ISO 37001 Part 1: raising the standard for anti-bribery compliance?

In Part 1 of this two-part series of articles, Charlotte Wright, Associate at Kingsley Napley LLP, looks at ISO 37001: Anti-Bribery Management Systems, and considers its content, significance and how it might affect companies' anti-bribery and corruption programmes

On 15 October 2016 the International Organisation for Standardisation ('ISO') published ISO37001 ('Standard'), its first standard on anti-bribery management systems (ABMS). The Standard is intended to support organisations in their contribution towards combating bribery.

The Standard seeks to reflect international good practice for anti-bribery compliance programmes. It is designed to apply to all organisations, whether large or small, public, private or not-for-profit, and across all jurisdictions and sectors.

The project to create the Standard was led by the British Standards Institution ('BSI') and the drafting process involved experts from 37 participating countries across six continents, 22 observer countries and 8 liaison organisations, including the Organisation for Economic Co-operation and Development ('OECD') and Transparency International ('TI'). http://www.transparency.org.uk/international-anti-bribery-standard-iso-37001/

Why create an international standard?

It is now widely accepted that private companies and other organisations are required to contribute to global anti-corruption efforts. Legislation such as the US Foreign Corrupt Practices Act ('FCPA') and the UK Bribery Act 2010 ('UKBA') gives authorities the power to prosecute and punish severely those companies which do not take steps to prevent bribery within their organisations, or which encourage or facilitate it.

In consequence, an approach to anti-bribery compliance has developed around the requirements of these laws and their respective guidance documents. However the proliferation of developing laws, many of them with extra-territorial effect, is a minefield for companies and other organisations to navigate.

This new Standard seeks to assist by rationalising and creating a consistent global approach. The aspiration is to create a common standard for organisations to strive towards, to promote positive business cultures where commitment to an anti-bribery programme is recognised and rewarded, and thus the incentives to engage in bribery are reduced.

Who will provide certification?

As with other ISO standards, independent bodies such as the BSI will be licensed to audit ABMS and provide certification to organisations which meet the Standard's requirements.

Of course, such an audit does not come for free. It is difficult to estimate the costs, which will vary depending upon factors such as the size of the organisation and its risk profile, but they are likely to be in the thousands, even for small companies. Organisations must also consider the cost of purchasing the ISO (currently 158 Swiss francs, around £125) and also the investment required to implement the ABMS.

What is the likely impact of an international standard?

In the short term, what is significant about the Standard is simply the fact that it suggests there is now a global understanding of what is required from an anti-bribery compliance programme.

The Standard may not make a big impression on large organisations which have already invested significant time and money in developing anti-bribery and corruption ('ABAC') programmes to bring them in line with the existing FCPA and UKBA guidance (though they may want to check their policies against the Standard to ensure they are in line). However, the impact may be felt by smaller organisations, many of whom might welcome firm guidance and see ISO-certification as a selling point sufficient to justify the investment. That, in turn, could ultimately be felt by the organisations doing business with them.

This wider impact will likely depend upon the extent to which the Stand-

ard is adopted by businesses and other organisations. The Standard has the potential to create a method by which organisations can take comfort that those they work with are taking adequate steps to prevent bribery, and reduce the risks in such relationships. It could become a key part of doing business - companies could require that any organisation tendering for a contract must be ISO 37001 certified, for example. Any such impact is unlikely to be immediate and will develop over time.

What are the advantages of seeking certification under the Standard?

As certification is not obligatory, organisations - particularly those which already have robust anti-bribery programmes in place - may consider that certification does not warrant the investment of time and money. However, there could still be benefits to using the Standard as more than a benchmarking tool.

First, until now, compliance officers have had to sell anti-bribery programmes to their businesses based on what, for many, is the remote threat of a criminal investigation and potential FCPA and UKBA sanctions. Certification, on the other hand, may be a carrot to the criminal sanction's stick. It can be sold as a positive, an accolade, something that an organisation can be proud of. It could be publicised and used to demonstrate that the organisation takes anti-bribery compliance seriously - something that is increasingly attractive to stakeholders and potential business partners.

Second, the costs of certification may prove a sound investment if companies are able to use the certificate to reduce their costs in the long-run. For example, if ISO-certification is made a requirement of all contracts with business associates, companies could save on the costs of due diligence.

Third, certification may be relied upon as part of a defence or mitigation strategy, in the event that the worst happens and an organisation faces criminal bribery allegations. While there are no guarantees, certification would tend to demonstrate a commitment to bribery prevention within an organisation. For example, it may be relied upon to demonstrate that the organisation had in place adequate procedures to prevent bribery, as part of a defence to a section 7 UKBA offence. Or there are some jurisdictions in which certification might be considered a mitigating factor and a basis on which to offer a reduction in sentence.

Finally, obtaining certification could be seen as an opportunity to take leadership in a new era of anti-bribery compliance, making a strong anti-bribery programme a crucial part of doing business and encouraging others to do the same.

> ***"The aspiration is to create a common standard for organisations to strive towards, to promote positive business cultures where commitment to an anti-bribery programme is recognised and rewarded, and thus the incentives to engage in bribery are reduced"***

Is there anything to be wary of in using the Standard? Are there any pitfalls?

The first thing to note is that the Standard does not represent what is required by the local laws of every jurisdiction across the globe. While many countries have agreed it represents good practice, commentary on the process acknowledges that inevitable compromises had to be made to reach consensus.

The Standard will also not be updated regularly, so will not capture changes in the law. Following the Standard, or obtaining certification, would therefore not relieve an organisation from the need to continue to keep abreast of legal developments and reflect them in an organisation's anti-bribery programme as required.

On a related point, the ISO devotes a lot of space to reminding organisations that they must continue to monitor and develop their procedures over time. It is not clear, in those circumstances, how quickly a certification would go out of date, and how often companies will need to be audited in order for certification to mean anything.

Further, the Standard is quite different from one that, say, sets out specifications for a particular type of product made by a particular industry, to ensure that the product performs to a specific standard regardless of who makes it and where in the world it is used. Product specifications are specifically measurable and can be based upon scientific analysis, so lend themselves to the creation of universal quality standards.

Anti-bribery compliance, however, is an art rather than a science. All organisations face different levels of bribery risk, so the Standard cannot be prescriptive and can only really provide guidance. There is a huge reliance in the Standard on the phrase "reasonable and proportionate" when stating how an organisation should address the risks it faces - which of course requires judgment calls to be made.

Some companies may also need to go much further than the measures set out in the Standard, depending upon their particular level of risk - and others may find it overly cumbersome given the low risks in their business.

Given these variables, there is also a question over how much such systems lend themselves to being audited. There is a risk that auditors may find the requirement placed upon them quite onerous, resulting either in

(Continued on page 4)

(Continued from page 3)

an overly cautious approach, or in an increase in costs. This may in turn discourage companies from seeking certification.

What does the Standard say?

The Standard sets out a step-by-step process for implementing an ABMS – which will be familiar as it does not venture too far from the six principles of adequate procedures set out in the guidance to the UKBA. The body of the Standard contains ten sections plus an Annex which provides more in-depth guidance on issues such as the meaning of the phrase "reasonable and proportionate" and the factors to be considered in conducting due diligence on employees and third parties.

For the most part, the body of the Standard uses the word "shall" – which should be taken to mean "must" and therefore required for certification; the Annex uses the word "should" – so its content is more advisory.

A section by section review follows, giving more detail of the focuses of the Standard. This review is intended as an indicator of what the Standard covers, and as a guide for navigating what is quite a large document. It is not intended to be a substitute for reading the Standard itself in full.

Section 3: definitions (and Annex A.21)

Section 3 contains the definitions. Most noteworthy of these is the description of a public official for the purposes of the Standard, supported by the examples of public officials given at A.21. This definition is wide – covering the definition set out in the UKBA, but also including specific reference to candidates for office, for example. The list of examples at A.21 is not exhaustive, nor will it apply to all jurisdictions. It will therefore still be necessary to refer to the definition of a public official in the individual countries in which an organisation operates.

Section 4: context of the organisation (and Annexes A.2 - A.4)

This section covers the first step in creating an ABMS, the risk assessment phase. In order to risk assess, an organisation must:

- take steps to understand itself, by considering factors such as its size and structure, the locations in which it operates, and the nature of its interaction with public officials;
- understand who the stakeholders of the ABMS are, and what their requirements are; and
- conduct regular risk assessments which identify and analyse the bribery risks the organisation faces, and evaluate the suitability of the organisation's existing controls for mitigating those risks.

"The Standard sets out a step-by-step process for implementing an ABMS – which will be familiar as it does not venture too far from the six principles of adequate procedures set out in the guidance to the UKBA"

A.4 provides further detail on conducting a risk assessment and gives examples of how the factors at the first bullet point above might affect the organisation's assessment of its bribery risk.

Interestingly, A.4(h) states that an organisation should not only look at the factors indicated; it should also assess the extent to which it may influence or control the risks posed by those factors. It notes that an organisation may change the nature of a transaction, for example, to reduce the bribery risk to a level that can be adequately managed.

While A.4.4 states that "this bribery risk assessment exercise is not meant to be an extensive or overly complex exercise", in reality, risk assessments for large organisations often must be fairly complex. This is an example of where it may be important to do work beyond what is required by the Standard.

A.2 and A.3 also give further colour on this section. A.2 provides guidance on the meaning of facilitation and extortion payments and notes that an ABMS should prohibit the former but may have a policy authorizing their personnel to make the latter where there is fear of imminent danger to another.

A.3 gives guidance on the meaning of the all important phrase "reasonable and proportionate", giving examples of the lengths that different types of organisation may need to go to with their ABMS. The key point is that such measures should be commercial – not so onerous that the business cannot function or so that the measures are doomed to failure, but not so scant as to be ineffectual. The Standard recognizes that businesses are unlikely to be able to entirely eradicate bribery – but says they should nevertheless be trying their best to.

Section 5: leadership (and Annexes A.5 - A.6)

This section reflects the "tone from the top" requirements already very familiar in the ABAC compliance sphere. It sets out a three-pronged approach to the management of an ABMS, involving the governing body of an organisation (for example, its board), its "top management" (for example, the heads of particular divisions) and its compliance function.

First, it is made clear that both top

management and the governing body should have involvement with the ABMS to ensure that it is properly implemented and promoted within an organisation.

Perhaps the most interesting part of this section is at 5.3.2, which provides a detailed description of the responsibilities of the anti-bribery compliance function (meaning any person with responsibility and authority for the operation of the ABMS). There is no provision for an organisation not to have someone in this role – though it is acknowledged at A.6 that in a small organisation this may be someone who is responsible on a part-time basis. This is once again a question of risk and proportionality, but the Standard makes clear that whoever has these responsibilities must have the appropriate "competence, status, authority and independence". This recognises the important role that Compliance Officers play, and emphasises that they should be adequately resourced and have a direct line to top management as part of an adequate ABMS.

This section also sets out a checklist of what should be covered in an anti-bribery policy (5.2).

Section 6: Planning

This is a purely procedural provision which requires little comment.

Section 7: Support (and Annexes A.7 – A.9 and A.17)

What is interesting about Section 7 is that it not only covers awareness and training, but requires that companies consider ABAC issues right from the outset of an employee relationship – namely at the recruitment stage. This is briefly referred to under the 'Proportionate Procedures' heading of the UK guidance, but is given a significant amount of space in the ISO.

This sounds intensive but is not much beyond what an organisation would already do during the recruitment process (for example, checking qualifications, obtaining references) but, depending upon the person's role, also discussing the ABAC policy at interview and taking "reasonable steps" to ensure that the person has not previously been involved in bribery and to check their relationships with public officials. As with the rest of the Standard, the extent to which companies must undertake these processes is risk-based.

A.8 contains guidance on the different controls that an organisation might use depending upon whether the bribery risk is "outbound" (payment of bribes by its employees) or "inbound" (payment of bribes to employees).

For example, the former may require restrictions on performance incentives such as bonuses contingent on sales volume or contract wins; the latter the provision of a robust mechanism for reporting bribery.

Many organisations will already be familiar with the requirements of the remaining parts of this section, which deal with awareness and training, communication, and documentation. Advertising anti-bribery policies and measures, giving training at appropriate levels to different sections of the business, and recording the efforts made are a key part of any ABMS.

There is extensive guidance at A.8, A.9 and A.17 on meeting these requirements.

"section 5.3.2… provides a detailed description of the responsibilities of the anti-bribery compliance function….the Standard makes clear that whoever has these responsibilities must have the appropriate "competence, status, authority and independence". This recognises the important role that Compliance Officers play, and emphasises that they should be adequately resourced and have a direct line to top management"

Section 8: operation (and Annexes A.10 – A.16 and A.18)

This section covers the operational phase and has a broad remit covering due diligence, financial and non-financial controls, dealing with third parties, gifts and hospitality policies, whistle-blowing and investigating bribery.

It is difficult to go into the extensive detail of Section 8 in the space available, but the key headings are expanded upon briefly here:

Due diligence (8.2)

This should be conducted where the organisation's bribery risk is "more than low" so as to obtain sufficient information to assess the risk.

A.10 sets out factors that may assist in the analysis and gives examples of the types of associate that may pose significant risk (such as agents helping an organisation to win a contract award) and those that pose a low risk (for example suppliers selling to the organisation). At A.10.3 there are some examples of the activities that might be undertaken by way of due diligence.

Controls (8.3 and 8.4)

The financial controls section is interesting and merits consideration.

(Continued on page 6)

(Continued from page 5)

Financial controls are liable to be taken for granted as they are likely to already be in place at large organisations, but their inclusion here is a useful reminder of their fundamental importance in ensuring that organisations can control and identify how their money is being spent.

Non-financial controls will generally come into play within the operational functions of the organisation. A list of example controls is provided at A.12. Crucial among these is a consideration of the "necessity and legitimacy of the services to be provided" and "whether any payments to be made to the business associate are reasonable and proportionate to those services". Payment of disproportionate fees for unnecessary services is a key bribery red flag, and looking for these signs is an important control.

Anti-bribery controls and commitments (8.5 and 8.6)

A distinction is made between those over whom an organisation has control (such as a joint venture in which it has management control) and its business associates.

Where an organisation has control of an entity, an organisation must require that the entity implements anti-bribery controls generally (i.e. it is not sufficient for the controls to apply only to a specific transaction).

Where an organisation is merely a business associate and has no ownership control, it must require such controls to be implemented "in relation to the relevant transaction, project or activity". Where it is not possible to implement such controls, this should be a factor taken into account in evaluating the bribery risk of the project.

Further, where business associates pose a "more than low" bribery risk, the organisation should require that the associate will commit to preventing bribery in connection with the relevant project and that the organisation is able to terminate the relationship in the event of bribery being committed by the associate in connection with that project.

Gifts, hospitality, donations and similar benefits (8.7)

A.15 provides quite extensive guidance on the implementation of a gifts and hospitality policy, setting out examples of the types of benefit that should be covered, and the types of procedures that could be implemented – such as controlling the extent and frequency of gifts and hospitality by, for example, setting expenditure limits. This is useful given that it is an issue that comes up regularly for organisations.

Managing inadequacy of anti-bribery controls (8.8)

This section is interesting as it makes clear that, where bribery risk cannot be managed, the organisation must terminate or suspend an existing relationship, or postpone or decline a prospective one. This raises interesting questions such as what an organisation can do if, for example, there is only one supplier of a crucial element of its product, and it cannot manage the bribery risk for that supplier. There appears to be no 'get out' for this situation. While this is unsurprising, it may create difficulties for organisations purchasing niche products or services.

This section also covers raising concerns and investigating and dealing with bribery (8.9 and 8.10).

Section 9: performance evaluation (and Annexes A.16 and A.19)

This section highlights the need for monitoring of the ABMS, both by internal audit and by the three management divisions referred to in Section 5. It highlights that putting an ABMS in place is not enough – it must be continually reviewed to ensure it is doing the job.

Section 10: improvement (and Annex A.20)

The focus of this section is upon undertaking corrective and preventative actions. Any non-conformities identified through the review processes identified at Section 9 must be documented and the organisation shall determine whether any action is required to fix the non-conformity. A.20 sets out further guidance on how to do this.

Other Annexes

Finally, A.22 notes that, while it is not a requirement of the standard, an organisation may find it useful to participate in other anti-bribery initiatives. This emphasises that the Standard is a minimum rather than a maximum standard, and that other actions may be advisable depending upon factors such as the activities of an organisation, or the sector in which it operates.

Conclusion

The debate over the need for and usefulness of ISO 37001 will no doubt continue within the compliance community for some time. Viewed on its own merits, however, the Standard is a decent attempt to rationalise the competing guidance in this area – and with the potential to raise the profile and importance of ABAC compliance within the global business community, it is worth a look to see if it could help achieve your organisation's anti-bribery aims.

In Part 2 of this article, we will take a more detailed look at the risk assessment element of the Standard and ask to what extent it can help Compliance Officers .

Charlotte Wright

Kingsley Napley LLP

cwright@kingsleynapley.co.uk