MetricStream

What You Need to Know about the ISO 37001 Standard for Anti-Bribery Management Systems

In October 2016, the International Organization for Standardization (ISO) issued ISO 37001 for anti-bribery management systems. The new standard provides requirements and guidance for organizations to prevent, detect, and address bribery related risks, thereby reducing overall enterprise risk and associated costs. Most of the guidelines mentioned in the standard are aligned with regulations such as the Foreign Corrupt Practices Act (FCPA) issued by the US Department of Justice (DOJ) and the Securities and Exchange Commission (SEC), as well as the adequate procedures guidance for the UK Bribery Act, issued by the Ministry of Justice, UK.

Why Organizations Should Adopt ISO 37001 to Certify Their Anti-Bribery Program

Many organizations have operations, subsidiaries, suppliers, or other business associates located in countries where the risk of corruption and bribery is high. These companies will benefit immensely by adopting ISO 37001 or by benchmarking and certifying their anti-bribery management program against the ISO standard.

While compliance with the standard does not absolve an organization from bribery-related liabilities, it does provide assurance and evidence in the event of an investigation that the organization has taken reasonable steps to prevent wrongdoing.

In the past, enforcement authorities repeatedly highlighted the lack of internal anti-bribery controls and management systems as a key reason for the huge fines imposed on organizations. The introduction of the ISO standard is likely to reduce the incidence of such penalties.

With several countries adopting anti-bribery programs, it will be important for organizations to follow suit. Global business giants such as Walmart and Microsoft have already committed to complying with the ISO standard, and it won't be long before they ask their vendors and business associates to do the same.

Quick Facts about ISO 37001

First international standard for anti-bribery management systems

Drafted with inputs from 59 countries and 8 liaison organizations

Can be used by any organization, large or small, in the public, private, or voluntary sector, and in any country

Aims to prevent bribery of and by an organization

ISO 37001 and Third-Party Management

If adopted and implemented properly, the ISO 37001 certification process can be leveraged to manage the risk of corruption among third parties. Currently, this risk is kept in check through verification audits, independent due diligence processes, and other such approaches that often end up being costly for both organizations and their third parties.

To minimize these costs, there needs to be a common language for corruption and bribery risk management, both at the organizational and third-party levels – which is where the ISO 37001 standard helps. In the future, organizations may require only that a supplier obtain an ISO 37001 certification before onboarding, instead of undergoing multiple, costly audits. Having an ISO certification may also help small and medium-sized third-party firms skip repeated corruption and bribery risk assessments. In fact, firms may appear more eligible by demonstrating compliance with the ISO standard, and by providing evidence of independent verification.

When it comes to due diligence, the ISO 37001 standard emphasizes that a third party's direct and indirect shareholders, as well as top management cannot be ignored. Their identities, backgrounds, reputations, and potential direct/ indirect links to Politically Exposed Persons (PEPs) must be taken into consideration. This aspect of due diligence could end up being challenging. In large third-party firms, there will be multiple shareholders to evaluate, while in smaller firms, the number of shareholders may be less, but the information available on them is likely to be scant and insufficient.

When it comes to "watch list' screenings, the ISO standard does not provide specific comments. However, it does state that organizations may leverage questionnaires, search engine research, "government, judicial and international resources," debarment lists, and reputational inquiries. Therefore, any program that is purely based on the watch list methodology may not be sufficient for due diligence.

What Is Required?

According to ISO 37001, the anti-bribery management program -- including policies, procedures, and controls -- should be "reasonable and proportionate" to the organization's size and bribery risk exposure. In other words, smaller organizations, as well as those with a lower risk of bribery, wouldn't need to establish the same level of procedures and controls as larger organizations, or those with a higher risk of bribery.

While there is no one-size-fits-all approach to complying with the ISO standard, organizations need to have the following elements in place:

- Anti-bribery policies and procedures, including those around gift-giving, hospitality, donations, and other such benefits
- An effective compliance team to oversee the anti-bribery program
- A strong tone at the top with management level leadership on, commitment to, and responsibility for anti-bribery
- Anti-bribery risk assessments
- Controls to mitigate bribery risks (including financial, procurement, commercial, and contractual controls)
- Training and awareness on anti-bribery policies and measures
- Due diligence on projects, transactions, personnel, and business associates/ third parties with a high risk of bribery
- Procedures for reporting, investigating, and reviewing suspected or actual bribery
- Continuous monitoring and regular audits
- Corrective action and continual improvement

Certification by Independent Auditors

ISO 37001 includes a provision that allows an independent third party to issue a certificate confirming that an organization's compliance program does indeed adhere to the standard. However, before embarking on the audit, organizations should conduct an internal assessment to check if they have all the required documents, processes, controls, system, and internal activities like due diligence and training in place to show auditors that they have done their homework.

To conduct the audit, qualified auditors with anti-bribery experience and in-depth knowledge will be required. They will most likely carry out their evaluations at various offices, and may require interviews with top management, department heads, sales people, HR, Legal, Internal Audit, and other key functions.

Meeting the Anti-Bribery Standard – Best Practices

Considering the multitude of requirements and elements involved in ISO 37001 compliance, here are a few best practices for organizations to optimize the value of their compliance and anti-bribery management program:

Establish a Centralized, Standardized Policy Database
In large, global organizations, anti-bribery policies are often developed and managed in silos, resulting in multiple versions of the same policy scattered across systems. To avoid this chaos, it helps to have a single, centralized policy database that stores all anti-bribery policies in one place, maps them to other anti-corruption requirements, and more importantly, ensures consistency in anti-bribery policies across the enterprise.

Automate Where Possible
Many organizations still manage anti-bribery programs in the traditional, manual manner, using cumbersome spreadsheets or paper-based tools. However, much efficiency can be gained by streamlining and automating anti-bribery management processes – be it continuous monitoring, surveys, risk and control assessments, or audits – thereby saving time and costs, while also strengthening overall compliance.

Facilitate Cross-Functional Collaboration

While the responsibility for anti-bribery management may lie with the compliance team, it is ultimately an enterprise-wide effort that requires support from and coordination across multiple functions, including Risk Management, Legal, Finance, and Internal Audit. Everyone needs to be speaking the same language, and sharing and communicating relevant data with each other for analysis and review. To this end, a unified system can help cut across business and geographic silos, providing a single point of reference for teams to collaborate on, plan, and schedule anti-bribery management activities.

Focus on Third-Party Management

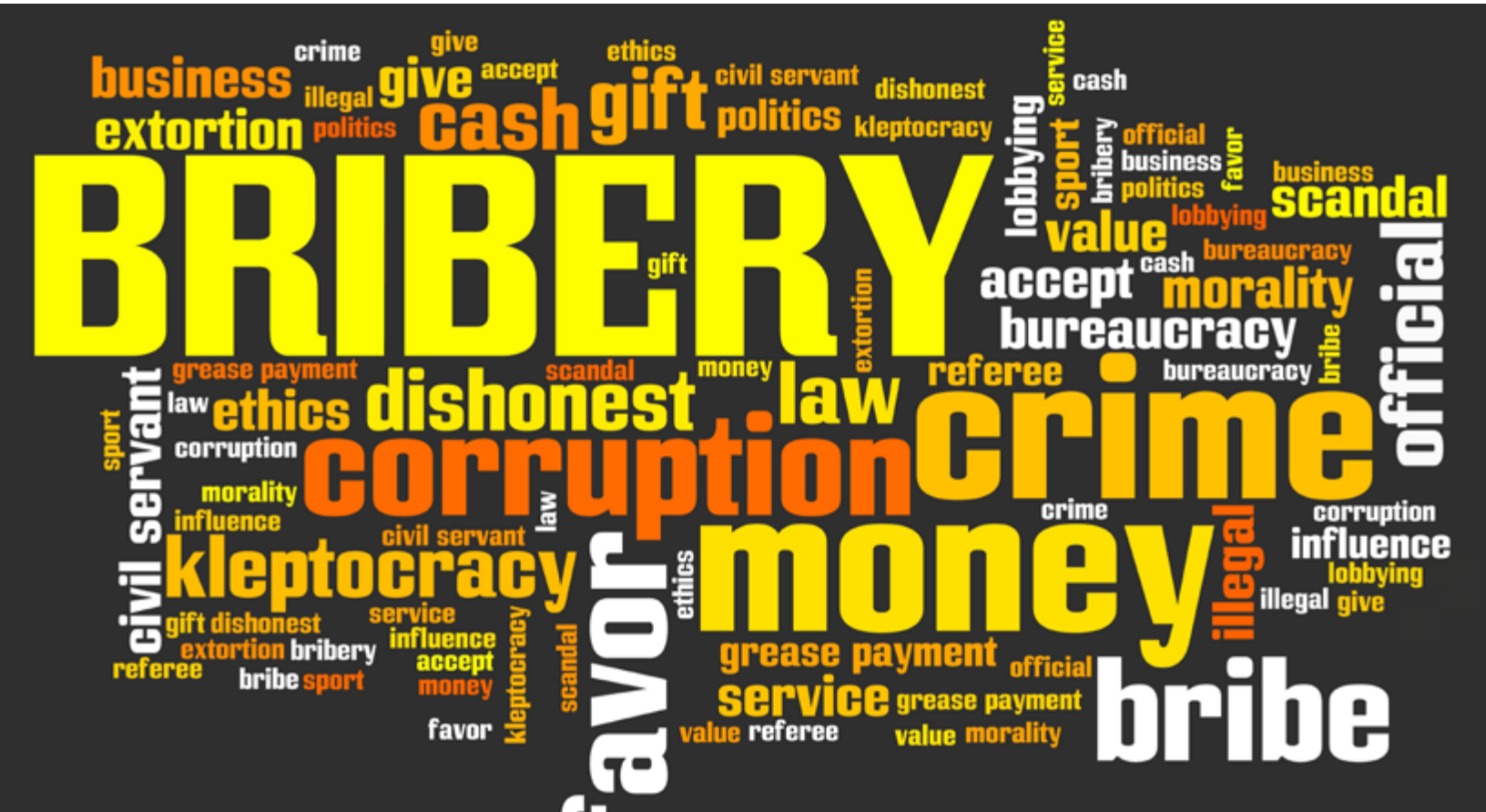
Since third parties can often be the weakest link in anti-bribery management efforts, companies need to have well-thought-out procedures for third-party screening, contract management, due diligence, risk assessments, monitoring, and non-conformance management. A risk-based approach to due diligence can help ensure that the third parties with the highest risk receive the most focus. Meanwhile, integrating with external data on PEPs, sanction lists, Special Interest Persons (SIPs), and adverse media listings can be useful in validating third-party bribery related data.

Build Visibility into Compliance

The better a company's visibility into anti-bribery data, the more effectively stakeholders can make decisions. Reporting tools, dashboards, and analytics play an important role in aggregating, correlating, and rolling up compliance related data from across the enterprise, and transforming it into valuable business intelligence that can help decision-makers act swiftly to close compliance gaps, and improve the company's anti-bribery posture.

Leverage Integrated Technology

Instead of struggling with multiple different tools and software, many companies are establishing a single, unified system to manage the whole gamut of anti-bribery requirements, including policy management, third-party management, risk assessments, audits, training, case management, and corrective action. The result of this integrated approach is greater control over anti-bribery measures, more visibility into compliance data, better reporting, and ultimately, stronger compliance.



In Summary

In contrast to the overall trend of deregulation that is sweeping across the US, anti-bribery and corruption enforcements are intensifying worldwide. Today, a company's anti-bribery efforts are pivotal to its reputation and brand value. In that light, compliance with the ISO 37001 standard can be a key market differentiator. Not only can it help organizations conform better to global anti-bribery regulations such as FCPA and the UK Bribery Act, but it can also minimize the risk of unlawful behavior, and showcase the organization's dedication to ethical practices – all of which build customer and investor confidence in the organization's integrity and credibility.

MetricStream, the independent market leader in enterprise and cloud applications for Governance, Risk, Compliance (GRC) and Quality Management, makes GRC simple. MetricStream apps improve business performance by strengthening risk management, corporate governance, regulatory compliance, vendor governance, and quality management for hundreds of thousands of users in dozens of industries, including Financial Services, Healthcare, Life Sciences, Energy and Utilities, Food, Retail, CPG, Government, Hi-Tech and Manufacturing. MetricStream is headquartered in Palo Alto, California, with an operations and R&D center in Bangalore, India, and sales and operations support in 12 other cities globally. (www.metricstream.com)

Email: info@metricstream.com

US: +1-650-620-2955 **UK:** +44-203-318-8554

India: +91-(0)80-4049 6600 **UAE:** +971-50-728-7247 **Australia:** + 61 2-8036-3130