GIACC
Global Infrastructure Anti-Corruption Centre

Committee on Anti-Corruption (CAC)
Lima, Peru 2016

An overview of ISO 37001

Anti-bribery management system standard

Eng. Martin Manuhwa

&

Eng. Jaime Santamaria

[07 December 2016]

Subjects to be covered

1. **What is ISO 37001?**

   This section looks at:

   - The changes to the international legal and ethical environment which have led to ISO 37001
   - How ISO 37001 was developed
   - The purpose and scope of ISO 37001
   - The benefits of ISO 37001.

2. **Implementing ISO 37001**

   This section looks at:

   - The decision to implement ISO 37001
   - The requirements of ISO 37001.

What is ISO 37001?

Bribery is a significant business risk

- Bribery is widely acknowledged as a significant business risk in many countries and sectors.

- Previously, bribery has in many cases been tolerated as a “necessary” part of doing business.

- Now, increasing awareness of the damage caused by bribery to countries, organizations and individuals has resulted in calls at international and national level for effective action to be taken to prevent bribery.

International treaties

- Many international treaties have been signed during the last 20 years requiring member states to implement anti-bribery laws and procedures:

- Most internationally significant:
  - The United Nations Convention against Corruption (2003)
  - The OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (1999).

Laws

- Most countries have changed their laws in accordance with treaty requirements. Bribery and other corruption offences are therefore crimes worldwide.

- All OECD countries have now made it a crime for their nationals and organizations to bribe overseas. As a result, a person or organization may be liable for bribery both:
  - In the country where the bribery took place; and
  - In the person or organization’s home country.

Prosecution

- Prosecution agencies worldwide are now starting to investigate and prosecute companies and individuals for bribery. There have been many recent major cases.

Global Infrastructure Anti-Corruption Centre

Corporate anti-bribery programme (1)

- While good laws and enforcement are vital, it is also important that organizations implement anti-bribery measures.
- Bribery prevention is increasingly seen as a management issue.
- Good management in government, in companies and on projects can materially reduce bribery.
- Bribery prevention should be treated in a similar manner to safety, quality and environmental management.

Corporate anti-bribery programme (2)

- Significant number of organizations internationally have responded to the changing legal and ethical environment by implementing anti-bribery management systems within their organizations.

- Ethical organizations also need to ensure that their partners and supply chain implement appropriate controls.

- Government departments, funders, and companies should all adopt anti-bribery measures within their organization.

BS 10500

- Organizations are now requiring proof that their own organization, and their clients, agents, joint venture partners, and major sub-contractors, suppliers and consultants have implemented adequate anti-bribery measures.

- This led to a call for a standard which provides minimum requirements and allows independent verification.

- This led to development of British Standard BS 10500 - Specification for anti-bribery management system. Published 2011.

- BS 10500 successfully adopted by numerous companies. Many are now certified to it on a similar basis to IS0 9001 and 14001.

Development of ISO 37001(1)

- ISO in 2013 established a Project Committee to publish a new ISO anti-bribery management system standard, ISO 37001.

- **Participating countries (37):** Australia, Austria, Brazil, Cameroon, Canada, China, Colombia, Croatia, Czech Republic, Denmark, Ecuador, Egypt, France, Germany, Guatemala, India, Iraq, Israel, Kenya, Lebanon, Malaysia, Mauritius, Mexico, Morocco, Nigeria, Norway, Pakistan, Saudi Arabia, Serbia, Singapore, Spain, Sweden, Switzerland, Tunisia, UK, USA, Zambia.

- **Observing countries (22):** Argentina, Armenia, Bulgaria, Chile, Cyprus, Cote d'Ivoire, Finland, Hong Kong, Hungary, Italy, Japan, Korea, Lithuania, Macau, Mongolia, Netherlands, New Zealand, Poland, Portugal, Russia, Thailand, Uruguay.

Development of ISO 37001(2)

- **Liaison organizations (8):** ASIS, European Construction Industry Federation (FIEC), Independent International organization for Certification (IIOC), International Federation of Consulting Engineers (FIDIC), IQNet, OECD, Transparency International, World Federation of Engineering organizations (WFEO).
- **Committee Secretariat and Chair:** UK.

Development of ISO 37001(3)

- First draft of ISO 37001 based on content of BS 10500 merged into ISO standard management systems template. Uses same template as ISO 9001 and 14001, so is consistent with these standards.
- The drafts were circulated for international comment, and were modified at six international drafting meetings over three years to take account of international comments.
- Over 80 experts from over 20 countries participated in these meetings, which were held in London, Madrid, Miami, Paris, Kuala Lumpur and Mexico City.
- Decisions on text made by consensus of participating countries.

Development of ISO 37001(4)

- ISO 37001 was published on 15th October 2016.
- ISO 37001 replaces BS 10500.
- Is a Type A requirements standard, so can be independently certified.
- Contains supporting guidance to help with implementation.
- Focuses on bribery, but can be expanded to include other corruption offences.

GIACC
Global Infrastructure Anti-Corruption Centre

Purpose and scope of ISO 37001 (1)

- ISO 37001 is intended to help an organization to implement an effective anti-bribery management system.
- It requires organizations to implement various anti-bribery measures in a reasonable and proportionate manner according to the type and size of the organization, and the nature and extent of bribery risks faced.
- Requirements of internationally recognised good practice are taken into account.
- It is applicable to small, medium and large organizations in the public, private and voluntary sectors.

Purpose and scope of ISO 37001 (2)

- ISO 37001 cannot provide absolute assurance that no bribery will take place in relation to an organization. But it can help establish that the organization has implemented reasonable and proportionate measures designed to prevent bribery.
- organization can obtain certification to ISO 37001 in a similar way to obtaining certification to 9001and 14001.
- Provides assurance to owners, directors, employees and business associates that organization is taking steps to prevent bribery.
- Can be used as project pre-qualification requirement.
- Can enhance organization’s reputation.

Cost of Certification

- Cost of certification is likely to vary according to the size of the organization (which is the same as with e.g. ISO 9001).
- Cost is unlikely to be a competitive disadvantage. Likely to be an advantage if:
  - a procuring entity requires all its bidders to be certified to ISO 37001; or
  - additional points given in the procurement evaluation for evidence of anti-bribery policies.
- Cost of implementing system likely to be minimal when compared to loss and damage which could be suffered by organization which gets involved in bribery. System can help prevent loss.

Outcome

- ISO 37001 cannot provide absolute assurance that no bribery will occur. But can help establish that organization has implemented reasonable and proportionate anti-bribery measures.
- The risk of bribery is reduced and the playing field is levelled for organizations if certification to ISO 37001 is a project pre-qualification requirement.
- The risk of corrupt or negligent certification is reduced by the use of major, well known, accredited international certifiers.
- The publication and use of ISO 37001 is therefore a major step forward in the fight against bribery.

Implementing ISO 37001

General principles (1)

- ISO 37001 specifies various anti-bribery policies and procedures which an organization must implement to assist it prevent bribery, and identify and deal with any bribery which does occur.
- An organization is only compliant with ISO 37001 if it has implemented all of the required measures.
- However, these measures should be implemented by the organization in a reasonable and proportionate manner according to the type and size of the organization, and the nature and extent of bribery risks it faces.

General principles (2)

- An organization cannot achieve compliance with ISO 37001 just by ticking boxes. It requires:
  - The development of policies and procedures designed to prevent bribery.
  - The genuine commitment of the organization's top management to make the system work.
  - The effective implementation of these policies and procedures by the organization.
  - Monitoring and review by the organization of the effectiveness of these policies and procedures.
  - Continual improvement of the policies and procedures to ensure their effectiveness.

GIACC
Global Infrastructure Anti-Corruption Centre

The methodology used in these slides

- The following slides examine the different requirements of ISO 37001 which need to be planned, designed and implemented.
- The key requirements of ISO 37001 are included in summary form in the following slides in red text.
- GIACC comments on the relevant requirements are included in blue text.
- Cross references to the relevant ISO 37001 clause number and to GIACC's free on-line guidance materials are contained in grey text.
- References to "ABMS" mean an ISO 37001 compliant anti-bribery management system.

ISO restrictions

- **NOTE:** Any organization implementing ISO 37001:
  - must purchase its own copy of ISO 37001 from ISO’s web-site*; and
  - should rely on the full text of ISO 37001, not on the summary in these slides.

*** www.iso.org/iso/catalogue_detail?csnumber=65034**
Cost = 158 Swiss Francs

Decision to implement the ABMS

- The organization's governing body or top management must take the decision whether to implement an Anti-Bribery Management System (ABMS). In making this decision it will consider:
  - Does the organization face bribery risk, and what are the possible consequences of this risk?
  - Should the organization implement an ABMS in order to manage this risk?
  - What are the costs and benefits to the organization of implementing an ABMS?

Who should lead implementation

- If the organization decides to implement an ABMS, the organization's governing body or top management must appoint an appropriate person(s) to lead the design and implementation of the ABMS. In making this decision it will consider:
  - Who is the appropriate person(s). This person must have the authority and commitment to be able to do so effectively.
  - What support this person(s) needs. This could include supporting personnel, expert outside advice, and resources (office, computers etc.).

Planning and designing the ABMS

- Before the ABMS can be implemented, it needs to be planned and designed. This includes the following steps:
  - Determining what anti-bribery laws are applicable.
  - Determining what types of bribery the ABMS should be designed to prevent.
  - Understanding the nature of the organization and its activities.
  - Understanding the organization’s stakeholder requirements.
  - Assessing the bribery risks faced by the organization.
  - Determining the scope and objectives of the ABMS.
  - Planning and designing the necessary anti-bribery controls (these are listed in the following slides).

Anti-bribery policy (1)

- The organization shall establish an anti-bribery policy that:
  - prohibits bribery;
  - requires compliance with applicable anti-bribery laws;
  - requires compliance with the ABMS.
- The anti-bribery policy commits the organization, its personnel and relevant business associates to avoid bribery and to comply with the ABMS.
- The policy shall be approved by the governing body (or by top management if no separate governing body (5.1.1 a)).

Anti-bribery policy (2)

- Personnel shall be required by their conditions of employment to comply with the policy (7.2.2.1 a)).

- More than low bribery risk personnel must sign a confirmation of compliance with the anti-bribery policy (7.2.2.2 c)).

- The organization shall where practicable require its more than low bribery risk business associates (suppliers, sub-contractors, consultants, agents etc.) to commit to prevent bribery (8.6).

- The anti-bribery policy shall be published through the organization’s internal and external communication channels (7.4.2).

- **ISO 37001: Clause 5.2**
- **WFEO (CAC)/policy.php**

Leadership and responsibility (L&R) (1)

- Responsibility for implementing and complying with the anti-bribery policy and ABMS are specifically allocated between:
  - governing body;
  - top management;
  - compliance function;
  - managers;
  - personnel.
- Under this allocated structure of compliance, it is not possible for an action to occur which is no-one’s management responsibility.

- **ISO 37001: Clauses 5.1 and 5.3**
- **WFEO (CAC)/Boardresponsibility.php**

L&R (2) – Governing body/top management (1)

- The organisation’s governing body shall:
  - approve the anti-bribery policy;
  - review the content of the ABMS;
  - exercise reasonable oversight over the implementation and effectiveness of the ABMS.
- The organisation’s top management shall:
  - have overall responsibility for the implementation of, and compliance with, the ABMS;
  - ensure that responsibilities for relevant roles are assigned and communicated throughout the organization.

L&R (3) – Governing body/top management (2)

- The anti-bribery policy and ABMS must be supported by and led from the top. The governing body and top management are ultimately responsible for the success of the programme.
- ISO 37001 distinguishes between "governing body" (non-executive supervisory body (e.g. board of directors)) and "top management" (executive body) (e.g. chief executive)).
- The governing body is responsible for approving and supervising the ABMS (5.1.1), and top management for implementing it (5.1.2).
- If the organization does not have two separate bodies, then top management will fulfil the obligations allocated both to the governing body and top management.

L&R (4) – Compliance function (1)

- Top management shall assign to an anti-bribery compliance function the responsibility and authority for:
  - overseeing design and implementation of the ABMS;
  - providing advice and guidance to personnel on the ABMS and issues relating to bribery;
  - ensuring that the ABMS conforms to the requirements of ISO 37001.
- The anti-bribery compliance function shall be adequately resourced and be assigned to person(s) who have appropriate competence, status, authority and independence.

L&R (5) – Compliance function (2)

- The compliance function shall have direct and prompt access to the governing body and top management in the event that any concern needs to be raised in relation to bribery or the ABMS.

- In a large organization, the compliance function may be several people. In a medium size organization, it may be one person full time. In a smaller organization, it may be one person part time, who combines the compliance function with other functions.

- **ISO 37001: Clause 5.3.2**
- **WFEO (CAC)/Compliancemanager.php**

L&R (6) – Managers and personnel

- Managers at every level shall be responsible for requiring that the ABMS requirements are applied and complied with in their department or function.
- All personnel shall be responsible for understanding, complying with and applying the ABMS requirements, as they relate to their role in the organization.
- **ISO 37001: Clause 5.3.1**

L&R (7) – Delegation of decisions (1)

- Where top management delegates to personnel the authority for making decisions in relation to which there is more than a low risk of bribery, the organization shall ensure that controls are in place which require that the decision process and the level of authority of the decision-maker(s) are:
  - appropriate to the level of bribery risk
  - free of actual or potential conflicts of interest.
- There are three elements to this process:
  - Seniority of decision maker
  - Number of decision makers
  - Absence of conflict of interest in relation to decision makers

L&R (8) – Delegation of decisions (2)

- The organization can develop a decision matrix, which grades decisions according to bribery risk. This matrix may also take account of other risks, such as technical contractual and financial.
- The matrix may provide for example that:
  - A very low value and low risk decision can be taken by one junior manager.
  - A slightly higher value and/or higher risk decision can be taken by one senior manager.
  - A medium value and / or medium risk decision must be taken by two or more senior managers.
  - A high value and / or high risk decision must be taken by the board.

L&R (10) – Delegation of decisions (3)

- The organization should identify the risk of conflicts of interest: E.g.
  - when the organization's sales manager is related to a customer's procurement manager, or
  - when an organization's line manager has a personal financial interest in a competitor's business.
- The organization should inform all personnel of their duty to report any actual or potential conflict of interest.
- The organization should keep a record of any circumstances of actual or potential conflicts of interest.
- **ISO 37001: Clause 5.3.3**
- **WFEO (CAC)/Decision-makingprocess.php**

Resources (1)

- The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the ABMS.

- **Human resources:** There should be sufficient personnel who are able to apply sufficient time to their relevant anti-bribery responsibilities so that the ABMS can function effectively. This includes assigning sufficient person(s) (either internal or external) to the compliance function.

Resources (2)

- **Physical resources:** There should be the necessary physical resources in the organization for the ABMS to function effectively, e.g. office space, furniture, computer hardware and software, training materials, telephones, stationery.

- **Financial resources:** There should be a sufficient budget for the ABMS to function effectively.

- **ISO 37001: Clause 7.1**
- **WFEO (CAC)/Resources.php**

Competence

- The organization shall:
  - determine what level of competence personnel and business associates require from an anti-bribery perspective;
  - ensure that personnel and business associates are competent on the basis of appropriate education, training, or experience.
- Appointing incompetent persons to a role can result in weakness in controls which can result in bribery. (E.g. an incompetent procurement manager may not implement effective procurement controls, which could result in the deputy procurement manager being able to receive bribes in return for appointing suppliers).
- **ISO 37001: Clause 7.2.1**

Employment process (1)

- The success of the organization’s anti-bribery policy and ABMS depends primarily on it having ethical personnel who can comply with, implement and enforce the policy and ABMS.
- Therefore, it is imperative that the organization carefully controls its employment and promotion processes to ensure as far as practicable that it only employs or promotes ethical personnel.
- These employment process requirements work in parallel with the:
  - competence requirements (7.2.1); and
  - training requirements (7.2.3).

Employment process (2)

- In relation to all of its personnel, the organization shall implement procedures such that:
  - conditions of employment:
    - require personnel to comply with the anti-bribery policy and ABMS, and
    - give the organization the right to discipline personnel in the event of non-compliance;
  - personnel receive a copy of the anti-bribery policy and training in relation to that policy;
  - the organization can take appropriate disciplinary action against personnel who violate the anti-bribery policy or ABMS;

Employment process (3)

- personnel will not suffer retaliation (e.g. by threats, demotion, preventing promotion, transfer, dismissal, bullying) for:
  - refusing to participate in any activity in respect of which they have reasonably judged there to be a more than low risk of bribery; or
  - concerns raised in good faith of attempted, actual or suspected bribery or violation of the anti-bribery policy or ABMS.

- **ISO 37001: Clause 7.2.2.1**
- **WFEO (CAC)/employment_terms.php**

Employment process (4)

- In relation to personnel positions exposed to more than a low bribery risk, the organization shall implement procedures by which:
  - due diligence is conducted on personnel before they are employed, transferred or promoted by the organization, to ascertain as far as is reasonable:
    - that it is appropriate to employ or redeploy them; and
    - that it is reasonable to believe that they will comply with the anti-bribery policy and ABMS requirements;

Employment process (5)

- performance bonuses and targets are reviewed periodically to verify that there are reasonable safeguards in to prevent them from encouraging bribery;
- such personnel, top management, and the governing body file a declaration at reasonable intervals confirming their compliance with the anti-bribery policy.

- **ISO 37001: Clause 7.2.2.2**
- **WFEO (CAC)/employment_terms.php**

Training (1)

- The organization shall provide adequate and appropriate anti-bribery training to personnel, which shall cover:
  - the organization’s anti-bribery policy and ABMS, and their duty to comply;
  - the bribery risk and damage to them and the organization which can result from bribery;
  - the circumstances in which bribery can occur in relation to their duties, and how to recognize, prevent and avoid these circumstances;

Training (2)

  - the consequences of not conforming with the ABMS requirements;
  - how they are able to report any concerns.
- Personnel shall be provided with anti-bribery training on a regular basis, as appropriate to their roles and the risks of bribery to which they are exposed.
- The training programmes shall be periodically updated as necessary to reflect relevant new information.

Training (3)

- The organization shall implement procedures addressing anti-bribery training for business associates acting on the organization’s behalf or for its benefit, and which could pose more than a low bribery risk to the organization.
- These procedures shall identify the business associates for which such training is necessary, its content, and the means by which the training shall be provided.
- The training requirements for business associates can:
  - be communicated through contractual or similar requirements,
  - be implemented by the organization, the business associate or by other parties appointed for that purpose.

Training (4)

- The formality and extent of the training depends on the size of the organization and the bribery risks faced. It could be conducted as an online module, or by in-person methods (e.g. classroom sessions, workshops, roundtable discussions between relevant personnel, or by one-to-one sessions).

- The intended outcome of the training is that all relevant personnel and business associates should understand the bribery risk, and their obligations to comply with the anti-bribery policy and ABMS.

- **ISO 37001: Clause 7.3**
- **WFEO (CAC)/Training.php**

Communication

- The organization shall determine the necessary internal and external communications relevant to the ABMS.
- The anti-bribery policy shall:
  - be made available to all the organization's personnel and business associates;
  - be communicated directly to both personnel and business associates who pose more than a low risk of bribery; and
  - be published through the organization's internal and external communication channels, as appropriate.

- **ISO 37001: Clause 7.4**
- **WFEO (CAC)/Communication.php**

Documented information

- The organization shall retain appropriate documentation in relation to the anti-bribery policy and design and implementation of ABMS:
- Documentation can be retained separately as part of ABMS, or can be retained as part of other management systems (e.g. compliance, financial, commercial, audit).

- **ISO 37001: Clause 7.5**
- **WFEO (CAC)/Records.php**

Risk assessment and due diligence (1)

- ISO 37001 has two levels of risk assessment:
  - overview risk assessment under 4.5; and
  - detailed risk assessment and due diligence under 8.2.

- **Overview risk assessment (4.5**): The organization takes an overview of its whole business, where it works, its business associates etc., and assesses the overall bribery risks facing the organization. In doing so, it assesses the risk of categories of transaction or business associates. E.g.
  - All transactions in certain countries where bribery is common may be treated as high risk.
  - All agents and intermediaries may be treated as high risk.

Risk assessment and due diligence (2)

  - All suppliers who supply goods over a specified financial threshold may be treated as medium risk.
  - All suppliers who supply goods below a specified low financial threshold and which have no interaction with the customer or government officials may be treated as low risk.

- The ABMS must be planned and designed to take account of these assessed bribery risks. A higher level of controls is likely to be required in relation to bribery risk which are more likely to occur, or which are likely to have a more significant adverse impact on the organisation.

Risk assessment and due diligence (3)

- **Detailed risk assessment and due diligence (8.2)**: Where the organization is to enter into a transaction with a specific business associate (e.g. agent, supplier etc.) which falls within a more than low risk category identified under the overview risk assessment (4.5), the organization will undertake a detailed risk assessment of that transaction. In doing so, it will undertake any necessary specific due diligence on the business associate.

- The purpose of the due diligence is to learn more about the relevant business associate, and the possible bribery risks it may pose to the organization.

Risk assessment and due diligence (4)

- Due diligence may include, e.g.
  - a questionnaire sent to the business associate;
  - a web-search on the business associate and its shareholders and top management to identify any bribery-related information;
  - searching appropriate government, judicial and international resources for relevant information;
  - checking publicly available debarment lists of organizations that are prohibited from contracting with public entities
  - making enquiries of appropriate other parties about the business associate’s ethical reputation.

Risk assessment and due diligence (5)

- The results of the due diligence would be fed back into the relevant risk assessment.

- The intention of the bribery risk assessment and due diligence is not to eliminate all possible risk of bribery. The purpose is to identify, after making reasonable and proportionate enquiries and giving the issue appropriate consideration, whether the risk of bribery appears to be sufficiently low that it is reasonable to allow the business relationship, transaction or project to proceed or continue.

- **ISO 37001: Clauses 4.3, 8.2 and A.10**
- **WFEO (CAC)/due_diligence.php**

Financial controls (1)

- The organization shall implement financial controls that manage bribery risk.
- Financial controls are the management systems and processes implemented by the organization to manage its financial transactions properly and to record these transactions accurately, completely and in a timely manner.
- Depending on the size of the organization and transaction, the financial controls could include, e.g.:
  - implementing a separation of duties, so that the same person cannot both initiate and approve a payment;

Financial controls (2)

- implementing tiered levels of authority for payment approval (so that larger transactions require more senior management approval);
- verifying that the payee’s appointment and work or services carried out have been approved by the organization’s relevant approval mechanisms;
- requiring at least two signatures on payment approvals;
- requiring the appropriate supporting documentation to be annexed to payment approvals;
- restricting the use of cash and implementing effective cash control methods;

Financial controls (3)

- requiring that payment categorizations and descriptions in the accounts are accurate and clear;
- implementing periodic management review of significant financial transactions;
- implementing periodic and independent financial audits and changing, on a regular basis, the person or the organization that carries out the audit.

- **ISO 37001: Clause 8.3**
- **http://WFEO (CAC)/FinancialControls.php**

Non-financial controls (1)

- The organization shall implement non-financial controls that manage bribery risk with respect to such areas as procurement, operational, sales, commercial human resources, legal and regulatory activities.

- Non-financial controls are the management systems and processes implemented by the organization to help it ensure that the procurement, operational, commercial and other non-financial aspects of its activities are being properly managed.

Non-financial controls (2)

- The non-financial controls which can reduce bribery risk could include, for example:
  - using approved contractors, suppliers etc. that have undergone a pre-qualification process under which the likelihood of their participating in bribery is assessed;
  - awarding contracts, where possible and reasonable, only after a fair and competitive tender process between at least three competitors has taken place;
  - requiring at least two persons to evaluate the tenders and approve the award of a contract;

Non-financial controls (3)

- assessing:
  - the necessity and legitimacy of the services to be provided by a business associate to the organization,
  - whether the services were properly carried out;
  - whether any payments to be made to the business associate are reasonable and proportionate to the services provided.
- implementing a separation of duties, so that personnel who approve the placement of a contract are different from those requesting the placement of the contract and are from a different department or function from those who manage the contract or approve work done under the contract;

Non-financial controls (4)

- requiring the signatures of at least two persons on contracts, and on documents which change the terms of a contract or which approve work undertaken or supplies provided under the contract;
- placing a higher level of management oversight on potentially high bribery risk transactions;
- protecting the integrity of tenders and other price-sensitive information by restricting access to appropriate people;

- **ISO 37001: Clause 8.4**
- **WFEO (CAC)/Commercialcontrols.php**

Controls of controlled organizations (1)

- The organization shall implement procedures which require that all other organizations over which it has control either:
  - implement the organization's anti-bribery management system, or
  - implement their own anti-bribery controls,

  in each case only to the extent that is reasonable and proportionate with regard to the bribery risks faced by the controlled organizations.

- An organization has control over another organization if it directly or indirectly controls the management of the organization.

Controls of controlled organizations (2)

- An organization which is genuine in its desire to prevent bribery must ensure that this commitment is shared by its controlled organizations. Otherwise, a parent company could claim to be bribery free at the same time as its subsidiary or controlled joint venture participates in bribery.
- Controlled organizations may also pose a bribery risk to the organization. E.g.:
  - a subsidiary of the organization paying a bribe with the result that the organization can be liable;
  - a joint venture or joint venture partner paying a bribe to win work for a joint venture in which the organization participates.

Controls of controlled organizations (3)

- Controls implemented by the controlled organization may help reduce these risks.

- ISO 37001 therefore requires the organization to ensure that all organizations which it controls implements its own reasonable and proportionate anti-bribery controls. These could be either:
  - A full ISO 37001 ABMS; or
  - A more limited set of controls (provided that these controls adequately take account of the controlled organization's bribery risk).

- **ISO 37001: Clause 8.5.1**
- **WFEO (CAC)/BusinessAssociateProgramme.php**

Controls of business associates (1)

- In relation to business associates not controlled by the organization for which the bribery risk assessment (4.5) or due diligence (8.2) has identified a more than low bribery risk, and where anti-bribery controls implemented by the business associates would help mitigate the relevant bribery risk, the organization shall implement procedures as follows:
  - the organization shall determine whether the business associate has in place anti-bribery controls which manage the relevant bribery risk;

Controls of business associates (2)

- where a business associate does not have in place anti-bribery controls, or it is not possible to verify whether it has them in place:
  - where practicable, the organization shall require the business associate to implement anti-bribery controls in relation to the relevant transaction, project or activity; or
  - where it is not practicable to require the business associate to implement anti-bribery controls, this shall be a factor taken into account in evaluating the bribery risk of the relationship with this business associate (4.5 and 8.2) and the way in which the organization manages such risks (8.3, 8.4, 8.5).

Controls of business associates (3)

- Business associates may pose a bribery risk to the organization. E.g.:
  - a procurement manager of a customer demanding a bribe from the organization in return for a contract award;
  - an agent of the organization paying a bribe to a manager of the organization’s customer on behalf of the organization;
  - a supplier or sub-contractor to the organization paying a bribe to the organization’s procurement manager in return for a contract award.
- Controls implemented by the business associate may help reduce these risks.

Controls of business associates (4)

- Recognising the reasonable and proportionate basis of ISO 37001, the organization is only required:
  - to implement this measure in relation to business associates which the bribery risk assessment (4.5) has identified as posing more than a low bribery risk;
  - to insist on business associate controls, or to verify the controls, if it is practicable for the organization to do so.

- **ISO 37001: Clause 8.5.2**
- **WFEO (CAC)/BusinessAssociateProgramme.php**

Anti-bribery commitments (1)

- For business associates which pose more than a low bribery risk, the organization shall implement procedures which require that, as far as practicable:
  a) business associates commit to preventing bribery by, on behalf of, or for the benefit of the business associate in connection with the relevant transaction, project, activity, or relationship;

  b) the organization is able to terminate the relationship with the business associate in the event of bribery by, on behalf of, or for the benefit of the business associate in connection with the relevant transaction, project, activity, or relationship.

Anti-bribery commitments (2)

- Where it is not practicable to meet the requirements of a) or b) above, this shall be a factor taken into account in evaluating the bribery risk of the relationship with this business associate (4.5, 8.2) and the way in which the organization manages such risks (8.3, 8.4, 8.5).

- It is important that the organization obtains a contractual anti-bribery commitment from its more than low bribery risk business associates as:
  - the commitment alerts the business associate to the importance of compliance; and
  - the organization would be entitled to claim damages for breach of contract if the business associate participates in bribery.

Anti-bribery commitments (3)

- It is also important that the organization obtains the contractual right to terminate the contract in the event of bribery by the business associate; as:
  - the organization may not wish to continue with the contract if the business associate has been involved in bribery; and
  - under requirement 8.8, the organization needs the ability to be able to withdraw from a corrupt transaction.

Anti-bribery commitments (4)

- Recognising the reasonable and proportionate basis of ISO 37001, the organization is only required:
  - to implement this measure in relation to business associates which the bribery risk assessment (4.5) has identified as posing more than a low bribery risk;
  - to insist on this contract clause if it is practicable for the organization to do so.

GIACC
Global Infrastructure Anti-Corruption Centre

Anti-bribery commitments (5)

- It will normally be practicable to require these commitments when the organization has influence over the business associate and it can insist on the business associate giving these commitments.
- The organization is likely to be able to require these commitments, for example, where the organization is appointing an agent to act on its behalf in a transaction, or is appointing a sub-contractor with a large scope of work.

Anti-bribery commitments (6)

- The organization may not have sufficient influence to be able to require these commitments in relation to, e.g.:
  - dealings with customers or clients, or
  - when the organization is buying components from a major supplier on the supplier’s standard terms.
- In these cases, the absence of such provisions does not mean that the project or relationship should not go ahead, but the absence of such commitment should be regarded as a relevant factor in the bribery risk assessment and due diligence (4.5 and 8.2).
- **ISO 37001: Clause 8.6**
- **WFEO (CAC)/contract_terms.php**

Gifts, hospitality, benefits (1)

- The organization shall implement procedures that are designed to prevent the offering, provision or acceptance of gifts, hospitality, donations and similar benefits where the offering, provision or acceptance is, or could reasonably be, perceived as bribery.
- These could include, for example:
  - gifts, entertainment and hospitality;
  - political or charitable donations;
  - client representative or public official travel;
  - sponsorship;
  - community benefits.

Gifts, hospitality, benefits (2)

- The procedures implemented by the organization could control the extent and frequency of gifts and hospitality by e.g.:
  - a total prohibition on all gifts and hospitality; or
  - permitting gifts and hospitality, but limiting them by, e.g.:
    - a maximum expenditure (which may vary according to the location and the type of gift and hospitality);
    - frequency (relatively small gifts and hospitality can accumulate to a large amount if repeated);
    - timing (e.g. not during, or immediately before/after tender);
    - reasonableness (taking account of the location, sector and seniority of the giver or receiver);

Gifts, hospitality, benefits (4)

  - identity of recipient (e.g. those in a position to award contracts or approve permits, certificates or payments);
  - the legal and regulatory environment (some locations and organizations may have prohibitions or controls in place).

- The organization may require personnel to record all gifts, hospitality and benefits received or given on a register, so that they can be verified by the compliance function and be audited.
- Perception is important. A gift could be perceived to be corrupt even if not intended to be. What would it look like in newspaper?
- **ISO 37001: Clause 8.7**
- **WFEO (CAC)/gifts_policy.php**

Managing inadequacy of controls (1)

- In cases where:
  - the due diligence (8.2) conducted on a specific transaction, project, activity or relationship with a business associate establishes that the bribery risks cannot be managed by existing anti-bribery controls, and
  - the organization cannot or does not wish to:
    - implement additional or enhanced anti-bribery controls; or
    - take other appropriate steps (such as changing the nature of the transaction, project, activity or relationship)

  to enable the organization to manage the bribery risks,

then the organization shall take the following steps:

Managing inadequacy of controls (2)

- in the case of an existing transaction, project, activity or relationship, the organization shall take steps appropriate to the bribery risks and the nature of the transaction, project, activity or relationship to terminate, discontinue, suspend or withdraw from it as soon as practicable;
- in the case of a proposed new transaction, project, activity or relationship, the organization shall postpone or decline to continue with it.

- **ISO 37001: Clause 8.7**

Managing inadequacy of controls (3)

- Under ISO 37001, the organization must prohibit any involvement in bribery, and take reasonable and proportionate steps to prevent bribery.

- Therefore, it is a logical consequence of this that if the organization does not believe that its anti-bribery controls in relation to a specific transaction or business associate are likely to be effective to prevent bribery, then it should not participate in, or should withdraw from, that transaction or relationship.

- **ISO 37001: Clause 8.7**

Raising concerns (1)

- The organization shall implement procedures which:
  - encourage and enable persons to report in good faith suspected bribery, or any violation of or weakness in the ABMS, to the compliance function or to appropriate personnel;
  - require that the organization treats reports confidentially (unless this is prohibited by applicable law);
  - allow anonymous reporting (unless this is prohibited by applicable law);
  - prohibit retaliation against persons who make reports in good faith;

Raising concerns (2)

  - enable personnel to receive advice from an appropriate person on what to do if faced with a concern or suspected bribery.

- The organization shall ensure that all personnel are aware of the reporting procedures and are able to use them, and are aware of their rights and protections under the procedures.

- These procedures can be the same as, or form part of, those used for the reporting of other issues of concern (e.g. safety, malpractice, wrongdoing or other serious risk).

- The organization can use a business associate to manage the reporting system on its behalf.

Raising concerns (3)

- It is vital for the success of a ABMS that procedures are in place to allow reporting of concerns by personnel and other interested parties (sometimes called "whistle-blowing").
- Personnel must be aware that, if they use these procedures in good faith, they will not be victimised as a result (8.9 d).
- Top management must promote the use of these procedures (5.1.2 k), and protect personnel from victimisation (5.1.2 l)).
- The organization must investigate the report under 8.10.
- Reports of the outcome will be made to top management (9.3)

- **ISO 37001: Clause 8.7**
- **WFEO (CAC)/reporting.php**

Investigating and dealing with bribery (1)

- The organization shall implement procedures that:
  - require assessment and, where appropriate, investigation of any suspected bribery, or violation of the anti-bribery policy or the ABMS;
  - require appropriate action in the event that the investigation reveals any bribery, or violation of the anti-bribery policy or the ABMS;
  - empower and enable investigators;
  - require co-operation in the investigation by relevant personnel;

Investigating and dealing with bribery (2)

  - require that the status and results of the investigation are reported to the anti-bribery compliance function and other compliance functions, as appropriate;
  - require that the investigation is carried out confidentially and that the outputs of the investigation are confidential.

- The investigation shall be carried out by, and reported to, personnel who are not part of the role or function being investigated.
- The organization can appoint a business associate to conduct the investigation and report the results to personnel who are not part of the role or function being investigated.

Investigating and dealing with bribery (3)

- It is vital for the success of ABMS that the organization implements procedures to investigate suspicions of bribery or breach of ABMS, and takes appropriate action in the event that any bribery or breach of ABMS is identified.
- If personnel or business associates are aware that breaches are not investigated and dealt with, or are covered up, then the ABMS will be regarded as a smokescreen and will not be complied with.
- Reports of the outcome of investigations will be made to top management (9.3).
- **ISO 37001: Clause 8.10**
- **WFEO (CAC)/reporting.php**

Monitoring, measurement and evaluation (1)

- The organization shall determine:
  - what needs to be monitored and measured;
  - who is responsible;
  - the methods for monitoring and measurement;
- The organization shall evaluate the organization’s anti-bribery performance and the effectiveness and efficiency of the ABMS.

Monitoring, measurement and evaluation (2)

- It is important to the success of the ABMS that the organization takes reasonable and proportionate steps to monitor, measure and evaluate the anti-bribery controls. Is the ABMS working?
- Examples:
  - Record gifts and hospitality in a register. Compliance manager monitors the register for unusual trends. Audit some expenses on a sample basis.
  - Record reports made by personnel under reporting procedures. Monitor success of investigations. Monitor trends in reporting (going up or down?). Any unusual trends?

Monitoring, measurement and evaluation (3)

  - Record training given to personnel. Question personnel on a sample basis on how effective they found training.
  - Undertake surveys of personnel of how effective they believe the ABMS is, and any suggestions for improvement.
- The monitoring should be undertaken on a planned basis, with specific managers made responsible, with the results being reported to top management.
- The reviews by internal audit (9.2), top management (9.3) and the compliance function (9.4) also form part of this evaluation process.
- **ISO 37001: Clause 9.1**
- **WFEO (CAC)/Reviewingandimproving.php**

Internal audit (1)

- The organization shall conduct internal audits at planned intervals to provide information on whether the anti-bribery management system:
  - conforms to:
    - the organization’s own requirements for its ABMS;
    - the requirements of ISO 37001;
  - is being effectively implemented and maintained.

Internal audit (2)

- The organization shall:
  - plan, establish, implement and maintain an audit programme(s);
  - define the audit criteria and scope for each audit;
  - select competent auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
  - ensure that the results of the audits are reported to relevant management, the anti-bribery compliance function, top management and the governing body (if any);

Internal audit (3)

- These audits shall be reasonable, proportionate and risk-based. Such audits shall consist of internal audit processes or other procedures which review procedures, controls and systems for:
  - bribery or suspected bribery;
  - violation of the anti-bribery policy or ABMS requirements;
  - failure of business associates to conform to the applicable anti-bribery requirements of the organization;
  - weaknesses in, or opportunities for, improvement to the ABMS.

Internal audit (4)

- To ensure the objectivity and impartiality of these audit programmes, the organization shall ensure that these audits are undertaken by one of the following:
  - an independent function established for this process; or
  - the anti-bribery compliance function; or
  - an appropriate person from a department or function other than the one being audited; or
  - an appropriate third party; or
  - a group comprising any of the above.
- The organization shall ensure that no auditor is auditing his or her own area of work.

Global Infrastructure Anti-Corruption Centre

Internal audit (5)

- The organization does not need to have its own separate internal audit function. But, it must appoint a suitable, competent and independent function or person with audit responsibility.
- An organization may use a third party to operate the whole or part of its internal audit, provided that the results are reported to an appropriate manager in the organization.
- The frequency of audit will depend on the organization’s requirements. Some sample projects, contracts, procedures, controls and systems may be selected for audit each year.

Internal audit (6)

- The sample selection can be risk-based. E.g. a high bribery risk project could be selected for audit in priority to a low risk project.
- The audits will normally be planned in advance. In some cases, the organization may undertake a surprise audit.
- The intention of the audit is:
  - to provide reasonable assurance that the ABMS has been implemented and is operating effectively;
  - to help prevent and detect bribery;
  - to provide a deterrent to any potentially corrupt personnel (as they will be aware that their department could be audited).
- **ISO 37001: Clause 9.2**
- **WFEO (CAC)/Reviewingandimproving.php**

Compliance function review (1)

- The anti-bribery compliance function shall assess on a continual basis whether the ABMS is:
  - adequate to manage effectively the bribery risks faced by the organization;
  - being effectively implemented.
- The compliance function shall report to the governing body and top management on the adequacy and implementation of the ABMS.
- The frequency of such reports depends on the organization’s requirements, but is recommended to be at least annually.

Compliance function review (2)

- The organization can use a business associate to assist in the review, as long as the other business associate's observations are appropriately communicated to the compliance function, top management and governing body.
- The reviews by internal audit and the compliance function are different, but complementary, in that:
  - the internal audit will review by way of sample specific projects, contracts, procedures etc. at planned intervals;
  - the compliance function review is an on-going overall observation of the effectiveness of the design and implementation of the whole ABMS.

Compliance function review (3)

- The compliance function would choose the best way of undertaking this review, but it could be by:
  - Routinely attending departmental and project meeting where matters with a compliance impact could be discussed.
  - Attending and observing on the effectiveness of personnel training workshops.
  - Periodically reviewing relevant documentation (e.g. risk assessments, due diligence, contracts) to ensure that the ABMS requirements are being observed.
  - Discussing with department heads how well they believe the ABMS is being implemented in their department.
  - Monitoring gifts and hospitality and conflict of interest registers.

Compliance function review (4)

- The compliance function would report to top management:
  - On a routine basis (no less than once per year) on the overall performance of the ABMS; and
  - As necessary if any issues are identified.

- **ISO 37001: Clause 9.4**
- **WFEO (CAC)/Reviewingandimproving.php**

Top management review (1)

- Top management shall review the organization's ABMS, at planned intervals, to ensure its continuing effectiveness.
- The review shall include consideration of:
  - the status of actions from previous management reviews;
  - changes in external and internal issues;
  - information on the performance of the ABMS;
  - opportunities for improvement to the ABMS (10.2).
- Top management shall:
  - take any necessary decisions on improvement to the ABMS.
  - report outcomes to the governing body (if any).

Top management review (2)

- Top management has overall responsibility for the effective design and implementation of the ABMS (as per 5.1.2), so must appropriately monitor and review the ABMS.
- These top management reviews should take place:
  - At planned intervals (at least annually);
  - Whenever a matter requiring immediate top management decision arises.

Top management review (3)

- Top management is likely to take account of matters such as:
  - Compliance function report
  - Internal audit report
  - Reports of bribery or breach of the ABMS
  - Investigation outcomes

- **ISO 37001: Clause 9.3.1**
- **WFEO (CAC)/Reviewingandimproving.php**

Governing body review (1)

- The governing body (if any) shall undertake periodic reviews of the ABMS based on information provided by top management and the anti-bribery compliance function and any other information that the governing body requests or obtains.

- The governing body (if any) has a supervisory responsibility for the ABMS (5.1.1). These governing body reviews should take place:
  - At planned intervals (at least annually);
  - Whenever a matter requiring immediate governing body decision arises.

Governing body review (2)

- The information provided to the governing body is likely to be less comprehensive than that provide to top management. It may comprise only a summary report from top management.
- However, the governing body may also wish to see a report from the compliance function and from internal audit, and any other relevant information to help them undertake their supervisory role.
- If the organization does not have a separate governing body from top management, then only the top management review (9.3.1) will take place.
- **ISO 37001: Clause 9.3.2**

Nonconformity and corrective action (1)

- When a nonconformity occurs, the organization shall:
  - react promptly to the nonconformity, and as applicable:
    - take action to control and correct it;
    - deal with the consequences;
  - evaluate the need for action to eliminate the cause(s) of the nonconformity, so that it does not recur or occur elsewhere, by:
    - reviewing the nonconformity;
    - determining the causes of the nonconformity;
    - determining if similar nonconformities exist, or could occur;
  - implement any action needed;

Nonconformity and corrective action (2)

  - review the effectiveness of any corrective action taken;
  - make changes to the ABMS, if necessary.

- It is vital to the success of the ABMS that, if there is any breach of anti-bribery policy or ABMS, then the organization must take appropriate action to deal with the breach and its consequences.
- It must also rectify any underlying problem with the ABMS which may have contributed to the breach.
- This provision works with 8.10 (investigating and dealing with bribery), 9.3 (management review) and 10.2 (improvement).
- **ISO 37001: Clause 10.1**
- **WFEO (CAC)/Reviewingandimproving.php**

Continual improvement

- The organization shall continually improve the suitability, adequacy and effectiveness of the ABMS.

- The need for an improvement to the ABMS may be identified by:
  - Internal audit (9.2)
  - Compliance function review (10.4)
  - Management review (10.3).

- Whenever the organization identifies the need for improvement in the ABMS, then it should design and implement the improvement.

- **ISO 37001: Clause 10.2.**
- **WFEO (CAC)/Reviewingandimproving.php**

GIACC
Global Infrastructure Anti-Corruption Centre

An overview of ISO 37001

Anti-bribery management system standard

End of Workshop