To all accredited and applicant certification bodies performing the audit and validation of environmental product declarations (EPD)
Att.: Scheme managers

To the associations of conformity assessment bodies

Our ref.: DC2017SSV337 *Milan,* 27/11/2017

Object: **Technical circular N° 28/2017 – Department of Certification and Inspection**
Informative circular regarding accreditation for the certification scheme ISO 37001 for the prevention of bribery/corruption

This communication replaces our **circular N° 33/2016**

Introduction

In specific sectors of many countries, in both the public and private areas, bribery is a widespread phenomenon and, in some commercial and geographical contexts, it is tolerated as a "necessary" part of business.

However growing awareness of the damage caused by bribery, thanks also to the work of the international organizations, of administrative authorities such as ANAC in Italy, and of national magistratures, has led to the definition of action strategies to reduce the risk and impact of the globalization of bribery by means of a wide-ranging normative tool to combat it.

The issue has grown in importance due to a combination of factors:

- the change of legal context in most countries which criminalize and prosecute bribery;
- growing awareness of the damage caused by bribery to people and to economies;
- the attention given by organizations to their social responsibilities and the ethical approach of businesses in Italy (see the Law Decree 231/2001 whereby bribery – active and passive – with respect to the Public Administration Authorities as well as bribery amongst private individuals);
- the financial risk and the risk to reputation which threatens business continuity run by entities which become involved in bribery/corruption.

ISO has therefore developed a specific standard for the prevention of bribery: ISO 37001 "*Anti- Bribery Management Systems*", an operative instrument to be added to the existing ones – both normative and regulatory – of individual countries. In the UK, for example, there is the Bribery Act and there are many measures in place in Italy in the so-called "Anti-corruption Package".

This new standard contributes to the definition of the modalities on the basis of which organizations will be able to declare themselves to be "compliant" concerning bribery prevention; they will be able to introduce preventive measures which are reasonable and proportional to the risk of bribery. The new standard is graded *High Level Structure,* also applicable to the new standards ISO 9001:2015 and ISO 14001:2015, and it is aimed at companies of all sizes and types, public and private.

ISO 37001 specifies the measures and controls which can be adopted by an organization for monitoring company activities for the prevention of bribery. Such measures include an anti-bribery policy pursued by top management, the appointment of an officer, the training of everyone involved (it should be remembered that this process must be constant and be conducted in such a way as to strengthen the organizational culture), specific risk assessment, the definition of procedures such as the regulations covering gifts, and the monitoring of suppliers and commercial partners.

Operative office and administration: Via Tonale, 26 | 20125 Milano - Italy | Tel. +39 02 2100961 | Fax +39 02 21009637
Registered office: Via Guglielmo Saliceto, 7/9 | 00161 Roma - Italy | Tel. +39 06 8440991 | Fax +39 06 8841199
milano@accredia.it | www.accredia.it | VAT: IT 10566361001

Being graded a *high level structure*, the standard can be easily integrated with the management system – such as ISO 9001 – and its goals can be included in the continuous improvement plan.

Compliance with the standard can be certified by third party bodies, possibly removing any criminal responsibility under certain juridical systems.

Normative context

The standard ISO 37001 is based on the *British Standard* BS 10500, the first standard, issued in 2011, to deal with this issue intended to aid public, private and non-governmental organizations of all sizes to prevent acts of bribery by its employees or collaborators, or by someone acting on its behalf, and to promote the diffusion of a company culture based on ethics and good commercial practices.

It should be emphasized that the meaning "bribery", referred to in ISO 37001 includes all conduct and activities which, although formally legal, are relevant (directly or indirectly) in terms of risks of bribery, constituting an obstacle to the pursuit of general interests of public and private organizations (for example the vast not-for-profit world in social cooperation, health, education, private companies undertaking public service tenders and NGOs).

The standard requires the implementation of a number of crucial elements such as:

- a policy for the prevention of corruption, procedures and controls;
- communication of this policy and the relative program to all interested and associated parties;
- leadership, commitment and responsibility;
- a surveillance procedure;
- anti-bribery training;
- risk assessment;
- due diligence for projects and business partners of organizations;
- reporting, monitoring, investigation and review of top management, if present, of the governance;
- requirement for its associates to sign a commitment for the prevention of bribery;
- implementation of financial controls to reduce the risk of bribery;
- corrective actions and continuous improvement.

The audit of the correct implementation of the requirements of the standard must focus on checking the correct definition and application of the procedures of the organization for the management of the so-called critical procedures as emerged from the risk assessment and any due diligences, as set out in the standard. A formal description of the sensitive activities is the first step for carrying out controls by means of audits.

Specific elements of the scheme ISO 37001 with respect to other management systems

Information submitted for audit provides to the CAB an essential element in the certification process. The first certification audit takes place in organizations regarding which the CAB does not have previous data other than data obtained from the declaration of the organizations themselves or from media news sources. This is an especially critical factor because it is not always possible to understand if the company, although it has the right procedures (adopted or not adopted in the application of the legislation in question in terms of corporate crime), constitutes a "pathological environment" concerning bribery. The standard has preventive aims which are incompatible with a pathological business environment requiring correction rather than prevention.

An environment which is contaminated by corrupt practices (with the criminal connections which frequently accompany them) even if there has been no police enquiry, is nonetheless a context where the development and effective application of the management system cannot have a preventive approach, but a corrective one, making it vulnerable as a hostage or a victim of people trying to create an image of apparent legality to the benefit of corrupt practices.

Differently, a company which "spontaneously" declares the possible existence of "critical" situations, or situations which are already at the judicial stage, could be a client which is suitable for certification with

a "corrective" approach as well as one of developing "preventive" practices. In the latter case, the adoption of the anti-bribery management system shall be an action aimed at and in line with a "therapeutic" corporate approach (broad and systemically structured action) which, it is to be hoped (this must be the object of evaluation), will be strongly supported by the management.

We speak about a "broad and systemically structured action" in that the culture of compliance shall be pervasive throughout the organization. Also an anti-bribery management system shall be applied to all company processes; otherwise a grey area is created which may obviate the application of the management system. A global vision of the application of the management system shall involve all organizational processes (also in outsourcing) at least during the phase of preliminary analysis of the context, and only subsequent to this evaluation will it be possible (with adequate reasoning) to single out the processes considered non-critical, for which the risk analysis can be limited to this first level of assessment.
This also means that it is necessary to interpret and attribute weight depending on the case, as indicated in the guidance Annex "A" of the standard, especially as stated in § A.4.1 concerning risk assessment.
A methodology is needed and if one does not exist, debatable situations will occur whereby certification will have areas of weak structural credibility. The time allocated to these audits, consequently, will have to be sufficient to understand if the management system is being effectively applied.

1) Rules of certification

Accreditation standard	UNI CEI EN ISO/IEC 17021:2015
Certification standard	ISO 37001:2016
Audit team competence criteria	See ISO/IEC 17021-9, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 9: Competence requirements for auditing and certification of anti-bribery management systems.* As an example, the competence requirements are considered fulfilled when the audit team contains one, or more than one, auditor (or technical expert/s) who, collectively, fulfill the following requirements: a) Considerable experience, meaningful sector competence and seniority gained from involvement in positions of responsibility in the anti-bribery or legal compliance management system or corporate crime (e.g. S&O, Law Decree 231/2001, Law 190/2012); b) Thorough and documented knowledge of the normative documents (legal, regulatory and regarding good practices) concerning the prevention of active and passive corruption and the management of applicable corporate integrity for the country where such company operates and has business. c) Training: course of 16 hours on ISO 37001 for persons who have already done a 40-hour course on management systems. Points a) and b) are considered fulfilled if the person is certified under accreditation for the anti-bribery scheme or Law Decree 231/2001, or if such person is a lawyer, accountant, audit reviser, ex-magistrate/judge or officer of a judiciary authority with specific experience in anti-bribery matters.
Competence criteria of decision-makers and contract reviewers	See ISO/IEC 17021-9, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 9: Competence requirements for auditing and certification of anti-bribery management systems.* For the decision-maker, knowledge is necessary of the anti-bribery and corporate crime normative documents of the country in which the audit is performed or where the business activities take place, with the influence

	perimeter.
Typologies of bodies/entities which can require certification and possible exclusions	ISO 37001 certification requested by any type of organization, of any size or nature. Certification is issued to only one legal entity and includes all sites, branches, activities and processes effectively undertaken by the organization. Exclusions of processes / personnel involved in the same country are not accepted. It is possible to limit application to specific countries, but the scope of application shall always include sensitive processes[1] undertaken abroad when undertaken under the responsibility and direct control of the organization (e.g. representative offices or branches or mediators). This aspect shall be explicit in the certificate. In cases of groups of companies, when sensitive activities/processes are performed by other companies in the group (head of the group and/or controlled) also abroad, par. 8.5 of ISO 37001 is applicable. Conformity with the requirements of prevention models and systems pursuant to the law (e.g. organization models in accordance with Law Decree 231/2001, PTPC in accordance with Law 190/2012) cannot be certified under accreditation.
Responsibilities of the CB	A certified or certifying organization shall inform without delay its CB when it becomes involved in a critical situation which could compromise the guarantee of the certification of the system (e.g. news of interest to the public, crisis or involvement in legal proceedings concerning bribery/corruption or similar). The organization should also inform the CB without delay of any event related to phenomena of bribery which might have involved any of its staff members, and the consequent actions implemented to contain its effects, the analysis of the root causes and the relative corrective actions. A CB which acquires knowledge directly from the organization or from other sources that the same organization is implicated with responsibility in a scandal or legal proceedings for corrupt actions shall immediately carry out specific investigations. In such cases it is recommended to inform the market of the fact that this organization is "the object of an assessment for specific events" (apart from the obligations of the law and of the regulated markets – for example the stock exchange). Following completion of the analysis, the CB can adopt provisions (e.g. closure and archiving of the assessment/investigation, implementation of provisions as set out in regulations for certification, increase of inspection activities) defined according to the adequacy of the response and the

Note [1] Non-exhaustive list of sensitive activities and processes: finance and control, commercial, agents and sales network, procurement, institutional figures company bodies, management offices and board, internal auditing, licensee management, competitive tenders and authorizations, HR management (including management, selection, hiring and career progress), cash administration and management, purchases, management of gifts and freebies, relations with institutional authorities and control bodies, sponsorship and financial support management, management of disputes and complaints, IT services, security management, control and testing activities.

	strategy adopted by the organization.
Audit times and frequency	The requirements of ISO/IEC 17021-1 are applicable The document IAF MD 05 is applicable Stage 1 audit shall always be done at the organization also in cases where the organization is not a large one. The organization shall provide evidence that it has performed the risk assessment on all processes and activities. **Assessment of equivalent staff** It is necessary to include the total number of staff involved in processes and activities considered sensitive by the organization as well as the processes and positions as stated in note 1. It is possible to perform an adjustment by means of the square root rule (equivalent number=√all personnel in low risk activities) for equivalent staff engaged in the operative and production activities or in the delivery of services only if such processes have a low bribery risk, on the basis of the risk analysis done by the organization, and, in all cases, always with the exclusion of staff involved in sensitive processes and activities as defined in note 1. Similarly, in cases where sensitive processes/activities of the organization are undertaken by outsourcing (e.g. consortiums) the calculation of staff shall include these people too. During the Stage 1 audit the CB shall re-examine the reasonableness of this adjustment according to the identified risks of bribery and shall verify the congruence of the number of personnel communicated by the organization during the drawing up of the contract. This evaluation shall be written in the audit report. **Decrease in audit time of the MS** Reduction factors are not applicable. The table for the EMS scheme is applicable, and for the choice of the right table amongst those reported it is necessary to evaluate the risk level on the basis of the following: ***High risk*** If the organization applying for certification has, in the last 5 years, been involved a legal investigation concerning corruption/bribery. Public Administrations. Public financial entities. Companies either fully or partially under public control. Associations, foundations and private law entities with majority financing by the Public Administration Authorities or entities in which all the members of the administrative and policy bodies are designated by the Public Administration Authorities. Third sector entities (e.g. voluntary organizations, bodies for cooperative activities) and company cooperatives. Category/umbrella associations (including political parties and trade unions) at national representation level. Professional associations and national boards. Companies located in countries with a CPI score of less than or equal to 30. The classification of perceived bribery is made by Transparency International. In cases of companies based in a number of countries coming within the scope of the certificate, the index of the country with the lowest score is applicable.

	Non-SME organizations in the following sectors: • health • construction • banking and insurance • utilities (gas, thermal energy, electricity, water, transport, communications, postal services) ***Medium risk*** Organizations which do not have a high risk level presenting at least one of the following conditions: • receiving public contributions, funds or financing – national and international – at a rate of over 30% of their revenue. • receiving, from public companies, entities or international institutions, any type of payment, including payment deriving from public contracts, at a rate of over 30% of their revenue. • located in countries in possession of a CPI score between 31 and 59[2]. • trading, intermediation and commercial companies not classifiable for their revenue as SMEs. High risk organizations certified for at least three years under EA/IAF MLA certification for ISO 37001 are classified as medium risk. This condition is not applied if the applicant organization for certification has been involved, in the previous five years, in legal proceedings concerning corruption/bribery. ***Low risk***: not coming within the two above categories. ***Limited risk:*** not applicable.
Scope of the certificate	The criteria for formulating the scope of certification are the same as those applied for ISO 9001, with special attention given to the activities performed. It must be clarified in the field of application if the organization has control over other organizations, specifying the characteristics of this control (e.g. capital investments, contractual constraints etc.). It is not necessary to give the IAF sector in the certificate.
IAF documents	All IAF documents relating to the MS are applicable, except in cases as clarified in IAF MD 05. For multisites, IAF documents currently in force are applicable. Sites where processes/activities at risk of bribery are being undertaken cannot be excluded from the sampling base (see note 1 and the risk analysis prepared by the organization).
Audit modalities and records	The audit team shall evaluate with greater frequency, commitment and thoroughness the processes/personnel identified by the organization and/or by the audit team as high risk, giving an explanation in the documentation of the audit, as well as the sensitive processes/personnel as stated in note 1. The audit team shall not limit itself to acknowledging the existence of the risk analysis. It is necessary to start from the definition of bribery which the organization adopted by the organization which cannot be less restrictive than the one required by law. The definition shall be coherent with the context of the analysis. The CB shall evaluate the competence and completeness of the bribery risk analysis, with reference to the applicable requirements of ISO 37001 and the

[2] In 2017 Italy had a score of 47, therefore, at the date of publication of the circular, Italian sites are all rated at least as medium risk.

	robustness of the internal auditing process for bribery cases, which shall be based (planning, programming and performance) on the results of the risk analysis and the mitigation adopted, on the residual risk analysis and on the testing of operative controls. It is also recommended to establish methods for ensuring representative sampling according to the risks, to dedicate enough time not to "abstract" and "paper-based" controls, but rather to the conduct of interviews, precise verifications of transactions, relations with business partners, processes which are at risk, analyses of news in the public domain related to tests on the diffusion of the internal control system. The audit documentation (e.g. audit reports, checklists etc.) shall include, amongst other things, the following; • The boundaries and applicability of the MS (§ 4.3 of ISO 37001) • The definition of bribery/corruption used for the organization, developed on the basis of an analysis of the context • Specific details regarding the activity at risk (describing, in detail, the sensitive processes/activities at risk) • Mapping the people (internal/external) involved in the higher risk activities • The business partners and the type of monitoring of them (type of management used by them with regard to anti-bribery) • Company relations • The specific legal references • Specific description of training activities • The list of orders audited • Analysis of episodes of bribery audited and the countermeasures implemented

2) The process of accreditation

A number of case histories can be presented according to the ACCREDIA accreditations already held by the CB making the application for accreditation or extension.

The requirements of ACCREDIA Regulations RG-01 and RG-01-01 are unchanged for the granting of accreditation or extension.

CBs already accredited to ISO/IEC 17021 do not need to have previously issued certificates in this scheme in order to make an application for accreditation or extension.

The accreditation certificate does not state the relative accreditation sectors.

If the CB is already accredited by other accreditation bodies it is necessary to perform an assessment on a case-by-case basis in accordance with the applicable EA / IAF MLA agreements.

A	CB already accredited for the scheme ISO/IEC 17021-1	Document review of 1 day (preferably performed at the CB's premises). 1 witness assessment of a duration in line with the size of the client organization. ACCREDIA may decide to assess case-by-case the suitability of the organization and of the audit teams proposed for the accreditation and for the subsequent surveillance activities.
B	CB not yet accredited for the scheme ISO/IEC 17021-1, but accredited for other	Document review of 1 day Assessment of 2 days at the head office of the CB.

	accreditation schemes	1 witness assessment of a duration in line with the size of the client organization. ACCREDIA may decide to assess case-by-case the suitability of the organization and of the audit teams proposed for the accreditation and for the subsequent surveillance activities.
C	CB not yet accredited for any scheme	Document review of 1 day Assessment of 4 days at the head office of the CB. 1 witness assessment of a duration in line with the size of the client organization. ACCREDIA may decide to assess case-by-case the suitability of the organization and of the audit teams proposed for the accreditation and for the subsequent surveillance activities.

Documentation to present to ACCREDIA for the document review:

a) Checklist or guideline or instruction prepared by the CB for the audit team;
b) Competence criteria of those performing the contract review, of the auditors and of the decision-makers;
c) CVs of the auditors and decision-makers and justification of their individual qualification;
d) Procedure for setting up and managing audit teams;
e) Declaration/certificate issued by the CB;
f) List of certificates already issued and of future audit activities (necessary information to plan the witness assessment);
g) Applicable contractual procedures / regulations applicable to audits and internal procedures for managing certifications (from the quotation to certification);
h) For CBs NOT accredited to ISO/IEC 17021, apart from the above documents, it is necessary to send all the documentation required for the application for accreditation.

3) Maintenance of'accreditation

For the maintenance of accreditation throughout the cycle of accreditation, apart from specific situations (e.g. handling of complaints and remarks, changes to the certification scheme or to the organization's structure, involvement in legal cases….) the following assessments shall be undertaken:

- If the CB has issued fewer than 50 certificates in the certification scheme 1 witness and 1 on-site assessment are required;
- If the CB has issued between 51 and 200 certificates in the certification scheme, 2 witness and 1 on-site assessment are required;
- If the CB has issued more than 201 certificates in the certification scheme, 2 witness and 2 on-site assessment are required;

We are available for any clarifications.

Emanuele Riva
Director of the Dept. of Certification and Inspection