FAIR BUSINESS®
COMPLIANCE CERTIFICATE
WWW.FAIRBUSINESS-CERTIFICATION.ORG

AUSTRIAN STANDARDS

Certification Scheme Y03

Compliance Management Systems

ISO 19600
ONR 192050
ISO 37001

Issue V5.0:2019-02-07

Austrian Standards plus GmbH

Dr. Peter Jonas
Heinestraße 38
1020 Wien

E-Mail: p.jonas@austrian-standards.at

1 Scope

This certification scheme specifies the procedure to certify a compliance management system (CMS) by the certification body of Austrian Standards (AS+C).

The assessment of a CMS will be conducted based on one or more of the following normative documents:

- ISO 19600:2014-12-15 Compliance management systems – Guidelines
- ONR 192050:2013-02-01 Compliance Management Systems (CMS) – Requirements and guidance for use
- ISO 37001:2016-10-15 Anti-bribery management systems – Requirements with guidance for use

The conduction of a certification procedure is governed by the International Standard ISO/IEC 17021-1[1].

Disclaimer: The application of the above listed normative documents is intended to assist organizations to implement an effective compliance management system, which significantly reduces the likelihood of rule violations by members of the organization. Such CMS, but also certification pursuant to this certification scheme does not guarantee that all members of the certified organization always act in conformity with the law. A compliance management system and its certification cannot prevent wilful misconduct and criminal behaviour of members of an organization entirely. Liability of the Austrian Standards plus GmbH and the auditors is excluded.

2 Criteria for certification of a CMS

For the issue of a certificate the criteria for a compliance management system in accordance with annex A and/or annex B apply.

Applicants may choose to seek certification according to the International Standard ISO 19600, ISO 37001 or according to the Austrian Standard ONR 192050 or any combination of these standards.

3 Certification process

3.1 Application

3.1.1 The applicant shall file an application using the form provided by the certification body.

3.1.2 The applicant shall appoint a contact person for the certification process.

3.1.3 The scope of the intended certification process is determined by the following parameters:

- identification of the legal person who will be the owner of the certificate,
- scope of the desired certificate relating to the organization or sub-units of the organization,
- locations to be certified
- compliance risk areas to be included in the scope of the certificate.

Certification procedures concerning inter-related legal persons (e.g. parent company and subsidiaries) may be combined in one procedure.

Together with the application the applicant shall provide documentation on the management system to be certified. This documentation shall contain the following:

a) the desired scope of the certification;

b) the general features of the applicant organization, including its name and the address(es) of its physical location(s), significant aspects of its process and operations, and any relevant legal obligations;

[1] ISO/IEC 17021-1:2015 Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren - Teil 1: Anforderungen

c) general information, relevant for the field of certification applied for, concerning the applicant organization, such as its activities, human and technical resources, functions and relationship in a larger corporation, if any;

d) information concerning all outsourced processes used by the organization that will affect conformity to requirements;

3.2 Application review

3.2.1 Before proceeding with the audit, the certification body will conduct a review of the application to ensure that:

- the information about the organization is sufficient for the conduct of the audit;
- any known difference in understanding between the certification body and the applicant is resolved;
- the scope of certification sought, the location(s) of the operations, time required to complete audits and any other points influencing the certification activity are taken into account.

3.2.2 Based on this review, the certification body will determine the competences it needs to include in its audit team. The audit team shall be composed of a Lead Auditor and co-auditors as required.

3.3 Initial certification audit

The initial certification audit of a management system shall be conducted in two stages: stage 1 and stage 2.

3.3.1 Audit stage 1

The audit stage 1 shall be conducted to prepare the actual certification audit (audit stage 2 in accordance with clause 3.3.2). The audit stage 1 may either be conducted on-site at the premises of the organisation to be certified or as a remote audit.

The stage 1 audit shall be performed to

a) audit the client's management system documentation;

b) evaluate the client's location and site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for the stage 2 audit;

c) review the client's status and understanding regarding requirements of the standard;

d) collect necessary information regarding the scope of the management system, processes and location(s) of the client;

e) review the allocation of resources for stage 2 audit and agree with the client on the details of the stage 2 audit;

f) evaluate the level of implementation of the management system

Stage 1 audit findings will be documented and communicated to the client, including identification of any areas of concern that could be classified as nonconformity during the stage 2 audit.

3.3.2 Audit stage 2

The purpose of the stage 2 audit is to evaluate the implementation, including effectiveness, of the client's management system. The stage 2 audit shall take place at the site(s) of the client.

3.4 Conducting audits

3.4.1 General

Audits shall include an opening meeting at the start and a closing meeting at the conclusion ot the audit.

Audits shall be attended by an accompanying person of the organisation. The auditor is authorized to exclude the accompanying person from individual parts of the interviews to avoid any influencing.

3.4.2 Multi-site sampling

Where multi-site sampling is used for the audit of a client's management system covering the same activity in various geographical locations, the certification body shall develop a sampling programme to ensure proper audit of the management system.

The rationale for the sampling plan shall be documented for each client.

The certification body specifies the number and sites of the locations to be audited. All functions of the organisation (see 4.4.2.3) have to be covered.

Sites, which are operating in the name and order of the organisation, are to be considered as own sites of the organization. These sites shall be considered within the planning of the audit.

3.4.3 Organizational units to be audited

The following organizational units and functions (if applicable) shall be considered within the framework of the audit:

a. Organizational functions, which are responsible for implementing and maintaining the compliance management system are:

Governing body, for example executive management and supervisory body

- Compliance function, regional and divisional compliance manager/officer
- HR manager including training officers
- Internal Audit, person responsible for internal control systems

b. All functions of the organisation, which are exposed to a certain risk concerning the scope of the compliance management system are:

- Head of sales, procurement, production, persons working with authorities
- All functions and persons identified during audit stage 1

3.4.4 Review of documentation

The following documents and records shall be reviewed within audit stage 2:

- compliance manual and instructions, process descriptions in connection with compliance
- mission statement, Code of Conduct
- written documentation of conduction of compliance-risk assessment and the results
- training materials
- minutes of meetings of the management or the supervisory body of the organization which cover compliance matters
- reports which are related to compliance matters (e.g. reports established by the Compliance Officer addressed to the management of the organization)
- communication concerning compliance to the members of the organization Review reports, e.g. Audit reports
- reports of any compliance violations and depiction of the measures carried out

3.4.5 Audit conclusions

Should nonconformities be detected during an audit, the auditor shall issue appropriate conditions to eliminate them. Nonconformities can be classified as follows:

Minor nonconformity: nonconformity that does not affect the capability of the management system to achieve the intended results.

Major nonconformity: nonconformity that affects the capability of the management system to achieve the intended results.

Note: Nonconformities could be classified as major in the following circumstances:

- if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements;
- a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.

3.4.6 Corrective actions

For every minor nonconformity the organisation shall:

- conduct an analysis of causes and
- create a plan to implement corrective actions

The effective implementation of corrective actions concerning minor nonconformities shall be verified within the following surveillance or recertification audit.

For every major nonconformity the organisation shall:

- conduct an analysis of causes and
- a plan to implement corrective actions

The effective implementation of corrective actions concerning major nonconformities shall be verified either trough

- a review of reports and documentation provided by the organisation or
- within the framework of a full or partial follow-up audit.

It it is not possible to verify the implementation of corrections and corrective actions of any major nonconformity within 6 months after the last day of stage 2, another stage 2 audit has to be performed.

3.4.7 Recommendations on the effectiveness of a management system

Beyond the determination of conformity, the auditors may give recommendations concerning the effectiveness and improvement opportunities of the management system. Recommendations will be documented within the audit report and they have no influence on the issuing the certificate (see 4.6).

3.5 Audit report for initial certification

The audit team shall analyse all information and audit evidence gathered during the stage 1 and stage 2 audits to review the audit findings and agree on the audit conclusions.

The information provided by the audit team to the certification body for the certification decision shall include, as a minimum,

a) the audit report, including comments on the nonconformities and, where applicable, the correction and corrective actions taken by the organisation,

b) documentation of the recommendations given by the audit team

c) a recommendation whether or not to grant certification, together with any conditions or observations.

3.6 Certification decision

3.6.1 Evaluation process

Prior to making a decision for granting certification, the certification body has to evaluate the following:

a) the information provided by the audit team is sufficient with respect to the certification requirements and the scope for certification;

b) for any major nonconformities, it has reviewed, accepted and verified the correction and corrective actions;

c) for any minor nonconformities it has reviewed and accepted the client's plan for correction and corrective action.

3.6.2 Issue of the certificate

Based on the audit conclusions and the recommendation by the lead auditor, the certification body will decide on the issue of the certificate.

The scope of a certificate is determined by the following:

- identification of the legal person who is the holder of the certificate,
- scope in terms of organization or –if applicable- sub-units of the organization,
- locations of the certified organization,
- the compliance risks examined within the scope.

The certificate has a validity of 3 years provided that the requirements to maintain the certificates are being met.

3.7 Surveillance activities

In order to maintain the certificate, surveillance audits shall be conducted on a yearly base.

Surveillance audits are on-site audits, but are not necessarily full system audits, and shall be planned together with the other surveillance activities so that the certification body can maintain confidence that the certified management system continues to fulfil requirements between recertification audits. The surveillance audit programme shall include, at least:

a. internal audits and management review;
b. a review of actions taken on observations, remarks and nonconformities identified during the previous audit;
c. effectiveness of the management system with regard to achieving the certified client's objectives;
d. progress of planned activities aimed at continual improvement;
e. continuing operational control;
f. review of any changes, and
g. use of marks and/or any other reference to certification.

The auditor will prepare a surveillance audit report. This report provides the base for the decision by the certification body to maintain the certificate.

3.8 Recertification

3.8.1 Recertification process

For the renewal of the certificate the following activities shall be conducted:

1. review of previous surveillance audit reports and review of performance of the management system over the most recent certification cycle,
2. conducting a recertification audit (see 4.8.2).

In case of significant organizational changes of the management system or the organizational environment, the certification body is allowed to arrange a further Audit stage 1 (see 4.4.1).

3.8.2 Recertification audit

The recertification audit shall include an on-site audit that addresses the following:

a. the effectiveness of the management system in its entirety in the light of internal and external changes and its continued relevance and applicability to the scope of certification;

b. demonstrated commitment to maintain the effectiveness and improvement of the management system in order to enhance overall performance;

c. whether the operation of the certified management system contributes to the achievement of the organization's policy and objectives.

When, during a recertification audit, instances of nonconformity or lack of evidence of conformity are identified, the certification body will define time limits for correction and corrective actions to be implemented prior to the expiration of certification.

3.8.3 Audit report for recertification

The certification body will make decisions on renewing certification based on the results of the recertification audit, as well as the results of the review of the system over the period of certification and complaints received from users of certification.

3.8.4 Issuing the certificate

When recertification activities are successfully completed prior to the expiry date of the existing certification, the expiry date of the new certification can be based on the expiry date of the existing certification. The issue date on a new certificate shall be on or after the recertification decision.

In case the recertification audit is not completed or the implementation of corrective actions for any major nonconformity prior to the expiry date of the certification is not verified, then recertification shall not be recommended and the validity of the certification shall not be extended.

Following expiration of certification, the certification body can restore certification within 6 months provided that the outstanding recertification activities are completed, otherwise at least a stage 2 shall be conducted. The effective date on the certificate shall be on or after the recertification decision and the expiry date shall be based on prior certification cycle.

3.9 Change of normative documents

Changes of the underlying normative documents on which the certification is based on will be communicated by the certification body to certificate holders immediately.

The certificate holder will be granted a period of 12 months to adapt its CMS according to the changes in the normative document(s). Evidence of compliance with the new requirements shall be provided as part of a surveillance audit. Upon successful proof, the certificate will be re-issued with a new reference to the changed normative documents.

3.10 Amendments to the scope of certificates

Should the certificate holder wish to extend the scope of his certificate in relation to further organizational units or compliance-related risks, he must request this in writing to the certification body. The certification body will specify the necessary steps (examination of documents and / or supplementary audits) for the expansion of the scope.

Should the certificate holder wish to reduce the scope of his certificate in relation to the certified organizational units and/or compliance related risks, he shall inform the certification body in writing. The certification body will reduce the scope of the certificate accordingly. From this point, the organization must not make any statements in relation to those organizational units and/or compliance risks which have been removed from the scope of the certificate. The verification of the relevant obligations of the certificate holder will be part of the following surveillance audit.

Changes of certificates related to formal specifications of the certificate holder (such as changes in the company name or address) must be notified in writing of the certification body. The certification body will issue an amended certificate without technical examination.

In case that the legal person who holds the certificate will be changed, a new certification procedure shall be carried out.

3.11 Withdrawal of certificates

The certificate becomes invalid immediately after termination of the contract by the certificate holder or withdrawal by AS+C.

The certificate is withdrawn by AS + C when

- the conditions for issuing the certificate are no longer met,
- the client refuses to accept the necessary surveillance activities in a timely manner
- the client does not meet the requirements of corrective actions requested,
- the client refuses to accept audits to check on corrective actions if required by the certification body,
- the conformity mark is used by the certificate holder in an abusive manner,

If the certificate is withdrawn, AS + C informs the certificate holder thereof in writing.

After withdrawal of a certificate of any reference to the invalid certificate is not permitted.

Annex A Criteria in accordance with ISO 19600 and ISO 37001

ISO 19600 Clause 4 Context of the organisation

ISO 19600 Clause 4.1 Understanding the organization and its context

A.4.1 The organization has determined external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its compliance management system.

ISO 19600 Clause 4.2 Understanding the needs and expectations of interested parties

A.4.2 The organization has determined:

- the interested parties that are relevant to the compliance management system; and
- the requirements of these interested parties.

ISO 19600 Clause 4.3 Determining the scope of the compliance management system

A.4.3 The organization has determined the boundaries and applicability of the compliance management system to establish its scope.

NOTE: The scope of the compliance management system specifies the geographical and/or organizational boundaries as well as the compliance risks to which the compliance management system will apply.

A.4.4 The scope is available as documented information.

ISO 19600 Clause 4.4 Principles of good governance

A.4.5 The organisation has established a compliance management system which meets the following governance principles:

1. direct access of the compliance function to the governing body;
2. independence of the compliance function;
3. appropriate authority and adequate resources allocated to the compliance function.

ISO 19600 Clause 4.5 Compliance obligations

A.4.6 The organization systematically identifies its compliance obligations and their implications for its activities.

A.4.7 The organization documents its compliance obligations.

A.4.8 Processes are in place to identify new and changed laws, regulations, codes and other compliance obligations.

A.4.9 Processes are in place to evaluate the impact of the identified changes and implement any necessary changes in the management of the compliance obligations.

ISO 19600 Clause 4.6 Identification, analysis and evaluation of compliance risks

A.4.10 The organization identifies and evaluates its compliance risks by relating its compliance obligations to its activities, products, services and relevant aspects of its operations.

A.4.11 The organization analyses compliance risks by considering causes and sources of noncompliance and the severity of their consequences, as well as the likelihood that noncompliance and associated consequences can occur.

A.4.12 Compliance risks are reassessed periodically and whenever there are:

- new or changed activities, products or services;
- changes to the structure or strategy of the organization;
- significant external changes;
- changes to compliance obligations ; and
- noncompliance(s).

ISO 19600 Clause 5 Leadership

ISO 19600 Clause 5.1 Leadership and commitment

A.5.1 The governing body and top management demonstrate leadership and commitment with respect to the compliance management system by:

1. establishing and upholding the core values of the organization;
2. communicating the importance of an effective compliance management system and the importance of conforming to the compliance management system requirements.

ISO 19600 Clause 5.2 Compliance policy

A.5.2 The governing body and top management of the organization have established a compliance policy.

A.5.3 The compliance policy articulates:

1. the scope of the compliance management system;
2. the application and context of the system;
3. the responsibility for managing and reporting compliance issues;
4. the required standard of conduct and accountability; and
5. the consequences of noncompliance.

A.5.4 The compliance policy is:

1. available as documented information;
2. communicated clearly within the organization and be made readily available to all employees;
3. updated, as required.

ISO 19600 Clause 5.3 Organizational roles, responsibilities and authorities

Governing body and top management

A.5.5 The governing body and top management ensure that the commitment to compliance is maintained and that non-compliance and noncompliant behaviour are dealt with appropriately.

A.5.6 Compliance responsibilities are included in position statements of top managers.

A.5.7 A compliance function is appointed.

Top management

A.5.8 Adequate and appropriate resources are allocated to the compliance management system.

A.5.9 Responsibilities and authorities for relevant roles are assigned and communicated within the organization.

A.5.10 Top management is measured against compliance key performance measures or outcomes.

Compliance function

A.5.11 The compliance function has authority and responsibility for the compliance management system.

A.5.12 The compliance function has authority to act independently.

A.5.13 The compliance function has no conflict of interest and has demonstrated:

1. effective communication and influencing skills;
2. relevant competence.

A.5.14 The compliance function has support from and direct access to governing body and top management.

A.5.15 The compliance function has access to:

1. senior decision-makers and the opportunity to contribute early in the decision-making processes;
2. all levels of the organization;
3. all information and data needed to perform the compliance tasks; and
4. expert advice on relevant laws, regulations, codes and organizational standards.

A.5.16 The compliance function is responsible for establishing compliance performance indicators and monitoring and measuring compliance performance.

Management responsibilities

A.5.17 Management is responsible for compliance within its area of responsibility.

Employee responsibility

A.5.18 Employees fulfil their obligations in the CMS.

ISO 37001 Clause 5.3.3 Delegated decision-making

AB.5.1 Where top management delegates to personnel the authority for the making of decisions in relation to which there is more than a low risk of bribery, the organization has established and maintains a decision-making process or has set of controls which requires that the decision process and the level of authority of the decision-maker(s) are appropriate and free of actual or potential conflicts of interest.

AB.5.2 Top management has ensured that these processes are reviewed periodically as part of its role and responsibility for implementation of, and compliance with, the anti-bribery management system.

ISO 19600 Clause 6 Planning

ISO 19600 Clause 6.1 Actions to address compliance risks

A.6.1 The organisation plans its compliance management system to:

1. assure the compliance management system achieves its intended outcome(s);
2. prevent, detect and reduce undesired effects;
3. achieve continual improvement.

A.6.2 The organization plans:

1. actions to address its compliance risks and
2. how to:

   — integrate and implement the actions into its compliance management system processes;

   — evaluate the effectiveness of these actions.

ISO 19600 Clause 6.2 Compliance objectives

A.6.3 The organization has established its compliance management system objectives at relevant functions and levels.

A.6.4 The compliance objectives:

1. are consistent with the compliance policy;
2. are measurable (if practicable);
3. take into account applicable requirements;
4. are monitored;
5. are communicated;
6. are updated and/or revised as appropriate.

ISO 19600 Clause 7 Support

ISO 19600 Clause 7.2 Competence and training

A.7.1 The organization has:

1. determined the necessary competence of person(s) doing work under its control that affects its compliance management system performance;
2. ensured that these persons are competent on the basis of appropriate education, training, and/or work experience.

A.7.2 The organization retains appropriate documented information including evidence of competence.

A.7.3 Education and training of employees is:

1. tailored to the obligations and compliance risks related to the roles and responsibilities of the employee;
2. undertaken at commencement with the organization and on-going;
3. assessed for effectiveness;
4. updated as required; and
5. recorded.

A.7.4 Compliance retraining is considered whenever there is a:

1. change of position or responsibilities;
2. changes in internal processes, policies and procedures;
3. changes in organization structure;
4. change in the compliance obligations;
5. change in activities, products or services; and
6. issues arising from monitoring, auditing, reviews, complaints and noncompliances.

7. **ISO 37001 Clause 7.2.2 Employment process**
8. **AB.7.1** In relation to all of its personnel, the organization has implemented procedures such that:
9. a) conditions of employment require personnel to comply with the anti-bribery policy and anti-bribery management system, and give the organization the right to discipline personnel in the event of non-compliance;
10. b) within a reasonable period of their employment commencing, personnel receive a copy of, or are provided with access to, the anti-bribery policy and training in relation to that policy;
11. c) the organization has procedures which enable it to take appropriate disciplinary action against personnel who violate the anti-bribery policy or anti-bribery management system;
12. d) personnel will not suffer retaliation, discrimination or disciplinary action (e.g. by threats, isolation, demotion, preventing advancement, transfer, dismissal, bullying, victimization, or other forms of harassment) for:
13. 1) refusing to participate in, or turning down, any activity in respect of which they have reasonably judged there to be a more than low risk of bribery that has not been mitigated by the organization; or

14. 2) concerns raised or reports made in good faith, or on the basis of a reasonable belief, of attempted, actual or suspected bribery or violation of the anti-bribery policy or the anti-bribery management system (except where the individual participated in the violation).
15. **AB.7.2** In relation to all positions which are exposed to more than a low bribery risk and to the anti-bribery compliance function, the organization has implemented procedures which provide that:
16. a) due diligence is conducted on persons before they are employed, and on personnel before they are 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 management system requirements;
17. b) performance bonuses, performance targets and other incentivizing elements of remuneration are reviewed periodically to verify that there are reasonable safeguards in place to prevent them from encouraging bribery;
18. c) such personnel, top management, and the governing body (if any), file a declaration at reasonable intervals proportionate with the identified bribery risk, confirming their compliance with the anti-bribery policy.

ISO 19600 Clause 7.3 Awareness

A.7.5 Persons doing work under the organization's control are aware of:

1. the compliance policy;
2. their role and contribution to the effectiveness of the compliance management system performance; and
3. the implications of not conforming with the compliance management system requirements.

A.7.6 Top management has assumed responsibility for:

1. encouraging all employees to accept the importance of achieving the compliance objectives;
2. encouraging employees to make suggestions that facilitate continual improvement in compliance performance;
3. ensuring that operational objectives and targets do not compromise compliance behaviour.

ISO 37001 7.3 Awareness and training

AB.7.3 The organization provides adequate and appropriate anti-bribery awareness and training to personnel. Such training addresses the following issues, as appropriate, taking into account the results of the bribery risk assessment:

a) the organization's anti-bribery policy, procedures and management system, and their duty to comply;

b) the bribery risk and the damage to them and the organization which can result from bribery;

c) the circumstances in which bribery can occur in relation to their duties, and how to recognize these circumstances;

d) how to recognize and respond to solicitations or offers of bribes;

e) how they can help prevent and avoid bribery and recognize key bribery risk indicators;

f) their contribution to the effectiveness of the management system, including the benefits of improved anti-bribery performance and of reporting suspected bribery;

g) the implications and potential consequences of not conforming with the anti-bribery management system requirements;

h) how and to whom they are able to report any concerns (see 8.9);

i) information on available training and resources.

AB.7.4 Taking into account the bribery risks identified, the organization has implemented procedures addressing anti-bribery awareness and training for business associates acting on its behalf or for its benefit, and which could pose more than a low bribery risk to the organization. These procedures identify the business associates for which such awareness and training is necessary, its content, and the means by which the training shall be provided.

ISO 19600 Clause 7.4 Communication

A.7.7 The organization has adopted appropriate methods of communication to ensure that the compliance message is heard and understood by all employees on an on-going basis.

A.7.8 The communication sets out the organization's expectation of employees.

A.7.9 An approach to external communication, targeting all interested parties, has been adopted.

ISO 19600 Clause 7.5 Documented information

A.7.10 Creating and updating documented information the organization has ensured appropriate:

1. identification and description;
2. format and media; and
3. review and approval for suitability and adequacy.

A.7.11 Documented information is controlled to ensure:

1. it is available, accessible and suitable for use, and
2. it is adequately protected.

ISO 19600 Clause 8 Operation

ISO 19600 Clause 8.1 Operational planning and control

A.8.1 The organization has implemented and controls the processes needed to meet compliance obligations by:

1. defining the objectives of the processes;
2. establishing criteria for the processes;
3. implementing control of the processes in accordance with the criteria; and
4. keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

ISO 19600 Clause 8.2 Establishing controls and procedures

A.8.2 Controls are in place to manage the compliance obligations and associated compliance risks.

A.8.3 Controls are periodically evaluated and tested to ensure their continuing effectiveness.

ISO 19600 Clause 8.3 Outsourced Processes

A.8.4 Outsourced processes are controlled and monitored.

A.8.5 If there is any outsourcing of activities, the organization undertakes due diligence to ensure that its standards and commitment to compliance will not be lowered.

A.8.6 The organization considers compliance risks related to other third-party related processes, such as supply of goods and services and distribution of products, and put controls in place as necessary.

ISO 37001 Clause 8.2 Due diligence

AB.8.1 Where the organization's bribery risk assessment has assessed a more than low bribery risk in relation to:

a) specific categories of transactions, projects or activities,

b) planned or on-going relationships with specific categories of business associates, or

c) specific categories of personnel in certain positions,

the organization has assessed the nature and extent of the bribery risk in relation to specific transactions, projects, activities, business associates and personnel falling within those categories.

AB.8.2 This assessment includes any due diligence necessary to obtain sufficient information to assess the bribery risk.

AB.8.3 The due diligence is updated at a defined frequency, so that changes and new information can be properly taken into account.

ISO 37001 Clause 8.3 Financial controls

AB.8.4 The organization has implemented financial controls that manage bribery risk.

NOTE: Financial controls are those in accordance with ISO 37001 clause A.11.

ISO 37001 Clause 8.4 Non-financial controls

AB.8.5 The organization has implemented non-financial controls that manage bribery risk with respect to such areas as procurement, operational, sales, commercial, human resources, legal and regulatory activities.

NOTE: Non-financial controls are those in accordance with ISO 37001 clause A.12.

ISO 37001 Clause 8.5 Implementation of anti-bribery controls by controlled organizations and by business associates

AB.8.6 The organization has implemented procedures which require that all other organizations over which it has control either:

a) implement the organization's management system, or

b) 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, taking into account the bribery risk assessment.

AB.8.7 In relation to business associates not controlled by the organization for which the bribery risk assessment or due diligence 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 has implemented procedures as follows:

a) the organization has determined whether the business associate has in place anti-bribery controls which manage the relevant bribery risk;

b) 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:

1) where practicable, the organization has required the business associate to implement anti-bribery controls in relation to the relevant transaction, project or activity; or

2) where it is not practicable to require the business associate to implement anti-bribery controls, this is a factor taken into account in evaluating the bribery risk of the relationship with this business associate and the way in which the organization manages such risks.

ISO 37001 Clause 8.6 Anti-bribery commitments

AB.8.8 For business associates which pose more than a low bribery risk, the organization has implemented 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.

ISO 37001 Clause 8.7 Gifts, hospitality, donations and similar benefits

AB.8.9 The organization has implemented 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.

ISO 37001 Clause 8.8 Managing inadequacy of anti-bribery controls

AB.8.10 Where the due diligence 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 to enable the organization to manage the relevant bribery risks, the organization has:

a) in the case of an existing transaction, project, activity or relationship, taken 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;

b) in the case of a proposed new transaction, project, activity or relationship, postponed or declined to continue with it.

ISO 37001 Clause 8.9 Raising concerns

AB.8.11 The organization has implement procedures which:

a) encourage and enable persons to report in good faith or on the basis of a reasonable belief attempted, suspected and actual bribery, or any violation of or weakness in the anti-bribery management system, to the anti-bribery compliance function or to appropriate personnel (either directly or through an appropriate third party);

b) except to the extent required to progress an investigation, require that the organization treats reports confidentially, so as to protect the identity of the reporter and of others involved or referenced in the report;

c) allow anonymous reporting;

d) prohibit retaliation, and protect those making reports from retaliation, after they have in good faith, or on the basis of a reasonable belief, raised or reported a concern about attempted, actual or suspected bribery or violation of the anti-bribery policy or the anti-bribery management system;

e) enable personnel to receive advice from an appropriate person on what to do if faced with a concern or situation which could involve bribery.

AB.8.12 The organization has ensured 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.

ISO 37001 Clause 8.10 Investigating and dealing with bribery

AB.8.13 The organization has implemented procedures that:

a) require assessment and, where appropriate, investigation of any bribery, or violation of the anti-bribery policy or the anti-bribery management system, which is reported, detected or reasonably suspected;

b) require appropriate action in the event that the investigation reveals any bribery, or violation of the anti-bribery policy or the anti-bribery management system;

c) empower and enable investigators;

d) require co-operation in the investigation by relevant personnel;

e) require that the status and results of the investigation are reported to the anti-bribery compliance function and other compliance functions, as appropriate;

f) require that the investigation is carried out confidentially and that the outputs of the investigation are confidential.

AB.8.14 Investigations are be carried out by, and reported to, personnel who are not part of the role or function being investigated.

ISO 19600 Clause 9 Performance evaluation

ISO 19600 Clause 9.1 Monitoring, measurement, analysis and evaluation

A.9.1 The compliance management system is monitored to ensure compliance performance is achieved.

A.9.2 A plan for continual monitoring has been established.

A.9.3 The organization retains appropriate documented information as evidence of the results of monitoring.

A.9.4 Procedures are implemented for seeking and receiving feedback on the compliance performance from a range of sources.

A.9.5 Measureable indicators are in place to quantify the compliance performance of the organisation.

A.9.6 It is ensured that the governing body, management and the compliance function are informed on the performance of the compliance management system and of its continuing adequacy.

A.9.7 The internal reporting arrangements ensure that:

1. appropriate criteria and obligations for reporting are set out;
2. timelines for regular reporting are established;
3. an exception reporting system is in place which facilitates ad hoc reporting of emerging noncompliance;
4. systems and processes are in place to ensure the accuracy and completeness of information;
5. information is provided to the correct functions or areas of the organization to enable preventative, corrective and remedial action to be taken; and
6. there is sign-off on the accuracy of reports to the governing body, including by the compliance function.

A.9.8 All noncompliance are appropriately reported.

A.9.9 Employees are encouraged to respond to and report noncompliance.

A.9.10 Records of the organization's compliance activities are maintained. Record-keeping include recording and classifying complaints, disputes and alleged noncompliance and the steps taken to resolve them.

A.9.11 Records are stored in a manner that ensures they remain legible, readily identifiable and retrievable.

A.9.12 Records are protected against any addition, deletion, modification, unauthorized use or concealment.

ISO 19600 Clause 9.2 Audit

A.9.13 The organization conducts audits at planned intervals to provide information on whether the compliance management system:

1. conforms to its own criteria and to the criteria of ISO 19600; and
2. is effectively implemented and maintained.

A.9.14 The organization:

1. has implemented an audit programme;
2. has defined audit criteria and scope for each audit;
3. selects auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
4. ensures that the results of the audits are reported to relevant management; and
5. retains documented information on the audit results.

ISO 19600 Clause 9.3 Management review

A.9.15 Top management reviews the compliance management system, at planned intervals.

A.9.16 Documented information as evidence of the results of management reviews is retained.

ISO 37001 Clause 9.4 Review by anti-bribery compliance function

AB.9.1 The anti-bribery compliance function assesses on a continual basis whether the anti-bribery management system is:

a) adequate to manage effectively the bribery risks faced by the organization;

b) being effectively implemented.

AB.9.2 The anti-bribery compliance function reports at planned intervals, and on an ad hoc basis, as appropriate, to the governing body (if any) and top management, or to a suitable committee of the governing body or top management, on the adequacy and implementation of the anti-bribery management system, including the results of investigations and audits.

ISO 19600 Clause 10 Improvement

A.10.1 When a noncompliance occurs, the organization:

1. reacts to the noncompliance;
2. evaluates the need for action to eliminate the root causes of the noncompliance;
3. implements any action needed;
4. reviews the effectiveness of any corrective action taken; and
5. makes changes to the compliance management system, if necessary.

A.10.2 Documented information is retained as evidence of:

1. the nature of the noncompliances and any subsequent actions taken; and
2. the results of any corrective action.

A.10.3 An escalation process has been be adopted and communicated to ensure all noncompliances are raised, reported and eventually escalated to relevant management and that the compliance function is informed.

A.10. 4 A mechanism for employees and/or others is in place to report suspected or actual misconduct or violations of the compliance obligations on a confidential basis and without fear of retaliation.

Annex B Criteria in accordance with ONR 192050

B.1 Role of the organization's top management

B.1.1 The conduct of the organization's top management shall be in line with the CMS.

B.1.2 The organization's top management shall ensure that the CMS is developed, implemented, maintained, regularly reviewed, documented and, if necessary, improved.

B.1.3 The organization's top management shall ensure that the required conditions for the CMS are created within the framework of both structural and process organization.

B.1.4 The organization's top management shall ensure that the resources needed for the CMS are made available as a function of the results of the compliance risk assessment.

B.1.5 The organization's top management shall ensure that, based on the results of the compliance risk assessment, measures are defined and implemented to reduce compliance risks.

B.1.6 The organization's top management shall demonstrably communicate the CMS and its contents to the organization members to the extent required. To this effect, the relevant materials and documents shall be made accessible to the organization members.

B.2 Compliance Officer (CO)

B.2.1 The tasks of a CO shall be performed either by a member of the organization's top management or by one or more other organization members.

B.2.2 The CO shall advise and support top management in the development, introduction, maintenance, regular review and improvement of the CMS.

B.2.3 The CO shall be appointed in writing by top management and accept this appointment (the appointment document has to contain a description of the CO's tasks).

B.2.4 The CO shall have the powers required for fulfilling his/her tasks.

B.2.5 The CO shall not be subject to instructions with regard to his/her tasks.

B.2.6 The CO shall have the possibility to communicate directly with top management.

B.2.7 The CO shall have the knowledge required for his/her activities and be essentially familiar with the organization's activities.

B.2.8 The CO shall have knowledge of compliance-related processes, regulations, compliance risk assessments, monitoring and auditing in relation to the organization.

B.2.9 The CO shall regularly – at least once a year – prepare a compliance report. This report shall be brought to the attention of the organization's top management.

B.3 Compliance risk assessment and measures

B.3.1 Within the framework of the CMS, the compliance risk has to be assessed and documented in accordance with a defined procedure.

B.3.2 This procedure shall comprise at least the following steps:

– identification of compliance-related processes with a view to the regulations;

– identification of compliance risks and assessment by their probability of occurrence and consequences;

– prioritization and, based thereon, implementation of measures.

B.3.3 The compliance risk assessment shall cover all the organization members.

B.3.4 The results of compliance risk assessment shall be documented and brought to the attention of the organization's top management.

B.3.5 The compliance risk assessment shall be performed regularly and at least once a year.

B.4 Instructions

B.4.1 The CMS shall include binding instructions documented in writing that have the purpose of preventing or, if applicable, detecting breaches of the regulations.

B.4.2 The instructions shall be derived from the results of the compliance risk assessment.

B.4.3 The instructions shall regulate how compliance-related processes are to be handled.

B.4.4 Before filling key positions identified on the basis of the compliance risk assessment, the candidates have to be reviewed with regard to compliance.

B.5 Training

B.5.1 The CMS shall make sure that the organization members are regularly trained on the basis of the results of the compliance risk assessment.

B.5.2 The method, scope and intensity of training shall be adjusted to the tasks of the organization members in question.

B.5.3 Organization members holding key positions shall be trained in face-to-face courses.

B.5.4 Training shall be documented. This documentation shall include the following minimum information: participants, date, duration and contents of training measures.

B.6 Effectiveness of the CMS

B.6.1 The CMS shall include activities for monitoring the observance of instructions in an appropriate frequency.

B.6.2 The CMS shall include random or incident-related checks of compliance-related processes.

B.6.3 The adequacy, suitability and effectiveness of the CMS shall be reviewed regularly, for example by monitoring the observance of instructions and verifying the performance of training. The review shall be performed in an objective and impartial way.

B.6.4 Organization members shall have the possibility to report breaches of regulations.

– Upon request of the reporting member, his/her identity shall be kept confidential unless there are legal disclosure obligations.
– It shall be possible to file anonymous reports.
– Sanctions shall not be imposed on organization members reporting breaches of regulations in good faith unless they were involved in such a breach.
– The possibility of filing such reports shall be brought to the attention of the organization members.
– All reported breaches of regulations shall be followed up on.

B.6.5 A procedure shall be defined for following up on breaches of regulations detected.

B.6.6 Sanctions and, if necessary, measures to improve the CMS shall be defined, implemented and documented for cases in which breaches of regulations are discovered. This shall be reported to the organization's top management in a timely fashion.

B.7 Communication

B.7.1 The organization's top management shall regularly state its commitment to compliance and communicate this through channels that are adequate for the organization.

B.7.2 The organization members shall be regularly informed of changes in the CMS that are relevant for them.