The ISO 37001 anti-corruption compliance program standard: What's good, what's bad, and why it matters

By Joe Murphy, CCEP[1]

I. Executive summary: Key points in this review

The promulgation of the ISO standard for anti-bribery management systems, ISO 37001, is undoubtedly a major development in the compliance and ethics field relating to the fight against bribery. It has, however, generated a considerable amount of controversy.[2] The following analysis of ISO 37001 is offered to shed light on this topic.

These are the key points covered in this review:

a. **Certification.** Organizations[3] can have their anti-bribery programs certified under ISO 37001.[4] Certification may be the raison d'être for the Standard, but it raises some real concerns.

---

[1] Joseph E. Murphy has worked in the compliance and ethics field for decades, co-authored the first book on this subject, Sigler & Murphy, Interactive Corporate Compliance: An Alternative To Regulatory Compulsion (Greenwood Press; 1988), and recently published **Policies in conflict: Undermining corporate self-policing,** 69 Rutgers U.L. Rev. 421 (2017), http://www.rutgerslawreview.com/wp-content/uploads/2017/07/Joseph-Murphy-Policies-in-Conflict-69-Rutgers-U.-L.-Rev.-421-2017.pdf

[2] Jaeger, The pros and cons of ISO 37001 certification, Compliance Week, 50, 51 (Dec. 2016)(noting that there has been "passionate debate" about whether this standard was necessary).

[3] ISO 37001 applies to all types of organizations – private, governmental and non-governmental. Throughout, references to companies, entities or organizations encompass this complete scope. This is also the same scope defined in the US Sentencing Guidelines' standard for compliance programs, http://www.ussc.gov/Guidelines/2016_guidelines/Manual_PDF/Chapter_8.pdf .

[4] International Organization for Standardization, The facts about certification, "ISO does not perform certification," https://www.iso.org/certification.html . In this paper I refer to "ISO certification," recognizing that ISO does not perform certification, but that companies retain outside entities to review their programs to determine whether they meet the ISO 37001 Standard.

i. First, the standard may be too general to permit real certification.
ii. Second, once a company has achieved certification, it has an implied incentive to backslide. Surveillance reviews are required, but will these be effective checks against backsliding?
iii. Third, there is a question about quality control. Is there sampling of the certification work sufficient to determine that no one is gaming the system?
iv. Fourth, there is an inherent conflict of interest in having companies select their own certifier. This could invite a race to the bottom using the least expensive supplier.
v. Fifth, certification can invite atrophy and failure to innovate.
vi. Sixth, there may be confusion about whether a company has been certified. Some may be certified by a reviewer that does not have credentials in accordance with the processes established by ISO. Moreover, each nation has its own ISO organization that can also issue credentials, so while certification might be difficult from a reviewer in the UK or the US, there are other countries around the world that could give reviewers the necessary credentials, even if not truly merited. There is no central database listing 1) what entities have been authorized to give accreditation by an ISO national authority, 2) what organizations have been legitimately certified, or 3) who conducted the certification for those organizations.[5]
vii. Seventh, it may be unclear what the fact of certification signals about a company's anti-bribery management system.
viii. On the positive side, a valid certification program could lead more companies to embrace compliance efforts, and move this effort down their supply chains. In some environments a company's having this

[5] Each nation's accreditation authority would have a list of accredited bodies.

certification might also signal to potential bribe seekers not to expect a bribe from that company, but to approach easier prey instead.

ix. The review and certification process can act as a catalyst to mobilize management to take steps to improve the program. While all may support a program in concept, it is important to get managers actually engaged in implementing appropriate steps. A review deadline can help enormously in this respect.

x. The certification process can also build positive team spirit for the compliance effort. Working together to prevent future problems can be a challenging effort, because there is no immediate reward. But working to achieve certification is goal-oriented, with a visible, positive result. Managers can see themselves as part of a team driving toward a specific goal.

b. **Standards as a revenue source.** Access to ISO 37001 must usually[6] be purchased. This is the only anti-bribery standard for which one has to spend money to obtain access. This restriction could severely limit access, make it less likely copies could be widely available in companies, present a cost for small businesses who are already fighting to control expenses, and possibly thwart public analysis and commentary.

c. **Drafting.** There are serious questions about the quality of the Standard's drafting. This may be behind some of the angry resistance to the Standard. In key areas where guidance is needed, readers may walk away unsatisfied.

d. **The Annex.** The guidance in the Annex is useful, but may be ignored because it is only "illustrative." The drafters failed to integrate the Annex properly with the Standards and the certification process.

e. **Management.** The Standard does an enormous service by emphasizing that compliance is about effective <u>management</u> steps. Compliance is not policies and preaching; it is about all the types of management steps spelled out in ISO 37001 (and

[6] The author was granted free access for purposes of conducting this review.

in other standards). The Standard also, at least arguably, provides a "common language" for communications about anti-bribery compliance programs globally.[7]

f. **CECO.** Compliance programs will live or die based on the empowerment and independence of the Chief Ethics and Compliance Officer (CECO). The Standard has some words intended to help, but misses a crucial point which may cause it to fall well short in this crucial mission.
g. **Evaluation.** The definition used for "effectiveness," one of the most important elements in any compliance standard, also raises serious questions.
h. **Industry practice.** An important missing piece is any reference to industry practice, or the need to keep up with innovations in the field.
i. **No in-house program.** The standard would permit organizations to outsource the entire compliance program.
j. **Third parties.** The Standard does a superior job of emphasizing the role of third parties. However, if companies indiscriminately accept ISO certification from third parties, instead of doing appropriate due diligence, the result could be a step backward.
k. **Other points.** There are a number of points throughout that should be improved or represent strong positive elements.

II. Introduction

a. Let us start with the basics. What is the International Organization for Standardization, "ISO"? https://www.iso.org/home.html As stated in the Foreword, it is a worldwide federation of over 160 national standards

[7] Gasiorowsky-Denis, How Microsoft is bursting the bribery bubble (Nov. 8, 2017) https://www.iso.org/news/ref2238.html

bodies. It has issued over 21,000 international standards,[8] including standards for quality, environment and safety.[9]

b. What is ISO 37001?
    - **i.** ISO 37001, is the standard issued in 2016, addressing anti-bribery management systems. It had its origins in a standard published by the British Standards organization, BS 10500:2011.
    - **ii.** There is also an ISO standard on the broader topic of compliance management systems, ISO 19600, which has its origins in Australia, with AS 3806. But that standard is only a guidance document and provides for no certification.
    - **iii.** The drafters were primarily representatives of the private sector. One of the participants in the process, however, reports that there were over 100 experts from companies, governments and NGOs, from 56 countries, plus 18 observer countries and 7 liaison organizations.[10] Meetings were attended by approximately 80 experts from 25 countries.[11]

c. The structure
    - **i.** Any standard issued by ISO is required to follow their format. Thus in order to adhere to that approach, ISO 37001 varies from the approach taken by other

---

[8] Crescenzi, ISO 37001 Certification: Understanding and navigating the process, Compliance & Ethics Professional 36 (Aug. 2018).

[9] Stansbury, The Purposes and Benefits of ISO 37001 (Feb. 8, 2018), available at https://www.ethic-intelligence.com/en/experts-corner/international-experts/43-the-purposes-and-benefits-of-iso-37001.html .

[10] Benton, A new anti-bribery management systems standard: ISO 37001, Compliance & Ethics Professional 43, 45 (Nov. 2016); see BakerMcKenzie, Singapore Adopts ISO Standard on Anti-Bribery Management Systems (May 11, 2017), reporting that the drafting committee represented 61 countries including Singapore, available at https://globalcompliancenews.com/singapore-iso-37001-cms-20170512/ ; see Crescenzi, ISO 37001 Certification: Understanding and navigating the process, Compliance & Ethics Professional 36, 37 (Aug. 2018), reporting 37 participating countries, 22 observing countries and 8 liaison organizations.

[11] Stansbury, The Purposes and Benefits of ISO 37001 (Feb. 8, 2018), available at https://www.ethic-intelligence.com/en/experts-corner/international-experts/43-the-purposes-and-benefits-of-iso-37001.html . It should be noted that while many entities may be listed as participating in the drafting process, this does not mean they all attended or participated in all the sessions.

compliance program standards worldwide. Generally other standards have been briefer and more practical in approach. They also tend to be written in a more conversational style, even when issued by government agencies.

ii. For a sense of how controlled this is, there is a 90-page directive on how to structure and draft an ISO standard. https://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/4230456/ISO_IEC_Directives%2C_Part_2%2C_Principles_and_rules_for_the_structure_and_drafting_of_ISO_and_IEC_documents_%2D_2018_%288th_edition%29_%2D_PDF.pdf?nodeid=19685788&vernum=-2

iii. Of particular note is this point from the Directive: "Those drafting ISO . . . documents should try to be aware of the particular needs of their intended users and to write in a style that is likely to be readily understood." Introduction p. xi. This point is important to remember in the discussion below about the drafting of this Standard.

iv. The Standard has "requirements," and an Annex which provides guidance. The value of the Annex was undercut by limiting it to being "illustrative." In hindsight it should have been a required part of any certification process. This is discussed in more detail below. Throughout this analysis "Standard" refers to the requirements portion, and "Annex" refers to the guidance portion.

d. What was the purpose of issuing ISO 37001? To the extent this causes companies to approach the fight against bribery as a management task and step up their compliance efforts, it could have great value. As a concept, that makes good sense. Compliance is a management task, and it is important that companies see it that way.

e. When looking at the Standard it also makes sense to ask what gap it may have filled and what other guidance was available already. It is not possible to argue that there was an absence of guidance on how to build an effective anti-bribery

compliance program. In point of fact, there was an enormous amount of guidance already available, including:

i. The US Sentencing Guidelines, http://www.ussc.gov/Guidelines/2016_guidelines/Manual_PDF/Chapter_8.pdf which can rightly be described as the origin of the modern approach to compliance and ethics.
ii. The OECD Good Practice Guidance, the first international guide to anti-bribery compliance programs, http://www.oecd.org/daf/anti-bribery/44884389.pdf
iii. There are a number of national governmental standards and guidance documents – e.g., US DOJ/SEC,[12] UK.[13]
iv. Many privately published guides exist on compliance programs in general and anti-bribery programs specifically.
v. There is also very useful guidance from non-governmental organizations, including the International Chamber of Commerce and Transparency International.
vi. There was plenty of free, practical guidance on how to develop an anti-bribery compliance program. Nor was there a perceived need to address conflicting standards and guides. While some had more detail than others, they were consistent and emphasized diligent management practices. They were also generally designed to be applicable to all kinds and sizes of organizations.

f. What is certification?
   i. The hook in this process was that companies could have their programs "certified" to the ISO standard. ISO certification was a concept that was expected to

[12] US Department of Justice and US Securities and Exchange Commission, FCPA: A Resource Guide to the US Foreign Corrupt Practices Act (Nov. 14, 2012), http://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf .
[13] UK Ministry of Justice, Bribery Act 2010, Guidance, https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf

appeal to companies and thus get them to pay attention to the new standard. This expectation was based on the fact that there are many ISO standards, and that companies are familiar with these and the certification process. Under this approach, a company's program would be reviewed by experts, who would determine whether the company's program met the ISO Standard.

g. What have been the reactions?

i. Perhaps surprisingly, there has been a fair amount of criticism and skepticism from those who are otherwise supporters of compliance programs and also support the anti-corruption effort. Tom Fox, whom some would call "Mr. FCPA," has been very vocal in his opposition to the standard.[14] The author of this paper has also raised questions on the FCPA Blog. Among these critiques there have been objections that ISO 37001 is intended as a revenue generator for consultants.

ii. On the other hand there have been early adaptors and reputable people in the field who have championed the ISO Standard.[15]

iii. There have also been unfair criticisms, and these can be addressed before analyzing the text of ISO 37001.

1. ISO certification will not make companies bulletproof. It should be clear that, at least to this author's knowledge, no ISO person has claimed certification will be a free pass with the government, although it could well be taken into consideration.[16] Consultants might

[14] See, e.g., Fox, "Defects in the ISO 37001 Certification," Feb. 7, 2018, available at http://fcpacompliancereport.com/2018/02/defects-iso-37001-certification/

[15] See, e.g., Kristy Grant-Hart on ISO 37001: Yes, we need one standard to rule them all, FCPA Blog, Apr. 26, 2016, available at http://www.fcpablog.com/blog/2016/4/26/kristy-grant-hart-on-iso-37001-yes-we-need-one-standard-to-r.html ; Montigny, ISO 37001: What Does It Involve? (May 1, 2016), available at https://www.ethic-intelligence.com/en/experts-corner/anti-corruption-compliance-blog/165-iso-37001-what-does-it-imply

[16] See, e.g., Benton, A new anti-bribery management systems standard: ISO 37001, Compliance & Ethics Professional 43, 45 (Nov. 2016)("ISO 37001 certification will

privately exaggerate the benefits, but that is certainly not authorized by ISO.

2. One prominent critic has denounced the ISO Standard because there were no empirical studies and no metrics showing the standard would reduce violations. This is an unfair objection to raise about the ISO standard on a number of levels. First, the standard is just being rolled out. How could there possibly be any metrics? Such a rigid requirement would freeze most policy initiatives. Second, the criticism itself may reflect too much faith in metrics; see Jerry Z. Muller, The Tyranny of Metrics (2018). Metrics should govern things that are readily quantifiable. One can count how many widgets are produced (but be sure also to check the quality). But as the saying goes, not everything that counts can be counted, and not everything that is counted counts. An over adherence to metrics can lead to numerous problems and policy mistakes.
   Moreover, numbers or metrics are not necessarily what should drive or does drive public policy. We have enforcement and regulation based on experience, not numbers. The Justice Department does not need numbers to show that stepped up enforcement deters crime. Nor does ISO or anyone else need metrics to prove that compliance efforts work. It may be unsatisfying to those who think metrics are a universal answer, but it is not how public policy is done. It is also worth recounting

---

not be a bar to liability, but it can provide some evidence to prosecutors that an organization has taken reasonable steps to implement an effective program to prevent wrongdoing."); Stansbury, The Purposes and Benefits of ISO 37001 (Feb. 8, 2018) (if it is genuine and in good faith, then a program is "highly likely" to act as a defense or mitigating factor), available at https://www.ethic-intelligence.com/en/experts-corner/international-experts/43-the-purposes-and-benefits-of-iso-37001.html .

the old categorization of fibs: that there are lies, damned lies, and statistics. Unfortunately, it is not so difficult to "prove" one's opinions by the manipulation of statistics. To condition law enforcement or compliance solely on "metrics" may represent misplaced faith in numbers and statisticians.

On the other hand, it should be expected in all compliance work that there is assessment and evaluation. Does the training work or put people to sleep? Do people feel confident in the helpline or are they afraid to use it? Are the controls working or have people developed work-arounds? No program should get credit unless it is constantly being tested and measured. But to resist ISO because it has not done something no one else has done seems misplaced.[17]

3. Another criticism is that one cannot certify that a company is not engaging in bribery. This also is misdirected. Certification only purports to show that a company has an anti-bribery compliance program in place. One may debate how effective the ISO certification process actually is, and how good a program really needs to be to reach the ISO Standard. But no one is claiming that certification, or even the world's best compliance program, can always be counted on to prevent any violation from happening. Indeed, the Standard states, in a note to item 4.4, "It is not possible to completely eliminate the risk of bribery, and no anti-bribery management system will be capable of preventing and detecting all bribery."

[17] Anyone considering measurement of the impact of a standard like ISO 37001 would have to note how many uncontrollable variables there would be in any such measurement. For example, ISO 37001 calls for training. Does training "work?" Just asking the question shows the unreasonableness of the challenge, because there are so many variables just involved in this one compliance element, training.

III. Certification – the challenge

a. The first substantive questions revolve around certification. This is the real driver for ISO 37001 – the ability to get a seal of approval for one's anti-bribery compliance program.
b. A key, starting question is how does one qualify to do certification? What experience and what level of expertise are required? Does one need to be an expert on anti-corruption activities, or is the real expertise focused on dealing with ISO standards? According to at least one expert interviewed for this paper, an entity needs to be accredited to conduct a true ISO certification.[18] This process can be long and expensive, at least in countries like France, the UK and the US. There is also surveillance of the entity's certification reviews, and after-the-fact inspections of review files to ensure the work was conducted rigorously. If this is the case across the board, and the actual work is monitored or reviewed after the fact, this would certainly be encouraging. But while ISO exists to promote consistency, the actual organization of ISO may permit individual countries to stray from a diligent approach. There was certainly controversy when the reportedly first company to receive ISO 37001 certification had its present and former CEOs under indictment for corruption; what standard was applied, and which entity honored this company with certification?[19] Fundamentally, the value of certification is a function of the skill and integrity of the specific auditors, and in a decentralized system like ISO, this raises serious concerns.
c. Can companies claim certification that do not deserve it? Some may claim they have been "certified" even though the reviewer did not have credentials in accordance with the ISO

[18] However, one commentator notes that entities that conduct audits (CBs or registrars) "are sometimes (*but not always*) accredited by bodies that sit one level above" known as regional accreditation agencies. Crescenzi, ISO 37001 Certification: Understanding and navigating the process, Compliance & Ethics Professional 36, 39 (Aug. 2018)(emphasis added).
[19] Fox, "Defects in the ISO 37001 Certification," Feb. 7, 2018, available at http://fcpacompliancereport.com/2018/02/defects-iso-37001-certification/

process. What stops such a company from claiming it is ISO 37001 certified? On the other hand, there may also be certifiers who do have an official ISO blessing – but does even this assure the right level of care in the review, given that each nation's ISO organization can issue credentials? Thus, while certification might be difficult from a reviewer officially designated by the ISO member in one country, there are other countries around the world that could give reviewers the necessary credentials, even if not truly merited. These reviewers could then be hired by a company to obtain official ISO certification, even if the reviewer does not follow the same diligent approach used by reviewers in the US or the UK.

d. After determining who are the certifiers, the question becomes whether there are any controls on certifiers? Is there any form of quality control? Is there any review of their work? Again, this may be a function of jurisdiction and diligence in each country that issues accreditations for reviewers.
e. One of the concerns is that if there are entities that specialize in ISO certifications, will companies hire what one company's compliance officer described as "certification factories" that mechanistically tick off boxes and cash clients' checks? Will the certifiers actually know anything about bribery, or only about the ISO process? There is an ISO standard that would apply, ISO/IEC/TS 17021-9, "Competence requirements for auditing and certification of anti-bribery management systems," that would require such reviewers specifically to have expertise in anti-bribery compliance. Here the concept is right, but the implementation would be the potential issue.
f. Reading ISO 37001 raises another difficult question: Is the ISO standard really certifiable? There are certainly threshold questions about how an auditor would determine whether to provide certification.
    i. Much of the language is fairly general. How does one certify whether something is "appropriate" or "adequate"? Are such terms objective enough to be

measured?[20]Were they intended to promote diligence, or were they intentionally soft to allow more companies to get a passing grade, and to expand the market for businesses doing certification work? It is asserted that the ISO standard had to be general to apply to all forms and sizes of organizations. However, this is certainly arguable. Governments and organizations around the world have been issuing compliance program standards and guidance for decades, with these applicable to all types and sizes of organizations. Yet they are nevertheless able to provide valuable detail. Indeed, in ISO 37001 itself, the Annex (which does not actually control the reading of the Standard) provides much more detailed guidance that applies easily to the entire range of organizations. This argument that vague generalities are necessary is simply not convincing. Likely, it has more to do with trying to get representatives from many countries and different levels of background in this area, to sign off on the language.

ii. Is or should certification be an all or nothing process? Or should there be grades or degrees of certification? In other words, should it be pass/fail or more nuanced? Would it have been better if the review process just resulted in a substantive report, describing what was found, pointing out strengths and weaknesses and suggesting improvements?[21] Was a "pass/fail" approach the wrong way to do this?

---

[20] Jaeger, The pros and cons of ISO 37001 certification, Compliance Week 50, 51 (Dec. 2016)(reporting comments of Alexandra Wrage of TRACE, concluding that "reasonable and proportionate" are not auditable standards and are "incredibly judgment-laden.")

[21] An analogy could be drawn to Service Organization Control (SOC) reports. In SOC audits Type 1 or Type 2 reports are issued on the internal controls. This is not a pass/fail approach. Rather, an opinion is issued supplemented by extensive documentation of controls and the results of testing of the controls. This way one can see the strengths and weaknesses in the systems.

Given the rigidity of ISO, an alternative approach may not even have been a possibility, but would it have been more useful and effective? Perhaps a pass/fail approach is inappropriate when it comes to systems designed to prevent and detect crime. As a side note, for a company serious about avoiding misconduct by companies with whom it does business, if the company requires ISO certification for those in its supply chain it should also ask to see the certification auditors' full report or notes, in order to get a real picture of the entity's compliance efforts and to check the validity of the certification.

iii. Is certification done in whole or in part? This is not as simple as it might seem, because different business units might be certified first, with others to follow as the company learns the process. At what point might an entire company claim it is ISO certified, if it has many units engaged in different businesses? If one contracts with unit X which is certified, but work is done by unit Y which is not certified, would one necessarily know this?

g. How deep is the review that is conducted for certification? Unless there is real depth, the process may be heavily criticized as "box ticking." Is there any transaction testing? Are field reviews required? Are there interviews with employees? How much freedom does the reviewer have to access facilities, access documents of all sorts, and talk with people at all levels of the business? This author has evaluated company compliance programs, and it is a quite difficult challenge, unless one is just doing a paper review. Even at this early stage in the roll-out of ISO 37001, where early adapters can be expected to be among the most diligent and committed, there may already be shopping on price and intrusiveness. In one case a certification company that made it clear that on-site reviews were mandatory was told by a potential customer that a competitor had said certification could be done with just a file review. If in fact only a file review were conducted, the certification would be close to worthless. Is there too much discretion among those doing

the reviews, such that the value and meaning of "certification" may become uncertain?

h. There is a basic question about what certification of a compliance management system will actually tell us. Will it just confirm that a company did certain things, but without telling whether they did a good job doing them? Will it provide any insight as to whether all or any of the steps in the program were effective?

   We can gain insight into this by considering specific elements of a program, such as training. Will there be tests to determine how much of the relevant audience was actually trained? Will there be review of whether all the training was accurate? Or a review of a sample of the training materials? For multinationals or those in multilingual jurisdictions, will all the translations of training be reviewed? Will sampling be statistically valid, or arbitrarily determined by the auditor, or subject to negotiation between the company and the auditor based on cost? Will there be any measure of whether the training worked? Will any employees be tested for retention? Will there be a way to measure whether the training was convincing to employees, or merely viewed as window dressing?

   Another program element example is the investigation process. What will certification tell us? Will it only confirm that the company had a process? Or that they actually conducted investigations? Or that the investigations were well done and effective? How many investigations will be reviewed? Will a statistically valid sample of cases be examined? If so, will the review simply stop with the file, or will there be any testing to determine if the file is accurate? Will there be checks to determine if discipline indicated by the file was actually carried out? Will there be a review of helpline logs to determine whether the selection of cases to investigate was legitimate?

   Training and investigations are just two of the elements in a program. When considering how many elements there are in

an anti-bribery program, and what would be involved in using statistically valid means to determine if each one was carried out, and then determining whether each one actually was effective in addressing the risk of bribery, the size of the task becomes much clearer.

It may be relatively straightforward to determine that certain steps were taken in a program, although even this requires fieldwork and sampling. But to determine whether and to what extent any of these steps actually worked can be an enormously intense and difficult process that can require a substantial amount of time and resources, and needs to be conducted by those with deep expertise. Bribery involves criminal conduct by people who can go to great lengths to avoid being caught. Measuring steps to prevent this crime is unlike measuring quality in activities like manufacturing. Simple process steps will not work to prevent and root out this type of illegal conduct. Given that the scope of the certification review appears to be largely up to the discretion of the reviewer, but that companies may well shop for the least expensive auditor, this is a troubling concern about the certification process.

i. How much can certifiers charge to review a company's program? Is this open-ended, or is there some inherent limitation in this process? Can companies shoot for the lowest bid?[22] Will small and micro businesses be disadvantaged or excluded from potential business by an inability to pay the cost of a certification review?
j. Conflicts of interest
    - **i.** I was told that companies are now looking for strong candidates to do their reviews and certifications. Of course, the first adaptors are typically the companies that want to show leadership
    - **ii.** What will happen down the road, though, when this is seen as a requirement, a cost of doing business, and like all costs something to be minimized?

[22] There is also the risk that the cost of certification will come out of the budget for the compliance program, possibly reducing the amount of resources available for the program.

iii. Can an entity that helps a company prepare for a certification review also be the one who conducts the certification? Would that not clearly be a conflict of interest: first get paid to prepare the student for the test, then conduct and grade the test? Is there anything in ISO that bans this? Will anyone connected with ISO police such conduct?[23]

iv. Will there be a race to the bottom with companies seeking the lowest cost provider, who can do this without any disruption, taking less time, and with the "right" results? Will there be reviewers that produce ISO certifications without truly deep reviews? Will there be certifiers whose real expertise is the ISO process, not compliance or anti-bribery work? ISO/IEC/TS 17021-9 requires that those conducting certification reviews have expertise relating to such things as bribery, risk assessment and anti-bribery controls. However, will this be policed and checked?

v. The entity conducting a certification review appears to have enormous power in this process. Because of the general language in the Standard, and the fact that there is no authority to provide binding interpretations, the ability to achieve certification will rest on the judgment and interpretations of the auditors. Should the company being reviewed have untrammeled freedom to make that selection?[24]

---

[23] An analogous case involving Equifax and its ISO 27001 certification reflects this tension. It was revealed that the company certifying its program, before Equifax's enormous information security breach, was an affiliate of the same company that conducted its audit. McKenna, Unit of Equifax's auditor EY certified the information security that was later breached (Dec. 20, 2018), available at

https://www.marketwatch.com/story/unit-of-equifaxs-auditor-ey-certified-the-information-security-that-was-later-breached-2018-12-20

[24] It is true that there are other areas where companies select their own reviewers, such as selecting an accounting firm. However, there are significant differences. As noted, an entity's compliance with the ISO standard could be reviewed and "certified" by anyone. Alternatively, a certifier could have credentials but have those granted by a national ISO authority that is less diligent than others. There is no

vi. One solution for this would be a system where someone else selects the reviewer, or the selection is random. This is no small matter, particularly if there is not a credible quality control mechanism.

vii. For companies that believe ISO certification now answers their diligence problem in dealing with third parties, at this stage it appears they are mistaken to rely on this. They must also engage in diligence to determine the real legitimacy of the certification review; they cannot simply rely on a supplier's assertion that it is ISO 37001 certified. They need to know who conducted the review, what their credentials were, and how diligent they were in their work.

k. What is the impact of certification?

i. In response to the concern about potential backsliding after being certified, those supporting the process have said that companies must keep renewing and refreshing their programs if they want to remain certified; there are supposed to be follow-up reviews.

ii. Those providing certification are certainly required to conduct "surveillance" reviews, but I have heard conflicting views on this. Do they check only or primarily to see if the applicant has fixed prior weaknesses, but not to see if the company kept up any of its prior steps? So if a company's training passes the first time, can it then simply dial training back, without being checked? Or will the follow-up review, which looks at any prior non-conformities, also follow-up to be sure the company does not cut back

---

governmental or quasigovernmental regulatory authority with any role in the certification process. There are no professional standards by which individuals conducting reviews could be held accountable. There is also not the structure seen in global accounting, where there are recognized, international giants – such as the big 4 – who are subject to other external standards. There is a risk that any third party that can claim it is certified to the ISO 37001 standard (because it found a cheap, pliable certifier) will get a pass from potential contracting parties, no matter what the actual state of its compliance program may be.

on what it had during the first review? If the follow up check is not diligent there may be a strong temptation, after getting a passing grade, to cut back on the cost and effort originally required to pass.

iii. Unlike the USSG and OECD standards, there is no requirement to meet or exceed "industry practices," which would otherwise create an imperative to network and keep up with developments in the compliance and ethics field. The absence of this element exacerbates the risk of stagnation or retrogression. (More on this later).

iv. There is a general risk of ossification in programs. That is, if a, b & c get you certified, why bother with d, e & f? Certification runs a risk of "ringing the bell" (in the words of the late Australian compliance expert, Brian Sharpe, who lamented that managers wanted someone to ring a bell signaling they had done enough diligence in their compliance efforts and could then stop)[25] so they know their work is "done". This is no small matter: the push in this direction could well be enormous.

v. There is also a risk of freezing development and innovation generally, especially without the requirement to consider evolving industry and best practice. Why do anything new or innovative if what you already did meets the ISO Standard?[26] The Standard tries to address this point by requiring "continual improvement" in the one-sentence item 10.2,[27] but this may face an uphill fight against human nature.

---

[25] Brian Sharpe, Management Beats Mystique: Comprehensible Due Diligence 8 (1997)(on file with author).

[26] See Stephanie Clifford, So many standards to follow, so little payoff https://www.inc.com/magazine/20050501/management.html , quoting a manager who had experience in ISO registrations at a company, that "it can help drive a company to a plateau of performance, but it will keep it at that level and, in fact, stifle improvement."

[27] Notably this includes reference to improving the program's "effectiveness," but this is undercut by the weak, circular definition of "effectiveness," see item 3.9.

l. Where are governments and others on ISO 37001?

i. ISO and its supporters have not claimed that certification or meeting this standard will mean a pass from any government enforcers or regulators. Nevertheless this has to figure in any company's approach

ii. There have been references to different countries "adopting" ISO 37001;[28] this has particularly been said of Singapore,[29] the Philippines and Peru. What does this mean?

iii. Is it ever correct to say, e.g., that "Singapore" or "The Philippines" or "Peru" has signed on to this standard? There are numerous parts of any government, so there should be care in such statements. Even within the same government there may well be different views about an ISO standard and any certification.

iv. It is helpful to recognize that governments may in various ways "endorse" a standard like this. For example, a government may require contractors to be certified. This is not the same as having enforcement officials take it into account in their enforcement decisions.

v. Will governments give it deference? We do not know this yet. Given how many governments, enforcement agencies and judicial systems there are dealing with corruption, there may in fact be no single answer to this.

---

[28] See, e.g., Garodiya, Transforming anti-bribery frameworks with ISO 3700 standard (Aug. 14, 2018) reporting that "Singapore, Peru, Canada, Middle East, France, Malaysia and many other countries have embraced ISO 37001", available at https://forensicdiariesblog.ey.com/2018/08/14/transforming-anti-bribery-frameworks-with-iso-37001-standard/ ; Kazem, ISO 37001: Checking the box on "doing compliance," Compliance & Ethics Professional 71 (Dec. 2017)("To date, Peru, Singapore, and the Philippines have adopted ISO 37001 as their respective government's standard . . .")

[29] BakerMcKenzie, Singapore Adopts ISO Standard on Anti-Bribery Management Systems (May 11, 2017), noting that Singapore adopted SS 37001 on anti-bribery management systems but that certification would not guarantee a finding that all reasonable steps had been taken by an entity to ensure compliance, available at https://globalcompliancenews.com/singapore-iso-37001-cms-20170512/ .

vi. It is also easy to see a day when at least bigger companies will recommend or require that those in their supply chains be certified. It may be easy for the big companies simply to push this off on suppliers, although they should also be offering to help those suppliers. (A really serious company would also insist that it, not the supplier, pick the entity doing the certification. It could also ask to see the auditors' notes from the certification review). But there may also be a risk that this will become a substitute for doing difficult third party due diligence, or assisting suppliers in implementing strong programs. If ISO certification is not carefully controlled, downstream companies may find it cost effective to find a pliable certifier, get certified, and then go back to paying bribes or whatever else they were doing without any further checking by the other contracting party who first insisted on certification.

vii. We should also consider the inevitable: some company that was certified is going to get into trouble.[30] How will that play out? Will it undermine ISO 37001's credibility? Or much worse, will it undermine the credibility of compliance and ethics programs generally, and reinforce the argument that it is really impossible ever to assess and evaluate compliance programs?

m. Government assessments vs. prior certifications. Is it possible to assess programs?

i. One question about certification is whether or how that differs from the generally accepted point that government enforcers and regulators should consider companies' compliance programs in enforcement

[30] A sense of how this could develop can be seen in the coverage of Equifax and its enormous data breach, notwithstanding its ISO 27001 certification. McKenna, Unit of Equifax's auditor EY certified the information security that was later breached (Dec. 20, 2018), available at

https://www.marketwatch.com/story/unit-of-equifaxs-auditor-ey-certified-the-information-security-that-was-later-breached-2018-12-20

actions. Is there a difference between after-the-fact assessments in the context of a case, and before-the-fact certifications of a program?

ii. The argument that government can and should assess programs in actual cases has much to support it. In an actual case there is context and an in-depth investigation. Evaluators are boring deeply into one situation. It is not staged, and it is after the fact.

iii. In actual enforcement cases, the burden is clearly on the company to prove its program was effective despite the fact of a violation. And the assessment is of a specific, historic fact, by a skeptical prosecutor or regulator. It is not a prediction into the future; but the ISO 37001certification will be read as such a prediction, especially because it purports to be good for three years.

iv. The government has no profit motive in giving a favorable grade. Instead, there is already deep skepticism because of an admitted offense. In prior certification as occurs in the ISO review, the incentives may all run the other way. The certifier gains nothing by giving a company a hard time or refusing the certification. Rather, certifiers may see a business incentive to grant certification.

v. Even in the context of an investigation, the government's conclusion is not necessarily ultimate, i.e., pass/fail. It is often graduated, e.g., a break on the fine, not having a monitor, having a non-prosecution agreement, etc. In contrast, certification for ISO 37001 is pass or fail.

vi. The incentives for companies are very different in the two processes. In certification, getting a passing grade is what matters. Arguably it makes no sense to do even one step more than the certifiers require. And after certification has been achieved, a company could conclude that there is no value in doing anything new.

vii. On the other hand, when designing a program that will pass muster in the event of a violation, the government – the evaluator – is already viewing the

company from a negative perspective. In anticipating this, the company is seeking to have a program that makes a very strong impression. The applicable standards, such as the USSGs and the OECD Good Practice Guidance, require the consideration of industry practices, so a company must keep up with whatever industry leaders are doing. The element of uncertainty never leaves, so the compliance effort must remain constantly dynamic. This makes sense, since law breaking including bribery is inherently dynamic. Moreover, the purse strings for the government's assessment are not controlled by the company, and the company does not tell the government who they may or may not talk with. There is no competitor who can offer the same result for less money or less work. As the government enforcers conduct their investigation they can ask people connected with the company about the alleged compliance program.

viii. The conclusion is that government assessments are more reliable and justifiable. Prior certifications, with the tendency of deterioration immediately after achieving the certification, carry much more risk.

IV. Charging and costs for access to the Standard

a. ISO charges for use of the Standard, and appears to be tough on copyright. The Copyright notice says:
    i. "All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below [Switzerland] or ISO's member body in the country of the requester."
b. My personal copy has on every page that it is "Licensed by ISO, to Joseph Murphy – Compliance & Ethics Professional and FCPA Blog – 2018-03-08". I am the editor of the SCCE

magazine Compliance & Ethics Professional; the FCPA Blog reference may be because I sometimes comment there.

c. Other anti-bribery compliance standards do not charge for access to or reproduction of the standard.[31]
d. This restriction may limit open debate and discussion, if commentators feel at risk for quoting passages. Will academics and students be as free to comment substantively? Will they even be willing to pay the price to buy the standard in order to develop commentary? In the various comments I have seen thus far on ISO 37001, there has tended to be less discussion of the actual contents of the standard. As I write this, for example, I cannot be sure that I will be safe in quoting what I quote here, or will be subject to restriction by ISO.
e. But ISO was very quick and open in providing my review copy, and in entering into email discussions about the standard. They showed no reluctance to engage.
f. One concern is what this cost does to small and medium-sized enterprises? Is there a way to make it available at a discount? Could trade groups enter into a special license with ISO to make the Standard available? Could compliance and ethics groups like the Society of Corporate Compliance & Ethics have a special license?
g. What if companies want to make copies widely available among their own business units and employees? I know of one company where there was only one copy for the entire company, and this was a global entity. Will companies try to make it broadly available within their own corporate walls through means that raise copyright questions, such as posting it on an internally accessible Intranet site? Or would this be permitted even though it limits ISO's revenue stream?
h. ISO 37001 has references to other ISO standards. Can one feel fully confident of understanding ISO 37001 and following it, if one has not also examined any other ISO standards referenced in 37001? And do the other ISO standards themselves reference more ISO standards? To be fully

[31] Of course, those who write books on the subject sell the books; but the actual standards such as the OECD Guidance and the USSGs, government guidance, and NGO guidance are all available for free.

confident of understanding the standard, can these lead to making more purchases of the standards from ISO?

i. In the fight against bribery we are all trying to make the work easier and encourage more participants in this fight. Charging for every copy of a standard is counter to this effort. If ISO needs revenue, why not get it on the certification side? Why not charge the certifiers, who stand to gain the most financially from this process?[32]

V. The drafting of ISO 37001 is troublesome

a. ISO 3700 is difficult to read and understand, and has very general language. Why could this not be a clear, specific, easily-understood standard?
b. One can debate the impact of the ISO Standard, and hope for good results. It might lead more companies to take compliance and ethics in this area seriously.
c. But on one point the conclusion is clear. The drafting is not what it could and should have been. In the important fight against bribery, this is a serious mistake. The document is too often verbose and convoluted. At other points it lacks the detail needed to be fully helpful for companies.
d. It is noticeable that among the other standards and sources available elsewhere, there tends to be a focus on readability and providing practical advice. The ISO Standard does not hold up as well to this comparison.
e. It is worth considering that two US Government agencies, the DOJ and SEC, were able to write their guidance on an anti-bribery compliance program in less than 10 pages, and provided some excellent detail, including examples. Their guidance can be used by any size and type of entity – business, government or non-governmental organization. And in great credit to the DOJ and SEC staff people who wrote it, the writing is amazingly clear and easy to follow. I could see how one could at least attempt to certify compliance with a usable, short guide like the FCPA guide. In any event, for

[32] Of course, the cost of obtaining certification could also be a barrier for smaller companies.

anyone who does decide to get ISO certified, I strongly recommend also applying the DOJ/SEC guide and benefiting from its examples.[33]

f. The ISO organization would be well advised to conduct a reading comprehension test on ISO 37001. If it is not readable for most business people, then it should be appropriately edited. While it must certainly be a difficult challenge to get agreement among representatives of over 160 countries, this is a challenge that needs to be met. If, in fact, this was not possible with that many countries participating, then maybe this was just a task that was not appropriate for ISO. Unlike the topics usually covered in ISO standards, this one is not just about management; it also addresses hard-core criminal conduct.

g. The drafting group should have focused more on the utility of the work, and also sought out and accepted the judgment of a competent editor. Was this troublesome drafting perhaps the result of having so many different languages that had to be accommodated, as has been suggested to me? This is not a convincing reason. It is fair to remember that large, multinational companies do this type of translation work every day in their codes of conduct and compliance guides – they also need to write in a variety of languages. But they know that no matter what the translation challenge, the end result must be readily understandable by all of their employees. If these companies can meet this standard, the ISO drafters could have done so also.

h. In some instances I have been told that this definition or that organizational element is just how ISO works or is used everywhere else in ISO standards. I do not purport to be an expert on how ISO works. My focus is how to prevent bribery. If a standard addresses the topic of bribery, then it should be designed to do that. An ISO standard should be designed best to fight bribery, not to meet some other agenda. "Everybody else is doing it" as the reason for doing

[33] I should note my personal bias, since I was one of the sources referenced in the FCPA guide. See US Department of Justice and US Securities and Exchange Commission, FCPA: A Resource Guide to the US Foreign Corrupt Practices Act (Nov. 14, 2012), http://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf .

something has never been an accepted mantra in the compliance and ethics field. If some extraneous element gets in the way of maximizing the effort against bribery, then that element should be removed, no matter how many other ISO standards embraced it.

i. Is this a quibble by someone who has done editing since his law review days at Penn? The readability and usefulness of ISO 37001 is a serious issue. Poor drafting can be a barrier to implementation. Normal business people will be challenged in being able to read and apply this in a meaningful way. What might not seem important to those familiar with bureaucratic language can be a real impediment to the battle against corruption.
j. There are a number of examples that show the nature of the problem. One provision states: "Corrective actions shall be appropriate to the effects of the nonconformities encountered." Item 10.1. Would anyone honestly describe this as "a style that is likely to be readily understood," per ISO's drafting standards? Does anyone actually talk like this?
k. There has been an unusual amount of early resistance to this ISO Standard by people who would usually champion anti-bribery efforts. I believe much of this is frustration generated by dealing with the language used in the standard.
l. The Standard and the Annex are 47 pages long.[34] There should have been quite a bit of useful detail here. But arguably it has less detail than much shorter guides such as the US Sentencing Guidelines and the OECD Good Practice Guidance.
m. One test of the writing level of the Standard's language is to compare it to what language would be acceptable for a company writing its own code of conduct. The drafters could ask themselves, if they were assessing a company's compliance program, what would they have thought of company codes and compliance guidance documents written

[34] Of course, there is apparent irony that while I complain about the length of the ISO Standard and Annex, this white paper is even longer. Readers will have to judge for themselves the value of this paper; it is not the first commentary that exceeds the length of the document being reviewed, as any American constitutional lawyer can attest.

in the same style as ISO 37001? Would they have considered the language as readable, and in a style employees were likely to read and follow? Or would an employee simply skim, not engage, and then sign?

n. Here are some specific points about the drafting. Everywhere ISO 37001 uses 3 words to make points. There are certainly times when a 3-adjective description would fit the need, but this draft has these in abundance. Moreover, the 3 words are typically general terms. One general word provides little or no guidance. Using 3 general words adds no more guidance than one general word. Often the best drafting solution would have been to eliminate all of the adjectives, or use just one. Of the great number of examples, 9.3.1 is illustrative: top management is to review the program for its "continuing suitability, adequacy and effectiveness." Would it actually make a difference if they reviewed it for "effectiveness" but not "suitability"? Also, if it is necessary to list those 3, are there not many more adjectives one could justify? An efficient drafter could have had just one note in the beginning, saying everything done under ISO 37001 needed to be "suitable, adequate, proportionate and effective" and reduced the repetition.
o. Another concern with the drafting is that once you start doing lists of words you may need to be sure you include all possibilities. Otherwise, inclusion of what purports to be comprehensive arguably excludes what is not included in the list. So in places where they list 3 words they could just as easily and correctly have listed 5, 6, or even more.
    i. The very beginning, Item 1, foreshadows the drafting style. It begins with a reference to "establishing, implementing, maintaining, reviewing, and improving an anti-bribery management system." Why was it necessary to list both establishing and implementing? If so many words were needed, then should they not also have included "planning"? Before you do something, should you not plan it also? (There is an entire section, 6, on planning, so it is recognized as important) They could also have listed "evaluating." How can you improve if you do not evaluate? The

message would probably have been clearer if it had just said "for an anti-bribery management system" without the long list of words.

ii. Item 4.4 instructs us to "establish, implement, maintain and continually review and, where necessary, improve" the compliance management system "including the processes needed and their interactions" in accordance with the Standard. The same point about inserting unnecessary word strings applies here. But given that all of these things are already spelled out in the Standard, if this 4.4 was even necessary, the one word "establish" would have done the job.

p. There is also a tendency to repeat modifying phrases throughout. It would appear that the alternative, of defining a term or setting out a point once, would have been more efficient and easier to read. For example, there are many references to the role of a board "if any." This point is made once and need not be repeated.

q. The definition of "organization" is another example, with the word defined as "person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives." In light of the ISO drafting instruction that "Those drafting ISO . . . documents should try to be aware of the particular needs of their intended users and to write in a style that is likely to be readily understood," the drafters should have tested each piece by how well business people would first be willing to read, and then accept and understand the language. Certainly for me, as a businessperson, for as many times as I have read their definition of "organization," I never remember it and am not sure I would recognize what the definition describes.

r. It makes sense that compliance activities should be proportional to the risk. The Standard needs only to say this once, rather than being repeated throughout. It is very logical that one would focus attention where there is an actual risk of bribery, and the greater the risk the more one should focus there. The drafters could have cut the word count

significantly by not repeating the phrase "more than a low risk of bribery" throughout.

s. The Standard offers to define things that need no definition. For example, it defines "requirement" as something that is "stated" and "obligatory." Logically one would then look for a definition of "obligatory," but there is none. Readers already know what that means, but they also know what "requirement" means. Also, saying that it needs to be "stated" seems to be obvious and unnecessary.
t. The drafters should also have avoided defining a word by using a variant of that same word in the definition. So the definition of "audit" 3.20 should not include "audit" in the definition (which it does, twice in one sentence). In addition, if one wants to understand this definition fully, the note refers to ISO 19011.
u. Another definition that could have been eliminated is 3.11, the definition of "objective" as "result to be achieved." If a definition does not add value, why not omit it? The more the Standard avoids wasted language, and focuses only on important points, the more valuable it is in the fight against bribery.
v. Another troublesome definition is "risk" which is "effect of uncertainty on objectives." This definition conveys no sense of the evil that is bribery. The "risk" in this field is the possibility of bribery occurring and how bad that conduct may be (i.e., impact). Moreover, the explanation is unnecessarily long, taking over 100 words to explain what one sentence can fully cover.
w. An even clearer example of a troublesome definition is the one for "measurement:" "process to determine a value." The drafters needed to ask if a reader has learned anything or obtained any guidance from a definition. Given the importance of evaluation and even measurement in dealing with compliance programs, this appears to be an opportunity that was underutilized, if not lost.
x. The definitions take 3 ½ pages of text. Editing could certainly have reduced this significantly.

y. The generality of the definitions is one of the elements that raises doubt on how certification would work under the standard.
z. Item 7.5 on "documented information" is likely one of the provisions that may frustrate readers. By the time the reader reaches 7.5 there have already been numerous references to documenting the program. But at this point there is almost an entire page to say what could have been said very succinctly, e.g.: "The program should be documented so that it is possible to know what happened in the program and when. This should be controlled to ensure the records are accurate."
aa. An example of a provision they could have omitted is item 8.1, on "operational planning and control." A short description of this section is that it tells you to do what the rest of the ISO Standard tells you to do.
bb. In comparison, for clarity and detail the Annex is superior to the Standard. In places the language is relatively crisp, and there are a number of useful pieces there. For example, A.10.3 a), covering factors to evaluate in due diligence on possible business associates, stands out as short and practical. Of course, there are areas where the Annex could also have benefited from editing, but as written is has more useful and readable guidance than does the Standard.
cc. The drafting issues undercut ISO 37001. Fortunately, this could easily be fixed by having a good editor tighten the language and eliminate much that is unnecessary. A shorter, clearer document would have been much more useful.

VI. Substantive points

a. When one gets past the drafting issues, there are substantive points that are worth attention. Among these, there are strengths and weaknesses, including some notable flaws.
b. **Management.** An enormous strength of the Standard is that it makes clear that compliance programs are about management.
Ironically although this point would seem obvious to people who manage companies, it is often missing in the work of

some academics, journalists and commentators. To this group, a compliance program is often just a policy (maybe a code) and training. In the recently highlighted area of harassment compliance, people working in that field labor under the illusion that having a policy, inflicting ineffective training on the workers, and telling people to call HR to report concerns is a compliance program and can accomplish something meaningful. ISO deserves great credit for making clear that compliance is about how you manage things in an organization, and calls for the full range of management tools. No company could get ISO certified if all it had was a policy, some training, and a phone number for calls; that is not how compliance or anything else that matters, is managed. If ISO 37001 wakes more people to the reality that compliance and ethics is about the focus of effective management steps to prevent and detect misconduct, then it will have made a meaningful contribution.

c. **CECO.** One structural element that is key to success for a compliance and ethics program is the chief ethics and compliance officer (CECO).[35]
    - **i.** Having the CECO underpowered or in a position without independence or line of sight sets the stage for failure.
    - **ii.** The ISO Standard and Annex are very good in calling for "competence, status, authority and independence." 5.3.2 The inclusion of "independence," for example, is a key insight, essential for effective operation of a compliance program.[36]

---

[35] See Leading Corporate Integrity: Defining the Role of the Chief Ethics and Compliance Officer (August 2007) http://www.corporatecompliance.org/Content/NavigationMenu/Resources/Surveys/CECO_Definition_8-13-072.pdf; Perspectives of Chief Ethics and Compliance Officers on the Detection and Prevention of Corporate Misdeeds (RAND 2009) http://www.rand.org/pubs/conf_proceedings/CF258/

[36] Oddly enough, the Annex, at A.6.2(d), incorrectly defines "independence" as being "not personally involved in the activities" exposed to risk, whereas this is actually impartiality or being disinterested. Instead, independence means not being under the control of those whose compliance you are dealing with. This ties in with the point that one cannot realistically be expected to "police up," i.e., enforce the rules against a person who is also your boss.

iii. But this is not consistently strong in important ways. First, the good language is undercut by adding the malleable word "appropriate." This could invite a corporate lawyer to make an argument that it is "appropriate" to have the mid-level lawyer who specializes in anti-corruption law become the manager responsible for managing the anti-bribery program. This could also allow a company to park this compliance manager where she can cause no harm and interfere with nothing that is important. Could a certification auditor successfully argue that the FCPA lawyer is not "appropriate?" Of course this lawyer is very likely to be ineffective by any measure. But does the Standard prevent this?

iv. But the single, enormous failure is that nowhere in the Standard or Annex is there a requirement or statement that the person responsible for the program must or should be an officer, or senior manager, or top manager.[37] Given how clear the Standard is in the various places where it is directed toward "top managers" it is a dangerous omission that should never have happened.[38] Drafting this correctly would have been so simple that the absence of this crucial point may make it impossible for someone to argue that it is a requirement for certification.

v. One apparent misconception among the drafters was that requiring a compliance officer or top manager to run the program meant having one person do this <u>full time</u>. This is incorrect and is totally separate from the

---

[37] ISO 19600 on Compliance Management Systems at least acknowledges that "Many organizations have a dedicated person (e.g. a compliance officer) . . ." (5.3.2). Yet "compliance officer" appears nowhere in the ISO 37001 Standard or Annex, although it could easily have been included.

[38] Spokespersons for ISO have asserted it requires "Appointing a compliance officer," see Gasiorowsky-Denis, How Microsoft is bursting the bribery bubble (Nov. 8, 2017) https://www.iso.org/news/ref2238.html , but that requirement simply does not appear anywhere in the Standard or the Annex, and there is nothing that requires anyone conducting an audit on ISO 37001 to follow the opinions of anyone associated with ISO.

question of the position of the compliance officer. In any small organization the top manager running the program will have other responsibilities; this is how things are done in smaller organizations. The key point is that whoever has this responsibility needs to be a top manager, but this was omitted from the Standard.

vi. This is an area where the much shorter but more specific OECD Good Practice Guidance nails the point. The person running the program must be a "senior corporate officer" or officers. "Senior" certainly means not a mid-level staff person; a senior officer is likely not even an officer who reports to another officer (e.g., not reporting to the general counsel). A senior officer should be someone reporting to the CEO and/or the board. The ISO Standard refers to "top managers" when it addresses the important people who run the company. Clearly the CECO should have been required to be a top manager. Yet ISO 37001 seems almost pointed in avoiding any reference, either in the Standard or the Annex, to the person(s) running the compliance programs being officers or top managers. This weakness could doom the ISO 37001 compliance effort; absence of power and positioning in the compliance function is the surest route to failure.

vii. This may be an area where the usual ISO focus on managing business processes may fall short. As noted, dealing with bribery means using tools designed to fight crime. Because an unfortunate amount of misconduct in this area occurs at the top management level, success requires a focus on that level. In addition, the prevention of corporate misconduct deals with the use and abuse of power in organizations; top managers direct others to follow their orders, and often become accustomed to having things their way. A boss who says "just make that sale in that new market and don't give me any excuses" expects that direction to be followed with no

nonsense. If someone is to stand up to powerful bosses that person has to have the position and power to do so. It takes power to deal with power. Any position less than a top manager starts from an enormous disadvantage.

viii. Here the nature of the certification process becomes critical. In dealing with other standards like the USSGs that are not as specific on this point, the key judgments will be made by skeptical enforcers in the context of a violation. A mid-level lawyer is not going to satisfy an enforcer's expectation of a true chief ethics and compliance officer (particularly in cases where the violation involves top level people, which is often the case). But for a certification company, especially if there is one that has most of its experience certifying quality programs (under ISO 9001) but lacks deep background in compliance or bribery prevention, and being aware of the ISO Standard's specific absence of any reference to an officer or top manager in this position, having a knowledgeable lawyer may well hit the target for certification purposes. While there may be those who worked on drafting the Standard or who are involved in other ways with ISO who would strongly disagree, unfortunately they do not make these decisions. The determination of what gets certified will be made regularly by auditors in different countries, subject to different levels of quality control, and under pressure from clients to complete the review process without excess cost or interference.

ix. The CECO is also potentially undercut by the language about the role of the board in 5.1.1. The general language there misses the board's key role in empowering the CECO. For example, it could easily have required that the CECO report to the board in person and have access to the board as needed (instead of the ambiguous reference to "planned intervals" for receiving information about the program from an unspecified source).

x. 5.3.2 deals with the anti-bribery compliance function, and does state that the "anti-bribery compliance function" reports on the program's performance to the board. It also provides for "direct and prompt access" to the board if any issue or concern needs to be raised regarding bribery or the compliance program. But there should also be an obligation of the board. Without ongoing, direct, unambiguous access to the board, the CECO's role is weakened when it comes to addressing top management misconduct. Of course, the further removed the compliance person is from being a top manager, the less power and impact the person is likely to have. The board could also have been given control over the role and treatment of the CECO, but the language also fails to do this.

xi. A.18.7 in the Annex has investigation results reported to top management, with no reference to the board. This ignores such obvious risks as addressing allegations involving senior management. Clearly in such cases the board needs to be advised.

d. **No in-house compliance function at all.** Item 5.3.2 ends by allowing top management to have absolutely no part of the compliance program be inside the organization. Instead, it grants a license to "assign some or all of the anti-bribery compliance function to persons external to the organization." (emphasis added) All management then has to do is designate someone to be responsible for those outsiders. Of course there is no issue with contracting for certain types of functions, such as running a helpline or providing an outside review of the program. See also A.6.[39] But unwisely the Standard appears to authorize companies to ship the entire compliance function off to outsiders, requiring only that "specific personnel" be responsible for the outsiders. The

[39] ISO 19600 on Compliance Management Systems refers at one point to the ability to "outsource elements to compliance experts" (5.3.2) but nowhere even suggests putting the entire program outside. The precursor to ISO 37001, BS 10500:2011 contains no such reference to farming out the entire program, and in fact requires that if a company has subsidiaries, a qualified manager be designated in each entity to oversee compliance, item 4.4.3 Multiple organizations.

drafters of the Standard must have known how ineffective a compliance program would be if it existed completely outside of the corporate walls. Nor is size of a company an excuse for this. Even a 3-person company can have one of its people designated as the compliance officer, even if the person has to contract out for certain specific compliance services.

e. **The compliance function's reporting to the board.**

i. A major concern about the role of top managers is that far too often top managers are complicit in the wrongdoing.[40] They may have failed to act to prevent wrongdoing, or may have been privy to the misconduct. Top managers may even be the prime movers in crime. Thus there needs to be balance in allocating responsibility to top management, while giving the CECO the mandate to report to the highest governing authority.

ii. What if there is no board? For drafting purposes, this is an easy fix. One provision, early on, can say that if there is no governing authority, then you rely on top management.

iii. The compliance function is called upon to assess the program and then report to the board, in 9.4. As noted, however, the "compliance function" is not required to be at officer level, nor is it clear enough that the reports will avoid heavy censorship by the general counsel and other managers. A reader might assume the reports should be in person, but it could just as well be interpreted as allowing an edited written report. It should be clear that "direct" reporting is personal and uncensored; it would have been better to require, in the words of one expert, "physical presence in management and board meetings" and not merely sending an edited power

[40] See Arent Fox, FCPA Study Reveals C-Suite Increasingly at Risk (June 25, 2018) "More than 50 percent of all individuals charged with an FCPA violation were their corporation's CEO, president, vice-president, or director." *available at* https://www.arentfox.com/perspectives/press-releases/arent-fox-fcpa-study-reveals-c-suite-increasingly-risk

point presentation. The Annex, in A.6.3, addresses this risk. It carefully directs that there should be communication to the board by the compliance function "without having to go through top management . . ." It is striking how specific and pointed this language is. But this is where the troublesome limitation of the Annex as being entirely "illustrative" stands out. This provision, and any language that is directive, should have been in the Standard, and not diminished by being described as "illustrative."

f. **The Annex.** The Annex is more practical and useful, and at some points it is even directive, making it clear that certain elements are really required. Its guidance appears to be at least as universally applicable as the more general language in the Standard. But the problem with the Annex is that its first provision, A.1, eviscerates it; the Annex is "illustrative only" and is not "prescriptive." In the language of business, this means that companies, and especially those doing certification, can ignore it if they wish. Because of this linguistic kneecapping, none of the Annex is part of the requirements, so we do not know whether it will figure into the certification process.

   The failure of the drafters to effectively integrate the Annex into the certification process is a regrettable weakness based on an apparent failure of imagination.

   The drafters apparently worked on an all-or-nothing basis, and elected nothing. But some thought could have led them to more useful approaches. For example, they could have at least been precatory, and directed that any entity pursuing certification or conducting certification processes must also be familiar with the Annex. Even better, they could have applied a balancing approach, directing that positive weight be given to organizations following the Annex. Those who failed to draw from the Annex could have had imposed on them the burden of proving what they did was significantly better than what was in the Annex. The drafters could have

required that organizations have programs at least as good as what was provided in the Annex.

Some of the points in the Annex, particularly those using the word "should," belonged in the Standard. For example, A.6.3 says the anti-bribery compliance function "should not have to report solely to another manager in the chain who then reports to top management" and should have direct communications to the governing body "without having to go through top management." This important message would be clear if it had been in the Standard. If these are things companies "should" do, then they should have been in the Standard.

The first sentence of the Annex is an invitation for implementers, auditors, and certifiers to ignore the valuable detail it contains. As it is now, if a certification auditor points to something in the Annex that the company being reviewed should have done, the company can say, "oh, no, we don't have to do that, it is only illustrative."

g. **Industry practice.** The US Sentencing Guidelines and the OECD Good Practice Guidance call for the program to address industry practice. This helps keep the program dynamic. There is no set, unchanging way to fight misconduct; compliance programs need to keep evolving and improving through innovation.[41] Any program should be judged in comparison to what others are doing. This requirement also keeps the field dynamic, as new approaches develop. This could have been included by adding one sentence, such as found in the US Sentencing Guidelines or the OECD Guidance.

    1. The USSGs state: *(B) Applicable Governmental Regulation and Industry Practice.—An organization's failure to incorporate and follow applicable industry practice or the standards*

[41] In the words of one commentator, "To be effective, compliance programs must evolve constantly – not only to company risk, but also to best practices and changes in the compliance landscape." Almy, Anti-corruption compliance: Five ways good certification can help, Compliance & Ethics Professional 19, 21-22 (Feb. 2015).

called for by any applicable governmental regulation weighs against a finding of an effective compliance and ethics program.

2. (It should be noted that there is a flaw in the USSGs drafting, in that "follow" really means to do no less than industry practice.)
3. OECD calls for "12. periodic reviews of the ethics and compliance programmes or measures, designed to evaluate and improve their effectiveness in preventing and detecting foreign bribery, taking into account relevant developments in the field, and evolving international and industry standards."
4. While this is a good point to cover in any standard on compliance programs, it is especially important in any approach that includes certification. There is a real risk that certification will stunt development and lead to a dry, checklist approach. Adding this reference as a required element forces an external view, taking into account developments and progress. So, for example, a program that might have been adequate before the development of smart phones would no longer be acceptable without appropriate use of this technology because of the way smartphones can enhance the compliance message. The dynamic aspect of "industry practice" would decrease the risk that certification will discourage innovation and freeze development; organizations, even when certified, would still be required to keep up with new practices.
5. The only reference even close to this point is in the Annex, A.22, which offers the mere suggestion that companies "may find it useful" to look at other initiatives for "good anti-bribery practice." Thus, not only is it not a requirement, it is not even recommended.

h. **Defining effectiveness.** A particularly surprising flaw in the Standard is the definition of "effectiveness" in 3.9. "Effectiveness" is the goal of compliance programs, and the standard by which they are to be measured. Usually it is considered a challenging standard to apply and to measure. It is much more difficult to measure than either design or implementation of a program. But here the Standard raises serious questions. Under item 3.9, "Effectiveness" is the:

    1. "extent to which planned activities are realized and planned results achieved".
    2. Note that this language would literally allow management to set any level it wants to determine effectiveness.[42]
    3. So if you "planned" to train x number of people and your planned result was that people were "trained," then by this definition you have been "effective," even if there was no benefit to society or anyone else from your training. Allowing companies to define "effectiveness" simply by how they define their "planned results" is an unnecessary invitation for gaming the system. It also invites measurement of implementation, rather than the far more important impact or effectiveness of the compliance program efforts. Certainly it is difficult to see any government enforcement agency accepting such a limited definition.
    4. Compliance and ethics programs exist to prevent and detect violations. That is a tough standard to apply, but just because something is difficult is not a reason to omit doing it. What matters is not whether companies hit their planned targets; we want to know that the company is doing things designed to prevent and detect wrongdoing.

[42] While ISO 19600 on Compliance Management Systems also uses the word "effectiveness," the drafters obviously did not think any such circular definition of effectiveness was needed. Nor was it included in BS 10500: 2011.

5. Of course, it can be argued that a company can only get certification by doing all the things listed in the Standard, and thus the "effectiveness" definition might not matter. But good standards do not create internal inconsistencies. This definition should either be eliminated entirely, or substantially revised to be meaningful. As written it is a serious mistake.

i. **Other points.** There are a number of points that raise concerns, including missing elements that are carefully addressed in the US Sentencing Guidelines and/or the OECD Good Practice Guidance that provide important detail that is missing from ISO 37001. There are also some strengths that deserve positive attention.

   i. Discipline for failure to prevent violations. The USSGs §8B2.1(b)(6)(B) calls for discipline for managers who fail to take reasonable steps to prevent and detect criminal conduct. This is a standard that can easily apply in any sized company, but is missing from ISO 37001. This provision is important to deter scapegoating, and to remind managers that they, not the compliance staff, are ultimately responsible for compliance.

   ii. Absence of ethics. One weakness is the absence of "ethics" from the Standard, and a failure to provide a sense that this is an evil being addressed: bribery

   1. The Introduction notes that bribery raises serious "moral" concerns and erodes justice. This brief piece does a nice job of reminding us why it is so essential to fight bribery.
   2. The Introduction also talks about organizations having a "leadership commitment to establishing a culture of integrity, . . . and compliance." It observes that an organization's culture is critical for success. There is force and power in this Introduction.
   3. The energy of this strong start is dissipated, however, when reading the rest of ISO 37001.

The rest of the Standard tends to treat the topic as if we were engaged in a purely mechanistic process. Item 5.1.2 does call for top management to "promote an appropriate anti-bribery culture" although the modification "appropriate" does not belong there. The Annex, A.6.4 reminds us that everyone is responsible for acting in an "ethical" manner, although as noted the Annex is only "illustrative."

4. It is not merely that value words like "ethics" are missing from the text. It is also that the words in the ISO Standard lack any sense of urgency or values. They could just as easily have been used to describe how to manage the production of lawn mowers - no force, no imperative, and no emotion.
5. One of the worst examples is Item 10.1, which talks about dealing with a "nonconformity." Bribing public officials is not a "nonconformity." Violating the safeguards against bribery is not a "nonconformity." If one is producing widgets then referring to "nonconformities" might be appropriate; not when it comes to bribery.
6. Other compliance standards include ethics and more focus on culture. For example, the DOJ/SEC FCPA guide includes ethics and culture in the text of the discussion. The USSGs were amended as early as 2004 to add a reference to ethics; the OECD Good Practice Guidance had it from the beginning. The trend in the field of compliance and ethics has been to recognize the importance of ethics and values.
7. Nor is this only a drafting point. If people think the battle against corruption is simply addressing some mere technical point, we would lose the battle for the public's commitment. Employees are not motivated by preventing "nonconformities," they are

motivated by preventing true wrongs. We need to call evil by its name.

iii. **How to evaluate programs.** There are areas in the compliance world where it is fairly obvious what needs to be done, and other areas where people are still struggling. One area that could greatly benefit from more guidance is how to evaluate/assess programs. Here is a missed opportunity for the ISO Standard. In section 9.1, instead of providing examples of how to evaluate programs, it merely provides reminders to evaluate, but no advice or guidance on how. For example, the Annex could have listed steps such as focus groups, exit interviews, deep dives, surveys, etc.[43] But it offers next to nothing (there is some coverage of audits, but no one should be misled into believing that simply doing audits will sufficiently inform management on the effectiveness of the compliance program).

iv. **Third parties.** ISO 37001 does a superior job in emphasizing the role of third parties. See 8.5 and 8.6. At least in the past, some companies thought it was enough to send a questionnaire to potential partners. Perhaps they thought asking the third party if they paid bribes actually had some value. Hopefully it has now dawned on people that a person who pays bribes is also very comfortable lying on questionnaires.

    1. What the ISO Standard reminds us to do is expect the same commitment to compliance programs down the supply lines. Getting companies to proselytize the compliance message this way is a leap forward, and ISO 37001 does this in a serious way. For example, in the Annex A.13.3.2 b) 1 is a good, gutsy provision. Where practicable the company is to require third parties to implement anti-bribery controls for the relevant activity. It is not

[43] The ease of providing such a list is illustrated by ISO 19600, 9.1.4, which does list these types of points. It is a mystery why ISO 3700 failed to do this.

enough just to make a suggestion that a supplier do this; the company must require it wherever it can.

2. But there is at least one anomaly. On this point of third parties the Annex makes a rather questionable point I have not seen in other standards. Where the Annex addresses "third parties the company does not control," it says it is not necessary to require implementation of controls if they "would not help mitigate the relevant risk." I spent too many years in corporate practice not to imagine how this one would play out in working with the deal team who just wants to get the transaction closed and does not want to give a "to do" list to third parties. I can hear it now: "We can't tell them to (do training; have audits; have a policy; have a compliance officer; or anything else), it wouldn't work anyway, and ISO 37001 says we don't have to do things that 'would not help mitigate the risk.'" But if the types of controls listed in the ISO Standard do not work, then why are they in the ISO Standard? Moreover, how would a company ever know that something "would not help"? When would training, for example, not work? Of course, there will be details that are not appropriate in given circumstances and this should have been written more specifically, but any company can implement the basics of a compliance program. Instead, inviting managers who are hungry for a deal to conclude that a control "would not help mitigate the relevant risk" is a potential invitation to play games and should not have been included in this guidance.
3. There is also a risk that companies retaining third parties in high-risk areas will simply accept any form of purported ISO 37001 certification as a substitute for the difficult

work of conducting due diligence on that third party. The intent of ISO 37001 could be completely turned on its head, leading to exactly the wrong result. Third parties that engage in corrupt activities are not averse to corrupting the certification process as well.

v. **Communications.** To its credit, ISO 37001 in item 7.4 recognizes that in addition to training there is also a need for "communications." Too often people refer to training and omit the rest of the picture. Unfortunately, the guidance on communications, in terms of how to reach people, is unnecessarily thin. There is, for example, no recognition of all the recent innovations, such as social media and apps. It would have been better for the Standard or the Annex to remind companies to include these tools.

vi. **Preventing retaliation.** Item 7.2.2.1 d) under "employment process" aggressively addresses retaliation by giving a good list of things that could represent retaliation, and calling for protection for those who raise issues. However, it would have been more valuable if it had provided guidance on what such protective procedures might be.

   1. Item 8.9 d) calls for a prohibition of retaliation against those raising concerns, but does not address protection for those cooperating in an investigation or those conducting the investigation. It would also have been helpful to bar retaliation against those engaged in the full range of compliance program activities.

vii. **Confidentiality in investigations.** Both 8.9 and 8.10, dealing with reporting and investigations, address confidentiality. 8.9 b) wisely recognizes that confidentiality is limited by the need to conduct an investigation, yet 8.10 f) omits that point. It would have been better also to have noted that disclosure may be required by law or by legal process, and voluntary disclosure of violations to the government may also necessitate yielding of confidentiality.

viii. **Controls.** Item 8.3 covers Financial Controls; all it says is that there should be such controls. Item 8.4 calls for non-financial controls, simply listing areas that might be subject to such controls. Given the central role such controls play in dealing with bribery, this is an anomalous approach; the Standard provides detail on documentation, but nothing on the essential topic of controls. It does cross reference the Annex (which does have some detail), but as discussed elsewhere the Annex is minimized as little more than suggested reading.

ix. **Backgrounds and incentives.** 7.2.2.2 is another area where the ISO Standard raises important points. Item a) calls for diligence in hiring and promoting people.[44] Item b) is equally on point, calling for taking steps to prevent incentives from encouraging bribery. It is appropriate to emphasize this with the unusual specificity shown here.[45] American experience with the Sentencing Guidelines is that management drags its heels in dealing with incentives as part of a compliance program, yet this is an essential element for programs to be effective.[46]

x. **Find in one place, look in others.** In looking at 10.1.b)3) there is a very good point that could be added to compliance and ethics standards globally: *when you find something wrong once in one place, look into whether it is happening elsewhere.* Certainly a lesson everyone should have learned from Wells Fargo – with over 5000 "rogue" employees! It is not

---

[44] This is a standard that had been in the US Sentencing Guidelines since 1991, U.S.S.G. §8B2.1(b)(3), http://www.ussc.gov/Guidelines/2010_guidelines/Manual_PDF/Chapter_8.pdf

[45] It should also have drawn from ISO 19600, item 5.3.4 d), calling for "the inclusion of compliance responsibilities in job descriptions and employee performance management processes".

[46] See Murphy, Using Incentives in Your Compliance and Ethics Program (SCCE; 2012), http://www.corporatecompliance.org/Resources/View/tabid/531/ArticleId/814/Using-Incentives-in-Your-Compliance-and-Ethics-Program.aspx .

enough to find and "fix" a specific problem in one location. There is also a need to determine whether there is just one mouse in the cupboard, or that the one that was caught indicates there are many more. One or two cases may be a symptom of something more serious, including corporate culture issues.

xi. **Planned frequency.** How often one should do something is a tough question to cover in a standard. One approach is to use the term "regularly," so it is clear that doing something once is not enough. Industry practice may also provide a guide or a minimum. A more rigid bureaucratic approach is to pick an arbitrary standard. So the State of California, for example, had decided, in the difficult area of harassment prevention, that 2 hours every 2 years was the correct standard (perhaps with the end result of discouraging any better practices). But the ISO Standard is odd. Rather than offer any specific guidance, it merely calls for things to be done on a "planned frequency." Of course, doing training every 10 years is "planned" and also inadequate. Such a standard makes it easy to tick the box.

xii. **Risk appetite.** A.4.1 in the Annex uses the buzzword "risk appetite." Risk appetite is fine when talking about willingness to lose money in a new business venture, but has no place when it comes to crime. There is no such thing as a bribery "risk appetite." Certainly it is necessary to prioritize, but no manager should have an appetite for crime – it is unseemly. In the next version, they should simply drop this phrase.

xiii. **Training the board/top management.** A.9.3 says in-person training is "recommended" for the board and other personnel and business associates exposed to other than low risk. This use of "recommended" is ambiguous, because it leaves open the question whether you could have a program that merited certification without <u>any</u> training for the board and/or senior management. The standard in the Sentencing Guidelines is better targeted than this, in

that training at those levels is required. A particular type of training (e.g., live training) may appropriately be "recommended" but some training is essential. A program should not be acceptable and not be certified if only the workers are trained. It is also important that not just those who might break the law get training, but also those who might be witnesses or helpers.

xiv. **Monitoring.** The Annex in A.19 rightly addresses monitoring as an important function, but then only lists things that can be monitored. Of course, any and all elements of the compliance program can be monitored, as well as substantive monitoring of the company's activities. Where it could have been very helpful is in explaining how monitoring differs from auditing, and what steps one could take to engage in monitoring, i.e., providing a "how to" guide.[47]

xv. **Integration with other compliance program activities.** There is an area where ISO 37001 is better than many other compliance standards, but could have done more. In today's environment it is fiction to approach any area of compliance as if it were being done in isolation. Companies and other organizations today simply do not address only one area of compliance and ethics; the reality is that there are numerous areas that call for attention. ISO 37001 at least acknowledges this reality, and refers readers to a broader ISO standard on compliance management systems, ISO 19600. This recognition contrasts sharply with such complete lapses as the American approach to harassment, where prevention of harassment is treated as if no one had done anything in any other compliance area, and the tools used in other compliance areas are ignored.

[47] See Murphy, "We're supposed to "monitor"? What does that mean," Compliance & Ethics Professional 70 (May 2018).

An excellent example of how to do this is provided by the OECD in its Guidance. The OECD quite clearly recognized this point by calling for integration with other compliance efforts. In its advice on anti-corruption programs: "It recognises that to be effective, such programmes or measures should be interconnected with a company's overall compliance framework." ISO 37001 addresses this in the Introduction but not with the forceful language used by OECD tying integration into effectiveness. Interestingly, integration is referenced in the Annex, such as A.9.5 observing that anti-bribery training could be part of the overall compliance training program. Going forward, it would make much more sense to recognize this reality in all standards relating to compliance efforts, using the type of strong statement found in the OECD Guidance.

xvi. **Inbound bribery.** ISO 37001 attempts to address bribery of a company's own people, while admitting that this is a different type of problem and not subject to the same types of steps used to address outbound bribery. See A.8.4. This is a controversial matter to cover in the ISO Standard, and is generally not covered in government and other standards. One reason for this is that companies have their own, inherent financial interest in preventing bribery of their own people; it is much less a matter of altruism or of public interest. Also, the prevention of outbound bribery is a difficult enough societal and economic problem, and adding in steps that protect the company's bottom line arguably dilutes the effort. On the other hand, if a government agency is adopting a compliance program, then inbound bribery does take on a public policy aspect.

xvii. **Too small to try?** In item A.13.3.3 c) the drafters fall into a common trap, relating to small businesses. The item states flatly: "It will normally not be practicable when the business associate lacks the resources or expertise to be able to implement controls." Without

saying so explicitly, this is obviously aimed at small businesses. But as spelled out in Murphy, A Compliance & Ethics Program on a Dollar a Day: How Small Companies Can Have Effective Programs (SCCE; 2010) http://www.corporatecompliance.org/Portals/0/PDFs/Resources/ResourceOverview/CEProgramDollarADay-Murphy.pdf , it can actually be considerably easier for a small company to implement an effective program, in part because spans of control are much more limited. The boss can know what all his or her people are doing. Also the reality is that money cannot buy compliance or ethical conduct; commitment is the key for this. There is no excuse for bribery in a small business, unless the owners/managers want to engage in bribery. Lack of resources and expertise is just not a legitimate excuse. Resources mean commitment and doing a little work; expertise means doing a little bit of reading in readily available online sources. Controls, after all, can be as simple as having the boss look into what is actually happening in the business, talking to employees, and checking a few vouchers. Every company, no matter what size, can make at least some effort not to break the law.

xviii. **Checking on third parties.** On a small point, A.13.3.6 attempts to help by suggesting a company check on its third party's compliance efforts by, e.g., requesting copies of its relevant policies. This is what people like to do, but it is a waste. If one is going to ask for one thing, just ask to talk with the third party's compliance officer. If there is none, then there is no compliance program. Paper policies are so clearly discredited that it makes no sense to make any judgment based on them. But if there is no one driving the program, then there is no program.

xix. **GDPR.** Of course it is not the place of an ISO standard to address political issues. But there are serious issues that those fighting bribery need to address. In

A. 10.3 4) & 5) we are advised in our due diligence to check possible business associates to determine whether they have been "investigated, convicted, sanctioned or debarred for bribery or similar conduct." How else are we to avoid dealing with bribers? 7.2.2.2 a) calls for diligence in hiring and promoting people. Item 8.9 tells us to treat reports of concerns confidentially and to permit anonymous reports, yet in a note advises that in some jurisdictions this is prohibited by law.[48] Yet now we face an enhanced risk that privacy regulators, using the newly issued big guns of the General Data Protection Regulation (GDPR), will severely undermine the fight against bribery under the banner of privacy. The power and penalties of these regulators are enormous and intimidating, and in creating the GDPR they have failed to address this crucial public policy issue. Given that in the past European privacy regulators were quick to undercut compliance efforts (see the various attacks on compliance speak-up systems), there is serious cause for concern. See Joseph E. Murphy, **Policies in conflict: Undermining corporate self-policing,** 69 Rutgers U.L. Rev. 421 (2017), http://www.rutgerslawreview.com/wp-content/uploads/2017/07/Joseph-Murphy-Policies-in-Conflict-69-Rutgers-U.-L.-Rev.-421-2017.pdf

xx. **Confidentiality and privilege.** Will certification auditors have unlimited access to confidential or privileged information (potentially causing waiver of legal protections), or will companies be able to refuse

[48] As a lawyer I would advise not to take such a quick conclusion of illegality at face value, but at least to explore ways to permit reporting legally within the framework of overly aggressive privacy laws, e.g., possibly permitting face-to-face reporting but with no written or digital records – the basis for privacy regulators' assertions of jurisdiction. In other words, explore legal ways employees can raise concerns about illegal conduct while minimizing their exposure to retaliation by their bosses. I would also advise working to change such restrictive laws, so they do not interfere with the fight against corruption.

them access? Will companies be able to achieve certification even if they deny access to important materials? Will the notes and work product of the auditors be protected, or will they be subject to discovery, disclosure and use against the company? This is also a broader political issue that ISO cannot solve, but that raises concerns for compliance program reviews.[49]

xxi. **Bibliography.** Bibliographies may be minor points, but there are some notable omissions in ISO 37001's bibliography. Among the sources excluded were those promulgated by the groups most experienced in dealing with bribery: enforcers and regulators from the US DOJ and SEC, and those from the UK's work on the Bribery Act. Also missing was the original source for compliance programs of all sorts, the USSGs. Yet these contain very important insights into what should be in compliance programs. If the purpose was to avoid appearing to align with any one country, this seems an unfortunate sacrifice of utility for political purposes.

[49] See LaNeve, ISO 37001: A year on (Feb. 14, 2018) "Confidentiality," available at https://ethicalboardroom.com/iso-37001-a-year-on/