



ISO 37001:2016

A systemic approach to prevention, detection, and management of bribery

Presented by: Joseph Krolkowski,
ABMS Program Manager/
Executive Committee Member



Please note:

- ▶ All participants have been muted.
- ▶ Please type your questions in the “Question” section of the dashboard – we will take questions at the conclusion of this presentation.
- ▶ Please note that copies of today’s presentation will be available for download shortly.
- ▶ This webinar (and all other past PJR webinars) will also be available for re-viewing on our website under “Previously Recorded Webinars.”

A dark grey arrow points to the right from the left edge of the slide. Several thin, curved lines in shades of blue and grey originate from the left side and sweep across the slide towards the right.

Today's presentation will cover:

- What is ISO 37001:2016?
- What is bribery?
- Why an anti-bribery management standard?
- The development of ISO 37001:2016
- Annex SL
- Three key provisions (prevention, detection, response)
- Benefits of certification
- Conclusion/Questions



What is ISO 37001:2016?

- ▶ ISO 37001:2016 is the first ISO published standard written for the topic of bribery.
- ▶ It's full title is "*Anti-bribery management systems — Requirements with guidance for use*"



What is bribery?

- ▶ ISO 37001 acknowledges that the term “bribery” has different legal definitions depending on local laws and statutes, but nevertheless an attempt was made to provide a general definition for use within the standard:
- ▶ *“Offering, promising, giving, accepting or soliciting of an undue advantage of any value (which could be financial or non-financial), directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person’s duties” – (ISO 37001:2016, clause 3.1)*

A dark blue arrow points to the right from the left edge of the slide. Several thin, light blue lines curve upwards from the bottom left towards the title area.

Why an Anti-Bribery Management Standard?

- ▶ Bribery is an ugly practice that undermines the trustworthiness of any organization, industry, or region.
- ▶ To even be suspected of involvement in an incident of bribery can greatly affect an organization's ability to even be considered for bidding on future business.
- ▶ Without mutually respected standards for combatting bribery, how can an organization shake it's "reputation"?



Past efforts



- Various groups (some governmental, some non-governmental) have attempted to provide guidelines or resources for bribery management. These included:
 - Federal Corrupt Practices Act (FCPA) of 1977
 - Transparency International founded in 1993
 - Sarbanes Oxley Act of 2002
 - UK Anti-Bribery Act of 2010
 - BS 10500 issued in 2011

A dark grey arrow points to the right from the left edge of the slide. Several thin, curved lines in shades of blue and grey originate from the left side and sweep across the slide towards the right.

ISO 37001's development process

- ▶ Like any other ISO published standard, ISO 37001 was developed by an assigned committee.
- ▶ ISO Project Committee 278
- ▶ Work began on Feb 7, 2014 and following the usual path:
 - ▶ Committee Draft – Fall 2014
 - ▶ Draft International Standard – Fall 2015
 - ▶ Final Draft International Standard – Fall 2016
 - ▶ ISO 37001 officially published 10/13/16



Rooted in Annex SL

- ▶ Like nearly every ISO published standard from the past several years, ISO 37001:2016 is rooted in Annex SL.
- ▶ Annex SL was first published in 2012 and represented the output of a special committee of the ISO called the Joint Technical Coordination Group (JTTCG.)
- ▶ A 10 section “blueprint” for authoring all of the ISO family of standards.




Why this matters

- ▶ Any organization that has successfully implemented an Annex SL rooted standard within the last 4-5 years will be able to add ISO 37001 to their certification portfolio with relative ease. Among the standards that fall into this category are:
 - ▶ ISO 9001:2015
 - ▶ ISO 14001:2015
 - ▶ ISO 45001: 2018
 - ▶ ISO 50001:2018
 - ▶ TL9000
 - ▶ IATF 16949
 - ▶ AS9100D



A lot of familiar requirements

- ▶ Any company with experience following one of the standards listed on the prior slide will find a lot of familiar content in ISO 37001:2016, including:
 - ▶ Management Review
 - ▶ Internal Audit
 - ▶ Corrective Action
 - ▶ Competency
- ▶ Existing programs for these requirements can be brought to bear in implementing ISO 37001.

A dark blue arrow points to the right from the left edge of the slide. Several thin, light blue lines curve upwards from the bottom left towards the main text area.

How does an anti-bribery management system work?

- ▶ ISO 37001:2016 focuses on three key areas in establishing a system for anti-bribery management.
 - ▶ Prevention of bribery incidents
 - ▶ Detection of bribery incidents
 - ▶ Response to bribery incidents



Prevention controls



- ▶ The bulk of requirements written into ISO 37001:2016 focus on prevention of bribery, as clearly this is the ideal state for an organization. Specific requirements related to prevention include:
 - ▶ Bribery Risk Assessments (4.5) – these are supposed to be performed on a “regular” basis and serve as a means to evaluate current and potential bribery risks. Records of these assessments are required.
 - ▶ Anti-Bribery Policy (5.2) – this is a required statement from the management of the organization, intended to ensure that the organization’s stance on bribery is made clear to the organization and serves to raise awareness of the ABMS program.



Prevention controls (cont.)

- ▶ The Anti-Bribery Compliance Function (5.3.2) – this mandatory party (usually a group of people) is tasked with multiple responsibilities relative to the ABMS. These include development of the system, ensuring its full deployment, and ABMS effectiveness reporting. Per the standard this function has to be staffed with parties that are both empowered and independent.
- ▶ Employment, Awareness, and Training (7.2) – one of the more extensive and prescriptive of the requirements found within ISO 37001. Requirements include screening requirements prior to hiring personnel, whistleblower protections, reviews of performance bonuses/incentives, and compulsory bribery training.



Prevention controls (cont.)

- ▶ Due diligence (8.2) – this requirement is directly related to the risk assessments mentioned in section 4.5. It calls for appropriate investigations to be performed in relation to pending transactions, projects, etc. if a bribery risk is identified.
- ▶ Financial and Non-Financial controls (8.3, 8.4) – when paired with the extensive guidance given in Annex A these two clauses represent wide ranging requirements that cover a myriad of potential controls that could be pursued including tiered payment rights, separation of duties, cash use restrictions, dual signoffs on contracts, and access restrictions on tenders and other price sensitive information.



Prevention controls (cont.)

- ▶ Controls associated with “controlled organizations” and business associates (8.5) – requires the flow down of ABMS controls to both of these classes of external providers.
 - ▶ “Controlled organizations” receives a bit of clarity in a note – *“An organization has control over another organization if it directly or indirectly controls the management of the organization.”*
- ▶ Gifts, Hospitality, Donations (8.7) – a fairly self explanatory requirement. Annex A provides an extensive amount of guidance on this issue and makes the point that these items don’t have to be expressly forbidden, just carefully monitored and controlled.



Detection controls

- ▶ Bribery Risk Assessment (4.5) and the Anti-Bribery Compliance Function (5.3.2) – these are viewed as both a means of prevention and detection.
- ▶ Raising Concerns (8.9) – the other primary means of detection written into ISO 37001 revolves around personnel feeling empowered and unafraid to come forward and report actual or perceived incidents of bribery. Controls found in section 8.9 that are intended to facilitate this reporting include mandatory anonymity for whistleblowers, confidential treatment of reported incidents, and protections against retaliation for whistleblowers.



Response controls

- ▶ Investigating and dealing with bribery (8.10) – a series of requirements pertaining to response protocol. Among other mandates, this section requires full cooperation with those tasked with the incident's investigation, as well as empowerment of the investigators. The results of the investigation are shared with the anti-bribery compliance function and treated in a confidential matter (except where required by law.) Annex A provides further guidance on what this process might consist of.



Mandatory procedures



- ▶ ISO 37001:2016 is a unique standard in that there are several required procedures. Here's the complete list:
 - ▶ Employment Process (7.2.2)
 - ▶ Anti-Bribery Awareness (7.3)
 - ▶ Anti-Bribery Control by Controlled Organizations and Business Associates controlled by the Organization (8.5.1)
 - ▶ Anti-Bribery Control by Business Associates not controlled by the Organization (8.5.2)



Mandatory procedures



- (list continues)
 - Anti-Bribery Commitments by Business Associates not controlled by the Organization (8.6)
 - Control of gifts, hospitality, donations, and similar benefits (8.7)
 - Bribery Reporting/Raising Concerns (8.9)
 - Bribery Response (8.10)
 - Internal Audit (9.2.3)

- As a reminder – the official definition of “procedure” (taken from ISO 9000:2015) reads as follows: “*Specified way to carry out an activity or a process.*” The expected interpretation of this requirement relative to an ABMS is that the procedure will be documented.



ISO 37001: 2016 Annex A

- ▶ Users of ISO 37001:2016 would do well to review the myriad of guidance provided in Annex A.
- ▶ Every one of the ABMS specific requirements (due diligence, financial controls, non-financial controls, etc.) is given a thorough explanation in this section.
- ▶ Numerous helpful examples are also provided for organizations that are trying to decide the best method to meet a requirement.



The ABMS audit process

- ▶ PJR's assessment of the ABMS program is layered and rooted in a variety of audit techniques.
- ▶ Organizations should expect a thorough review of procedures, contracts, terms and conditions, and other related materials.
- ▶ Many employees will be interviewed about their role in the organization and ensuring that they're aware of anti-bribery protocols and policies.
- ▶ The auditor will review various resources (online, etc.) to determine if the origination has been involved in an alleged incident of bribery.



Benefits of ISO 37001 certification

- ▶ There are numerous material and intangible benefits to pursuing a certification to ISO 37001:2016. These include:
 - ▶ Providing assurance to outside stakeholders that the organization takes business ethics seriously and works to promote a culture of honesty and trustworthiness.
 - ▶ Provides a means to select reliable partners in regions or industries with a reputation (deserved or not) for bribery and corruption.
 - ▶ Can lead to overall cost reductions.
 - ▶ Prevention of conflict of interest.
 - ▶ Can be used as a resource for information in the event of an outside (governmental) investigation of an alleged bribery incident.



Conclusion



- ▶ ISO 37001:2016 is an intriguing standard with the potential to make a real difference in the world of commerce.
- ▶ It is our hope that you will use the points of this presentation to consider the benefits to your organization in pursuing ISO 37001:2016 certification.
- ▶ Special note: as of November 2021, PJR is the only USA headquartered certification body to achieve ANAB accreditation for ISO 37001:2016.



Please tune in for one of our other webinars

- ▶ *“The Interaction of Processes and its importance to a successful audit”* is shown on a semi-annual basis.
 - ▶ This webinar explores the crucial topic of processes and how to correctly understand them.
- ▶ *“Non-Applicable Clauses, Permissible Exclusions, Exemptions - Developing a better understanding of what can and what cannot be excused in an audit assessment”* is presented on a semi-annual basis.
 - ▶ This webinar explores the critical topic of exemptions and the right approach to take in determining which apply to you.
- ▶ We offer a variety of webinars on other topics including Stage 1 Audits, ISO 9001:2015, AS9100, ISO 13485:2016, IATF 16949, and ISO 14001:2015.

A dark grey arrow points to the right from the left edge of the slide. Below it, several thin, curved lines in shades of blue and grey sweep across the left side of the slide.

Want to keep in touch?

- ▶ Do you want to be kept informed of the latest news automatically?
- ▶ Please opt in for future updates by visiting our website at www.pjr.com
- ▶ At the bottom of the page, enter your email address in the provided space and click “Subscribe.”

Questions?

Thank you!

Learn more at www.pjr.com



**PERRY JOHNSON
REGISTRARS, INC.**