Code of Good Practice for Assuring Conformance with Social and Environmental Standards

Version 1.0 – September, 2012

Table of Contents

Foreword

The ISEAL Alliance is an international non-profit organisation that codifies best practice for the design and implementation of social and environmental standards systems. ISEAL Alliance members are leading organisations in social and environmental standard setting and certification, and are committed to compliance with ISEAL Codes of Good Practice. Further information about the ISEAL Alliance and its membership is available at www.isealalliance.org.

ISEAL works from the premise that sustainability standards systems that are effective and accessible can bring about significant positive social, environmental, and economic impacts. The continuing strong growth in size and scope of sustainability standards is an indication of the influential role that these systems can play in bringing about positive change on a global scale. However, it also highlights the pressing need for a broadly shared understanding of good operating practices for the sustainability standards movement as a whole.

Since 2004, ISEAL has been facilitating international consultations to determine what good practice should look like for social and environmental standards systems. Through this work, we aim to maintain an evolving suite of credibility tools that support the effective implementation of sustainability standards systems. Various Codes of Good Practice each contribute in part to that goal. This currently includes Codes of Good Practice in final form focused on standard-setting procedures and measuring impacts of standards systems, as well as a draft Code on assurance practices.

Code Review Process

Subsequent to the first revision of the ISEAL Code of Good Practice for Assuring Compliance with Social and Environmental Standards (the Assurance Code), the public review and revision process will take place every four years. The next review is scheduled for 20xx. This process is managed by the ISEAL Stakeholder Council and includes at least the following steps:

- establishment of a Steering Group to undertake the revision;
- a public consultation period of 60 days, incorporating comments previously received;
- synopsis of how comments were addressed and proposal on revision prepared by the Steering Group;
- a second consultation period of 30 or 60 days, where outstanding issues exist;
- synopsis of how the additional comments were addressed and proposal for a second revision prepared by the Steering Group;
- recommendation by the ISEAL Stakeholder Council whether to approve proposed revision, with or without amendments, based on the results of the consultation;
- decision whether to approve the Code taken by the ISEAL Board and based on the quality of the process followed; and
- one year transition period for compliant standard-setting organisations.

The ISEAL Alliance welcomes comments on the Assurance Code at any time. Comments will be incorporated into the next review process. Please submit comments by mail or email to the address

below. All enquiries and comment submissions related to the Assurance Code can be made through the following central focal point:

ISEAL Alliance
secretariat@isealalliance.org
www.isealalliance.org/programs
The Wenlock Centre
50-52 Wharf Road
London N1 7EU
United Kingdom

Introduction

Purpose of the Assurance Code

The purpose of the ISEAL Assurance Code is to provide a framework for assurance that supports standards systems to achieve their social and environmental objectives and to improve the effectiveness of their assurance models. To achieve this purpose, the Assurance Code sets out minimum criteria for implementation of the assurance process while also recognising that different assurance models can be effective for different purposes. The Assurance Code builds on a set of principles for effective assurance and describes how these principles are applied in practice.

The Assurance Code references and builds on existing normative guidance for good practices in certification and accreditation. The intent of the Assurance Code is not to duplicate existing requirements but to provide additional guidance on practices that are relevant to the implementation of social and environmental standards systems.

Within sustainability standards systems there are many different models of assurance that can be credible and appropriate for specific purposes. Assurance models that are fit for the purposes they serve are capable of scaling-up while at the same time continuing to serve as effective tools to mitigate the risks of non-conformance. Different models of assurance will fulfil the principles of assurance in different ways, depending on the needs of the users of the standards system.

ISEAL Codes of Good Practice build credibility

The goal of all ISEAL Codes of Good Practice is to assist standards systems to deliver positive social and environmental impact. ISEAL Codes of Good Practice work together to achieve this:

- The Standard-Setting Code supports transparency, consistency, and relevance of the standard;
- The Impacts Code supports standards systems to measure and improve the results of their work and to ensure that standards are delivering the desired impact; and
- The Assurance Code helps to encourage conformance by clients and instil public confidence in the results of assurance, thereby increasing the use of the standard.

Individually, each Code is useful in strengthening a component of a standards system. However, only when the Codes are taken together do they provide end users and other interested parties with confidence in the effectiveness of the standards system as a whole.

1 Referenced Publications

ISO 17000:2004 Conformity assessment – Vocabulary and general principles

ISO 17011:2004 Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies

ISO 17021:2011 Conformity assessment -- Requirements for bodies providing audit and certification of management systems

ISO FDIS 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services

ISO DIS 17067 Conformity assessment -- Fundamentals of product certification

ISO 26000:2010 Guidance on Social Responsibility

ISO 31010:2009 Risk management – Risk assessment techniques

MSC Chain of Custody Methodology, v7 (2010)

2 Scope

The ISEAL Assurance Code specifies normative requirements for carrying out assurance of conformance with social and environmental standards. The Code defines a minimum set of normative requirements that are applicable to all assurance models. It is the responsibility of the standards system owner to ensure that these requirements are complied with throughout the assurance system.

The Assurance Code focuses primarily on those aspects of the assurance process that are not adequately addressed elsewhere in normative documents. It does not include the basic requirements for certification and accreditation that are described in ISO 17000 series standards, except where there is some inconsistency between ISO 17065 and ISO 17021.

The Assurance Code includes a number of criteria that are identified as Optional Good Practice. These criteria do not form part of the normative requirements of the Assurance Code but standards system owners are encouraged to incorporate them into their assurance programmes, where relevant. Additionally, the Assurance Code incorporates guidance that provides supplemental information to the Code criteria as well as interpretation of key terminology and phrases in the criteria. The guidance is an integral non-binding supplement to the Assurance Code and should be taken into account when carrying out assurance activities. It is included here primarily as a capacity building tool for organisations that are applying the Assurance Code. The guidance is interspersed in italics between the Code criteria.

3 Definitions

The Assurance Code uses established definitions whenever possible, to ensure consistent use of terms in the standards realm. However, the Assurance Code applies to many forms of assurance, so established terms such as 'certification' and 'accreditation', are not appropriate for all standards systems expected to use this Code. For this reason the Assurance Code uses the term oversight, for example, as a broader term that encompasses the traditional concept of accreditation. Similarly the Assurance Code employs the term assurance provider instead of certification body. A table of synonyms is presented at the end of this section.

1) Assessment

The combined processes of audit, review, and decision on a client's conformance with the requirements of a standard

2) Assurance

Demonstrable evidence that specified requirements relating to a product, process, system, person or body are fulfilled (adapted from ISO 17000)

3) Assurance provider

Body responsible for performing the assessment.

NOTE: In the context of this Code, an accreditation body is considered an oversight body rather than an assurance provider.

4) Audit

Systematic, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled. (adapted from ISO 17000)

5) Auditor

Person who performs the audit.

6) Calibration

The process by which different auditors and other personnel involved in assurance exchange knowledge and learn from each other to achieve more consistent interpretation and application of the standard

7) Certificate

Generic expression used to include all means of communicating that fulfilment of specified requirements has been demonstrated (Adapted from ISO 17000)

8) Client

The person or enterprise that is seeking assurance of their conformance with the requirements in a standard

9) External Assessment

In group assurance the systematic inspection and review of the Internal Management System performed by the assurance provider.

10) Group

An organized body of persons or enterprises that share similar characteristics are part of a shared internal management system and, for assessment purposes, are considered as a single client (eg: groups of farmers, of retail stores, of distributors).

11) Group Member

The individual enterprise (eg: farmer, retail store owner, distributor) that is enrolled in a group assurance scheme.

12) Internal Assessment

In group assurance the inspection and review of a sample of group members performed by the Internal Management System.

13) Internal Management System

In group assurance, the documented set of procedures and processes that a group will implement to ensure it can achieve its specified requirements. The existence of an Internal Management System allows the assurance provider to delegate inspection of individual group members to an identified body within the group.

14) Multi-site Operation

An enterprise with multiple production sites that are centrally managed and are assessed as one client.

15) Oversight

Assessment of an assurance provider's demonstration of competence to carry out specific assurance tasks. (adapted from ISO 17000)

16) Peer review

Assessment of a client against specified requirements by other clients in, or candidates for, an organised group (adapted from ISO 17000)

17) Risk

The chance of something happening that will have an impact on objectives. It is measured in terms of a combination of the probability of an event and its consequence

18) Risk mitigation (Risk reduction)

Actions taken to lessen the probability, negative consequences, or both, associated with a risk

19) Stakeholder

Individual or group that has an interest in any decision or activity of an organization (ISO 26000)

20) Standards System

The collective of organisations responsible for the activities involved in the implementation of a standard, including standard setting, capacity building, assurance, labelling and monitoring.

21) Standards system owner

The organisation that is responsible for the standards system. The standards system owner determines the objectives and scope of the standards system, as well as the rules for how the scheme will operate and the standards against which conformance will be assessed.

NOTE: The standards system owner can be the standards owner, assurance provider, a governmental authority, trade association, group of assurance providers or other body

22) Third-party assurance

Assurance activity that is performed by a person or body that is independent of the person or organization that provides the object of assurance and of user interests in that object (adapted from ISO 17000)

Table of Common Synonyms

Term	Synonyms
Assurance	Certification, verification
Assurance Provider	Certification body, verification body, conformity assessment body (CAB)
Audit	Inspection, evaluation, verification
Auditor	Inspector, verifier, assessor
Certificate	Statement of conformity, Assurance Statement
Client	Operator, enterprise, entity, participant, producer, member
Oversight	Accreditation
Standards System	Standards Scheme

4 Principles of Assurance

The following principles describe the essential values that encourage conformance and instil trust in an assurance system. They provide the intent behind the requirements in the Assurance Code and they can be used to evaluate an assurance model to ascertain its credibility. Standards systems that conform to the requirements in the Assurance Code will have embodied these principles within their assurance programme. Depending on the model of assurance chosen, standards system owners may put varying emphasis on each of these principles, according to the needs of the system's users.

- **Consistency:** Assurance systems that achieve the same results when applied in different contexts or involving different staff are consistent. The objective of having a consistent assurance programme is to ensure replicable results across the programme.
- **Rigour:** A rigorous assurance programme is more likely to provide accurate results. The level of rigour refers to the intensity of the assurance process eg: how many clients are sampled, how often, and how thoroughly, intensity of surveillance, and the breadth of stakeholder engagement in the assurance process.
- **Competence:** Competence applies most directly to the individuals who are engaged in different aspects of the assurance process. Competent personnel have technical knowledge of assurance and are able to interpret and apply the intent of the standards. Having competent management of the assurance programme ensures greater integrity and efficiency in implementation of the system.
- **Impartiality:** Clients of impartial assurance programmes are treated fairly and objectively. Impartiality can be demonstrated through independence or through provisions for transparency and stakeholder engagement.
- **Transparency:** Assurance that is transparent is under the scrutiny of stakeholders so has less risk of corruption or conflict of interest. Transparency also builds confidence in assurance as the public is more trusting of institutions that are open.
- **Accessibility:** Assurance programmes that are accessible help support the sustainability objectives of the standards system. Accessible assurance is affordable to clients who fall within the scope, is culturally sensitive, comprehensible, and within reach of the target clients.

4.1 Achieving the Principles

Principles	Code Requirements and Optional Good Practices	How the Requirements help to achieve the Principles
Consistency	5.2.1 Documented Management system	ensures consistent application of requirements across the assurance scheme
	6.3.3 Calibration of Assurance Personnel	ensures auditors are applying the standard in a consistent manner
	5.1.2 Requirements for Assurance Providers	requirement for a management system ensures consistency within assurance providers
	5.2.4 System Review	requires standards system owners to review the assurance system with the objective to improve it
	6.4 Consistent Assessment	ensures audits are performed uniformly across the assurance scheme
Rigour	6.4.2. Audit Procedures (Optional Good Practice)	standards systems can require that all, or a high proportion of clients are audited
	6.4.1 Assessment Methodology	ensures a sample of clients receive an audit
	6.4.5 Representative Sampling	Ensures established practice is employed in sample selection
	6.6.1 Oversight Mechanism	ensures oversight of assurance providers
Competence	6.3 Personnel Competence	a series of requirements designed to ensure competence in assurance personnel
	6.3.1 Defining Personnel Requirements (Optional Good Practice)	suggests procedures for recruiting auditors based on aptitude
	6.6.5 Oversight Procedures	ensures auditors are assessed at the oversight level
	6.6.6 On-site Appraisal	ensures the performance of auditors is assessed
Impartiality	5.1.2 Requirements for Assurance Providers	standards systems can choose to include more independence in their assurance scheme

	6.4.2 Audit Procedure (Optional Good Practice)	suggestion to rotate auditors to reduce the risk associated with over-familiarity
	6.1.1 Publicly Available Information (Optional Good Practice)	adoption of these suggestions will reduce the risks to impartiality
	5.2.3 Conflicts of Interest	requirements for managing the risks to impartiality
	6.4.6 Use of Translators	requirements to ensure translations are impartial
Transparency	6.1.1 Publicly Available Information	list of requirements to ensure transparency of the assurance system
	6.1.1 Publicly Available Information (Optional Good Practice)	suggestions for providing extra amounts of transparency
	6.1.3 Client Continuity	ensures transparency within the assurance process
	6.1.4 Stakeholder Engagement (Optional Good Practice)	involvement of stakeholders in the assessment is an obvious aid to transparency
Accessibility	6.5 Assessment of Groups	use of group assessment reduces cost and regulatory burden for groups of clients
	6.6.1 Oversight Mechanism	provides flexibility for oversight
	6.4.10 Remediation and Sanctions	encourages the 'helping aspect' of assurance
	6.2.1 Provision of Information	providing information to clients during the audit supports their compliance
	5.1.2 Requirements for Assurance Providers	provides flexibility for alternative models of assurance

5 General Provisions

5.1 Obligations for Scheme Implementation

5.1.1 Responsibility for Conformity

Standards system owners shall be responsible for conformance with the Assurance Code. Standards system owners shall use the provisions for oversight (Section 6.6) to ensure that assurance providers conform to the Assurance Code.

5.1.2 Requirements for Assurance Providers

Standards system owners shall ensure that, in addition to the requirements in this Code, scheme requirements for the assurance process conform or are equivalent to ISO standards 17065 or 17021, except where the imposition of ISO norms would hinder the objectives of the standards system by restricting practices used in some models of assurance. In these cases, it is the prerogative of the standards system owner to determine an alternative assurance management system that is appropriate to the scale, intensity, and market for the products or services that are within the scope of the standards system. The alternative management system shall be designed so as to fulfil the intent of the Principles of Assurance (Section 4).

NOTE: Standards system owners are required to comply with all other aspects of the Assurance Code, regardless of the approach taken.

5.2 Management of the Assurance Programme

5.2.1 Documented Management System

Standards system owners shall have a documented assurance management system in place that complies with the Assurance Code. Documentation of the assurance management system shall include, at a minimum:

- Normative standard or standards[1]
- Risk management plan (5.2.2)
- Criteria for accepting assurance providers to the scheme
- Criteria for accepting clients to the scheme
- Criteria for Group Assessment in schemes where this applies (6.5)
- Methodology for assessment of clients e.g. application, audit, review and decision, surveillance, sanctions, complaints and appeals, etc. (6.4)

[1] In compliance with the ISEAL Standard-Setting Code

- Requirements for the certificate, which identifies the product, process, or service to which it applies (6.4.11)
- Requirements for oversight of assurance providers (6.6)

5.2.2 Risk Management Plan

Standards system owners shall document a plan for how they are addressing the risks to the integrity of their assurance system. The plan shall include:

- a list of the most significant risks in their system;
- a description of the strategies being employed by the standards system owner to address each of these risks

Guidance: Risks to the integrity of the assurance programme are those risks that would prevent the standards system from fulfilling the Principles of Assurance. Standards system owners can use the Principles of Assurance as a framework for identifying relevant risks, e.g. what are the risks to the impartiality or to the rigour of the standards system? The list of risks in Annex B can be seen as a partial list of potential system risk events.

Standards system owners need to determine what combination of strategies are best able to mitigate the critical risks to a level that is acceptable to the standards systems' users. In making that determination, standards system owners will need to weigh considerations of cost (to implement a strategy) and acceptable level of risk. While the requirements in the Assurance Code are mandatory strategies to mitigate risk, the standards system owner can also look to the Optional Good Practices as effective strategies for addressing specific risks.

Risk management is a tool that can be used to focus limited resources. For example, a standards system can employ risk management to move resources toward high-risk areas and away from low-risk areas. ISO 31010 "Risk management — Risk assessment techniques" is a useful resource for developing a risk mitigation plan. Also see Annex B for a brief description of risk management and examples of risk assessment.

5.2.3 Conflicts of interest

Standards system owners shall describe to all entities working within the assurance programme what constitutes a conflict of interest within the assurance scheme, how to reduce the incidences of conflict of interest, and measures to be taken when conflicts of interest occur.

Guidance: A conflict of interest is defined as an actual or perceived interest in an action that results in or has the appearance of resulting in personal, organizational, or professional gain. For example, an auditor would be in a conflict of interest if they were to audit a business with which they have a monetary relationship (as a contractor or employee). Potential conflicts of interest are prevalent in assurance, not least because of the inherent conflict in seeking to keep the client or expand the service for future financial security. The primary aim of the standards system owner should be to ensure potential conflicts are detected and mitigated, rather than seeking to exclude all scenarios where a potential conflict of interest could occur. Transparency around the potential conflicts is the single most effective mitigation

strategy for most potential conflicts. However, where there are actual conflicts, such as assessing one's own work, these require that the individual with the conflict is excused from the activity.

In the context of assurance, many of the prevalent potential conflicts can be grouped in four categories:

- *benefit to individuals or external organisations;*
- *institutional financial benefits;*
- *pursuit of mission; and*
- *assessing one's own work (see 6.2.1)*

5.2.4 System review

Standards system owners shall have procedures and timelines for reviewing their assurance programme at planned intervals or after significant changes to their programme, to ensure its continuing integrity, adequacy, and effectiveness. Standards system owners shall use the results of the review to improve their assurance programme where indicated and shall maintain records of any corrective actions taken.

As part of the system review, standards system owners shall undertake a review and potential revision of the risk management plan to assess its continued applicability and to update both the prioritisation of risks and the strategies used to mitigate those risks. The Risk Management Plan shall be updated as new strategies are implemented and new learning occurs.

Guidance: The purpose of the system review is to ensure standards system owners take responsibility for the integrity of the assurance scheme. A standards system is a complex entity and requires vigilance to ensure client conformity and end user (consumer) confidence. Ultimately, the standards system-owner is responsible for the integrity of the standards system but receives advice and support from other organisations involved in it (e.g. assurance providers, oversight bodies). Assurance integrity includes assurance related activities but also includes quality control measures or integrity checks at the levels of the product or service, client population and assurance providers. Standards system owners need to check whether their systems are working, through a combination of activities, and to feed this into the review and monitoring of the standards system.

A system review can include:

- *Internal and external system audits of the assurance scheme as a whole;*
- *Systematic review of client assessments (audits);*
- *External audits of assurance providers;*
- *Chain-of-custody checks;*
- *Customer (and public) surveys;*
- *Client surveys;*
- *Monitoring labelled products in the market (see clause 6.8.1);*
- *Stakeholder consultation regarding the quality of the assurance system;*
- *Analysis of market and scientific trends.*

ISO 17065 clause 8.5 Management Review is a useful resource for this activity

Assessment of the continued applicability of the risk prioritisation should take account of data collected over the previous year about strengths and weaknesses in the assurance process. This can include data from the system's monitoring and evaluation programme, audit reports, oversight reports, auditor evaluations, complaints and stakeholder feedback.

5.2.5 Changes to the Assurance System

Standards system owners shall ensure that organisations and individuals involved in or affected by the assurance system are promptly notified of changes in requirements. Standards system owners shall have defined protocols for implementation of changes in requirements, including timelines by which changes come into effect.

6 Strategies for Effective Assurance

6.1 Transparency

6.1.1 Publicly available information

Standards system owners shall ensure the following information regarding their assurance system is maintained and made publicly available in a timely manner. Where this information is produced by the assurance provider or other entity involved in the assurance scheme, the standards system owner shall require publication by that entity:

- Description of the structure of the assurance programme, including the chain of authority and decision-making leading up to the governing body of the standards system;
- Description of the type of assessment process employed, including how clients are assessed, how often, and by whom. For group assurance, this shall include the representative sampling formula;
- Current list of assurance providers that are approved to work in the assurance scheme;
- Description of the oversight mechanism employed in the standards system, including the name of the accreditation body (or bodies), in standards systems where they are employed;
- Current list of clients and expiry date of their certificate (where expiry dates are used) (the list can be made available at the assurance provider level);
- List of clients whose certificate has been rescinded or withdrawn, (this shall be consolidated at the owner or oversight body level);
- Policy on information provision (knowledge sharing) to clients by assurance providers (6.2.1);
- Policy on sanctions for different levels of non-conformity (6.4.10);
- Policy on exceptions (6.4.8)

NOTE: The term publicly available refers to publication at least on the relevant organisation's website (eg: standards system owner, assurance provider, oversight body).

Guidance: The list of certified clients can include the following fields:

- *Name of enterprise*
- *Address or region of business*
- *Nature of business*
- *Scope of assurance*
- *Status of the enterprise within the assurance scheme (e.g. certified, verified, suspended, other)*

Optional Good Practice: The standards system owner can determine whether to make the following information publicly available:

- Summary reports of assessments for every client, where applicable
- Fee schedule and sources of funding for each assurance provider
- Public summary of resolved complaints (6.7.3)

6.1.2 Information from Clients

Standards system owners shall ensure that assurance providers require disclosure by applicants and clients of current enrolment with other assurance providers in the same or in a different standards system.

Guidance: The disclosure of current enrolment in with other assurance providers assists assurance providers to communicate with each other in the case of suspected fraud, and to co-ordinate in the case of joint audits. This requirement can be implemented by including a requirement for disclosure in the client contract with the assurance provider.

6.1.3 Client Continuity

Standards system owners shall ensure that when clients choose to transfer their assurance from one assurance provider to another within the standards system, the new assurance provider requires clients:

- to disclose previous enrolment with other assurance providers in the standards system;
- To provide a copy of their last assessment report where applicable, in order to ensure that unresolved nonconformities on the part of the client are taken into account by the new assurance provider

Guidance: The practice of skipping from one assurance provider to another in order to access a favourable assessment is a risk factor for the integrity of the standards system. Standards system owners can take an active role in this transfer of information between assurance providers or they may set policies that leave this activity to assurance providers. Active monitoring of client lists should help to alert standards system owners to instances of client transfer.

6.1.4 Stakeholder Engagement

Standards system owners shall ensure that stakeholders are informed of the points where they may provide input to the assurance process and shall encourage their engagement at these points. When stakeholders are involved in assessments, the role and limits of stakeholders in the assessment process shall be clearly defined.

Guidance: Stakeholder input can be seen as another source of information for evaluating conformance, along with audit findings, surveillance activities, and similar strategies. Active inclusion of stakeholders in the assurance process increases the transparency and thus public confidence in the process, and can be a vital source of information for assurance. Stakeholders can be involved in:

- *Pre-audit consultation*
- *Assessments (commenting on or participating in)**
- *Assessment of assurance providers**
- *Review of policies and procedures*
- *The complaints system*
- *Dispute Resolution*

** In these cases, auditors need to have training in how to engage stakeholders effectively.*

Optional Good Practice: Stakeholders can be involved in the assessment process; as participants in the audit and review, or as observers.

6.2 Knowledge Sharing

6.2.1 Provision of Information within the Audit

Standards system owners shall have a clearly defined and publicly available policy on the provision of information to clients by auditors. This policy shall define what type of information can be provided by auditors (or other assurance personnel) to clients. Where advice is provided, this shall be in accordance with guidance notes and other information issued by the standards system, consistent across the standards system, and offered to clients in a consistent manner (treating all clients equally). Advice provided by the auditor shall be recorded in the audit report.

Guidance: There is a risk to impartiality when an assurance provider or auditor provides information (or instruction) to a client for whom they are also providing assurance services. The specific risk is that if an assurance provider provides advice to clients about how to come into compliance with a standard, then when the assurance provider is evaluating the client, they are assessing the results of their own advice and are less likely to act impartially.

However, knowledge sharing as part of the assessment process is also a form of risk mitigation, because informed clients are more likely to follow the standard if they understand it. Rather than prohibit this activity, which can be beneficial for all parties, standards system owners need to ensure advice provided to clients is accurate and is available to all clients in a consistent fashion. This way, there is less opportunity for one client to be favoured over another.

6.3 Personnel Competence

Auditors need to be able to use their judgement to come to a quick understanding of a client's performance. Similarly, individuals responsible for audit reviews and decisions also need to be competent in their responsibilities. Among the strategies to mitigate the risks of non-conformity, having competent auditors is one of the most important. Basic requirements for supporting auditor competence are included in ISO17065 (6.1.2) and in ISO 17021-2 Section 7 and Annexes A to D in that document.

The standards system owner must take ultimate responsibility for the competence of auditors working in their assurance programmes, though much of the activity required in Section 6.3 can be undertaken by assurance providers, training organisations, or oversight providers.

6.3.1 Defining Personnel Requirements

Standards system owners shall define the qualifications and competency requirements for auditors and other personnel engaged in their assurance scheme, as well as the verification mechanisms to assess whether the requirements are fulfilled.

Guidance: See Annex C for an example of how these requirements can be set.

6.3.2 Training

Standards system owners shall ensure that auditors and other assurance personnel receive initial and ongoing training and professional development according to the requirements of their respective positions. Standards system owners shall require auditors and other assurance personnel to complete on-the-job training during which they are supervised by qualified staff.

Guidance: On the job training can include being provided with mentoring and other learning opportunities and can recur over time. Continuing professional development can cover changes in requirements or new interpretations. As well as generic training, standards system owners can provide specific training in the following areas:

- *The intent of each requirement in the standard, to assist in interpreting the standard(s) in different contexts;*
- *Conducting qualitative interviews;*
- *Weighing conflicting statements from stakeholders;*
- *Performing sampling tasks;*
- *Technical writing skills;*
- *Assessment process;*

- *Collecting monitoring and evaluation data;*
- *Guidelines and limits on providing information and advice during an audit.*

See also ISO 17021-2 clause 7.2.8 or ISO 17065 clause 6.1.2.1

Optional Good Practice: Standards system owners can develop a screening process for the selection of auditors, to be applied by assurance providers. The screening tool could include a ranked list of desirable personal attributes applicable to different roles within the assurance process. Personnel could then be selected based on how well their personalities match with the desired attributes.

Guidance: The single most important factor that differentiates effective auditors is that they exhibit relevant personality attributes. While there are methods to test personality attributes, this is not an exact science. Annex C provides a list of generic personal attributes along with guidance for selecting candidates for auditors based on desired personal attributes.

6.3.3 Calibration of Assurance Personnel

Standards system owners shall develop and implement directly or through assurance providers, a recurring programme of auditor and assurance personnel calibration.

Guidance: Calibration can be an effective tool for exchange and learning between assurance personnel and for improving consistency of interpretation of the standard and the audit process. Learning from calibration discussions should be captured by the standards system owner in guidance that is made available to assurance personnel. While in-person meetings of auditors can be an effective means of exchange and learning, alternative models are also valuable, including virtual meetings. Standards system owners who are designing calibration procedures could include calibration exercises for field auditors, programme managers (for policies), accreditation auditors, and assurance providers. Learning from calibration sessions may also be useful for integration into standards and procedures review processes. Calibration sessions are most effective when they include staff from multiple assurance providers working in a standards system.

6.3.4 Evaluation of competency

Standards system owners shall ensure that the competence of auditors is demonstrated on an ongoing basis through evaluation by assurance providers or other entities. Clients shall be provided the opportunity to comment on auditors' performance which, when provided, shall be used in the evaluation of auditors. However, client comments on auditor performance shall not be considered as impartial and shall form only a portion of the auditor evaluation.

Guidance: To support evaluation of competency, standards system owners can develop an evaluation protocol with their assurance providers for the evaluation of auditors and other assurance personnel. The protocol may include:

- *The entity responsible for evaluations;*
- *Types of evaluation to be employed;*
- *How each evaluation is applied: rules, administration, scoring and pass rates, etc.;*
- *Exercises to assess abilities*
- *Records of evaluations; and*
- *Frequency of evaluations.*

ISO 17021-2 Annex B describes possible evaluation methods. A combination of evaluation activities will yield the best results and in fact, certain evaluation activities on their own will not produce sufficient evidence of competence.

Optional Good Practice: Evaluation of auditor competence can include on-site witness audits.

6.4 Consistent Assessment

ISO 17065 and 17021 differ in their requirements for assessment of clients. ISO 17021 provides extensive detail regarding the requirements for an audit, how it occurs, and how often. On the other hand, ISO 17065 requires only that an evaluation take place and does not specify the need for an audit. For this reason there is a need for the Assurance Code to define minimum requirements for assessment for all users of the Code.

6.4.1 Assessment Methodology

Standards system owners shall ensure consistent application of their documented methodology for assessment of clients. The methodology shall include procedures for at least the following activities:

- Evaluation of conformance to the standards (eg: audit of sites, or inspection of records or of self-assessment declarations)
- Review and decision
- Issuance of a certificate
- Periodic re-assessment

The assurance programme shall include provisions for periodic on-site audits of at least a sample of clients.

6.4.2 Audit Procedures

Standards system owners shall define and document procedures for audits and shall require these procedures to be followed by assurance providers consistently across the standards system. The procedures shall include at least the following:

- Requirements for audits (on-site and desk audits), including:
    - frequency and intensity of audits (6.4.3)
    - sampling protocol for audits (unless 100% sample is used) (6.4.4);
    - structure of the audit team (if audit team is used);
    - minimum set of issues that need to be checked in every audit;
    - a transparent means of calculating the time needed for an audit;
    - documentation to be reviewed;
    - timelines for submission of completed reports, following audits; and
    - minimum content of audit reports, including a requirement for auditors to explain their rationale for their choice of samples in the audit.
- Requirements for self-declarations, if used, including:
    - frequency of reporting; and
    - content and level of detail required.

Standards system owners can choose to delegate authority for this clause to oversight bodies but shall ensure the requirements are carried out by the oversight bodies.

Guidance: The term intensity in relation to audits refers to the factors that contribute to a rigorous audit, eg: how long an audit should take, how many interviews should occur, how many sites should be investigated, how many samples should be taken, the use of unannounced audits.

6.4.3 Audit Frequency and Intensity

Standards system owners shall set the audit frequency and intensity to be employed by assurance providers in the standards system. Where an assurance programme uses a risk-based approach to determine audit frequency and intensity, the standards system owner shall develop a procedure that identifies the risk factors for assurance providers to assess the risk level of clients, the overall risk categorisation, and the resulting audit frequency and intensity associated with each risk category.

Guidance: A simple risk-based procedure would consist of the following steps:

1) Describe the risk factors. These could include:

- *History of the client within the standards system (past conformance records);*
- *Type of production or service;*
- *Length or complexity of supply chain;*
- *Level of staff turnover at the management level;*

- *Presence of any unusual pressures on management;*
- *Complexity of the production process;*
- *Number of production variables to be managed;*
- *Overall conditions within the sector;*
- *Culture or regional context in which the enterprise operates*[2].

2) *Assign values to the risk factors so that a ranking scale can be developed*

3) *Quantify what constitutes different categories of risk (high, medium or low)*

4) *For each category of risk, determine the audit frequency and intensity. An example of this could be:*

   - *High-risk enterprises: full audit once every six months;*
   - *Medium-risk enterprises: full audit once a year ;*
   - *Low-risk enterprises: full audit once every two years.*

6.4.4 Sampling Within the Audit

Standards system owners shall define the sampling procedure that auditors shall use during the audit and shall provide this direction to assurance providers. The procedure shall require that the auditor, rather than the client, chooses the sample.

The sampling procedure shall include, at minimum:

- A description of when sampling is to be employed in the audit; and
- Guidelines for the type of sampling and size of the samples, to be employed in each instance.

Guidance: Sampling in the audit can include choosing which documents or records to review, which sites to visit, or what issues to focus on. Sampling procedures on-site cannot be strictly dictated ahead of time as auditors must be free to use their judgment in choosing samples. Standards system owners therefore need to provide detailed guidance that will lead to consistent on-site sampling procedures.

There are four main types of audit sampling, the latter three of which are judgmental in nature:

1. *Representative sampling*[3]*: based on random sampling of a group or of the client's operations. If done well, this should enable inferences to be made about the overall conformity of the group or client.*
2. *Corrective sampling: a focus on areas of known difficulty and non-conformity. This type of audit sampling is beneficial in assurance schemes that have an improvement focus.*

---

[2] The Transparency International Corruption Perceptions Index may be helpful for this risk factor

[3] Also referred to as statistical or probability sampling, this is a sampling method that utilizes some form of random selection. This means that each individual unit (e.g., site, item, client) in the population has an equal probability of being chosen to be included in the sample. Examples of random sampling are: simple, stratified, systematic, cluster and multi-stage.

3. *Protective sampling: a focus on the issues that are of highest impact to the standards system's environmental or social objectives. In this case non-conformities could go undetected, but in areas of less impact. For example, protective sampling could concentrate on field activities and not record keeping.*

4. *Preventive sampling: a focus on preventing the client from predicting which samples will be examined, and therefore being able to correct any non-conformity. For example, there should be little predictability in the choice of samples from audit to audit.*

Judgmental sampling (where subjective judgment is applied in determining what to sample) is prevalent throughout social and environmental auditing. While judgmental sampling can be effective, being explicit and transparent about the type and extent of sampling required can strengthen the system.

Auditors can make efficient use of their time by choosing samples that display a range of standards requirements e.g. an active logging site in preference to a completed or planned site.

6.4.5 Representative Sampling

Where the assurance provider seeks to extrapolate audit findings in order to draw conclusions about conformity of a whole population, (e.g. sampling in groups or multi-site operations) standards system owners shall require representative sampling. Standards system owners shall define a standardized formula for determining sample size and shall require its use by assurance providers.

Guidance: Inferences about the whole population cannot be made from judgmental samples. If judgmental sampling identifies non-conformity, there is no way of knowing the frequency of non-conformity within the population sampled and hence the reliability of claims made about any member of that population. A representative sample should be taken to measure non-conformity levels in the population as a whole. This sampling may be completed before the physical audit as it may affect the cost of audit.

6.4.6 Use of Translators

Standards system owners shall require that when translators are used in audits the translators are independent of the enterprise being evaluated. Where this is not feasible due to logistical difficulties, the name and affiliation of translators shall be included in audit reports.

NOTE: This clause applies to assurance providers and to oversight bodies.

Guidance: Ideally, the audit team has the necessary language skills to avoid the use of translators.

6.4.7 Information from Other Sources

Standards system owners shall define the criteria by which information obtained from sources other than the assurance provider may be included in the assessment.

Guidance: Examples of information from other sources can include test results from labs, assessment results from other assurance providers, interviews with a government agency that manages forests and protected areas, or NGOs working on specific topics in the country (e.g. Worker's rights, child labour).

6.4.8 Exceptions

Standards system owners shall have a procedure for regulating exceptions to the standard or assessment process, where this occurs, and shall make this procedure publicly available. The procedure shall require:

- that assurance providers receive prior approval from the standards system owner or oversight body for each exception;
- that the standards system owner or oversight body makes a list of current exceptions available to all assurance providers working within the standards system so that these are applied consistently; and
- that exceptions are only valid until the next standard review exercise, when they shall be integrated into the standard, or removed from use

NOTE: Requirements within a standard that are not applicable to a particular client are not considered exceptions.

Guidance: A requirement for a client to keep a record of pesticide applications when the client does not use pesticides is an example of a standard requirement that is not applicable and therefore not considered an exception.

6.4.9 Decision-Making Mechanism

Standards system owners shall define the decision-making mechanism (e.g. scorecard, traffic light, critical criteria, etc.) and shall provide specific direction on how to determine levels of non-conformity. Standards system owners shall require assurance providers to apply this mechanism consistently.

Guidance: An example of direction on determining levels of non-conformance:

Minor Non-Conformance: *A minor non-conformance is raised when a single observed lapse has been identified in a procedure required as part of the client's management system. A non-conformance may be considered minor if:*

- *it is a temporary lapse; or*
- *it is unusual / non-systematic; or*
- *the impacts of the non-conformance are limited in their temporal and spatial scale; and*
- *prompt corrective action has been put in place to ensure that it will not be repeated.*

Major Non-Conformance: *A non-conformance can be considered major if, either alone or in combination with further non-conformities of other requirements, it results in, or is likely to result in a fundamental failure to achieve the objectives of the standards system. Such fundamental failure may be indicated by non-conformities which:*

- *continue over a long period of time, or*
- *are repeated or systematic, or*
- *affect a wide area, or*
- *are not corrected or adequately responded to by the member once they have been identified.*

6.4.10 Remediation and Sanctions

Standards system owners shall define and make publicly available how different gradations of non-conformance are addressed and remediated (for clients and for assurance providers). In the case of systemic failures, this shall include definitions of the points at which non-conformance of the client and of the assurance provider result in suspension or termination from the programme.

Guidance: The objective of assurance is to ensure conformance, so it is sensible to encourage clients to resolve non-conformities before punitive sanctions are enforced. The first stage of this process is to identify the root-cause of the problem and try to remedy it. When these attempts fail, or when the non-conformances pose a serious risk to the integrity of the assurance programme, sanctions can be employed.

In the case of systemic failures, standards systems can choose to employ a range or combination of sanctions:

- *Suspensions (including loss of marketing ability during period of suspension)*
- *Public notification of suspensions or terminations*
- *Publishing summary reports including non-compliances*
- *Extra audits, resulting in extra scrutiny*
- *Termination of certificates*

As one of a number of elements that encourage conformance, the threat of sanctions can be seen as an incentive to conform rather than an attempt to penalise transgressors. Sanctions should not be idle threats and criteria for imposing sanctions should be unambiguous so as to achieve their desired effect. Publicizing imposed sanctions serves the dual purpose of creating an incentive and illustrating that the sanctions are serious.

6.4.11 Certificates

Standards system owners shall set requirements for the use of certificates and marks of conformity, which shall include at least the following:

- How the certificates are issued: by whom and to whom, and under what authority;
- Their duration;
- Information to be included in a certificate, including the scope;
- How they can be withdrawn from use; and,
- How they can be used in public communications.

6.5 Assessment of Groups

The clauses in this section apply to standards systems that allow for assurance of groups of enterprises (or individuals). These requirements do not apply to multi-site operations, which are assessed according to the other requirements in this Code.

6.5.1 Internal Management System

Standards system owners shall specify the requirements for a documented internal management system required by groups. The internal management system shall include at least the following:

- Description of the roles, responsibilities and competencies of individuals responsible for different aspects of the internal management system;
- Procedures for obtaining agreements with all group members to ensure group members understand what is required of them and to allow for assessments, both internal and external;
- Procedures for approval and removal of members;
- Procedures for annual decision-making on the assurance status of each member in the group;
- Chain of custody / product flow;
- Group and group member record keeping requirements;
- Procedure for internal assessment; and
- Procedure for sanctions and appeals.

6.5.2 External Assessments

Standards system owners shall specify the requirements and frequency for the external assessment of groups by assurance providers. The assessment shall focus on the competence of the group's internal management system to identify and resolve non-conformities within the group. The external assessment shall include:

- A review of the documentation of the internal management system to ensure internal assessments have been carried out, records are complete and non-conformities are resolved;
- An audit of a sample of group members (see 6.4.5 and 6.5.3) to assess the accuracy of the results of the internal management system. The audit sample shall conform to the standards system procedures as required by 6.4.5 Representative Sampling;
- Procedures to address non-conformities including sanctions in the case of systemic failure of the internal management system.

6.5.3 Non-conformities in Group Members

Standards system owners shall define the actions to be taken by assurance providers if they identify non-conformities in individual group members during external assessments. Where the number of non-conformances signifies a systemic problem with the group's internal management system, standards system owners shall define the repercussions, consistent with how the assurance programme addresses other non-conformities (6.4.10).

The group members that have critical or major non-conformities shall be subject to the regular repercussions defined by the assurance programme for non-conformance and shall be required to undergo a mandatory re-assessment before re-entering the group.

Guidance: This requirement obliges standards system owners to develop an objective procedure for the actions to be taken on the discovery of non-conforming group members within a sample. The discovery of non-conformance in individual group members could indicate a problem within a number of group members, or it could indicate a systemic failure of the internal management system. Standards system owners need to provide guidance or requirements that will enable auditors to detect the difference. That procedure can include both a quantitative and qualitative approach (e.g. is the group working to resolve the non-conformance?) and might include a table identifying the number of non-conforming group members that are allowed for different total sample sizes, for example:

Number of Group Members in a sample	*Threshold Number of non-conforming members Allowed*
2-5	*1*
6-10	*2*
11-15	*3*
16-20	*4*
21-25	*5*
26-30	*6*
31-40	*7*
41-50	*9*
51-60	*11*
61-70	*13*
71-80	*15*
80+	*18*

Source: adapted from ISO 2859 (via MSC CoC Methodology)

6.6 Oversight

Third-party accreditation is the predominant form of oversight and provides a level of independence that contributes to impartial assessments. However, the Assurance Code allows for different approaches to oversight in recognition of the needs and resources of diverse and emergent standards systems. Regardless of the approach taken, it is critical that oversight of assurance providers is undertaken by competent and impartial bodies.

6.6.1 Oversight Mechanism

Standards system owners shall ensure that the competence and consistent performance of assurance providers is periodically reviewed. Standards system owners shall specify the approach to be used in oversight, ensuring that the oversight mechanism is independent of the assurance providers being assessed. Standards system owners shall define the frequency of oversight or the procedure for determining the frequency, applicable in the case of risk-based oversight (6.6.4).

Standards system owners shall periodically assess the effectiveness of the oversight mechanism as part of their system review (5.2.4).

Where standards system owners incorporate accreditation as an oversight mechanism, they shall ensure that accreditation bodies comply with ISO 17011 in addition to the relevant Assurance Code requirements.

Where the standards system owner is the assurance provider, they shall ensure that oversight is carried out by personnel independent of those engaged in the assurance process.

Guidance: Oversight of assurance providers is typically managed through an ISO 17011 accreditation process, but can be accomplished in other ways, depending on the needs of the standards system. For example, a standards system could employ an independent assurance body to review the assurance scheme. Alternatively, a standards system owner could arrange to oversee the work of assurance providers directly, recognizing that this model provides less independence and requires the owner to have the competencies described in this section. Less formal standards systems could develop a scrutiny committee of peers or stakeholders to oversee the assurance process. In all models of oversight, independence of the oversight mechanism from the assurance provider is necessary.

Though this clause requires conformance with ISO 17011 for accreditation bodies, it does not prescribe membership by accreditation bodies in the International Accreditation Forum[4]. In contrast to national accreditation, international accreditation is a better model for international social and environmental standards systems. International accreditation bodies operate internationally in a particular sector, rather than nationally in a wide variety of sectors. This creates certain advantages including the ability to build greater expertise in evaluating assurance in specific sectors. Additionally, international accreditation

[4]The International Accreditation Forum is an association of national accreditation bodies. Its members have a country-specific scope of work – membership in the IAF specifically does not include accreditation bodies with an international scope of work.

bodies accredit certifiers worldwide, thus establishing a basis for equivalence and recognition of statements of conformity issued by different assurance providers around the world.

6.6.2 Competence of Oversight Bodies

Standards system owners shall ensure that the oversight body or mechanism possesses the following competencies:

- in-depth knowledge of the standard and its intent (and other requirements) and an understanding of the goals of the standards system, and in particular, the critical issues, e.g. high conservation values, indirect impact, indigenous rights, child labour, etc.;
- competence to review sampling protocols and practice, where this is undertaken by the assurance provider; and
- competence to review assessment of groups (6.5), where this is undertaken by the assurance provider.

In the case of proxy accreditation, where standards system owners accept assurance providers that have been accredited against other scopes, standards systems owners shall employ additional measures to assess the performance of assurance providers. Such measures shall include at least some of the strategies listed in the Optional Good Practice connected with clause 6.6.3

Guidance: Guidance: It is sometimes the case that a standards system-owner accepts accreditation of assurance providers to other standards systems or to generic competency scopes (e.g. ISO 17065 for agriculture scope). While this is a reasonable and cost-effective solution, it is necessary for the standards system owner to ensure that all personnel involved in their assurance scheme (auditors and decision-makers at the certification and oversight levels) have a demonstrated knowledge and understanding of that standards system's content and procedures and the skills to assess compliance.

The competence of oversight bodies can be assessed by:

- *Contacting references from other customers (of the oversight body);*
- *Reviewing records of internal audits*
- *Reviewing public materials provided by the oversight body*
- *Interviewing staff of the oversight body*
- *Interviewing staff of assurance providers*

6.6.3 Oversight Procedure

Standards system owners shall document the procedures to be followed in oversight and shall require the oversight body or mechanism to implement them. At a minimum, oversight shall include a review, at regular intervals, of requirements for assurance providers described in this Code, including:

- the management system of assurance providers (5.1.2);
- the competence of assurance personnel (6.3); and
- the assessment process (6.4)

Optional Good Practice: In order to strengthen the oversight of assurance providers, standards system owners can require the oversight body to undertake certain activities including:

- In-depth monitoring of a specific issue across all assurance providers in the standards system, to compare, and therefore determine the level of competence and consistency of assurance across the standards system;
- Review audits: onsite visit to a client without the auditor but with the last inspection report. This is not a full inspection but more a spot check to see if the inspection report of the assurance provider correlates with what is seen at the time. This also includes a client interview to get their impression of their assurance provider. Review audits generally do not last more than a few hours but can yield valuable insight into the competence of assurance providers;
- Review of information obtainable from the databases of assurance providers in order to reduce onsite visits to offices of assurance providers. Time and money can be saved if data review is performed remotely, rather than onsite;
- Review of the effort (usually measured as time) spent on audits. If this information is entered in a database the oversight body could have a good idea of the effort expended for different types of audits and could compare this with the performance of assurance providers.
- Review of client assessment reports (audit reports) and subsequent follow-up of discrepancies discovered

6.6.4 Risk-based Approach

Standards system owners that prescribe a risk-based approach to determine the frequency and intensity of oversight of assurance providers shall develop a separate procedure that characterizes the risk factors and categories appropriate to oversight and that contains the same elements as described in Audit Frequency and Intensity (6.4.3).

Guidance: Risk factors to consider in developing a sampling protocol include:

- *History of the assurance provider within the standards system;*
- *Growth rate of the assurance provider;*
- *History of low quality of audits in evaluations by assurance provider (e.g. where non-conformities have been raised previously about the quality of an assurance provider's audits);*
- *Complaints*

6.6.5 On-site Appraisal

Standards system owners shall ensure that the oversight process includes a review of the performance of assurance providers and auditors in the field.

Guidance: Oversight includes checking auditors' understanding and application of the standard as a reflection of whether the assurance provider's management system is working. On-site reviews help to assess assurance provider performance as well as individual auditor competence. Results of on-site reviews should be made available to assurance providers and to the standards system owner to use in their own monitoring and improvement programmes. Where confidentiality is an issue, the results of on-site reviews can be made available in aggregate or summary form.

6.7 Ongoing Scrutiny

6.7.1 Market Surveillance

Standards system owners shall define a procedure for surveillance activities that will be undertaken by the standards system owner or delegated to the oversight body. At a minimum the procedure shall include:

- market checks for fraudulent products, e.g. through tracking chain of custody certificates
- responding to tips and complaints about fraudulent products or services.

NOTE: This requirement is not applicable to local programmes where clients only engage directly with consumers

Guidance: Surveillance activities can also include:

- *Monitoring products or services produced by a client, e.g. checking labels on products, batch testing, etc.;*
- *Monitoring and tracing products or services produced by uncertified enterprises, based on tips or complaints received;*
- *Customer interviews and surveys;*
- *Reviewing communications on client's or other websites; and*
- *Undertaking unannounced audits.*

Where tips or complaints refer to misrepresentation by certified enterprises, these can be referred to the relevant assurance provider in the first instance.

6.7.2 Fraud or Misrepresentation

Standards system owners shall define and document the actions, repercussions and who is responsible for dealing with cases where misrepresentative or fraudulent references to the standards system are being claimed.

Guidance: This includes fraud or misrepresentation both in the certified enterprises and in the assurance providers. When cases are discovered the standards system owner needs to take steps to protect consumers and to protect the integrity of the standards system. Suggested activities include:

- *Steps to recall or restrict mislabelled product;*
- *Revocation of statements of conformity (certificates) where fraud is found within the standards system;*
- *Notification of regulatory agencies where appropriate;*
- *Notification of the brand owner and appropriate supply chains;*
- *Public notification (media, website);*
- *Steps to review supply chains to ensure integrity of the assurance system*

6.7.3 Complaints

The standards system owner shall have a documented complaints procedure that is accessible and responsive. The procedure shall be implemented by the standards system owner and shall facilitate complaints regarding:

- the standards system (from clients or the public);
- fraud or potential fraud

The procedure shall require the standards system owner to:

- investigate and take appropriate action regarding relevant complaints;
- review and take any necessary corrective action to the standards system or assurance requirements; and
- keep a record of all complaints and resulting actions to be made available for the system review (5.2.2).

NOTE: Complaints and appeals about specific assurance cases (certification or accreditation) shall be taken up first with the respective assurance or oversight body.

Guidance: Standards system owners may consider the complaints system an essential component of the assurance scheme, as it allows them to include stakeholders in the assurance process. The knowledge that stakeholders (including peers) are watching them has a modifying effect on a client's behaviour. Some complaints will lead to discovery of infractions, but the larger effect of the complaints system is the incentive it provides for everyone to comply with the requirements of the standards programme.

Annex A – Sample of Risks to Assurance

The following list represents a sample of risks to assurance systems:

Standards-Related Risks

- Poorly written and vague standards leading to varying interpretations
- Intent of standards unclear or missing
- Frequent changes to standards, interpretive guidance, or assurance methodologies
- Lack of leadership by the standards system owner on the need for standards clarification

Assessment Process Risks

- Lack of client understanding or incentive to conform
- Lack of personnel competence (skills, knowledge or attributes)
- Audit staff become overly-familiar with clients, leading to lack of impartiality
- Inadequate calibration between auditors (leading to inconsistent audit results)
- Lack of local or relevant auditor capacity (not enough auditors trained and fluent in the local language in a region)
- Inconsistent audit planning and lack of coordination
- Inadequacy of sampling methodology
- Lack of knowledge of cultural attitudes to assurance

Systems Risks

- Undercutting among assurance providers may result in reduced assurance quality
- Clients moving between assurance providers in a quest for a more lenient assessment
- Potential for corruption (auditors, clients, assurance provider)
- Lack of adequate safeguards to prevent positive or negative bias by auditors
- Difficulty engaging stakeholders where their input is necessary to the assurance process (lack of interest, lack of resources)
- Fraudulent representation of products and services (claims and labelling issues)
- Inadequate complaints system
- Inadequate surveillance system
- Lack of follow-up of non-conformities

Annex B – Risk Management

Risk can be expressed as the probability of an event occurring multiplied by the consequences if it does occur. Risk management is used in different circumstances, always following a similar sequence of activities:

1) Identify and assess the risks (called risk assessment) – including their size
2) Identify possible risk control measures
3) Implement risk controls; review the results

Details on the steps

1) Identify and assess risks - The first step is to identify the threats (risks) for each activity or step in the process under consideration. This may be done by creating a flowchart of all the steps of the process. Then, for each step of the flowchart, the risks are identified along with the consequences of those risks (this is the 'risk assessment').

To place risks in rank order, the best possible estimate of the probability and consequences of a risk compared to other risks that have been detected must be made.

Using a risk assessment matrix (see example below) the consequences and probability for each risk are estimated and the risk level identified. This process should be based upon as much data as possible, and the basis for making decision should be recorded. In this example each risk is labelled with its significance (extremely high, high, medium, and low) – numeric scores could be used instead. Users would need to determine consequences and probability according to the specifics of their own programme. The aim of ranking the risk events is to understand which risk events are likely to be most consequential and, therefore, most important to manage or mitigate.

		Probability of Occurrence					
Consequences		**Frequent** **A**	**Likely** **B**	**Occasional** **C**	**Seldom** D	**Unlikely** E	**Unknown** **0**
Catastrophic	**1**	Extremely high	Extremely high	High	High	Medium	Unknown
Critical	**2**	Extremely high	High	High	Medium	Low	Unknown
Moderate	**3**	High	Medium	Medium	Low	Low	Unknown
Negligible	**4**	Medium	Low	Low	Low	Low	Unknown
Unknown	**0**	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown

Before analysis, the consequences and probability must be defined so a consistent approach can be taken by those assessing risk (standards system owners could do this).

2) **Identify and analyse risk control measures -** The second step is to identify and analyse the effectiveness of a range of potential risk control measures for each identified risk. Ideally, the risk should be eliminated. If this is not possible the level of risk arising from the hazard should be reduced by taking actions to reduce either the probability of an event happening or the consequences of events.

   The overall goal of risk management is to plan operations or design systems that do not contain risks. A hierarchy of preference for dealing with hazards and reducing risk is:

   1. **Design equipment, processes, and systems to eliminate hazards.** Without a hazard there is no probability of an event and hence no risk.
   2. **Isolate hazards.** Reduce risk by isolating hazards by limiting access to them.
   3. **Minimize hazards.** Take steps to reduce either the probability or consequences of an incident.
   4. **Develop procedures and training.** The first three actions are usually "hard" or physical solutions. Where these are not practical, "soft" or human solutions are needed.

3) **Implement risk controls; review results -** After deciding which risk controls to use, the risk controls must be implemented.

Annex C - Competence of Personnel

The following table provides an example of the qualifications, competencies and means of verification for some of the skills and knowledge required of an audit team leader. The example is meant to be indicative and does not represent an exhaustive list.

Knowledge and Skills	Qualifications	Competencies	Possible Confirmation Mechanisms
General	Academic qualifications in business, economics, science or technical subject E.g.: supply chain and logistics management, natural resources management		CV, certificates
Understanding of the standard	Attendance at annual lead assessor training course	Demonstrate an understanding of the principles and criteria	On-line lead auditor training and examination
Interviewing stakeholders	Attend a formal training course approved by the standards system owner of at least 1 day duration in facilitation / interviewing techniques	Demonstrate: • An understanding of the principles of sampling techniques with respect to group or individual interviews and cultural considerations. • The ability to interview personnel without compromising the source of information.	Work experience and witnessed audits
Report Writing		Produce: • Written documents that can be understood by the intended audience. • Clear and accurate reports on audit findings and clearly articulate these in relation to legal requirements and relevant codes.	Writing samples, previous assessment reports or other audit reports, employer reference letters, certifier records, accreditation assessment reports

Auditor Personal Attributes

Good auditing skills can be taught, but often the qualities that make a good auditor reside in the personality of the person. Individuals who possess more of the attributes suggested in the list below are more likely to become good auditors than those who possess less of those qualities. Determining if someone possesses the right attributes, and in what measure, has always been a challenge for employers and recruiters.

Individuals responsible for recruitment of auditors could use the following list of desirable personal attributes as a starting point for developing a screening process for potential auditors:

- ethical, i.e. fair, truthful, sincere, honest and discreet;
- open-minded, i.e. willing to consider alternative ideas or points of view;
- diplomatic, i.e. tactful in dealing with people;
- collaborative, i.e. effectively interacting with others;

- observant, i.e. actively aware of physical surroundings and activities;
- perceptive, i.e. instinctively aware of and able to understand situations;
- versatile, i.e. adjusts readily to different situations;
- tenacious, i.e. persistent and focused on achieving objectives;
- decisive, i.e. reaches timely conclusions based on logical reasoning and analysis;
- self-reliant, i.e. acts and functions independently;
- professional, i.e. exhibiting a courteous, conscientious and generally business-like demeanour in the workplace;
- morally courageous, i.e. willing to act responsibly and ethically even though these actions may not always be popular and may sometimes result in disagreement or confrontation;
- organized, i.e. exhibiting effective time management, prioritization, planning, and efficiency.

For social and environmental auditing, standards systems could add a few more qualities:

- Fluency in the languages of the clients (and the local language for stakeholder interaction) they will be expected to audit
- Commitment to the social and environmental goals of the standards system

In developing a screening process for potential auditors, standards systems can develop a list of desirable qualities with ranking attached to those qualities determined to be more crucial or less crucial to the auditing process. Standards systems owners could bear in mind that auditors are often required to be evaluators, ambassadors, and trainers; all of which require different skill-sets.

It is important to do a thorough job of interviewing candidates for auditing and focusing on identifying those who have the best possible aptitude for the job, regardless of whether they have they training or experience (although both are also important).

As writing skills are essential to effective audits, it is helpful to have prospective auditors complete a writing exercise before the interview. Some examples of writing exercises include:

- Give candidates a handout with clients' lengthy, detailed responses to various auditor questions. Ask candidates to summarize client responses in a clear, concise manner
- Give candidates a handout with a scenario describing a number of weaknesses in an internal control system. Ask them to write a letter detailing the findings and giving recommendations to strengthen the ICS
- For a candidate with prior experience preparing audit reports, ask him or her to write review notes for sample audit reports with a number of needed improvements