NAVIGANT

COMPLIANCE

ISO 37001: A GAME CHANGER FOR BRIBERY COMPLIANCE

DAVID LAWLER
MANAGING DIRECTOR, NAVIGANT

DAVID LAWLER
Managing Director
+44 207.469.1189
david.lawler@navigant.com

JAY PERLMAN
Director
+1.202.973.3220
jay.perlman@navigant.com

BENJAMIN M. WHITFIELD
Director
+1.202.973.3281
benjamin.whitfield@navigant.com

JOSEPH CAMPBELL
Director
+1.202.973.4595
joseph.campbell@navigant.com

JOHN LOESCH
Director
+1.202.973.3235
john.loesch@navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the Firm primarily serves clients in the healthcare, energy and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

ISO 37001 is the new international standard for anti-bribery and corruption (ABC) management systems. It is an internationally agreed set of measures which organizations should implement to prevent and detect bribery.

WHAT HAS CHANGED?

ISO 37001 is the new global standard for anti-bribery and corruption (ABC) management systems.[1] This means that, for the first time, there is an internationally-recognised minimum set of measures for an organisation to have in place to prevent and detect bribery.

ISO 37001 will be a game-changer for ABC. It is designed for use in both the public and private sector, and we expect to see international adoption by public sector organisations, that will, in turn, require that organisations wanting to do business with them are certified to the same standard.

For compliance officers, ISO 37001 certification ensures that their program represents international good practice. In addition, certification of an organisation provides suppliers with reassurance that adequate procedures are already in place within their counterpart.

We think that ISO 37001 will become - like ISO 9001 - almost essential for companies wanting to work in some sectors, and we will see it permeate through industries. Companies not certified will be at a disadvantage.

1. http://www.iso.org/iso/iso37001

WHAT DOES ISO 37001 REQUIRE?

ISO 37001 is designed to help an organisation establish, implement, maintain and improve an anti-bribery compliance program. It specifies a series of measures which the organisation must implement in a reasonable and proportionate manner.

In terms of its specific elements, the ISO 37001 standard does not differ materially from the guidance available from the UK Ministry of Justice[2], the US Department of Justice[3], the OECD[4] and other sources in multiple jurisdictions, although there are few important nuances which are explained later in this paper.

The approach is one that both compliance professionals and business managers will recognise. The language is plain English – not legalese – which simplifies adoption and avoids a long and complex comparison between various competing national guides.

Active and Passive Bribery

Like the UK Bribery Act, ISO 37001 deals with both active (paying) and passive (receiving) bribes, and so it specifies measures which an organisation must adopt to address:

- Bribery by the organisation, its personnel or associates acting on the organisation's behalf or for its benefit.
- Bribery of the organisation, its personnel or associates in relation to the organisation's activities.

Public and Private Sector

The standard can be used by organisations in any country. It is flexible and can be adapted to a wide range of enterprises, including:

- Public and private sector
- Large and small
- Non-governmental organisations

FOLLOWING IN THE FOOTSTEPS OF ISO 9001?

Is ISO 37001 going to become widely adopted by business, or will it become yet another well-meaning but fringe pursuit?

This is a big unknown, but one indicator is given by the wide take-up of ISO 9001, the certified quality management system for organisations who want to prove their ability to consistently provide products and services that meet the needs of their stakeholders.

ISO 9001 has become a standard adopted by over 1.2 million organisations in 178 countries. At its inception, ISO 9001 was intended for manufacturing companies engaged in global trade, and was a natural corollary to the ISO standards for electronics, fabricated metals, rubber and plastic products which these businesses were having to comply with. Similarly, ISO 14001, the framework for an effective environmental management system, is now used by over 220,000 organisations around the world.

It is understandable then that the majority of registrations for ISO 9001 and 14001 still come from manufacturing industries, however they have steadily gained momentum in the service sector. Maintenance of ISO 9001 and/or 14001 is now almost essential for many companies, especially those working for public sector organisations.

ISO 37001 has the same structure as ISO 9001 and 14001, and can easily slot into to management systems already in place. ISO 9001 increases the chance of winning public and private sector contracts

For many years, both central and local government have stipulated quality management systems in their tenders. By demanding ISO 9001 and 14001 certification from contractors, the public sector can prove it is spending tax payers' money wisely, whilst not having to waste time checking an organisation's credentials. They just look for the ISO certification. Procurement specifications often require certification as a condition to supply, so gaining certification to the standard opens doors. And as major organisations also realised the benefits of ISO certification, they started to demand it of their suppliers.

2. https://www.gov.uk/government/publications/bribery-act-2010-guidance
3. https://www.justice.gov/criminal-fraud/fcpa-guidance
4. http://www.oecd.org/corruption/keyoecdanti-corruptiondocuments.htm

Several countries have already committed to having some central governmental agencies certified to ISO 37001. It will follow that organisations wanting to win tenders from those agencies will also need the certification. It seems inevitable that ISO 37001 will soon become a requirement for international public tender work, throughout the entire supply chain.

Widespread adoption of the standard will be quickened if it becomes the de facto substitute for the many and varied supply chain anti-corruption questionnaires that are sent out daily from procurement departments. Being certified to ISO 37001 should deal with many, if not all, of the detailed ABC questions asked of companies by their customers. And of course it serves, for early adopters, as a compliance and marketing differentiator.

WHAT IT MEANS FOR COMPANIES SEEKING TO COMPLY

For companies seeking to comply with the new standard, it means putting plans together to ensure their anti-bribery systems meet the exacting standards of ISO 37001.

Consistency with other international management standards

ISO 37001 follows the common ISO method for management system standards, consistent with ISO 9001 and 14001.

Compliance professionals will find nothing new in this standard, with each section promoting processes that are 'reasonable'. It follows the usual "Plan-Do-Act-Check" approach, including the requirement to:

- Implement an anti-bribery policy and programme.
- Appoint a compliance manager (who can be full time or part time) to oversee the programme.
- Assess bribery risks, including appropriate due diligence.
- Take reasonable and proportionate steps to ensure that business associates have implemented appropriate anti-bribery controls.
- Control gifts, hospitality, donations and similar benefits to ensure that they do not have a corrupt purpose.
- Implement appropriate financial, procurement and other commercial controls so as to help prevent the risk of bribery.
- Implement reporting (whistle-blowing) procedures.
- Communicate the policy and programme to all relevant personnel and business associates.
- Provide appropriate ABC training to personnel.
- Verify as far as reasonable that personnel will comply with the anti-bribery policy.
- Investigate and deal appropriately with any actual or suspected bribery.

THE KEY COMPONENTS OF AN ANTI-BRIBERY SYSTEM

Context of the Organisation

Part of the preliminary work of establishing a system involves building an understanding and documenting the organisation, as well as the needs and expectations of its stakeholders. It stresses the crucial risk assessment step in which the bribery risks are identified, assessed and prioritised. The risk assessment must be documented, and reviewed on a regular basis, including in the event of a significant change to the structure or activities of the organisation.

Leadership

The 'Tone from the Top' is an essential and vital part of every anti-bribery management system, and there is a continued requirement for the person or group of people who direct and control an organisation at the highest level to be active in the process.

The standard explicitly sets out that the person(s) with responsibility and authority for the operation of the system shall have direct and prompt access to the governing body and top management in order to communicate relevant information. They should not have to report solely to another manager in the chain who then reports upwards.

Planning

In planning their anti-bribery system, organisations must take steps to identify and assess their bribery risks. Organisations are encouraged to categorise risks into different levels, from low to high. For example "Agents or intermediaries who interact with the organisation's clients or public officials on behalf of it are likely to pose a "medium" or "high" bribery risk, particularly if they are paid on a commission or success fee basis."

The organisation can then determine the type and level of anti-bribery controls which apply to each risk category, and assess whether existing controls are adequate. If not, the controls can be appropriately improved. The organisation may change the nature of the transaction, project, activity or relationship such that the nature and extent of the bribery risk is reduced to a level that can be adequately managed by existing, enhanced or additional anti-bribery risk controls. It follows that activities that the organisation determines to be high risk, but that it cannot manage, should not be undertaken.

Support

To comply with the standard, organisations should devote adequate resources to establishing, implementing, maintaining and continually improving their system. There must be adequate and appropriate training and communication of the anti-bribery management system and documentation of the information provided.

Three areas in particular may need some work to bring their existing processes up to those demanded by the standard.

The first is the requirement that the anti-bribery compliance function shall be staffed by people who have the appropriate competence, status, authority and independence, and this must be documented. Specifically, the standard requires:

a. *determine the necessary competence of person(s) doing work under its control that affects its anti-bribery performance;*

b. *ensure that these persons are competent on the basis of appropriate education, training, or experience;*

c. *where applicable, take actions to acquire and maintain the necessary competence, and evaluate the effectiveness of the actions taken;*

d. *retain appropriate documented information as evidence of competence.*

The second is the requirement for **due diligence on all personnel** in positions which are exposed to more than a low bribery risk, and to all personnel employed in the anti-bribery compliance function. Specifically:

a. *due diligence is conducted on persons before they are employed, and on personnel before they are transferred or promoted by the organisation, to ascertain as far as is reasonable that it is appropriate to employ or redeploy them and that it is reasonable to believe that they will comply with the anti-bribery policy and anti-bribery management system requirements;*

Thirdly, the anti-bribery policy shall be made available to all the organisation's personnel and business associates, be communicated directly to both personnel and business associates who pose more than a low risk of bribery, and shall be published through the organisation's internal and external communication channels as appropriate.

Operation

The operational planning and control of ISO 37001 includes due diligence, financial controls and non-financial controls. It covers the reporting of suspected and actual bribery, as well as investigating on and dealing with such findings.

In this section there are two areas that an organisation might need to pay particular attention to:

Due Diligence:
Conducting checks of on certain transactions, projects, activities, business associates, or an organisation's personnel is a key component of the standard, as it informs the decision on whether to postpone, discontinue, or revise those transactions, projects, or relationships with business associates or personnel. As expected, and in line with all its requirements, the standard does not adopt the 'one-size-fits-all' approach, and due diligence must be weighted according to risk.

Low-risk business associates such as retail customers or suppliers may not require in-depth screening. However due diligence on business associates who act on the organisation's behalf or for its benefit is likely to be **as comprehensive as possible**.

Compliance in the supply chain
Significantly, an organisation will be required to ensure adequate systems not only within its own borders but for **all organisations over which it has control** (defined as directly or indirectly controlling the management).

In relation to non-controlled business associates, for which the bribery risk assessment or due diligence has not identified as low, the organisation should obtain anti-bribery commitments, and require the business associate to implement anti-bribery controls in relation to the relevant transaction, project or activity. This might be limited to training, and controls over key payments and gifts/hospitality. In the case of a major high bribery risk business associate with a large and complex scope of work, the organisation might require the business associate to have implemented controls equivalent to those required by ISO 37001. The organisation will normally impose these requirements on the business associate as a pre-condition to working it, and/or as part of the contract document.

If the organisation does not have sufficient influence to be able to require these commitments in relation to major suppliers or clients, this should be regarded as a relevant factor in the bribery risk assessment and due diligence.

Performance evaluation

Organisations are required to review periodically the ABC compliance system, either via an independent internal audit or a competent and independent third party. Such audits consist of internal audit processes or other procedures which review procedures, controls and systems for:

a. *bribery or suspected bribery;*
b. *non-compliance with the anti-bribery policy or anti-bribery management system requirements;*
c. *failure of business associates to conform to the applicable requirements of the organisation; and*
d. *weaknesses in or opportunities for improvement to the anti-bribery management system.*

Improvement

The standard concludes with the expected requirements to have in place processes to deal with problems, and to continually update the process.

'ADEQUATE PROCEDURES' AND THE DOJ GUIDANCE

The UK Bribery Act 2010 introduces an offence of corporate failure to prevent bribery. The defence for a company against this liability is to prove that it had 'adequate procedures' in place to prevent bribery. Long-awaited guidance to the Bribery Act 2010 was published by the Government in March 2011, in accordance with Section 9 of the Act.

Although adequate procedures are not a formal defence to prosecution under the FCPA, the Department of Justice has declined to prosecute companies where it considers that good ABC controls were in place and bribery was the work of a rogue actor (some would call this a de facto "adequate procedures" defence to FCPA violations). There is similar guidance under the US Foreign Corrupt Practices Act, and several NGOs including the OECD have published their own similar interpretations.

Like this guidance, ISO 37001 addresses tone at the top, due diligence, training, gifts and hospitality, books and records and risk assessments. And, like the guidance, which speaks in terms of compliance programs that are "reasonable", "appropriate" and "proportionate." ISO 37001 reflects this same "reasonable and appropriate" language.

Does ISO 37001 confer immunity from prosecution?

The ISO gives more clarity to the Bribery Act's 'adequate procedures' defence. Obtaining certification will not make a company immune to prosecution: prosecutors will always have the final word on this. However, it will make prosecution much less likely in the first place, and it can certainly help to demonstrate to outsiders that adequate procedures are in place.[5]

Certification considers the design and implementation of the system. It is not a guarantee of performance. Certification to ISO 37001 does not mean that no bribery has or will occur in the organisation. But certification looks beyond the mere existence of a paper program that is not being implemented. As with the Bribery Act and the DOJ/SEC requirements, there is an expectation that organisations that implement such systems are more likely to successfully identify and comply with applicable legal requirements.

At the launch of BS 10500, the UK predecessor to ISO 37001, the City of London Police gave comfort to companies that when the police are using their discretion over whether to investigate and seek to prosecute an organisation, they will take BS 10500 into account in assessing a company's efforts to have properly implemented adequate procedures to prevent bribery, and they stated that they are unlikely to look beyond the certificate and carry out their own assessment of procedures and controls.[6]

WHAT DOES CERTIFICATION ENTAIL?

ISO 37001 is a requirements standard, making it capable of independent certification by third-party auditors.

Although it is not compulsory for the ISO standard to be certified, and if so, there are no restrictions on who does the certification, there are huge benefits to getting certified from an accredited certification body. The United Kingdom Accreditation Service (UKAS) is the sole national accreditation body recognised by the British government to assess the competence of organisations that provide certification, testing, inspection, and calibration services.[7] It evaluates these conformity assessment bodies and then accredits them where they are found to meet the standard. Certification by a UKAS-registered body ensures that the certification is taken seriously.

The path to ISO certification would normally involve the assistance of a consultant, who would help the company to implement the quality management system, once this was in place they would put them forward to a UKAS accredited certification body for assessment.

It has been said as a criticism of ISO-type certifications that 'certification' is merely another lucrative revenue stream for consulting organisations. In fact, relatively few organisations will likely be able to grant the certification, at least initially, and none of those may provide ABC consulting services:

5. The DOJ declined to prosecute Morgan Stanley because of its because of its strong compliance program. https://www.justice.gov/opa/pr/former-morgan-stanley-managing-director-pleads-guilty-role-evading-internal-controls-required
6. https://globalanticorruptionblog.com/tag/bs-10500/
7. A full list of UKAS-accredited certification bodies is available on www.ukas.com.

the auditors of ISO 37001 must be independent, and are not allowed to provide management systems consultancy, or certify an organisation that received management systems consultancy where the relationship between the consultancy organisation and the certifying body poses an unacceptable threat to its impartiality.

Indeed, so strict is the delineation between consulting advice and auditing, that the ISO 37001 auditor is not able to provide recommendations for improvement: either the organisation entity meets the requirements or it does not. If it does not meet the requirements of the standard, then the auditor has only to explain why not.

The annual ISO audit and re-certification process will ensure a basic level of resources and structure for the ABC compliance program, which in many places throughout the world is much more than they currently have in place.

APPENDIX I: THE DEVELOPMENT OF AN INTERNATIONAL STANDARD FOR BRIBERY COMPLIANCE

The International Organisation for Standardisation (ISO) develops and publishes international standards. Its members are the national standards bodies from 163 countries. It has published over 21,000 standards. These range from traditional activities such as to food safety and engineering to the newest communications technologies; on areas such country codes (ISO 3166) through to quality management (ISO 9001).

ISO standards are voluntary. ISO is a non-governmental organisation and it has no power to enforce the implementation of the standards it develops, although some ISO standards - mainly those concerned with health, safety or the environment - have been adopted by some countries as part of their regulatory framework.

British Standard 10500 - Specification for an anti-bribery management system – was published in 2011, and the process towards expanding this to an international standard for anti-bribery systems was started in June 2013.

Experts from 59 participating and observing countries and 8 liaison organisations (including the OECD and Transparency International) were involved in the drafting of ISO 37000 under the leadership of the British Standards Institute, using BS 10500 as the base document. These are not inter-governmental negotiations: the participants on the committee negotiate as peers under the umbrella of national standards bodies.

ISO 37001 is expected to be published in early October 2016 by the International Standards Organization.

APPENDIX II ISO 37001 - THE HEADINGS

Context of the Organisation

- Understanding the organisation and its context
- Understanding the needs and expectations of stakeholders
- Determining the scope of the anti-bribery management system
- Anti-bribery management system
- Bribery risk assessment

Leadership

- Leadership and commitment
  - Governing body
  - Top management
- Anti-bribery policy
- Organisational roles, responsibilities and authorities
  - Roles and responsibilities
  - Anti-bribery compliance function

Planning

- Actions to address bribery risks and opportunities
- Anti-bribery objectives and planning to achieve them

Support

- Resources
- Competence
  - General
  - Employment procedures
- Awareness and training
- Communication
- Documented information
  - General
  - Creating and updating
  - Control of documented information

Operation

- Operational planning and control
- Due diligence
- Financial controls
- Non-financial controls
- Implementation of anti-bribery controls by controlled organisations and by business associates
- Anti-bribery commitments
- Gifts, hospitality, donations and similar benefits
- Managing inadequacy of anti-bribery controls
- Raising concerns
- Investigating and dealing with bribery

Performance evaluation

- Monitoring, measurement, analysis and evaluation
- Review by anti-bribery compliance function
- Internal
- Top management review
- Governing body review

Improvement

- Nonconformity and corrective action
- Continual improvement