ evaluation titled “Third Party Management,” the document requires an AUSA to ask “how has the company monitored the third parties in question.”

So what is the solution to minimize risk? Minimally, multinational companies should familiarize themselves both with the ISO Standard and the DOJ evaluation and endeavor to tailor their own anti-corruption compliance program to those best standards. Companies also should seriously consider becoming ISO certified, as have Microsoft and Wal-Mart, and require their high-risk third parties to also be certified. Doing so, however, does not alleviate the need to conduct an appropriate level of risk-based due diligence with respect to partners, agents and other third parties consistent with regulatory guidance. Such due diligence should include the use of an effective risk assessment solution that enables the company to categorize its third parties into different risk levels, thereby allowing the company to focus its resources on their high-risk third parties. Due diligence for high-risk third parties should include, among other things, conducting database screening, open source investigations and “boots on the ground” investigations.

## ABOUT THE AUTHORS

**Michael Heller** currently serves as the Director of Risk and Compliance Americas for Dow Jones. He has held multiple consulting roles focused on risk management and enhanced due diligence, which include serving as CCO and counsel at Abacus Wealth Partners. Michael worked as a consultant with the Business Intelligence Group, and later the Anti-Money Laundering Group at Goldman Sachs and Co in New York City. At Goldman, Michael collaborated with counsel to conduct domestic and internationally focused investigative due diligence reviews of transactions involving principal investments, capital markets and private wealth management. Michael earned a Bachelor of Arts degree with honors in International Affairs from the University of Colorado at Boulder, and holds a Juris Doctor from the University of San Diego School of Law. He is a member of the State Bar of California.

**Jim Lord** is a Shareholder with the Denver based law firm Inman Flynn. His practice largely focuses on regulatory compliance issues, including anti-corruption, anti-money laundering, and anti-human trafficking programs; as well as managing global due diligence investigations for organizations. Jim previously served as a federal prosecutor for over twenty years, including serving as Chief of the Corporate Fraud Task Force for the Western District of Washington and as the Legal Advisor to Tanzania. Jim also consults with Dow Jones in relation to RiskAverter, a third-party risk management solution offered by Dow Jones.

## CITATIONS

<https://www.law360.com/articles/919703/13-fcpa-enforcement-actions-resolved-in-2017-so-far>  
<http://www.fcpablog.com/blog/2017/5/11/microsoft-and-wal-mart-seek-iso-37001-anti-bribery-certifica.html>  
<https://www.justice.gov/criminal-fraud/page/file/937501/download>  
ISO 37001 Anti-bribery management systems

## DOW JONES RISK & COMPLIANCE

Dow Jones Risk & Compliance is a global provider of risk management and regulatory compliance information, delivering targeted content to organizations around the world. Our market-leading data helps financial institutions and businesses have greater control managing Anti-Money Laundering, Anti-Bribery and Corruption, Economic Sanctions, Third Party Due Diligence and Commercial Risk operations. With a global team of expert researchers covering more than 60 languages, our risk and compliance data is information-rich, accurate and timely, enabling our clients to make better quality decisions faster and with greater confidence.

---

For more information  
visit [dowjones.com/risk](https://www.dowjones.com/risk)

