Anti-Corruption Regulation 2018

In association with:

LALIVE

2018

GETTING THE DEAL THROUGH

Risk and compliance management systems

Daniel Lucien Bühr
Lalive

Can standard-based and independently certified anti-bribery management reduce supply-side corruption? The question remains current despite the fact that companies such as Alstom, Walmart and Microsoft have decided to implement International Organization for Standardization (ISO) Standard 37001 – Anti-bribery management systems, and seek independent certification (see Global overview).

The development of an anti-bribery programme into an anti-bribery management system is a change-management effort. And like all change-management projects, the implementation of an anti-bribery management system will meet resistance and scepticism. And for sure, someone will mention the deflection of Murphy's Law ('If anything can go wrong, it will') whereafter, 'If anything can go wrong, it's a system.'

In many organisations, it is essential to systematically manage product and service quality, information security and occupational health and safety, to quote a few examples. And yet, when it comes to managing risk and compliance, and especially evading or reducing the likelihood of bribery, most organisations do not yet appear to follow a standards-based approach, preferring to mix and match instead. Governmental and enforcement agency compliance guidelines are mixed with topical guidelines issued by trade or political organisations and then matched to the organisation's own management concepts. The final product is then often spiced up using 'home-made' ingredients. The result is that most organisations that manage risks and compliance use management programmes or systems that are couched in undefined terms and are based on discretionary principles and approaches, priorities and instruments. These home-made programmes and systems are therefore often not transparent, not comparable to anything and, consequently, not certifiable – that is to say they cannot be benchmarked. Independent auditors tasked with evaluating a particular organisation's impromptu risk and compliance management will need an above-average amount of time and resources to understand how the organisation is actually managed before it can conclude a reliable assessment. In practice, however, resources for highly individualised audits are not readily available and the upshot is that assessing non-standardised programmes and systems is a 'naturally flawed' process and generally unreliable.

Despite 'Murphy's Law of Systems', my guess would be that the true Law of Systems is: 'If anything can go wrong, it is piecemeal management.' Management is systematic and transparent when it follows documented, defined rules and involves planned, structured action; it can be easily understood by outsiders who are familiar with the rules; and the results can be, and are, independently audited. Since the beginning of the financial crisis in 2007 we have seen countless cases of long-standing organisational governance, risk and compliance failures, such as banks turning a blind eye to competition law, conflicts of interest and money laundering, and manufacturers willing to do business without honest and reliable product information. In many cases, the leadership breakdowns continued for several years under the averted gaze of governing bodies and top management. The costs of such managerial breakdowns are astronomical and the effects on reputation disastrous. After 40 years of modern compliance management (since the Lockheed scandal in 1976 and the USA's adoption of the Foreign Corrupt Practices Act in 1977), it clearly now makes sense to try a new, and hopefully more effective, approach to risk and compliance management.

Over the past few years, one of the most noteworthy steps aimed at making risk and compliance management more effective has been the development of standard-based risk and compliance management systems.

Management systems based on generally accepted international standards and best practices are an integrated process. They consist of a documented strategy, clear organisation, adequate planning, disciplined implementation, meaningful monitoring, accurate measuring of effectiveness and continual improvement. These systems follow the plan-do-check-act procedure, an iterative four-step management method used in businesses around the world to control and constantly improve processes and products.

A well-known example of this procedure is the ISO Standard 9001 – Quality Management Systems, which has been successfully used by more than one million businesses worldwide. The key reason for applying standard-based management systems is that standardisation reduces complexity and cost while harmonising technical specifications for processes, products and services, and this in turn increases transparency, comparability and efficiency. For the same reasons, businesses worldwide apply generally accepted accounting standards such as America's generally accepted accounting principles and International Financial Reporting Standards (IFRS).

Effective risk management is a prerequisite for effective compliance management. Without a reliable procedure for identifying, analysing and evaluating risks in order to deal with them in good time, any business is likely to hit the iceberg that no one on the command bridge ever saw coming. According to a 2014 report by the Organisation for Economic Co-operation and Development (OECD) (Risk Management and Corporate Governance), ISO Standard 31000 has become the de facto world standard in risk management. It was published in 2009 and is currently being revised. It is the only international risk management standard. Another key document, while not an international standard, is by the American private sector initiative Committee of Sponsoring Organizations of the Treadway Commission (COSO): 2017 Enterprise Risk Management Framework.

Defined terms are indispensable ingredients of any modern management system. ISO 31000 establishes clear terms and definitions. For instance:

- 'risk' is the effect of uncertainty on objectives;
- 'risk attitude' is the organisation's approach to assess and eventually pursue, retain, take or turn away from risk;
- 'risk assessment' is the overall process of risk identification, risk analysis and risk evaluation; and
- 'risk treatment' is the process to modify risk.

Based on its clear set of terms and definitions, ISO 31000 recommends that (senior) management commit to effective risk management and provide a documented mandate for designing and implementing a framework for managing risk. Once introduced, the framework needs to be monitored, reviewed and continually improved. The ISO Standard provides detailed guidance on the risk-management framework, risk-assessment and risk-treatment techniques and provides a multilingual risk-management vocabulary (ISO/IEC 31010 – Risk assessment techniques; ISO Guide 73 – Risk management – Vocabulary).

Some of the key risk management mistakes made by organisations are the:

- absence of a clear top management statement on the organisation's risk tolerance;
- reliance on mere risk governance models (which do not explain risk management on substance, such as the three lines of defence model) instead of genuine risk management standards and frameworks;

- (mal)practice of multiplying likelihood with consequences of an event or development, whereby worst-case scenarios are factored out; and
- massive underestimation of gradual developments (such as climate change, shifts in public attitudes to modern slavery, etc) compared to one-off events.

The standards-based management system approach also applies to best-practice compliance management. Examples of compliance management system standards are:

- Australian Standard AS 3806–2006 – Compliance Programmes;
- German Audit Standard IDW AS 980 – Principles for properly auditing compliance management systems; and
- ISO Standard 19600 – Compliance Management Systems (since 2014).

These aim to provide guidelines or minimum requirements for all private and public organisations wanting to design, implement, maintain and improve effective best-practice compliance management systems.

The fundamental managerial difference between compliance management based on a stand-alone corporate compliance programme and compliance management built on a generally accepted management system standards is transparency, confirmability and comparability.

Whereas classic standalone programmes, despite the frequent high-gloss codes of conduct, are often opaque, rather poorly documented, bottom-up (ie, single-risk rather than values-oriented) fragmentary compliance efforts, compliance management systems based on standards are transparent, top-down and driven by leadership, values and principles oriented and comprehensive, documented systematic compliance management efforts.

In practice, it makes a huge difference whether a business or a public organisation reinvents the wheel of compliance management on its own or whether it follows a structured, transparent, auditable and externally certifiable process based on an international standard.

ISO Standard 19600 introduces defined terms (eg, 'compliance', which means meeting all the organisation's compliance obligations, compliance culture, compliance function, etc) so that everyone speaks the same language, sets out the key role of leadership, tone at the top and ethical values and explains what good governance in compliance management requires.

Furthermore, the ISO Standard sets out in detail the responsibilities at all levels of an organisation, the planning, implementation and monitoring, measuring and continual improvement of the best practice compliance management processes and tools.

Good compliance governance explicitly or implicitly always includes the compliance function's direct access to the board, its independence from operational management, adequate organisational authority and availability of appropriate resources. The standards mentioned heretofore all equally underline a board's and top management's responsibility for compliance and the essential role of the right tone and good example they visibly set. They also address the key role of the compliance function in day-to-day management and the need for a written compliance policy, effective risk management and specific organisational (clear and easy to understand regulations, credible and effective reporting mechanisms, etc) and procedural measures (targeted training, timely and meaningful support, effective audits, etc).

The single most important legal risk to many organisations is corruption, either that their employees pay bribes to win business or that their officers demand bribes in exchange for steering business to the briber.

Bribery is one of the world's most destructive phenomena because it undermines good governance, hinders development and distorts competition. According to the World Bank, around US$1 trillion is paid each year in bribes, helping to perpetuate poverty worldwide.

ISO Standard 37001

In addressing the challenges of corruption faced by organisations, on 15 October 2016 the ISO published ISO 37001 – Anti-bribery Management Systems. ISO 37001 is a management system standard to fight bribery and promote an ethical business culture by setting out requirements and guidance for establishing, implementing, maintaining, reviewing and improving an effective anti-bribery management system. The standard was drafted by experts from 60 countries and international organisations, including the OECD and Transparency International.

ISO 37001 holds that organisations can contribute to combating bribery by means of anti-bribery management systems and with leadership commitment to establishing cultures of integrity, transparency, openness and compliance. It then states that the nature of an organisation's culture is critical to the success or failure of an anti-bribery management system. The standard is based on the position that the actual drivers of compliance are leadership, values and culture. Without this foundation, compliance efforts can never be any more than window dressing.

ISO 37001 only applies to bribery risks. It sets out requirements and guidance for a management system designed to help an organisation prevent, detect and respond to bribery, comply with anti-bribery laws, and make voluntary commitments applicable to its activities. In addition to what ISO 19600 recommends for effective compliance management, ISO 37001 defines the terms 'bribery', 'business associate' and 'public official', and specifically requires organisations to:

- establish an anti-bribery function in addition to an anti-bribery policy;
- conduct due diligence on specific transactions, projects, activities, business associates and staff to obtain sufficient information to assess the bribery risk;
- implement anti-bribery controls by business associates; and
- introduce procedures on gifts, hospitality, donations and other similar benefits.

ISO 37001 provides detailed guidance on its use (ISO 37001 Annex A), and the ISO Technical Standard 17021–9:2016 specifies the competence required for auditing and certifying anti-bribery management systems.

Independent auditing and certification of an organisation's anti-bribery management system does not provide a guarantee that employees will never become involved in bribery. However, by implementing a planned, structured and documented anti-bribery process and by independently benchmarking it against ISO 37001, organisations will be able to enhance their anti-bribery management. Even though any audit is only as good (or bad) as the audit framework and the auditor, the fact that independent audits are actually carried out will have a direct, material effect on the effectiveness of anti-bribery management.

Conclusion

It is time to rethink risk and compliance management and take them to the next level. An educated and reasonable approach is to implement standards-based risk and compliance management systems, including anti-bribery management systems. By doing this, management adopts the same approach to risk and compliance management that it has most certainly adopted in one way or another in its operative management of product and service quality or IT security.

Applying a transparent and generally accepted management process is more effective and less costly (including the cost of non-compliance) than standalone spur-of-the-moment risk and compliance management. All risk-exposed organisations, multinational as well as small or medium-sized businesses and public organisations, will appreciate the low cost of information on generally accepted best practices and the financial and operational advantages of following a well-established path. And finally, independent certification of best practice risk and compliance management will boost an organisation's learning curve, the pride of its employees and the trust of its stakeholders.

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-912377-49-7