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

Public Draft for Consultation, v 0.2 – 02 April, 2012 Comment Version

Please respond to questions in the text, save the file and send it to paddy@isealalliance.org

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 movement as a whole.

Since 2004, ISEAL has been facilitating international consultations to determine what good practice should look like for voluntary 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 and draft form focused on standard-setting procedures, measuring impacts of standards systems, and 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 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 that is specific to the implementation of social and environmental standards systems and that is not sufficiently addressed elsewhere.

Assurance helps to ensure that clients conform to a standard, resulting in achievement of the social and environmental impacts desired by the scheme. In assurance, the aim of a standards scheme should be to increase the likelihood that enterprises are conforming to the standard. The Assurance Code is structured around a set of strategies that seek to encourage conformance and detect non-conformance when it occurs.

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-conformity. The Assurance Code does not prescribe a single model of assurance but rather describes the basic features of different models, and when these might be applied.

ISEAL Codes of Good Practice

The goal of all ISEAL Codes of Good Practice is to assist standards systems to deliver 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 ensure that enterprises who agree to comply with the standards are actually doing so.

Taken together, the Codes provide end users and other interested parties with information that engenders confidence in the effectiveness of standards systems.

1 Referenced Publications

AS/NZS 4360:2004 Risk Management

IFOAM Accreditation Criteria (IAC) for Bodies Certifying Organic Production and Processing (2009)

ISEAL Common Requirements for the Certification of Producer Groups (2008)

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

ISO WD 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 compliance with social and environmental standards systems. The Code defines a minimum set of normative requirements that are applicable to all assurance models. It is the responsibility of the scheme owner to ensure that these requirements are complied with throughout the assurance system.

The Assurance Code focuses 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. Depending on the assurance model chosen by a scheme owner, substantially fulfilling these ISO standards is required in addition to meeting the Code requirements. Requirements for compliance with ISO standards are defined in section five.

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 scheme 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

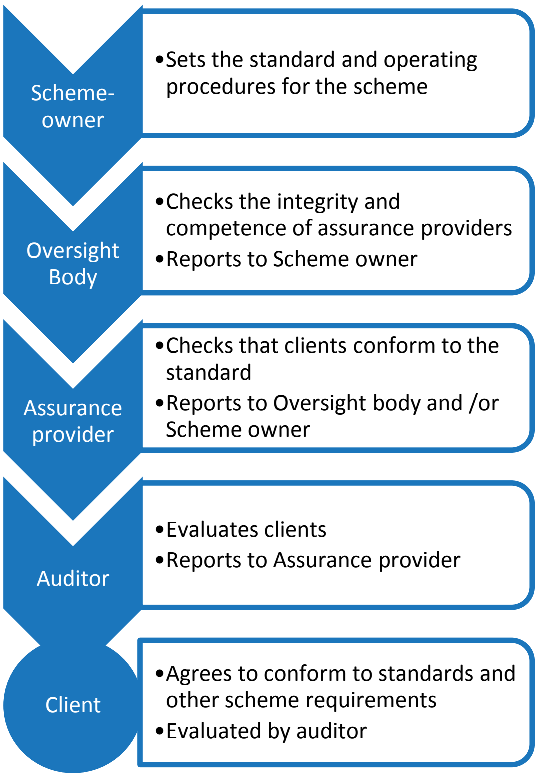
The Assurance Code uses established definitions whenever possible, to ensure consistent use of terms in the standards realm. However, the Assurance Code applies to many forms of assurance, so established terms such as 'certification' and 'accreditation', are not appropriate for all envisioned users. 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.

1) Standards System

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

2) Scheme owner

Organisation or governance body that is responsible for developing and maintaining the standard and the assurance scheme. The scheme owner sets the goals, vision, and specific scope of the scheme, as well as the rules for how the scheme will operate.



- Sets the standard and operating procedures for the scheme
- Checks the integrity and competence of assurance providers
- Reports to Scheme owner
- Checks that clients conform to the standard
- Reports to Oversight body and /or Scheme owner
- Evaluates clients
- Reports to Assurance provider
- Agrees to conform to standards and other scheme requirements
- Evaluated by auditor

NOTE: The scheme owner can be the standards owner, assurance provider, a governmental authority, trade association, group of assurance providers or other body (adapted in part from ISO 17067)

3) Assurance

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

4) First-party assurance (self-assessment)

Assurance activity that is performed by the person or organization that provides the object of assurance (adapted from ISO 17000)

5) Second-party assurance

Assurance activity that is performed by a person or organization that has a user interest in the object of assurance

NOTE: Persons or organizations performing second-party assurance activities include, for example, purchasers or users of products, or potential customers seeking to rely on a supplier's management system, or organizations representing those interests. (Adapted from ISO 17000)

6) 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)

7) Peer review

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

8) Assurance provider

Body that assesses compliance of a client with a standard. Also known as a verification body, certification body, or conformity assessment body

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

9) Assessment

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

10) Evaluation

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. An audit is the most typical form of evaluation (adapted from ISO 17000)

11) Auditor

Person who performs the evaluation. Also known as an inspector, verifier or assessor

12) Oversight

Assessment of an assurance provider’s demonstration of its competence to carry out specific assurance tasks. Formal, third-party oversight and attestation is known as accreditation (adapted from ISO 17000)

13) Calibration

The process by which different auditors, and other personnel involved in the assessment process, working in the same scheme, exchange and learn from each other to achieve more consistent interpretation and application of the standard

14) Client

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

15) Stakeholder

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

16) Statement of conformity

Generic expression used to include all means of communicating that fulfilment of specified requirements has been demonstrated (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 (adapted from AS/NZS 4360)

18) Risk mitigation (Risk reduction)

Actions taken to lessen the probability, negative consequences, or both, associated with a risk (adapted from AS/NZS 4360)

Question 1: Are there any definitions missing? Suggestions for improving the definitions?

4 Models of Assurance

This section describes the basic features exhibited by a set of the most common assurance models that occur in the voluntary standards realm. In some cases, the models are not compliant with the Assurance Code without the addition of extra requirements, which are featured in the descriptions. Scheme owners develop their assurance model to meet the objectives of the scheme and the needs of scheme users, balancing the needs of the market, the geographic and sector scope of the scheme, and the regulatory environment, among other factors. The descriptions do not capture every possible configuration of assurance models, rather they provide an overview of the models that commonly occur.

Model A: Third-party Assurance

In this model, assurance is carried out by one or more organisations that are independent from the client, the supply chain, and the scheme owner. Assurance providers and the auditors they employ have specific competencies for the scope of the standards systems that they audit. In many cases, the competence of the assurance providers in this model is assessed by an independent accreditation body. The focus of this model is on independence (e.g. separation of the person doing the evaluation from the person making the decision) to achieve impartiality, which will inspire confidence in the system.

In addition to compliance with the Assurance Code, scheme owners that operate third-party assurance systems are required to ensure that their assurance providers fulfil the requirements of either ISO 17065 or ISO 17021. Where this is assessed through accreditation, scheme owners are required to ensure that the accreditation body's management system is consistent with ISO 17011.

Model A is employed in many standards schemes including all ISEAL Full Members and industry led schemes such as Starbucks Cafe Practices.

Model B: Combination of 2nd and 3rd Party Assurance

Where an independent assessment of all clients is not feasible, a model that combines second and third party assurance is sometimes applied. This model usually involves a set of individuals or enterprises being organised into a structured group. The group is then responsible for internal monitoring of its members' compliance, often through (second-party) internal inspections. The internal management system of the group is then assessed through an independent (third-party), external audit. The external audit looks at both the effective functioning of the management system and cross-checks the performance of a sample of group members.

The third-party aspect of this model needs to be consistent with ISO 17065 or ISO 17021 as well as requirements for oversight described in the Assurance Code. As with Model A, confidence is inspired through independence and rigorous assessment, but also through group peer pressure and internal sanctions.

Model B is commonly employed for group certification within many agriculture and other product-based standards systems.

Model C: Combination of 1st and 3rd Party Assurance

This model builds off a self-assessment approach to assurance, with independent external audit checking conformance of a sample of clients. For this type of system to comply with the Assurance Code, the assurance provider would still need to evaluate the self-assessment, make a decision, and provide a statement of conformance. Additionally, the assurance provider would need to audit a sample of clients periodically. The assurance process would need to fulfil the requirements of ISO 17065, as well as requirements for oversight as described in the Assurance Code (Section 6.7). Extra elements of transparency help instil confidence while strong sanctions (for non-conformance) and provisions for market surveillance help ensure that clients conform to the standards.

The Green Electronics Council manages a scheme called EPEAT which closely resembles model C. 'European Conformity' (CE) marking employs some elements of Model C, but includes a cascade of increasing requirements dependent on the risk associated with the specific production.

Model D: Combination of 1st and 2nd Party Assurance

This model is built on the premise that participating clients can assess each other's compliance on a volunteer basis, and that external stakeholder participation in the review process adds to the integrity of the review. As in model B, individuals or enterprises are organised in groups. The groups may however also include other stakeholders, such as consumers, buyers, extension service operatives, and NGOs. The assessment of each member of the group is done by one or several other members of the group, possibly accompanied by other stakeholders. Involvement in the assessment is primarily voluntary; hence, assurance is a collective responsibility and not a business. This lack of exchange of fees removes a significant potential conflict of interest from this model and is what gives the model credibility even while it lacks the independence required by ISO 17000 series standards. Additionally, this model relies on extra amounts of transparency to inspire confidence.

As with model C this system needs to comply with requirements for oversight described in the Assurance Code (Section 6.7). This peer-review model is provided with specific exemptions in the Assurance Code, recognising that while it does not meet the ISO standards for independence, other factors (eg: extra transparency, reduced potential for conflict of interest) ensure its credibility.

The common use of Model D is with Participatory Guarantee Systems, primarily in organic certification.

Models Features Table

Model	Pros	Cons
A: 3rd Party Assurance	Widely accepted, strongest assurance model if the sampling is robust, independent	Expensive, potentially bureaucratic, less scalable
B: Combination of 2nd and 3rd Party Assurance	Accessibility, particularly for small enterprises, commonly accepted in the market, strong assurance if external assessment is robust	External assessment is reliant on very small samples (high audit risk)
C: Combination of 1st and 3rd Party Assurance	Inexpensive, minimal bureaucracy and cost	Requires strong sanctions to mitigate risk of self-assessment fraud, lack of independence
D: Combination of 1st and 2nd Party Assurance	Inexpensive, minimal bureaucracy, good for knowledge sharing	Reliant on volunteers, not widely accepted in international trade

Question 2: The models are included as explanatory guidance, to show how different assurance systems meet the needs of their users. Do the models add to the usefulness of the Assurance Code? Can you suggest any improvements?

5 General Provisions

5.1 Obligations of Scheme Partners

5.1.1 Responsibility for Compliance

Scheme owners shall be responsible for complying with the Assurance Code, including ensuring compliance of the organisations and individuals involved in delivering their assurance system.

5.1.2 Requirements for Assurance Providers

Scheme owners shall ensure that assurance providers substantially fulfil the requirements of ISO 17065 or ISO 17021 in addition to the relevant requirements in the Assurance Code, except under the following circumstances:

- Systems that employ a peer review process (e.g. Model D in section 4) for the client evaluation and decision are exempted from the requirements of ISO 17065 7.5.1 & 7.6.2

Question 3: Comments on the exception for participatory guarantee systems.

NOTE: The use of the language ‘substantially fulfil’ recognizes that some scheme owners adapt ISO 17065 or ISO 17021 to their schemes while also incorporating additional requirements. As long as these adaptations substantially fulfil the requirements of ISO 17065 or ISO 17021, they can be used as an acceptable basis for assurance provider requirements.

Question 4: Does the note above seem like a reasonable approach to the use of ISO standards in the Assurance Code?

Guidance: ISO 17065 and ISO 17021 are sufficient as a basis for good practice in the mechanics of assurance provision. However, these ISO standards do not account for all possible models of credible assurance, and in some cases compliance with them would work against innovation by restricting practices that are appropriate for that model. For this reason the Assurance Code provides exemptions in particular circumstances; where the exemptions serve to encourage innovation and enhance the ability of standards schemes to provide credible assurance.

5.1.3 Requirements for Accreditation

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

Guidance: Not all assurance models require accreditation as a formal mechanism to assess the competence of the assurance providers. However, all systems require some form of oversight and quality control of the assurance providers. In the case of accreditation, ISO 17011 provides a sufficient basis for good practice. For other oversight mechanisms, minimum requirements are defined in section 6.7.

Though this criterion requires conformance with ISO 17011, it does not prescribe membership by accreditation bodies in the International Accreditation Forum[1]*. In contrast to national accreditation, international accreditation is a better model for 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 bodies accredit certifiers worldwide, thus establishing a basis for equivalence and recognition of certificates issued by different assurance providers around the world.*

5.2 Scheme Management

5.2.1 Documented Assurance system

Scheme owners shall have a documented assurance system in place that complies with the Assurance Code.

Guidance: Minimum elements of an assurance system include:

- *Normative standard or standards*[2]
- *Criteria for accepting assurance providers to the scheme (including where the scheme-owner is the assurance provider)*
- *Criteria for accepting clients to the scheme*
- *Criteria for the assurance process e.g.: application, evaluation, review and decision, surveillance, sanctions, and complaints*
- *Criteria for the statement of conformity, (eg: certificate) which identifies the product, process, or service to which it applies*
- *Criteria for oversight of assurance providers*

[1] 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.

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

5.2.2 Subcontracting

If the scheme permits subcontracting of assurance activities such as testing, inspection or auditing, then the scheme-owner shall define the minimum requirements for these activities, and the degree to which prior permission must be gained from the scheme-owner or the client whose products are being certified under the scheme.

5.2.3 Reporting

Scheme owners shall set requirements for reporting by assurance providers and other organisations and individuals involved in delivering the assurance system. These requirements shall include:

- How assessment results are reported to the scheme owner;
- How results of surveillance activities are reported to the scheme owner.

Guidance: Having current information from the organisations involved in the scheme is essential for ensuring the integrity of the scheme, but information can also be useful for monitoring and evaluation of the scheme. Knowledge gained from regular receipt of information can be used to improve the efficiency and effectiveness of the scheme.

5.2.4 System review

Scheme owners shall have procedures and timelines for reviewing their assurance system at planned intervals to ensure its continuing integrity, adequacy, and effectiveness; including policies related to the fulfilment of this Code. Scheme owners shall use the results of the review to improve their assurance system where indicated and shall maintain records of any amendments.

Guidance: The purpose of the system review is to ensure scheme owners take responsibility for the integrity of the scheme. A standards system is a complex entity and requires vigilance to ensure client conformance and end user (consumer) confidence. Ultimately, the scheme-owner is responsible for the integrity of the scheme but receives advice and support from other organisations involved in the scheme (eg: assurance providers, accreditation bodies). Scheme 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. Scheme 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 scheme.

A system review can include:

- *Internal and external system audits of the scheme as a whole;*
- *Systematic review of client assessments (audits);*
- *Internal and 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*
- *Analysis of market and scientific trends*

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

5.2.5 Changes to the Assurance System

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

5.2.6 Selecting Assurance Providers (Optional Good Practice)

Scheme owners can have a policy that sets criteria for assurance providers that wish to participate in the scheme.

Guidance: This clause is specifically written for schemes that follow ISO 17011, as clause 4.3.3 in that document requires an accreditation body to, "...make its services accessible to all applicants whose requests for accreditation fall within the activities (see 4.6.1) and the limitations as defined within its policies and rules". The scheme owner however, has the ability to set policies that will guide accreditation bodies to determine whether to engage with assurance providers according to predefined criteria. Scheme owners may wish to set these policies in order to control the type and number of assurance providers operating in their scheme, for quality purposes or for other reasons such as capacity building.

Question 5: Do you feel this clause is a reasonable response to the need for schemes to control type and number of assurance providers working in their system?

6 Strategies for Effective Assurance

As one primary goal of the Assurance Code is to assist standards schemes to improve the effectiveness of their assurance systems, it is prudent for scheme owners to review common threats to the integrity of the assurance system in order to determine which strategies to employ to mitigate those threats. The following list represents a sample of the key risks to non-conformance:

Standards-Related Challenges

- Poorly written and vague standards leading to varying interpretations
- Reliance of assurance provider on standards setter for interpretation
- Frequent standards changes

Assessment Process Challenges

- Lack of client understanding or incentive
- Lack of auditor competence (skills, knowledge or attributes)
- Inadequate calibration between auditors (leading to inconsistent audit results)
- Lack of local or relevant auditor capacity (not enough trained and fluent auditors in a region)
- Inconsistent audit planning and lack of coordination
- Inadequacy of sampling methodology
- Lack of attention to absence of 'conformance culture' in a population

Systems Challenges

- Cost competitiveness between assurance providers reduces assurance quality
- Clients moving between assurance providers in a quest for a more relaxed assessment
- Assurance providers and/or auditors not understanding or applying the intent of the scheme
- Corruption (auditors, clients, assurance provider)
- Lack of adequate safeguards to prevent positive or negative bias
- Difficulty to engage stakeholders (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

Strategies to Address these Challenges

Scheme owners need to understand where are the greatest risks to the ability of their schemes to deliver standards compliant practices and need to determine what combination of strategies are best able to mitigate those risks to a level that is acceptable to the schemes' users. In making that determination, scheme owners will need to weigh considerations of cost (to implement a strategy) and acceptable level of risk.

The following strategies can assist standards systems to ensure conformance and instil confidence in the scheme. Those indicated with an asterisk fall outside of the scope of assurance and are not elaborated in this Code:

- **Clear standards (and accompanying guidance)*** are more likely to result in consistent application across the scheme
- **Increased transparency (6.2)** instils public confidence in the scheme

- **Capacity building of clients (6.3)** means they are more likely to understand and conform to standards and other requirements[3]
- **Auditor training and evaluation (6.4)** results in competent auditors who are more likely to detect errors and inform clients
- **Consistency of the assurance process (6.5)** ensures clients are treated uniformly and that results are consistent and accurate
- **Effective sampling (6.5)** contributes to an accurate picture of conformance throughout the scheme
- **Sanctions (and peer pressure) (6.6)** or the threat of sanctions encourages conformance
- **Oversight of the assurance process (6.7)** ensures consistency, competence and integrity amongst assurance providers
- **Market surveillance (6.8)** helps to detect and reduce instances of fraud

6.1 Risk Mitigation

Within an assurance system, risks occur at the client level (e.g. understanding the standard), at the assurance provider level (e.g. auditor competence) and at the scheme level (e.g. capacity to oversee the assurance system). As part of any assurance system, scheme owners need to consider the consequences of non-conformance for the integrity of their system, the types of risk relevant to their scheme, where these might occur within the scheme, and how to address or mitigate them.

6.1.1 Risk Mitigation Plan

Scheme owners shall document a plan for how they are addressing the risks of non-conformance within their system. The plan shall include:

- a list of the most significant risks in their system that are likely to lead to instances of non-conformance;
- a description of the strategies being employed by the scheme-owner to address each of these risks.

The scheme owner shall make this plan publicly available, at least through publication on its website.

Guidance: The list of challenges (see introduction to Section 6) can be seen as a partial list of potential system risk events. Rather than individual strategies (see list of strategies above) addressing individual risks, it is the combination of strategies that is likely to mitigate the risks. Risk evaluation is a tool that can be used to focus limited resources. For example, a scheme can use risk assessment 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 A for a brief description of risk management and examples of risk assessment.

[3] Other requirements refers to those requirements that are beyond the standard, such as requiring access by auditors, provision of public information, etc.

6.1.2 Review of the Risk Mitigation Plan

Scheme owners shall undertake a review and potential revision of the risk mitigation plan at least on the same interval as the system review, (clause 5.2.4) to assess its continued applicability and to update both the prioritisation of risks and the strategies used to mitigate those risks.

Guidance: 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 scheme's monitoring and evaluation programme, audit reports, oversight reports, auditor evaluations, complaints and stakeholder feedback.

6.2 Transparency

6.2.1 Publicly available information

Scheme owners shall ensure the following information regarding their assurance system is made publicly available. Where this information is produced by the assurance provider, the scheme-owner shall require publication by the assurance provider:

- Description of the structure of the assurance system, including the chain of authority and decision-making leading up to the governing body of the standards-scheme;
- Description of the type of assessment process employed, including how clients are assessed, how often, and by whom, and the audit sampling plan;
- The risk identification and mitigation plan (6.1.1);
- Current list of assurance providers that are approved to work in the scheme;
- Current list of certified clients (this can be made available at the assurance provider level);
- Current list of clients whose status has been rescinded or withdrawn (this shall be consolidated at the scheme-owner or oversight body level);
- Description of potential conflicts of interest at the organisation and individual levels for the scheme owner, assurance provider and oversight body (6.2.6);
- Policy on information provision (knowledge sharing) to clients by assurance providers (6.3.1);
- Policy on sanctions for different levels of non-conformance (6.6.1);
- Procedures for complaints to the scheme and public summary of resolved complaints, available on a continuous basis (6.8.2) NOTE: Complaints directed towards assurance providers or oversight bodies shall be handled first by those bodies;
- Procedure for granting exceptions in standards compliance and a list of current exceptions (6.5.11)

Optional Good Practice

The scheme-owner can determine whether to make the following information publicly available:

- Self-declaration attestations for every enterprise, where applicable

- Summary reports of assessments for every enterprise, where applicable[4]
- Fee schedule and sources of funding for each assurance provider (see 6.2.4)

Question 6: The list of public information is long, but commentators have been asking for more transparency in assurance. Do you feel the public information clause provides the right level of detail?

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

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

Complaints to the scheme can be from the public, from clients, or from assurance providers.

6.2.2 Information for Clients

Scheme owners shall ensure that clients have access to inspection findings and other documentation related to their assurance status, unless the documents are confidential (eg: filed complaints, confidential section of audit reports). This right shall be communicated to clients by the assurance providers. (adapted from IAC 5.4.8)

6.2.3 Information from Clients

Scheme owners shall ensure that assurance providers require disclosure of current enrolment in any other standards scheme by applicants and current clients.

Guidance: The disclosure of current enrolment in other schemes assists assurance providers to communicate with other schemes in cases of suspected fraud, and to co-ordinate with other schemes in the case of joint audits.

[4] Examples of publicly available assessment reports are available at the Forest Stewardship Council

6.2.4 Transfer of Clients

Scheme owners shall ensure that when clients choose to transfer their assurance business between assurance providers within the scheme, the new assurance provider:

- Requires clients to disclose previous enrolment with another assurance provider;
- Communicates with the previous assurance provider to ensure that outstanding issues with the client are taken into account by the new assurance provider;

Guidance: Assurance is generally a competitive business so the practice of 'shopping' for the best deal cannot be prohibited but measures can be instituted that will reduce the possibility of corruption. The practice of skipping from one assurance provider to another in order to access a favourable assessment is a high risk factor for the integrity of the scheme.

Scheme 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 scheme owners to instances of client transfer.

Question 7: Can you think of any other measures that will help mitigate the risk associated with clients moving from one assurance provider to another?

6.2.5 Fee Schedule

Schemes-owners shall ensure, either directly or through the oversight body, that fees charged by organisations involved in delivering their assurance system are applied consistently across clients. Scheme owners shall require these organisations to make general information on the fees charged to clients available both to the oversight body and to their clients.

Guidance: Though assurance provision is generally a competitive service, this competition for clients can work against conformance by encouraging cost-cutting that results in poor quality assurance.

6.2.6 Stakeholder Engagement

Scheme owners shall ensure that stakeholders are informed of the points where they may comment (or participate in) the assurance process.

Optional good practice:

Stakeholders can be involved in the assessment process; as participants in the evaluation and review, or as observers.

Guidance: Active inclusion of stakeholders in the assurance process increases the transparency, and thus public trust in the process. Inclusion of stakeholders can improve the effectiveness of assurance as *stakeholders can act as eyes and ears for the assurance provider as a component of surveillance activities. 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. Additionally, the role and limits of stakeholders in the assessment process need to be clearly defined.*

6.2.7 Conflicts of interest

Scheme owners shall describe what constitutes a conflict of interest within their scheme and set parameters on what is permissible; to ensure consistent application of conflict of interest rules across the scheme.

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, a person who is applying for a contract from an organisation would be in a conflict of interest if they also sat on the board of that organisation. Potential conflicts of interest are prevalent in service delivery, 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 scheme-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, there remain potential conflicts, such as assessing one's own work, that require an exclusionary response.

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 6.3.1)*

6.3 Capacity Building

6.3.1 Provision of Information

Scheme owners shall have a clearly defined and publicly available policy on the provision of information to clients by assurance providers. This policy shall define what type of information, if any, can be provided by auditors (or other assurance personnel) to clients. Where information or advice is provided, this shall be in accordance with guidance notes and other information issued by the scheme, consistent across the scheme, and offered to clients in a consistent manner (treating all clients equally).

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 that organisation is evaluating the client, they are assessing the results of their own advice and are less likely to act impartially.

However, knowledge sharing or capacity building 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, scheme owners need to ensure information 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. Information provided by assurance providers should be generic, not client-specific, and should be limited to interpretation of standards requirements and their rationale.

An auditor should never give direct advice about how to achieve compliance with a standard requirement (as different auditors might make different suggestions). However, an auditor should feel free to provide feedback on why an identified issue is a non-compliance (often clients don't quite understand what the problem is and helping them understand this is essential), provide good practice through observations or identified opportunities for improvement, or provide examples of how other clients have addressed similar issues (sharing experience without giving direct advice whilst maintaining confidentiality and respecting proprietary information).

Question 8: This clause has been controversial, but we feel we have the right mix of requirements and criteria to allow assurance personnel to be helpful while still being seen as impartial. Comments please.

6.4 Auditor Competence

Auditors play a crucial role in the assurance process that requires a certain personal aptitude combined with knowledge, experience, and common-sense. Not only do auditors perform the evaluation, but they are often the eyes and ears of the standards system, and sometimes a client's only personal connection to the scheme.

Auditing is not a simple matter of completing a checklist of questions. Auditors need to be able to use their judgement to come to a quick understanding of a client's shortcomings, assets, and needs; and to deduce the correct interpretation of what they observe. Among the strategies to mitigate the risks of non-conformance, 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).

6.4.1 Defining Auditor Requirements

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

Guidance: 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.

Example of generic requirements model for an audit team leader

Knowledge and Skills	**Qualifications**	**Competencies**	**Possible Verification Mechanisms**
General	Degree or equivalent in business, economics, science or technical subject E.g.: supply chain and logistics management, natural resources management		CV, certificates
Understanding of the scheme standard	Attendance at annual scheme-led lead assessor training course	Demonstrate an understanding of the principles and criteria	On-line lead assessor training and examination
Interviewing stakeholders	Attend a formal training course approved by the scheme 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.	Previous assessment reports or other audit reports, employer reference letters, certifier records, accreditation assessment reports

6.4.2 Training

Scheme owners shall ensure that auditors and other personnel receive initial and ongoing training according to the requirements of their respective positions (see ISO 17021-2 clause 7.2.8 or ISO 17065 clause 6.1.2.1). Beyond this basic training, scheme owners shall ensure that auditors are trained in the following:

- Interpreting the standard(s) in different contexts by understanding the intent of each criterion;
- Conducting qualitative interviews;
- Performing sampling tasks;

- Guidelines and limits on providing information and advice during an audit.

6.4.3 Auditor Calibration

Scheme owners shall develop and implement directly or through assurance providers, a 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 scheme 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. Scheme owners who are designing calibration procedures should consider including a wide range of personnel involved in assurance (eg: auditors, managers, decision-makers).

6.4.4 Mentoring

Scheme owners shall ensure that auditors new to the scheme are required to complete a probationary period during which they are supervised by qualified auditors and are provided with mentoring and other on-the-job learning opportunities. The scheme-owner shall define and document the probationary and mentoring requirements with the assurance providers.

Guidance: Auditors must be trained but it also essential that an auditor's performance is observed by competent mentors or trainers working in the field before they are expected to undertake audits on their own. This can be accomplished simply by including newly-hired auditors as part of an audit team. Alternatively, new auditors can accompany experienced auditors for a number of probationary (mentoring) audits. At the end of the probationary period new auditors should be evaluated.

6.4.5 Continuing Employment (Optional good practice)

Scheme owners can work with assurance providers to increase the quantity of work allocated to each auditor (towards full-time employment). This can be achieved through scheduling, joint audits, or sharing auditors between similar schemes.

Guidance: A significant factor in the competence of auditors is that they have sufficient opportunity to conduct audits, providing them with a breadth of experience in interpreting the standard(s) for different contexts. It is difficult to prescribe continuous employment as a requirement and schemes should be aware of potential trade-offs such as potential increased costs of using experienced auditors who may have to travel further.

6.4.6 Evaluation of competency

Scheme owners shall ensure that the competence of auditors and other assurance personnel is demonstrated on an ongoing basis through evaluation by the assurance providers or other entities (see ISO 17021-2 clause 7.1.3). Evaluations of auditor competence shall include witness audits.

To support evaluation of competency, scheme owners shall develop and document an evaluation protocol with their assurance providers for the evaluation of auditors and other assurance personnel. The protocol shall include at least:

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

Optional Good Practice:

Scheme owners can develop a screening process when recruiting and hiring auditors, which could include a ranked list of desirable personal attributes applicable to different roles within the assurance process. Auditors could then be selected based on how well their personalities match with the desired attributes.

Question 9: There are a number of clauses in the Assurance Code that include an optional best practice. How do you feel about this method of providing suggestions without being overly prescriptive?

Guidance: 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. ISO 17021-2 Annex B describes possible evaluation methods. Regardless of the tools used (personality or aptitude testing or interviewing) this process is likely to include large margins of error.

Question 10: Comments on section 6.4 Auditor Competence

6.5 Consistency of 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. Consistent requirements will ensure fair treatment of all clients across a scheme and will prevent competition (amongst assurance providers) from eroding the integrity of the assurance process.

6.5.1 Assessment Required

Scheme owners shall ensure that their assurance system includes an assessment of an enterprise’s compliance with the relevant standards. The assessment shall include at least the following activities:

- Evaluation (eg: audit of sites, or inspection of records or of self-assessment declarations)
- Review and decision
- Issuance of a statement of conformity
- Periodic re-assessment

At minimum, the assurance system shall include provisions for periodic on-site audits of at least a sample of clients.

6.5.2 Assessment Procedure

Scheme owners shall define and document procedures for assessments and shall provide these procedures to assurance providers. The procedures shall include at least the following:

- Requirements for audits (on-site and desk audits), including:
    - frequency of audits;
    - sampling protocol for audits (unless 100% sample is used) (6.5.4);
    - structure of the audit team (if used);
    - minimum set of issues that need to be checked in every audit;
    - protocol for calculating audit time, and criteria for when time can be reduced;
    - approximate balance of time between office, field, and interviews;
    - documentation to be reviewed;
    - timelines for submission of completed reports, following evaluations; and
    - minimum content of evaluation reports.
- Requirements for self-declarations, if used, including:
    - frequency of reporting; and
    - content and level of detail required.

Question 11: Are these list detailed enough; or perhaps too detailed? Can you provide suggestions for improvements?

Optional Good Practice

Scheme owners may wish to include a stakeholder consultation as part of the assessment process. In this case stakeholders would be informed of the assessment and asked to provide input.

Guidance: Standardised forms and reporting documents are helpful for ensuring consistent application of the scheme across numerous assurance providers. Self declarations are often used in addition to audits – the client first submitting the self-declaration, which is later verified through an on-site audit.

6.5.3 Audit Frequency and Intensity (Optional good practice)

Scheme owners can choose to use a risk-based approach to determine audit frequency and intensity. Scheme owners can 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 scheme (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*[5]*.*
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 .*

6.5.4 Sampling Within the Audit

Scheme owners shall define and document the sampling procedure that auditors shall use during the audit and shall provide this direction to assurance providers, as well as making the procedure publicly available.

The sampling procedure shall include, at minimum:

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

- A description of when sampling is to be employed in the audit; and
- The sampling formula or procedure to employed in each instance.

Optional Good Practice:

Scheme owners can require assurance providers to direct auditors to include at least 25% random samples in any audit sampling.

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

1. *Representative sampling: 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.*
3. *Protective sampling: a focus on the issues that are of highest impact to the scheme'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. Including some component of random sampling can also increase the likelihood of identifying non-conformities.

When sampling is included within an audit it is important that the auditor chooses the sample, not the client. 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.

6.5.5 Assessment of Groups or Multi-Site Operations (Optional good practice)

Scheme owners that include assessment of groups of producers or enterprises or of multi-site operations should comply with the ISEAL Common Requirements for the Certification of Producer Groups.

6.5.6 Random Samples

Where the scheme seeks to extrapolate audit findings in order to draw conclusions about conformity of a whole population (e.g. sampling in group certification or multi-site operations), the scheme-owner shall require that assurance providers choose the sample at random. The scheme-owner shall define a standardized formula for determining sample size based on the total population and, potentially, on defined risk factors, 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 random sample should be taken to measure non-conformity levels in the population as a whole.*

An example of a procedure for determining sample size could be:

1. *Determine the risk factors influencing the integrity of the group or client, such as:*
   - *Similarity of group members' production;*
   - *Status of internal inspection reports;*
   - *Level of competence of internal inspectors;*
   - *Previous issues raised in internal inspections;*
   - *Previous issues raised in external assessments;*
   - *Growth rate in group size;*
   - *Stability of group management.*
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 group audit sample size. An example of this could be:*
   - *High-risk groups: 2 x square root;*
   - *Medium-risk groups: square root;*
   - *Low-risk groups: ½ x square root.*

6.5.7 Failed Random Samples

Scheme owners shall define the repercussions for the status of the group or multi-site client of identifying non-conformities in individual samples. Should the number of samples with critical or major non-conformities exceed a defined threshold, the scheme-owner shall require that the group or client be immediately suspended.

Guidance: This criterion requires that the scheme-owner develops an objective procedure for the repercussions of finding failed random samples. That procedure should include a table identifying the number of failed samples that are allowed for different total sample sizes, for example:

Number of Samples	Threshold Number of Failed Samples 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)

Question 12: Please comment on the utility of this clause for your assurance system.

6.5.8 Use of Translators

Scheme owners shall request that when assurance providers use translators in evaluations, the translators are independent of the enterprise being evaluated. Where this is not feasible, the assurance providers shall be required to include the name and affiliation of translators in evaluation reports.

6.5.9 Decision-Making Mechanism

Scheme owners shall clearly define the decision-making mechanism (e.g. scorecard, traffic light, critical criteria, etc.) and shall provide specific direction on the determination and handling of non-conformities. Scheme owners shall require assurance providers to apply this protocol consistently.

6.5.10 Other information

Scheme owners shall define the criteria by which information obtained from other sources (eg: test results, other assurance results) may be included in the assurance process.

NOTE: Other sources are sources that are not under the contractual control of the assurance provider.

6.5.11 Exceptions

Scheme owners shall have a procedure for granting exceptions in standards compliance where this occurs. The rationale for exceptions shall be recorded and made available for use in subsequent decisions (as a precedent) and as input to the subsequent standards review exercise. A list of current exceptions shall be made publicly available. Exceptions shall only be valid until the next standards revision process where a decision shall be made about whether to incorporate them into the standard.

Question 13: Do you agree that the list of exceptions should be made publicly available?

6.5.12 Statement of conformity

Scheme owners shall set requirements for the use of statements and marks of conformity, which shall include at least the following:

- How they are issued: by whom and to whom, and under what authority;
- Their duration;
- How they can be withdrawn from use; and,
- How they can be used in public communications.

Question 14: Comments on section 6.5

6.6 Sanctions

6.6.1 Sanctions

Scheme owners shall define and make publicly available the repercussions or sanctions for different levels of non-conformance (for clients and for assurance providers). This shall include definitions of the points at which non-conformity of the client and of the assurance provider result in suspension or termination from the programme.

Guidance: Standards systems can employ a range or combination of sanctions:

- *Suspensions (including loss of marketing ability during period of suspension)*
- *Publishing summary reports including non-compliances*
- *Extra audits, resulting in extra scrutiny*
- *Fines*
- *Termination of statements of conformity*

As one of a number of elements that encourage conformance, the threat of sanctions should 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.

6.7 Oversight

6.7.1 Competence of Assurance Providers

Scheme owners shall ensure that the competence and consistent performance of assurance providers is periodically reviewed. Scheme owners shall determine which organisation(s) shall provide oversight and shall specify the approach to be used in oversight. Scheme owners shall periodically assess the effectiveness of the chosen approaches.

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 self-declaration scheme could employ an independent assurance body to review the assurance system. Alternatively, a scheme owner could arrange to oversee the work of assurance providers directly.

6.7.2 Extent of Oversight (Optional Good Practice)

Scheme owners that use a risk-based approach to determine the extent of oversight of assurance providers can 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 (6.5.3).

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

- *History of the assurance provider within the scheme;*
- *Growth rate of the assurance provider;*
- *History of low quality of audits in evaluations by assurance provider;*
- *Complaints*

6.7.3 Oversight Procedure

Scheme owners shall define the procedures to be followed in oversight. At a minimum, oversight shall include a review, at regular intervals, of:

- 〉 the management system of assurance providers;
- 〉 the competence of assurance personnel (including a selection of witness audits); and
- 〉 the results of the assurance activity.

Optional Good Practice:

Scheme owners can choose to prescribe specific activities for oversight including:

- In-depth monitoring of a specific issue across all assurance providers in the scheme, to compare, and therefore determine the level of competence and consistency of assurance across the scheme;
- 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.

6.7.4 Witness Audits

Scheme owners shall define a sampling protocol for witness audits in oversight, including how to determine which auditors to evaluate.

Guidance: Carrying out witness audits is about checking auditors' understanding and application of the standard as a reflection of whether the assurance provider's management system is working. Witness audits help to assess assurance provider performance as well as individual auditor competence. Results of witness audits should be made available to assurance providers and to the scheme owner to use in their own monitoring and improvement programmes.

Question 15: Do you agree that oversight procedures should include a selection of witness audits?

6.7.5 Competence of Oversight Bodies

Scheme owners shall ensure that entities providing oversight of assurance providers have the following competencies and apply these in their evaluation of assurance providers:

- in-depth knowledge of the standard and its intent (and other requirements) and an understanding of the goals of the scheme, and in particular, the critical issues of the scheme 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 of enterprises (group certification), where this is undertaken by the assurance provider.

Where oversight bodies do not have in-depth knowledge of the standard, scheme owners shall undertake their own evaluation of an assurance provider's competency in this area.

Question 16: How do you feel about requiring scheme owners to evaluate assurance providers in cases where the oversight body does not have in-depth understanding of the standards programme?

Guidance: To evaluate an assurance provider's competence regarding standards criteria, the scheme owner may choose to monitor assessment reports, acting as a stakeholder in the assurance system. Scheme owners should refer to sections 10 and 11 of the ISEAL Common Requirements for the Certification of Producer Groups for criteria against which to assess the assurance provider's competence to assess groups.

6.7.6 Proxy Accreditation

Where scheme owners accept assurance providers that have been accredited against other scopes, they shall assess whether the external accreditation body meets the relevant requirements in this section (6.7.3 to 6.7.5). Where this is not the case, scheme owners shall ensure that additional oversight of the assurance providers is carried out to comply with these requirements. In addition, scheme owners shall ensure that external accreditation bodies include the scheme scope when they undertake internal audits and management reviews of their accreditation programme.

Guidance: It is sometimes the case that a scheme-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 scheme-owner to ensure that all personnel involved in their scheme (auditors and decision-makers) have a demonstrated knowledge and understanding of that scheme's content and procedures and the skills to assess compliance.

6.8 Ongoing Scrutiny

6.8.1 Market Surveillance

Scheme owners shall define and implement a procedure for surveillance activities that will be undertaken by the scheme-owner. 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.

Question 17: Is it reasonable to ask the scheme owner to do the above?

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.*

Guidance: Depending on risk assessment, and the needs of the market, scheme owners can choose from the activities listed above (and other activities, not listed). There are many ways to encourage conformance whilst instilling confidence in the scheme and a mix of methods targeted to high-risk clients may provide more veracity than relying on an individual audit at a single point in time.

6.8.2 Fraudulent claims

Scheme owners shall define and document the actions, repercussions and who is responsible for dealing with cases where assurance under the scheme is being fraudulently claimed.

Guidance: When cases of fraud are discovered the scheme-owner needs to take steps to protect consumers and to protect the integrity of the scheme. Suggested activities include:

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

Question 18: Can you think of any additional steps to take when enrolment in the scheme is being fraudulently claimed?

6.8.3 Complaints

The scheme-owner shall document and implement a complaints procedure that is accessible and responsive. The procedure shall facilitate complaints regarding:

- the scheme (from clients or the public);
- fraud or potential fraud; and
- the assurance system or assurance providers.

The procedure shall require the scheme-owner to:

- investigate and take appropriate action regarding relevant complaints;
- review and take any necessary corrective action to the scheme or scheme requirements; and
- keep a record of all complaints and resulting actions.

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

Scheme owners should consider the complaints system an essential component of the assurance system, 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 programme. The complaints systems should be easy to access on the standards system's website and should allow users to file a complaint electronically at the very least.

Question 19 Space for more comments on the text

Annex A - 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**	**Likely**	**Occasional**	**Seldom**	**Unlikely**	**Unknown**
		A	**B**	**C**	D	E	**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 (scheme 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.

Example: Scheme risk assessment

5.1.1 Scheme Risk Prioritisation: Scheme owners shall determine, categorise and rank the risk events that could compromise the integrity of their assurance system and its contribution to the objectives of the scheme.

1) Identify possible risks to the integrity of the assurance system[6]:

   - Auditor does not visit all relevant sites
   - The audit sample is not representative of the population
   - Assurance provider only interested in keeping enterprises happy – overlooks non-compliances
   - Enterprise is forewarned of the audit so covers-up the non-compliances

[6] These are four examples of what could be many risks to the integrity of the assurance system

2) Rank the risk events according to their probability of occurrence, and the consequences if they do occur:

Risk event	Probability	Consequences	Risk Level
Auditor does not visit all relevant sites	Occasional	Moderate	Medium
The audit sample is not representative of the population	Likely	Critical	High
Assurance provider only interested in keeping enterprises happy	Occasional	Critical	High
Enterprise is forewarned of the audit so covers-up the non-compliances	Occasional	Critical	High

3) Once the risk events are ranked the next step is to identify strategies to manage the risks that are most crucial, (high) though medium and low risks should be managed if controls are simple to implement. Examples of strategies for mitigating the high risk events:

- The audit sample is not representative of the population
    - Employ statistical sampling techniques – 6.5.6 Random Samples
    - Sample 100% of the population (every audit round, or over a certain period)
- Assurance provider only interested in keeping enterprises happy
    - Involve stakeholders in the assurance process - 6.2.6 Stakeholder Engagement (Optional good practice)
    - Implement procedures for selection of assurance providers – 5.2.6 Selecting Assurance Providers (Optional good practice)
- Enterprise is forewarned of the audit so covers-up the non-compliances
    - Integrate unannounced audits into the periodic assessment process
    - Implement surveillance activities – 6.8.1 Market Surveillance

4) The next step is to implement strategies to mitigate risk. Rank possible risk control strategies (there could be many more than the examples provided) according to cost, feasibility, and possible effectiveness. Then make a decision about which controls to employ.

5) Review the results: it is especially important to review the strategies at intervals to see whether and how well they have worked.