European
co-operation for
Accreditation

Publication Reference **EA-7/03**

EA Guidelines for the Accreditation of Bodies Operating Certification/ Registration of Information Security Management Systems

PURPOSE

The text of this document has been produced by a working group in the European co-operation for Accreditation (EA). The purpose of this document is to provide explanations with a view to harmonise the application of ISO/IEC Guide 62 / EN 45012 in the field of Information Security Management Systems, by accreditation bodies, their assessors and certification/ registration bodies preparing for accreditation. This document was approved by the EA General Assembly in November 1999.

ISO/IEC Guide 62 / EN 45012 remains the authoritative document and in case of dispute concerning the application of this document, the individual accreditation bodies will adjudicate on unresolved matters.

Authorship
This document has been written by EA C5 WG7 on Information and Communication Technology.

Official language
The text may be translated into other languages as required. The English language version remains the definitive version.

Further information
For further information about this publication, contact your national member of EA. Please check our website for up-to-date information http://www.european-accreditation.org

CONTENTS

INTRODUCTION TO THE EA GUIDELINES FOR THE ACCREDITATION OF BODIES OPERATING CERTIFICATION/ REGISTRATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)

The text in this document is drawn from three main sources: original text of ISO/IEC Guide 62:1996 (to which EN 45012:1998 is identical), original text of IAF Guidance to ISO/IEC Guide 62, and specific text giving additional guidance on the application of EN 45012 to bodies involved in ISMS certification/ registration. The Guide 62 text and the IAF Guidance text have been modified as necessary to suit Information Security Management Systems (ISMS). The (minimum) alterations in the original texts and the specific ISMS guidance text were initially developed by an UK working group sponsored by UKAS and have been further developed by EA working group EA-C5-WG7 on Information and Communications Technology.

The source of the texts can be identified by the use of different fonts:

- **Text of ISO/IEC Guide 62 – with minimum alterations to make it applicable in the field of ISMS. EA acknowledges ISO's ownership of this material and will revise this document in the event that ISO/IEC publish the material in final form.**
- IAF Guidance to ISO/IEC Guide 62 – with minimum alterations to make it applicable in the field of ISMS.
- EA Guidance to ISO/IEC Guide 62 specifically for ISMS.

The term "shall" is used throughout this document to indicate those provisions which, reflecting the requirements of ISO/IEC Guide 62, are mandatory. The term "should" is used to indicate those provisions which, although they constitute guidance for the application of the requirements, are expected to be adopted by a certification/registration body. Any variation from the guidance by a certification/registration body shall be an exception. Such variations will only be permitted on a case by case basis after the certification/registration body has demonstrated to the accreditation body that the exception meets the relevant requirements clause of ISO/IEC Guide 62 and the intent of this Guidance in some equivalent way.

INTRODUCTION TO CERTIFICATION/REGISTRATION OF ISMS

Standards for Information Security Management Systems (ISMS) provide best practice rules for organisations. The standard BS 7799 Part 2 and other normative documents are specifications for information security management, suitable for ISMS based certification/ registration. They provide a comprehensive set of security controls comprising the best information security practices in current use. Their objective is to provide organisations with a common basis for providing information security and to enable information to be shared between organisations. This is particularly important where organisations wish to inter-connect electronically.

Certification/ registration of an organisation's information security management system (ISMS) is one means of providing assurance that the certified/ registered organisation has implemented a system for the management of information security in line with a standard or normative document.

This publication specifies requirements, the observance of which is intended to ensure that certification/ registration bodies operate third party certification/ registration systems in a consistent and reliable manner, thereby facilitating their acceptance on a national and international basis. This publication should serve as a foundation for the recognition of national systems in the interests of international trade.

The publication is intended for use by bodies, however described, which carry out the functions of assessment and ISMS certification/ registration. For convenience of drafting, such bodies are generally referred to as 'certification/ registration bodies'. This wording should not be an obstacle to the use of this document by bodies with other designations, which undertake activities, which are covered in this publication. Indeed, this publication should be usable by any body involved in ISMS certification/ registration.

ISMS certification/ registration involves the assessment of an organisation's ISMS but does not imply achievement of specific levels of information security related to its products and services. Evidence of conformity to the standard or normative document and any supplementary documentation will be in the form of a certification/ registration document. ISMS certification/ registration ensures that the organisation has undertaken a risk assessment and has identified and implemented controls appropriate to the information security needs of the business.

Certification/ registration of an ISMS is entirely voluntary. Organisations which successfully complete the certification/ registration process can have greater confidence in their information security management and will be able to use the certificate to help assure trading partners with whom they share information. The certificate makes a public statement of capability whilst permitting the organisation to keep details of its information security measures confidential.

While this publication is intended for use of bodies concerned with recognising the competence of certification/ registration bodies, many provisions contained herein may be useful in second party assessment procedures.

SECTION 1 GENERAL

1.1 Scope

This publication specifies general requirements for a third-party body operating ISMS certification/ registration to meet, if it is to be recognised as competent and reliable in the operation of ISMS certification/ registration.

NOTE 1 In some countries, the bodies which verify conformity of ISMS to specified standards are called "certification bodies", in others "registration bodies", in others "assessment and registration bodies", or "certification/ registration bodies", and in others still, "registrars". For ease of understanding, this publication always refers to such bodies as "certification/ registration bodies". This should not be understood to be limiting.

The requirements contained in this publication are written, above all, to be considered as general requirements for any body operating ISMS certification/ registration.

1.2 References

ISO/IEC Guide 2: 1996, General terms and their definitions concerning standardisation and related activities.

ISO 8402: 1994, Quality management and quality assurance - Vocabulary

ISO/IEC Guide 62: 1996, General requirements for bodies operating assessment and certification/ registration of quality systems.

BS 7799 Part 1: 1999, Code of practice for information security management.

BS 7799 Part 2: 1999, Specification for information security management systems.

ISO 10011-1: 1990, Guidelines for auditing quality systems - Part 1: Auditing

ISO 10011-2: 1991, Guidelines for auditing quality systems - Part 2: Qualification criteria for quality system auditors

ISO 10011-3: 1991, Guidelines for auditing quality systems - Part 1: Management of audit programmes

1.3 Definitions

For the purposes of this publication, the relevant definitions in ISO/IEC Guide 2, BS 7799 Part 1 and BS 7799 Part 2 and the following definitions apply.

1.3.1 Organisation

Company, corporation, firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration and is able to ensure that information security is exercised.

1.3.2 Certification/registration body

A third party that assess*es* and certifies/ registers the ISMS of an organisation with respect to published ISMS standards, and any supplementary documentation required under the system.

1.3.3 Certification/registration document

Document indicating that an organisation's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system.

1.3.4 Certification/registration system:

System having its own rules of procedure and management for carrying out the assessment leading to the issuance of a certification/ registration document and its subsequent maintenance.

IAF Guidance

G.1.3.1. The following definitions apply to the guidance in this document:

Assessment: All activities related to the certification/ registration of an organisation to determine whether the organisation meets all the requirements of the relevant clauses of the specified standard necessary for granting certification/ registration, and whether they are properly implemented, including documentation review, audit, preparation and consideration of the audit report and other relevant activities necessary to provide sufficient information to allow a decision to be made as to whether certification/ registration shall be granted.

Logo: A symbol used by a body as a form of identification, usually stylised. A logo may also be a mark.

Mark: A legally registered trade mark or otherwise protected symbol which is issued under the rules of an accreditation body or of a certification/ registration body indicating that adequate confidence in the systems operated by a body has been demonstrated or that relevant products or individuals conform to the requirements of a specified standard.

Nonconformity: The absence of, or the failure to implement and maintain, one or more required management system elements, or a situation which would, on the basis of objective evidence raise significant doubt as to the capability of the ISMS to achieve the security policy and objectives of the organisation.

The certification/registration body is free to define grades of deficiency and areas for improvement (e.g. Major or Minor Nonconformities, Observations, etc). However, all deficiencies, which equate to the above definition of nonconformity should be dealt with as laid down by G.3.5.2 and G.3.6.1.

G.1.3.2. The accredited scope(s) of a certification/ registration body is expressed in terms of one or more elements from the list of industrial sectors or product categories, known as the "scope of accreditation" (refer to Annex 1).

G.1.3.3. Other limitations to the accreditation may apply, for example a restriction to certain offices or locations.

ISMS Guidance

IS.1 The accredited scope(s) of a certification/ registration body is closely related to auditor competence, which is among other things important in auditing risk analysis as carried out by organisations in the development and maintenance of their ISMS. The certification/ registration body is required to demonstrate to the accreditation body that auditors are competent in the industrial sectors in which ISMS are assessed and certified/ registered.

SECTION 2 REQUIREMENTS FOR CERTIFICATION/ REGISTRATION BODIES

2.1 Certification/ registration body

2.1.1 General provisions

2.1.1.1 The policies and procedures under which the certification/ registration body operates shall be non-discriminatory and they shall be administered in a non-discriminatory manner. Procedures shall not be used to impede or inhibit access by applicants other than as specified in this publication.

2.1.1.2 The certification/ registration body shall make its services accessible to all applicants. There shall not be undue financial or others conditions. Access shall not be conditional upon the size of the organisation or membership of any association or group, nor shall certification/ registration be conditional upon the number of organisations already certified/ registered.

2.1.1.3 The criteria against which the ISMS of an applicant are assessed shall be those outlined in the ISMS standard or other normative documents relevant to the function performed. If an explanation is required as to the application of these documents to a specific certification/ registration programme, it shall be formulated by relevant and impartial committees or persons possessing the necessary technical competence and published by the certification/ registration body.

2.1.1.4 The certification/ registration body shall confine its requirements, assessment and decision on certification/ registration to those matters specifically related to the scope of the certification/ registration being considered.

<u>IAF Guidance</u>

G.2.1.1. The provision “if an explanation is required” in clause 2.1.1.3 of ISO/IEC Guide 62 should be applied by limiting such documents to those recognised by the accreditation body. The term “and supplementary documentation required under the system” used in clauses 1.3.1 and 1.3.3 of ISO/IEC Guide 62 should mean documentation recognised by the accreditation body, which provides additional or supplementary guidance as to the application of the relevant standard or guide. See also guidance G.2.1.9. In exceptional cases the certification/ registration body itself may issue supplementary documentation, subject to the requirements of clause 2.1.1.3 of ISO/IEC Guide 62.

G.2.1.2. Certification/ registration of an ISMS shall give adequate confidence that the system meets specified requirements. A certification/ registration of conformity of an organisation’s ISMS shall demonstrate that an organisation has implemented and is maintaining an effective ISMS in the area specified on the certificate, and is operating its processes in accordance with that system.

G.2.1.3. In practice “specified requirements” in Guidance G.2.1.2 means the requirements agreed between the client and the organisation. If an organisation provides services to a claimed specification, the client may make these “agreed requirements” by the act of purchasing. “Agreed requirements” include “legal requirements” if compliance with them is claimed by, or mandatory upon, the organisation. In any case compliance with applicable legal requirements applying to a product or service will normally be a client requirement if only as an implied term of contract to be considered under contract review.

G.2.1.4. Certification/ registration bodies shall not practice any form of discrimination such as hidden discrimination by speeding up or delaying applications.

G.2.1.5. Clause 2.1.1.2 of ISO/IEC Guide 62 requires certification/ registration bodies to make their services available to all applicants. They may, however, provide a certification/ registration service, which excludes areas of activity where the certification/ registration body is not qualified to certify/ register, or has elected not to provide service to any organisation in a particular category. For example, a certification/ registration body may, in so far as the law permits, limit its service to applicants operating in a defined geographic region, or it may limit its service to organisations operating within the technical sector, or part of a sector, in which the certification/ registration body has its accredited scope.

G.2.1.6. A certification/ registration body may offer product conformity certification or quality system certification/ registration linked with ISMS certification/ registration, or may offer ISMS certification/ registration only.

G.2.1.7. Where a certification/ registration body certifies/ registers organisations against a normative document other than a standard, the document shall be publicly available.

G.2.1.8. The term "a specific certification/ registration programme" used in clause 2.1.1.3 of ISO/IEC Guide 62 may include sector-specific schemes.

G.2.1.9. The formulations of explanations as to the application of these documents as referred to in clause 2.1.1.3 of ISO/IEC Guide 62 should be restricted by certification/ registration bodies accredited by an accreditation body which is a member of the EA to guidance published by EA – see guidance G.2.1.1.

2.1.2 Structure

The structure of the certification/ registration body shall be such as to give confidence in its certification/ registrations.

In particular, the certification/ registration body shall

a) be impartial;

b) be responsible for its decisions relating to the granting, maintaining, extending, reducing, suspending and withdrawing of certification/ registration;

c) identify the management (committee, group or person) which will have overall responsibility for all of the following:

1) performance of assessment and certification/ registration as defined in this publication,

2) the formulation of policy matters relating to the operation of the certification/ registration body,

3) decisions on certification/ registration,

4) supervision of the implementation of its policies,

5) supervision of the finances of the certification/ registration body,

6) delegation of authority to committees of individuals, as required, to undertake defined activities on its behalf;

d) have documents which demonstrate that it is a legal entity;

e) have a documented structure which safeguards impartiality, including provisions to ensure the impartiality of the operations of the certification/ registration body; this structure shall enable the participation of all parties significantly concerned in the development of policies and principles regarding the content and functioning of the certification/ registration system;

f) ensure that each decision on certification/ registration is taken by a person or persons different from those who carried out the assessment;

g) have rights and responsibilities relevant to its certification/ registration activities;

h) have adequate arrangements to cover liabilities arising from its operations and/or activities;

i) have the financial stability and resources required for the operation of a certification/ registration system;

j) employ a sufficient number of personnel having the necessary education, training, technical knowledge and experience for performing certification/ registration functions relating to the type, range and volume of work performed, under a responsible senior executive;

k) have a quality system, as outlined in 2.1.4, giving confidence in its ability to operate a certification/ registration system for organisations;

l) have policies and procedures that distinguish between certification/ registration of organisations and any other activities in which the body is engaged;

m) together with its senior executive and staff, be free from any commercial, financial and other pressures which might influence the results of the certification/ registration process;

n) have formal rules and structures for the appointment and operation of any committees which are involved in the certification/ registration process; such committees shall be free from any commercial, financial and any other pressures that might influence decisions (see note 2);

o) ensure that activities of related bodies do not affect the confidentiality, objectivity, or impartiality of its certifications/ registrations and shall not offer or provide

1) those services that it certifies/registers others to perform,

2) consulting services to obtain or maintain certification/ registration,

3) services to design, implement or maintain ISMS or related management systems (see note 3);

p) have policies and procedures for the resolution of complaints, appeals and disputes received from organisations or other parties about the handling of certification/ registration or any other related matters.

NOTES

2 A structure where members are chosen to provide a balance of interests where no single interests predominates, will be deemed to satisfy this provision.

3 Other products, processes or services may be offered, directly or indirectly, provided they do not compromise confidentiality or the objectivity or impartiality of its certification/ registration process and decisions.

IAF Guidance

G.2.1.10. Accreditation shall only be granted to a body which is a legal entity as referenced in clause 2.1.2.d) of ISO/IEC Guide 62 and will be confined to declared scopes, activities and locations. If the certification/ registration activities are carried out by a legal entity which is part of a larger entity, the links with other parts of the larger entity shall be clearly defined and should demonstrate that no conflict of interest exists as defined in guidance G.2.1.22 and G.2.1.23. Relevant information on activities performed by the other parts of the larger entity shall be given by the certification/ registration body to the accreditation body.

G.2.1.11. Demonstration that a certification/ registration body is a legal entity, as required under clause 2.1.2.d) of ISO/IEC Guide 62, means that if an applicant certification/ registration body is part of a larger entity, accreditation shall only be granted to the entire legal entity. In such a situation, the structure of the entire legal entity may be subject to audit by the accreditation body, in order to pursue specific audit trails and/ or review records relating to the certification/ registration body. The part of the legal entity that forms the actual certification/ registration body may trade under a distinctive name, which should appear on the accreditation certificate.

For the purposes of clause 2.1.2.d) of ISO/IEC Guide 62, certification/ registration bodies that are part of government, or are government departments, will be deemed to be legal entities on the basis of their governmental status. Such bodies' status and structure shall be formally documented and the body shall comply with all the requirements of ISO/IEC Guide 62.

G.2.1.12. Impartiality and independence of the certification/ registration body should be assured at three levels:

1) Strategic and policy;

2) Decisions on certification/ registration/ registration;

3) Auditing.

The guidance to clause 2.1.2 of ISO/IEC Guide 62 is intended to provide for impartiality and independence at all three levels.

G.2.1.13. Impartiality, as required by clause 2.1.2.a) of ISO/IEC Guide 62 can only be safeguarded by a structure, as required by clause 2.1.2.e) of ISO/IEC Guide 62, that enables "the participation of all parties significantly concerned in the development of policies and principles regarding the content and functioning of the certification/ registration system".

G.2.1.14. The management established to meet the requirements of ISO/IEC Guide 62 clause 2.1.2.c) does not have to be the same as the structure required under ISO/IEC Guide 62 clause 2.1.2.e).

G.2.1.15. Conformance with clause 2.1.2.e) of ISO/IEC Guide 62 has the effect of counteracting any tendency on the part of the owners of a certification/ registration body to allow commercial or other considerations to prevent the consistent technically objective provision of its service. This is particularly necessary when the finance to set up a certification/ registration body has been provided by a particular interest, which predominates in the shareholding and/ or the board of directors.

G.2.1.16. Clause 2.1.2.e) of ISO/IEC Guide 62, therefore, requires that the documented structure of the certification/ registration body has built into it provision for the participation of all the significantly concerned parties. This should normally be through some kind of committee. The structure established should be prescribed in the certification/ registration body's written constitution and should not be subject to change without notification to the accreditation body.

G.2.1.17. It is always a question of judgement whether all parties significantly concerned in the system are able to participate. What are essential is that all identifiable major interests should be given the opportunity to participate, and that a balance of interests, where no single interest predominates, is achieved.

ISMS Guidance

IS.2 The parties referred to in Clause 2.1.2.e) may be customers and suppliers in industry and commerce, regulators, trade bodies, information security management professionals and related professionals, and government.

IAF Guidance

G.2.1.18. The management responsible for the various functions described in clause 2.1.2.c) of ISO/IEC Guide 62 should provide all the necessary information, including the reasons for all significant decisions and actions, and the selection of persons responsible for particular activities, in respect of certification/ registration, to the committee or equivalent referred to in clause 2.1.2.e) of ISO/IEC Guide 62, to enable it to ensure proper and impartial certification/ registration/ registration. If the advice of this committee or equivalent is not respected in any matter by the management, the committee or equivalent shall take appropriate measures, which may include informing the accreditation body.

G.2.1.19. If the certification/ registration body and an applicant or certified/ registered organisation are both part of government, they should not report directly to a person or group having operational responsibility for both. The certification/ registration body shall, in view of the impartiality requirement, be able to demonstrate how it deals with such a case.

G.2.1.20. If the decision to issue or withdraw certification/ registration in accordance with clause 2.1.2.n) of ISO/IEC Guide 62 is taken by a committee comprising, among others, representatives from one or more certified/ registered organisations, the operational procedures of the certification/ registration body should ensure that these representatives do not have a significant influence on decision making. This can for example be assured by the distribution of voting rights or some other equivalent means.

G.2.1.21. Clause 2.1.2.o) of ISO/IEC Guide 62 addresses two separate requirements. Firstly, the certification/ registration body shall not under any circumstances provide the services identified in sub-paras 1), 2) and 3) of that clause. Secondly, although there is no specific restriction on the services or activities a related body may provide, these shall not affect the confidentiality, objectivity or impartiality of the certification/ registration body.

G.2.1.22. Consultancy is considered to be participation in an active creative manner in the development of the ISMS to be assessed by, for example:

a) preparing or producing manuals, handbooks or procedures;

b) participating in the decision making process regarding management system matters;

c) giving specific advice towards the development and implementation of management systems for eventual certification/ registration.

Note: Management systems as referred to in guidance G.2.1.22 include all aspects of such systems, including financial.

G.2.1.23. Certification/ registration bodies can carry out the following duties without them being considered as consultancy or having a potential conflict of interest:

a) certification/ registration including information meetings, planning meetings, examination of documents, auditing (not internal auditing or internal security reviews) and follow up of non-conformities;

b) arranging and participating as a lecturer in training courses, provided that where these courses relate to information security management, related management systems or auditing they should confine themselves to the provision of generic information and advice which is freely available in the public domain, i.e. they should not provide company specific advice which contravenes the requirements of G.2.1.22.c);

c) making available or publishing on request information on the basis for the certification/ registration body's interpretation of the requirements of the assessment standards;

d) activities prior to audit aimed solely at determining readiness for assessment; but such activities should not result in the provision of recommendations or advice that would contravene G.2.1.22 and the certification/ registration body should be able to confirm that such activities do not contravene these requirements and that they are not used to justify a reduction in the eventual assessment duration;

e) performing second and third party audits according to other standards or regulations than those being part of the scope of accreditation;

f) adding value during assessments and surveillance visits, e.g., by identifying opportunities for improvement, as they become evident, during the audit without recommending specific solutions.

G.2.1.24. Consultancy by a related body and certification/ registration should never be marketed together and nothing should be stated in marketing material or presentation, written or oral, to give the impression that the two activities are linked. It is the duty of the certification/ registration body to ensure that none of its clients is given the impression that the use of both services (certification/ registration and consultancy), would bring any business advantage to the client so that the certification/ registration remains, and is seen to remain, impartial.

G.2.1.25. Nothing should be said by a certification/ registration body that would suggest that certification/ registration would be simpler, easier or less expensive if any specified consultancy or training services were used.

G.2.1.26. A related body, as referred to in clause 2.1.2.o) of ISO/IEC Guide 62, is one which is linked to the certification/ registration body by common ownership or directors, contractual arrangement, a common name, informal understanding or other means such that the related body has a vested interest in the outcome of an assessment or has a potential ability to influence the outcome of an assessment.

G.2.1.27. The certification/ registration body should analyse and document the relationship with such related bodies to determine the possibilities for conflict of interest with provision of certification/ registration and identify those bodies and activities that could, if not subject to appropriate controls, affect confidentiality, objectivity or impartiality.

G.2.1.28. Certification/ registration bodies shall demonstrate how they manage their certification/ registration business and any other activities so as to eliminate actual conflict of interest and minimise any identified risk to impartiality. The demonstration shall cover all potential sources of conflict of interest, whether they arise from within the certification/ registration body or from the activities of related bodies. Accreditation bodies will expect certification/ registration bodies to open up these processes for audit. This may include, to the extent practicable and justified, pursuit of audit trails to review records of both the certification/ registration body and its related body for the activity under consideration. In considering the extent of such audit trails account should be taken of the certification/ registration body’s history of impartial certification/ registration. If evidence of failure to maintain impartiality is found there may be a need to extend the audit trail back into the related bodies to provide assurance that control over potential conflicts of interest has been re-established.

G.2.1.29. The requirements of clause 2.1 and clause 2.2.3 of ISO/IEC Guide 62 mean that people who have provided consultancy, including those acting in a managerial capacity, should not be employed to conduct an audit as part of the certification/ registration process if they have been involved in any consultancy activities towards the organisation in question, (or any company related to that organisation), within the last two years. Situations such as an employer’s involvement or previous involvement with the organisation being assessed may present individuals involved in any part of the certification/ registration process with a conflict of interest. The certification/ registration body has a responsibility to identify and evaluate such situations and to assign responsibilities and tasks so as to ensure that impartiality is not compromised.

G.2.1.30. The senior executive, staff and/or personnel mentioned in clause 2.1.2. of ISO/IEC Guide 62 need not necessarily be full-time personnel, but their other employment shall not be such as to compromise their impartiality.

G.2.1.31. The certification/ registration body should require all assessment sub-contractors or external assessors/auditors to give undertakings regarding the marketing of any consultancy services equivalent to those required by guidance G.2.1.24 and G.2.1.25.

G.2.1.32. The certification/ registration body should be responsible for ensuring that neither related bodies, nor sub-contractors, nor external assessors/auditors operate in breach of the undertakings that they have given. It should also be responsible for implementing appropriate corrective action in the event that such a breach is identified.

G.2.1.33. The certification/ registration body should be independent from the body or bodies (including any individuals) which provide the internal audit or internal security review of the organisation’s ISMS subject to certification/ registration.

G.2.1.34. An auditor shall explain the audit findings and/or clarify the requirements of the assessment standard during the audit and /or at the closing meeting but shall not give prescriptive advice or consultancy as part of an assessment.

G.2.1.35. The policies and procedures referred to in 2.1.2 p) of ISO/IEC Guide 62 should ensure that all disputes and complaints are dealt with in a constructive and timely manner. Where operation of such procedures has not resulted in the acceptable resolution of the matter or where the proposed procedure is unacceptable to the complainant or other parties involved, the certification/ registration body's procedures shall provide for an appeals process. This appeals procedure should include provision for the following:

a) the opportunity for the appellant to formally present its case;

b) provision of an independent element or other means to ensure the impartiality of the appeals process;

c) provision to the appellant of a written statement of the appeal findings including the reasons for the decisions reached.

The certification/ registration body shall ensure that all interested parties are made aware, as and when appropriate, of the existence of the appeals process and the procedures to be followed.

2.1.3 Subcontracting

When a certification/ registration body decides to subcontract work related to certification/ registration (e.g. audits) to an external body or person, a properly documented agreement covering the arrangements, including confidentiality and conflict of interests, shall be drawn up. The certification/ registration body shall

a) take full responsibility for such subcontracted work and maintain its responsibility for granting, maintaining, extending, reducing, suspending or withdrawing certification/ registration;

b) ensure that the subcontracted body or person is competent and complies with the applicable provisions of this publication and is not involved, either directly or through its employer with the design, implementation or maintenance of a ISMS or related management system(s) in such a way that impartiality could be compromised;

c) obtain the consent of the applicant or certified/ registered organisation.

NOTE 4 Requirements a) and b) are also relevant, by extension, when a certification/ registration body uses, for granting its own certification/ registration, work provided by another certification/ registration body with which it has signed an agreement.

IAF Guidance

G.2.1.36. A certification/ registration body may issue certificates on the basis of an assessment carried out by another body provided that the agreement with the subcontracted body requires it to comply with the all relevant requirements of ISO/IEC Guide 62, any other documents relevant to the scope of accreditation and, in particular, the requirements of clause 2.2 of ISO/ IEC Guide 62. Assessments carried out by subcontracted bodies shall give the same confidence as assessments carried out by the certification/ registration body itself. Evaluation of the audit report and the decision on certification/ registration shall be made only by the certification/ registration body itself, and not by any other certification/ registration body. Where joint assessments are undertaken, each certification/ registration body shall satisfy itself that the whole of the assessment has been satisfactorily undertaken by competent assessors / auditors.

G.2.1.37. Where a certification/ registration body issues certificates in accordance with guidance G.2.1.36 it shall have procedures that ensure conformity with all relevant clauses of this document by subcontracted bodies.

2.1.4 Quality System

2.1.4.1 The management of the certification/ registration body with executive responsibility for quality shall define and document its policy for quality, including objectives for quality and its commitment to quality. The management shall ensure that this policy is understood, implemented and maintained at all levels of the certification/ registration body.

2.1.4.2 The certification/ registration body shall operate a quality system in accordance with the relevant elements of this publication and appropriate to the type, range and volume of work performed. This quality system shall be documented and the documentation shall be available for use by the staff of the certification/ registration body. The certification/ registration body shall ensure effective implementation of the documented quality system procedures and instructions. The certification/ registration body shall designate a person with direct access to its highest executive level that, irrespective of other responsibilities, shall have defined authority to

a) ensure that a quality system is established, implemented and maintained in accordance with this publication, and

b) report on the performance of the quality system to the management of the certification/ registration body for review and as a basis for improvement of the quality system.

2.1.4.3 The quality system shall be documented in a quality manual and associated quality procedures, and the quality manual shall contain or refer to at least the following:

a) a quality policy statement;

b) a brief description of the legal status of the certification/ registration body , including the names of its owners, if applicable and, if different, the names of the persons who control it;

c) the names, qualifications, experience and terms of reference of the senior executive and other certification/ registration personnel, influencing the quality of the certification/ registration function;

d) a structure chart showing lines of authority, responsibility and allocation of functions stemming from the senior executive and in particular the relationship between those responsible for the assessment and those taking decisions regarding certification/ registration;

e) a description of the structure of the certification/ registration body , including details of the management (committee, group or person) identified in 2.1.2.c), its constitution, terms of reference and rules of procedure;

f) the policy and procedures for conducting management reviews;

g) administrative procedures including document control;

h) the operational and functional duties and services pertaining to quality, so that the extent and limits of each person's responsibility are known to all concerned;

i) the policy and procedures for the recruitment and training of certification/ registration body personnel (including auditors) and monitoring their performance;

j) a list of its subcontractors and details of the procedures for assessing, recording and monitoring their competence;

k) its procedures for handling non-conformities and for assuring the effectiveness of any corrective actions taken;

l) the policy and procedures for implementing the certification/ registration process, including:

1) the conditions for issue, retention, and withdrawal of certification/ registration documents,

2) checks of the use and application of documents used in certification/ registration of ISMS,

3) the procedures for assessing and certifying/ registering the organisation's ISMS,

4) the procedures for surveillance and reassessment of certified/ registered organisations;

m) the policy and procedure for dealing with appeals, complaints and disputes;

n) the procedures for conducting internal audits based on the provisions of ISO 10011-1.

<u>IAF Guidance</u>

G.2.1.38. The description required by clause 2.1.4.3.e) of ISO/IEC Guide 62 should include an indication of which party or parties each member of a committee, group or person is representing.

2.1.5 Conditions for granting, maintaining, extending, reducing, suspending and withdrawing certification/ registration

2.1.5.1 The certification/ registration body shall specify the conditions for granting, maintaining, reducing and extending certification/ registration and the conditions under which certification/ registration may be suspended or withdrawn, partially or in total, for all or part of the organisation's scope of certification/ registration. In particular, the certification/ registration body shall require the organisation to notify it promptly of any intended changes to the ISMS or other changes, which may affect conformity.

2.1.5.2 The certification/ registration body shall require the organisation to have a documented and implemented ISMS which conforms to applicable ISMS standards or other normative documents.

2.1.5.3 The certification/ registration body shall have procedures to:

a) grant, maintain, withdraw and, if applicable, suspend certification/ registration;

b) extend or reduce the scope of certification/ registration;

c) conduct reassessment in the event of changes significantly affecting the activity and operation of the organisation (such as change of ownership, changes in personnel or equipment), or if analysis of a complaint or any other information indicates that the certified/ registered organisation no longer complies with the requirements of the certification/ registration body.

2.1.5.4 The certification/ registration body shall have documented procedures, which shall be made available on request for:

a) the initial assessment of an organisation's ISMS, in accordance with the provisions of ISO 10011-1 and other relevant documents;

b) surveillance and reassessment of an organisation's ISMS in accordance with ISO 10011-1 on a periodic basis for continuing conformity with relevant requirements and for verifying and recording that an organisation takes corrective action on a timely basis to correct all nonconformities;

c) identifying and recording nonconformities and the need for corrective action by organisations on a timely basis for such items as incorrect references to the certification/ registration or misleading use of certification/ registration information.

IAF Guidance

G.2.1.39. On the subject of deciding on certification/ registration, clause 2.1.5 of ISO/IEC Guide 62 does not mention a specific period in which at least one complete internal audit and one management review and one security review of the organisation’s ISMS shall have taken place. The certification/ registration body may specify a period. Irrespective of whether the certification/ registration body has chosen to specify a minimum frequency, measures shall be established by the certification/ registration body to ensure the effectiveness of the organisation’s management review, security review and internal audit processes.

G.2.1.40. Certification/ registration shall not be granted to the organisation until there is sufficient evidence to demonstrate that the arrangements for management and security reviews have been implemented, are effective and will being maintained.

2.1.6 Internal audits and management reviews

2.1.6.1 The certification/ registration body shall conduct periodic internal audits covering all procedures in a planned and systematic manner, to verify that the quality system is implemented and is effective. The certification/ registration body shall ensure that:

a) personnel responsible for the area audited are informed of the outcome of the audit;

b) corrective action is taken in a timely and appropriate manner;

c) the results of the audit are recorded.

2.1.6.2 The body's management with executive responsibility shall review its quality system at defined intervals sufficient to ensure its continuing suitability and effectiveness in satisfying the requirements of this Guide and the stated quality policy and objectives. Records of such reviews shall be maintained.

IAF Guidance

G.2.1.41. Clause 2.1.6. of ISO/IEC Guide 62 does not mention a specific period in which at least one complete internal audit of the certification/ registration body's quality system and one management review of the certification/ registration body's quality system should take place. Complete internal audits followed by management reviews of the body's quality system should be carried out at least once each year. The accreditation body may specify a shorter period, depending on the degree of conformity with the requirements of ISO/IEC Guide 62, as found in internal audits and reviews as well as in reports to the accreditation body.

G.2.1.42. The records of internal audits and management reviews should be made available to the accreditation body on request.

2.1.7 Documentation

2.1.7.1 The certification/ registration body shall document, update at regular intervals, and make available (through publications, electronic media or other means) on request:

a) information about the authority under which the certification/ registration body operates;

b) a documented statement of its certification/ registration system including its rules and procedures for granting, maintaining, extending, reducing, suspending and withdrawing certification/ registration;

c) information about the assessment and certification/ registration process;

d) a description of the means by which the certification/ registration body obtains financial support and general information on the fees charged to applicants and certified/ registered organisations;

e) a description of the rights and duties of applicants and certified/ registered organisations including requirements, restrictions or limitations on the use of the certification/ registration body's logo and on the ways of referring to the certification/ registration granted;

f) information on procedures for handling complaints, appeals and disputes;

g) a directory of certified/ registered organisations, including their locations, describing the scope of certification/ registration granted to each.

2.1.7.2 The certification/ registration body shall establish and maintain procedures to control all documents and data that relate to its certification/ registration functions. These documents shall be reviewed and approved for adequacy by appropriately authorised and competent personnel prior to issuing any documents following initial development or any subsequent amendment or change being made. A listing of all appropriate documents with the respective issue and/or amendment status identified shall be maintained. The distribution of all such documents shall be controlled to ensure that the appropriate documentation is made available to personnel of the certification/ registration body or organisation, when required to perform any function relating to the activities of an applicant or the certified/ registered organisation.

IAF Guidance

G.2.1.43. The description of the means by which the body obtains financial support referred to in clause 2.1.7.1.d) of ISO/IEC Guide 62 should be sufficient to show whether or not the body can retain its impartiality.

2.1.8 Records

2.1.8.1 The certification/ registration body shall maintain a record system to suit its particular circumstances and to comply with existing regulations. The records shall demonstrate that the certification/ registration procedures have been effectively fulfilled, particularly with respect to application forms, assessment reports, and other documents relating to granting, maintaining, extending, reducing, suspending or withdrawing certification/ registration. The records shall be identified, managed and disposed of in such a way as to ensure the integrity of the process and confidentiality of the information. The records shall be kept for a period of time so that continued confidence may be demonstrated for at least one full certification/ registration cycle, or as required by law.

2.1.8.2 The certification/ registration body shall have a policy and procedures for retaining records for a period consistent with its contractual, legal or other obligations. The certification/ registration body shall have a policy and procedures concerning access to these records consistent with 2.1.9.

2.1.9 Confidentiality

2.1.9.1 The certification/ registration body shall have adequate arrangements, consistent with applicable laws, to safeguard confidentiality of the information obtained in the course of its certification/ registration activities at all levels of its structure, including committees and external bodies or individuals acting on its behalf.

2.1.9.2 Except as required in this publication, information about a particular organisation shall not be disclosed to a third party without the written consent of the organisation. Where the law requires information to be disclosed to a third party, the organisation shall be informed of the information provided as permitted by the law.

IAF Guidance

G.2.1.44. The requirement as to confidentiality includes anyone who might gain access to information, which the certification/ registration body should keep confidential. Subcontracted personnel shall be required to keep all such information confidential, particularly from fellow employees and from their other employers.

G.2.1.45. The 'written consent' mentioned in clause 2.1.9.2 of ISO/IEC Guide 62 only apply to confidential information.

2.2 Certification/ registration body personnel

2.2.1 General

2.2.1.1 The personnel of the certification/ registration body involved in certification/ registration shall be competent for the functions they perform.

2.2.1.2 Information on the relevant qualifications, training and experience of each member of the personnel involved in the certification/ registration process, shall be maintained by the certification/ registration body. Records of training and experience shall be kept up-to-date.

2.2.1.3 Clearly documented instructions shall be available to the personnel describing their duties and responsibilities. These instructions shall be maintained up-to-date.

IAF Guidance

G.2.2.1. Clause 2.1.2.j) of ISO/IEC Guide 62 means that across the whole of its accredited scope (or that part in which it operates) the certification/ registration body shall be able to conduct assessments using resources under its own control, which meet the requirements of ISO 10011 and applicable sector schemes.

G.2.2.2. The term "resources under its own control" can include individual assessors / auditors who work for the certification/ registration body on a contract basis, or other external resources. The certification/ registration body shall be in a position to manage, control and be responsible for the performance of all its resources and maintain comprehensive records controlling the suitability of all the staff it uses in particular areas, whether they are employees, employed on contract or provided by external bodies.

G.2.2.3. The management of the certification/ registration body shall have the resources to enable it to determine whether or not, and procedures to ensure that, individual assessors / auditors are competent for the tasks they are required to perform within the scope of certification/ registration in which they are operating. The competence of assessors / auditors may be established by verified background experience and specific training or briefing (which may be demonstrated by registration as ISMS auditor by an accredited auditor certification/ registration body). The certification/ registration body should be able to communicate effectively with all those whose services it uses.

G.2.2.4. Certification/ registration bodies shall have personnel competent to:

a) select and verify the competence of ISMS auditors for audit teams appropriate for the audit;

b) brief ISMS auditors and arrange any necessary training;

c) decide on the granting, maintaining, withdrawing, suspending, extending, or reducing of certification/ registrations;

d) set up and operate an appeals, complaints and disputes procedure.

ISMS Guidance

IS.3 Management competence

IS.3.1 General

The emphasis in this guidance is placed on the competence of the certification/ registration body to direct and manage the certification/ registration process. The essential elements of competence required to perform ISMS certification/ registration are to select, provide and manage those individuals whose collective competence is appropriate to the activities to be audited and the related information security issues.

IS.3.2 Competence analysis and contract review:

The certification/ registration body shall have systems, which ensure knowledge of the technological and legal developments relevant to the ISMS of the organisations, which it assesses.

The certification/ registration body shall have an effective system for the analysis of the competencies in information security management, which it needs to have available, with respect to all the technical areas in which it operates.

The certification/ registration body shall have relevant contract review capability*,* and be able to demonstrate that it has performed a competence analysis (assessment of skills in response to evaluated needs) of the requirements of each relevant industrial sector prior to undertaking the contract review for each client. In particular, the certification/ registration body shall be able to demonstrate that it has the competence to complete the following activities:

a) identify the typical information security related threats to assets, vulnerabilities and impacts on the organisation of the areas of activity of the sector;

b) define the areas of activity of the organisation;

c) confirm that the typical information security related threats to assets, vulnerabilities and impacts of the organisation, arising from the complete range of the organisation's activities, correspond to those identified in a) above;

d) define the competencies needed in the certification/ registration body to certify/ register in relation to the identified activities, and information security related threats to assets, vulnerabilities and impacts on the organisation;

e) confirm the availability of the required competencies.

IS.3.3 Training and selection of audit teams

The certification/ registration body shall have criteria for the training and selection of audit teams that ensures appropriate levels of:

a) understanding of the ISMS standard or normative document;

b) understanding of information security issues;

c) understanding of risk assessment and risk management

d) technical knowledge of the activity to be audited;

e) knowledge of regulatory requirements relevant to the ISMS;

f) management system audit competencies;

g) management system knowledge.

IS.3.4 Management of the decision taking process

The management function shall have the competence and procedures in place to manage the process of decision taking regarding the granting, maintaining, extending, reducing, suspending and withdrawing of ISMS certification/ registration.

2.2.2 Qualification criteria for auditors and technical experts

2.2.2.1 In order to ensure that assessments are carried out effectively and uniformly, the minimum relevant criteria for competence shall be defined by the certification/ registration body.

2.2.2.2 Auditors shall meet the requirements of the appropriate international documentation. For the assessment of an ISMS, relevant guidelines for auditing are found in ISO 10011-1 and relevant criteria for auditors in ISO 10011-2.

2.2.2.3 Technical experts are not required to comply with criteria for auditors covered in ISO 10011-2. Guidance on their personal attributes may be obtained from ISO 10011-2:1991, clause 7.

ISMS Guidance

IS.4 Auditor competence

Persons employed by certification/ registration bodies for performing audits of ISMS by themselves should comply with the following criteria, based on ISO 10011-2. When persons are employed to perform audits of ISMS, these attributes may be divided between the team members as described in IS.5.3:

a) education at university level (extensive experience and supplementary professional education and training can be equivalent to such level of education);

b) at least four years full time practical workplace experience in information technology, of which at least two years in a role or function relating to information security;

c) have successfully followed a five day training on the subject of auditing and audit management;

d) prior to assuming responsibility for performing as an auditor, the candidate should have gained experience in the entire process of assessing information security. This experience should have been gained by participation in a minimum of four assessments for a total of at least 20 days, including review of documentation and risk analysis, implementation assessment and audit reporting;

e) all relevant experience should be reasonably current;

f) have the following personal attributes: objective; mature; discerning; analytical; persistent; realistic. The candidate should be able to put complex operations in a broad perspective and should be able to understand the role of individual units in larger organisations;

g) Keep up own knowledge and skill in information security and auditing.

Auditors performing as lead auditor should additionally fulfil the following requirements:

h) have knowledge and attributes to manage the assessment process;

i) have acted as auditor in at least three complete ISMS audits;

j) have demonstrated to possess adequate knowledge and attributes to manage the assessment process;

k) have demonstrated the capability to communicate effectively, both orally and in writing.

2.2.3 Selection procedure

2.2.3.1 Selection of ISMS auditors and technical expert for audit teams, in general

The certification/ registration body shall have a procedure for:

a) selecting auditors on the basis of their competence, training, qualifications and experience; when required, the audit team may be supplemented by technical experts who can demonstrate specific competence in a field of technology appropriate to the audit - note should be taken that technical experts cannot be used in place of ISMS auditors;

b) initially assessing the conduct of auditors and technical experts during assessments and subsequently monitoring the performance of auditors and technical experts.

IAF Guidance

G.2.2.5. Clause 2.2.3.1.b) requires the certification/ registration body to assess and monitor the conduct and performance of ISMS auditors and technical experts. Such assessment and monitoring should include witnessing the activities of the assessors / auditors and technical experts on-site.

2.2.3.2 Assignment for a specific assessment

When selecting the audit team to be appointed for a specific assessment the certification/ registration body shall ensure that the skills brought to each assignment are appropriate . The team shall

a) be familiar with the applicable legal regulations, certification/ registration procedures and certification/ registration requirements;

b) have a thorough knowledge of the relevant assessment method and assessment documents;

c) have appropriate technical knowledge of the specific activities for which certification/ registration is sought and, where relevant, with associated procedures and their potential to cause information security failure (technical experts who are not auditors may fulfil this function);

d) have a degree of understanding sufficient to make a reliable assessment of the competence of the organisation to manage the information security aspects of its activities, products and services;

e) be able to communicate effectively, both in writing and orally in the required languages;

f) be free from any interest that might cause team members to act in other than an impartial or non-discriminatory manner, for example:

1) audit team members or their employer(s) shall not have provided consulting services to the applicant or certified/ registered organisation which compromise the certification/ registration process and decision,

2) in accordance with the directives of the certification/ registration body, the audit team members shall inform the certification/ registration body, prior to the assessment, about any existing, former and envisaged link between themselves or their employer(s) and the organisation to be assessed.

IAF Guidance

G.2.2.6. It is a condition of accreditation that accredited certificates are not issued until adequate resources can be deployed to conduct audits meeting the requirements of ISO/IEC Guide 62 and of this document. The certification/ registration body's procedures shall ensure that staff employed to assess organisations are competent in the field in which they are operating. Staff responsible for managing audits shall be identified and their competencies documented.

G.2.2.7. The term 'directives' in clause 2.2.3.2.f).2) of ISO/IEC Guide 62 means the same as the term 'the mandate' in clause 3.2.5. of ISO/IEC Guide 62.

G.2.2.8. The audit team needs a background to ensure that the members understand the requirements relating to the system they are assessing. Each audit team shall have a general understanding and background in each technological and industrial sector in which it operates.

G.2.2.9. In certain instances, particularly where there are critical requirements and special procedures, the background knowledge of the audit team may be supplemented by briefing, specific training or technical experts in attendance. The certification/ registration body may attach non-auditor experts to their audit teams. If a certification/ registration body does use technical experts, its systems shall include details of how technical experts are selected and how their technical knowledge is assured on a continuing basis. The certification/ registration body may rely on outside help, for example, from industry or professional institutions.

G.2.2.10. The requirements of clause 2.1 and clause 2.2.3.2 of ISO/IEC Guide 62 have a bearing on the employment of people who have provided consultancy. See guidance 2.1.29.

ISMS Guidance

IS.5 Audit Team competence

IS.5.1 The following requirements apply to certification/ registration assessment. For surveillance activities only those requirements which are relevant to the scheduled surveillance activity apply.

IS.5.2 The following requirements apply to each member of the audit team, except technical experts:

all members of the audit team shall be able to demonstrate appropriate experience and understanding of all of the following:

a) the ISMS standard or normative document;

b) the concepts of management systems in general;

c) issues related to various areas of information security;

d) the principles and processes related to risk assessment and risk management;

e) auditing principles.

IS.5.3 The following requirements apply to the audit team as a whole:

a) in each of the following areas at least one audit team member should satisfy the certification/ registration body's criteria for taking responsibility within the team:

i) managing the team,

ii) knowledge of the legislative and regulatory requirements and of legal compliance in the particular information security field,

iii) identifying information security related threats,

iv) identifying the vulnerabilities of the organisation and understanding their impact and their mitigation and control,

v) knowledge of the current technical state-of-art in the sector,

vi) knowledge of risk assessment related to information security;

b) the audit team should be competent to trace indications of security incidents in the organisation's ISMS back to the appropriate elements of the ISMS.

c) an audit team may consist of one person provided that the person meets all the criteria set out in a) above;

IS.5.4 Use of Technical Experts

Technical experts with specific knowledge regarding the process and information security issues and legislation affecting the organisation, but who do not satisfy all of the above criteria, may be part of the audit team. Technical experts should not function independently.

2.2.4 Contracting of assessment personnel

The certification/ registration body shall require the personnel involved in the assessment to sign a contract or other document by which they commit themselves to comply with the rules defined by the certification/ registration body, including those relating to confidentiality and those relating to independence from commercial and other interests, and any prior and/or present link with the organisations to be assessed. The certification/ registration body shall ensure that, and document how, any subcontracted assessment personnel satisfy all the requirements for assessment personnel outlined in this publication.

2.2.5 Assessment personnel records

2.2.5.1 The certification/ registration body shall possess and maintain up-to-date records on assessment personnel consisting of:

a) name and address;

b) affiliation and position held in the organisational structure;

c) educational qualification and professional status;

d) experience and training in each field of competence of the certification/ registration body;

e) date of most recent updating of records;

f) performance appraisal.

2.2.5.2 The certification/ registration body shall ensure, and verify, that any subcontracted body maintains records, which satisfy the requirements of this publication, of assessment personnel who are subcontracted to the certification/ registration body.

2.2.6 Procedures for audit teams

Audit teams shall be provided with up-to-date assessment instructions and all relevant information on certification/ registration arrangements and procedures.

2.3 Changes in the certification/ registration requirements

The certification/ registration body shall give due notice of any changes it intends to make in its requirements for certification/ registration. It shall take account of views expressed by the interested parties before deciding on the precise form and effective date of the changes. Following a decision on, and publication of, the changed requirements, it shall verify that each certified/ registered organisation carries out any necessary adjustments to its procedures within such time, as in the opinion of the certification/ registration body, is reasonable.

2.4 Appeals, complaints and disputes

2.4.1 Appeals, complaints and disputes brought before the certification/ registration body by organisations or other parties shall be subject to the procedures of the certification/ registration body.

2.4.2 The certification/ registration body shall:

a) keep a record of all appeals, complaints and disputes and remedial actions relative to certification/ registration;

b) take appropriate corrective and preventive action;

c) document the actions taken and assess their effectiveness.

IAF Guidance

G.2.4.1. Complaints represent a source of information as to possible nonconformity. On receipt of a complaint the certification/ registration body shall establish, and where appropriate take action on, the cause of the nonconformity, including any predetermining (or predisposing) factors within the certification/ registration body's management system.

G.2.4.2. The certification/ registration body should use such investigation to develop remedial / corrective action, which should include measures for:

a) restoring certification/ registration as quickly as practicable;

b) preventing recurrence;

c) assessing the effectiveness of the remedial / corrective measures adopted.

SECTION 3 REQUIREMENTS FOR CERTIFICATION/ REGISTRATION

3.1 Application for certification/ registration

3.1.1 Information on the procedure

3.1.1.1 A detailed description of the assessment and certification/ registration procedure, the documents containing the requirements for certification/ registration and documents describing the rights and duties of certified/ registered organisations, shall be maintained up-to-date as specified in 2.1.7.1. and shall be provided to applicants and certified/ registered organisations.

3.1.1.2 The certification/ registration body shall require that an organisation:

a) **always complies with the relevant provisions of the certification/ registration programme;**

b) **makes all necessary arrangements for the conduct of the assessment, including provision for examining documentation and the access to all areas, records (including internal audit reports and reports of independent reviews of information security) and personnel for the purposes of assessment, reassessment and resolution of complaints;**

ISMS Guidance

IS.6 Access to personnel records

The certification/ registration body should review before the assessment what records are considered as confidential or sensitive by the organisation such that these records could not be examined by the audit team during the assessment of the organisation. The certification/ registration body should judge whether the records that can be examined warrant an effective assessment. If the certification/ registration body concludes that an effective assessment is not warranted, the certification/ registration body should inform the organisation that the assessment can take place only when appropriate access arrangements have been accepted by the organisation.

c) **only claims that it is certified/ registered with respect to those activities for which it has been granted certification/ registration;**

d) **does not use its certification/ registration in such a manner as to bring the certification/ registration body into disrepute and does not make any statement regarding its certification/ registration which the certification/ registration body may consider misleading or unauthorised;**

e) **upon suspension or withdrawal of its certification/ registration (however determined), discontinues use of all advertising matter that contains any reference thereto and returns any certification/ registration documents as required by the certification/ registration body;**

f) **uses certification/ registration only to indicate that the ISMS is in conformity with specified standards or other normative documents, and does not use its certification/ registration to imply that a product or service is approved by the certification/ registration body;**

g) **ensures that no certification/ registration document, mark or report, nor any part thereof, is used in a misleading manner;**

h) in making reference to its certification/ registration in communication media such as documents, brochures or advertising, complies with the requirements of the certification/ registration body.

3.1.1.3 When the desired scope of certification/ registration is related to a specific programme, any necessary explanation shall be provided to the applicant.

3.1.1.4 If requested, additional application information shall be provided to the applicant.

3.1.2 The application

3.1.2.1 The certification/ registration body shall require an official application form, duly completed, and signed by a duly authorised representative of the applicant, in which or attached to which:

a) the scope of the desired certification/ registration is defined;

b) the applicant agrees to comply with the requirements for certification/ registration and to supply any information needed for its evaluation.

3.1.2.2 At least the following information shall be provided by the applicant prior to the on-site assessment:

a) the general features of the applicant, such as corporate entity, name, addresses, legal status, and, where relevant, human and technical resources;

b) general information concerning the ISMS and the activities it covers;

c) a description of the systems to be certified/ registered and the standards or other normative documents applicable to each;

d) a copy of the ISMS manual and, where required, the associated documentation.

The information gathered from the application documentation and the review of the ISMS documentation may be used for the preparation of the on-site assessment and shall be treated with appropriate confidentiality.

3.2 Preparation for assessment

3.2.1 Before proceeding with the assessment, the certification/ registration body shall conduct, and maintain records of, a review of the request for certification/ registration to ensure that

a) the requirements for certification/ registration are clearly defined, documented and understood;

b) any difference in understanding between the certification/ registration body and the applicant is resolved;

c) the certification/ registration body has the capability to perform the certification/ registration service with respect to the scope of the certification/ registration sought, the location of the applicant's operations and any special requirements such as the language used by the applicant.

3.2.2 The certification/ registration body shall prepare a plan for its assessment activities to allow for the necessary arrangements to be made.

3.2.3 The certification/ registration body shall nominate a qualified audit team to evaluate all material collected from the applicant and to conduct the audit on its behalf. Experts in the areas to be assessed may be attached to the certification/ registration body's team as advisers.

3.2.4 The organisation shall be informed of the names of the members of the audit team who will carry out the assessment, with sufficient notice to appeal against the appointment of any particular auditors or experts.

3.2.5 The audit team shall be formally appointed and provided with the appropriate working documents. The plan for and the date of the audit shall be agreed to with the organisation. The mandate given to the audit team shall be clearly defined and made known to the organisation, and shall require the audit team to examine the structure, policies and procedures of the organisation, and confirm that these meet all the requirements relevant to the scope of certification/ registration and that the procedures are implemented and are such as to give confidence in the ISMS of the organisation.

ISMS Guidance

IS.7 Statement of Applicability

The applicant shall prepare a Statement of Applicability describing which parts of the ISMS standard or normative document are relevant and applicable for the organisation's ISMS. The Statement of Applicability shall be part of the working documents provided to the audit team.

3.3 Assessment

The audit team shall assess the ISMS of the organisation covered by the defined scope against all applicable certification/ registration requirements.

IAF Guidance

G.3.3.1. Certification/ registration bodies shall allow auditors sufficient time to undertake all activities relating to an assessment or reassessment. The time allocated should be based on such factors as the size of the organisation, number of locations and the standards, which apply to the certification/ registration. The certification/ registration body shall be prepared to substantiate or justify the amount of time used in any assessment, surveillance or reassessment.

ISMS Guidance

IS.8 Scope of certification/ registration

Organisations should define the scope of their ISMS. A role of the certification/ registration body is to provide consistency in ensuring that organisations do not exclude from the scope of their ISMS elements of their operation, which should properly be included under it.

Certification/ registration bodies should therefore ensure that the organisation's information security risk assessment properly reflects its activities and extends to the boundaries of its activities as defined in the ISMS standard or normative document. Certification/ registration bodies should confirm that this is reflected in the organisation's Statement of Applicability.

Interfaces with services or activities that are not completely within the scope of the ISMS should be addressed within the ISMS subject to certification/ registration and should be included in the organisation's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. computers, telecommunication systems, etc.) with others.

IS.8.1 Multiple sites

Multiple sampling decisions in the area of ISMS certification/ registration are more complex than the same decisions are for quality systems. Certification/ registration bodies wishing to use a sample based approach to multiple site assessment need to maintain procedures, which include the full range of issues below in the building of their sampling programme.

Prior to undertaking its first assessment based on sampling, the certification/ registration body shall provide to the accreditation body the methodology and procedures which it employs and provide demonstrable evidence of how these take account of the issues below to manage multiple site ISMS assessment.

The certification/ registration body's procedures should ensure that the initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined in accordance with the provisions below.

Where an organisation has a number of similar sites covered by a single ISMS, a certificate may be issued to the organisation to cover all such sites provided that:

a) all sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review;

b) all sites have been audited in accordance with the organisation's internal security review procedure(s);

c) a representative number of sites have been sampled by the certification/ registration body, taking into account the requirements below:

    i) the results of internal audits of head office and the sites,

    ii) the results of management review,

    iii) variations in the size of the sites,

    iv) variations in the business purpose of the sites,

    v) complexity of the ISMS,

    vi) complexity of the information systems at the different sites,

    vii) variations in working practices,

    viii) variations in activities undertaken,

    ix) potential interaction with critical information systems or information systems processing sensitive information,

    x) differing legal requirements;

d) the sample should be partly selective based on the above in point c) and partly non-selective and should result in a range of different sites being selected, without excluding the random element of site selection;

e) every site included in the ISMS which is subject to significant threats to assets, vulnerabilities or impacts should be audited by the certification/ registration body prior to certification/ registration;

f) the surveillance programme should be designed in the light of the above requirements and should, within a reasonable time, cover all sites of the organisation or within the scope of the ISMS certification/ registration included in the Statement of Applicability;

g) in the case of a nonconformity being observed either at the head office or at a single site, the corrective action procedure should apply to the head office and all sites covered by the certificate/ registration.

The Audit described in IS.9 below should address the organisation's head office activities to ensure that a single ISMS applies to all sites and delivers central management at the operational level. The audit shall address all the issues outlined above.

IS.9 Audit Methodology

A certification/ registration body should perform its audit of an organisation's ISMS in at least two stages at the organisation's site(s), unless it can justify an alternative approach. Adaptation of the certification/ registration process to the needs of very small organisations may provide justification in particular circumstances. For the purposes of this guidance, two stages are described as "audit (stage 1)" and "audit (stage 2)". The key objectives of each, together with the minimum coverage, are described below.

The certification/ registration body should have procedures, which require that the applicant be able to demonstrate prior to commencement of the audit that the internal security review process is scheduled, and the programme and procedures are operational and can be shown to be operational.

Note: On the subject of auditing, also see IAF Guidance on Consultancy - G.2.1.10 to G.2.1.33 above.

IS 9.1 Audit (stage 1)

In this stage of the audit, the certification/ registration body should obtain documentation on the design of the ISMS covering at least the organisation's analysis of information security related risks, the Statement of Applicability, and the core elements of the ISMS.

The objectives of the audit (stage 1) are to provide a focus for planning the audit (stage 2) by gaining an understanding of the ISMS in the context of the organisation's security policy and objectives, and, in particular, of the organisation's state of preparedness for the audit.

The audit (stage 1) includes, but should not be restricted to, the document review. The certification/ registration body and the organisation shall agree when and where the document review is conducted. In every case, the document review should be completed prior to the commencement of audit (stage 2).

The results of the audit (stage 1) should be documented in a written report. The certification/ registration body should review the audit (stage 1) report for deciding on proceeding with the audit (stage 2) and for selecting audit (stage 2) team members with the necessary competence.

The certification/ registration body should make the organisation aware of the further types of information and records that may be required for detailed inspection during the audit (stage 2).

When the audit (stage 1), including document review, is not conducted by a single person the certification/ registration body should be able to demonstrate how the activities of the various team members are co-ordinated.

IS.9.2 Audit (stage 2)

The audit (stage 2) always takes place at the site(s) of the organisation. On the basis of findings documented in the audit (stage 1) report, the certification/ registration body drafts an audit plan for the conduct of the audit (stage 2). The objectives of the audit (stage 2) are:

a) to confirm that the organisation adheres to its own policies, objectives and procedures;

b) to confirm that the ISMS conforms with all the requirements of the ISMS standard or normative document and is achieving the organisation's policy objectives;

To do this, the audit should focus on the organisation's

c) assessment of information security related risks and the resulting design of the ISMS;

d) the Statement of Applicability;

e) objectives and targets derived from this process;

f) performance monitoring, measuring, reporting and reviewing against the objectives and targets;

g) security and management reviews;

h) management responsibility for the information security policy;

i) links between policy, the results of information security risk assessments, objectives and targets, responsibilities, programmes, procedures, performance data, and security reviews.

IS.10 Specific Elements of the ISMS Audit

IS.10.1 Evaluation of information security related threats to assets, vulnerabilities and impacts on the organisation and control of those deemed to be significant: The role of the certification/ registration body

In order to provide confidence that organisations are consistent in establishing and maintaining procedures for the identification, examination and evaluation of information security related threats to assets, vulnerabilities and impacts on the organisation, certification/ registration bodies should consider the following factors:

a) it is for the organisation to define the criteria by which information security related threats to assets, vulnerabilities and impacts on the organisation are identified as significant, and to develop procedure(s) for doing this;

b) the certification/ registration body should require the organisation to demonstrate that the analysis of security related threats is relevant and adequate for the operation of the organisation;

c) any inconsistency between the organisation's policy, objectives and targets and its procedure(s) or the results of their application.

The certification/ registration body should establish whether the procedures employed in analysis of significance are sound and properly implemented. If an information related threat to assets, a vulnerability or an impact on the organisation is identified as being significant, it should be managed within the ISMS.

IS.10.2 Regulatory Compliance: The role of the certification/ registration body

The maintenance and evaluation of legal compliance is the responsibility of the organisation. The certification/ registration body should restrict itself to checks and samples in order to establish confidence that the ISMS functions in this regard.

An organisation with a certified/ registered ISMS has a management system that should achieve continuing compliance with regulatory requirements applicable to the information security impacts of its activities, products and services. The certification/ registration body confirms that a system capable of achieving the required compliance is fully implemented.

The certification/ registration body should verify that the organisation has evaluated legal and regulatory compliance and can show that action has been taken in cases of non-compliance with relevant regulations.

IS.10.3 Integration of ISMS documentation with that for Other Management Systems

It is acceptable to combine the documentation for ISMS and other management systems (such as quality, health and safety, and environment) as long as the ISMS can be clearly identified together with the appropriate interfaces to the other systems.

IS.10.4 Combining Management Audits

The ISMS audit can be combined with audits of other management systems. This combination is possible provided it can be demonstrated that the audit satisfies all requirements for certification/ registration of the ISMS. All the elements important to an ISMS should appear clearly, and be readily identifiable, in the audit reports. The quality of the audit should not be adversely affected by the combination of the audits.

3.4 Assessment report

3.4.1 The certification/ registration body may adopt reporting procedures that suit its needs but as a minimum these procedures shall ensure that:

a) a meeting takes place between the audit team and the organisation's management prior to leaving the premises at which the audit team provides a written or oral indication regarding the conformity of the organisation's ISMS with the particular certification/ registration requirements and provides an opportunity for the organisation to ask questions about the findings and their basis;

b) the audit team provides the certification/ registration body with a report of its findings as to the conformity of the organisation's ISMS with all of the certification/ registration requirements;

c) a report on the outcome of the assessment is promptly brought to the organisation's attention by the certification/ registration body, identifying any nonconformity to be discharged in order to comply with all of the certification/ registration requirements;

d) the certification/ registration body shall invite the organisation to comment on the report and to describe the specific actions taken, or planned to be taken within a defined time, to remedy any nonconformity with the certification/ registration requirements identified during the assessment, and shall inform the organisation of the need for full or partial reassessment or whether a written declaration to be confirmed during surveillance will be considered adequate;

e) the report shall contain as a minimum:

1) date(s) of audit(s),

2) the names of the person(s) responsible for the report,

3) the identification of entities audited (e.g. the names and addresses of facilities and identification of organisational elements audited),

4) the assessed scope of certification/ registration or reference thereto including reference to the standard or normative document applied,

5) comments on the conformity of the organisation's ISMS with the certification/ registration requirements with a clear statement of nonconformity and, where applicable, any useful comparison with the results of previous assessments of the organisation,

6) an explanation of any differences from the information presented to the body at the closing meeting.

3.4.2 If the report authorised by the certification/ registration body differs from the report referred to in clause 3.4.1 c) and e), it shall be submitted to the organisation, with an explanation of any differences from the previous report.

The report shall take into consideration

- **a) the qualification, experience and authority of the staff encountered;**
- **b) the adequacy of the internal organisation and procedures adopted by the applicant body to give confidence in the ISMS;**
- **c) the actions taken to correct identified nonconformities, including, where applicable, those identified at previous assessments.**

3.5 Decision on certification/ registration

3.5.1 The decision whether or not to certify/ register an organisation's ISMS shall be taken by the certification/ registration body on the basis of the information gathered during the certification/ registration process and any other relevant information. Those who make the certification/ registration decision shall not have participated in the audit.

ISMS Guidance

IS.11 Certification/ registration decision

The entity which takes the decision on granting certification should not normally overturn a negative recommendation of the audit team. If such a situation does arise, the certification/ registration body shall document and justify the basis for the decision to overturn the recommendation.

3.5.2 The certification/ registration body shall not delegate authority for granting, maintaining, extending, reducing, suspending or withdrawing certification/ registration to an outside person or body.

3.5.3 The certification/ registration body shall provide to each of its organisations whose ISMS is certified/ registered, certification/ registration documents such as a letter or a certificate signed by an officer who has been assigned such responsibility. These documents shall identify for the organisation and each of its information systems covered by the certification/ registration:

- **a) the name and address;**
- **b) the scope of the certification/ registration granted, including:**
  - **1) the ISMS standards and/or other normative documents to which ISMS are certified/ registered,**
  - **2) the organisation's activities with respect to the product, process or service categories;**
- **c) the effective date of certification/ registration, and the term for which the certification/ registration is valid;**
- **d) reference to the specific version of the statement of applicability;**
- **e) appropriate certification/ registration body, accreditation, and other applicable logos or marks.**

3.5.4 Any application for amendment to the scope of a certification/ registration that has already been granted shall be processed by the certification/ registration body. The certification/ registration body shall decide what, if any, assessment procedure is appropriate to determine whether or not the amendment should be granted and shall act accordingly.

IAF Guidance

G.3.5.1. The information gathered during the certification/ registration process should be sufficient:

1) for the certification/ registration body to be able to take an informed decision on certification/ registration;
2) for traceability to be available in the event, for example, of an appeal or for planning for the next audit (possibly by a different team);
3) to ensure continuity.

In addition to the requirements for reporting in ISO/IEC Guide 62 clause 3.4.1.e), this information should cover:

- the degree of reliance that can be placed on the internal security reviews;
- a summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS;
- the conclusions reached by the audit team.

ISMS Guidance

IS.12 Reporting by audit teams to the certification/ registration body

In order to provide a basis for the certification/ registration decision, the certification/ registration body will require clear reports, which provide sufficient information to make the decision.

a) Reports from the audit team to the certification/ registration body are required at various stages in the assessment process. In combination with information held on file, these reports should at least contain:
   i) an account of the audit including a summary of the document review,
   ii) an account of the assessment of the organisation's information security risk analysis,
   iii) total audit time used and detailed specification of time spent on document review, assessment of risk analysis, implementation audit, and audit reporting,
   iv) clarification of nonconformities,
   v) audit enquiries which have been followed, rationale for their selection, and the methodology employed,
   vi) recommendation on certification/ registration by the audit team to the certification/ registration body;

b) A surveillance report should contain, in particular, information on clearing of nonconformities revealed previously. As a minimum, the reports arising from surveillance should build up to cover in totality the requirement of point a) above.

IAF Guidance

G.3.5.2. Certification/ registration shall not be granted until all nonconformities as defined in guidance G.1.3.1. have been corrected and the correction verified by the certification/ registration body (by site visit or other appropriate form of verification).

G.3.5.3. Clause 3.5.3.c) of ISO/IEC Guide 62 requires that a certification/ registration document shall include a statement of the term of validity. The term of validity of a certification/ registration should be compatible with the arrangements for reassessment.

ISMS Guidance

IS.13 Decision taking, in relation to the certification/ registration function

The entity, which may be an individual, which takes the decision on granting/withdrawing a certification/ registration within the certification/ registration body, should incorporate a level of knowledge and experience in all areas which is sufficient to evaluate the audit processes and associated recommendations made by the audit team.

3.6 Surveillance and reassessment procedures

3.6.1 The certification/ registration body shall carry out periodic surveillance and reassessment at sufficiently close intervals to verify that its organisations whose ISMS are certified/ registered continue to comply with the certification/ registration requirements.

NOTE 5 In most cases it is unlikely that a period greater than one year for periodic surveillance would satisfy the requirements of this clause.

IAF Guidance

G.3.6.1. Certification/ registration bodies shall have clear procedures laying down the circumstances and conditions in which certification/ registrations will be maintained. If on surveillance or reassessment, nonconformities, as defined in G.1.3.1, are found to exist, such nonconformities shall be effectively corrected within a time agreed by the certification/ registration body. If correction is not made within the time agreed certification/ registration shall be reduced, suspended or withdrawn. The time allowed to implement corrective action should be consistent with the severity of the nonconformity and the risk to the assurance of products or services meeting specified requirements.

G.3.6.2. Surveillance undertaken by the certification/ registration body shall give assurance that its certified/ registered organisations continue to comply with the requirements of the standard to which they are certified/ registered. The certification/ registration body should have the facilities and procedures to enable it to achieve this.

3.6.2 Surveillance and reassessment procedures shall be consistent with those concerning the assessment of the organisation's ISMS as described in this publication.

IAF Guidance

G.3.6.3. Clause 3.6.1 of ISO/IEC Guide 62 requires a certification/ registration body to conduct a surveillance and reassessment programme at sufficiently close intervals to verify that its certified/ registered organisations continue to comply with the certification/ registration requirements.

G.3.6.4. The purpose of surveillance is to verify that the approved ISMS continues to be implemented, to consider the implications of changes to that system initiated as a result of changes in the organisation's operation and to confirm continued compliance with certification/ registration requirements. Surveillance of an organisation's ISMS shall take place on a regular basis, normally it should be undertaken at least once a year. Surveillance programs should normally include:

- the system maintenance elements, which are internal audit, internal security review, management review and preventive and corrective action;
- communications from external parties as required by the ISMS standard or normative document;
- changes to the documented system;
- areas subject to change;
- selected elements of the certification/ registration standard or normative document;
- other selected areas as appropriate.

G.3.6.5. The surveillance activities shall be subject to special provision if an organisation with a certified/ registered ISMS makes major modifications to its system or if other changes take place which could affect the basis of its certification/ registration.

G.3.6.6. The purpose of reassessment is to verify overall continuing conformity of the organisation's ISMS to the requirements of the ISMS standard or normative document and that the ISMS has been properly implemented and maintained. In most cases it is unlikely that a period greater than three years for periodic reassessment of the organisation's ISMS would satisfy this requirement. The reassessment should provide for a review of past implementation and continuing maintenance of the system over the period of certification/ registration. The reassessment program should take into consideration the results of the above review and should at least include a review of the ISMS documents and a system audit (which may replace and/or extend a regular surveillance audit). It shall at least ensure

- the effective interaction between all elements of the ISMS;
- the overall effectiveness of the ISMS in its entirety in the light of changes in operations;
- demonstrated commitment to maintain the effectiveness of the ISMS.

G.3.6.7. If, exceptionally, the reassessment period is extended beyond three years, the certification/ registration body should demonstrate that the effectiveness of the complete ISMS has been evaluated on a regular basis, and should have a surveillance frequency that compensates for this in order to maintain the same level of confidence.

G.3.6.8. During surveillance audits, certification/ registration bodies should check the records of appeals, complaints and disputes brought before the certification/ registration body, and where any nonconformity or failure to meet the requirements of certification/ registration is revealed, that the organisation has investigated its own ISMS and procedures and taken appropriate corrective action.

G.3.6.9. A surveillance report should contain, in addition to the information required by guidance G.3.5.1, a report on the clearing of each nonconformity revealed previously.

ISMS Guidance

IS.14 Surveillance audits and reassessments

As a minimum, surveillance by the certification/ registration body should include, on an annual basis, the following considerations:

i) the effectiveness of the ISMS with regard to achieving the objectives of the organisation's information security policy;

ii) the functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations;

iii) action taken on nonconformities identified during the last audit;

and should at least cover the points listed for reporting in clause 3.4.2 above.

a) The certification/ registration body should be able to adapt its surveillance programme to the information security issues related threats to assets, vulnerabilities and impacts on to the organisation and justify this programme.

b) The surveillance programme of the certification/ registration body should be determined by the certification/ registration body. Specific dates for visits may be agreed with the certified/ registered organisation.

c) Surveillance audits may be combined with audits of other management systems. The reporting should clearly indicate the aspects relevant for each management system.

d) The certification/ registration body is required to supervise the appropriate use of the certificate and report.

e) The audit methodology for reassessments should be the same as for audit.

3.7 Use of certificates and logos

3.7.1 The certification/ registration body shall exercise proper control over ownership, use and display of its ISMS certification/ registration mark and logos.

3.7.2 If the certification/ registration body confers the right to use a symbol or logo to indicate certification/ registration of an ISMS, the organisation may use the specified symbol or logo only as authorised in writing by the certification/ registration body. This symbol or logo shall not be used on a product, or in a way that may be interpreted as denoting product conformity.

3.7.3 The certification/ registration body shall take suitable action to deal with incorrect references to the certification/ registration system or misleading use of certificates and logos found in advertisements, catalogues, etc.

NOTE 6 Such action could include corrective action, withdrawal of certificate, publication of the transgression and, if necessary, other legal action.

IAF Guidance

G.3.7.1. An accredited certificate should state the standard(s) or other normative document(s) against which certification/ registration is granted and the name of the certification/ registration body that issued it and the name of the relevant accreditation body or bodies. It should be made clear that the certificate is issued within the accredited scope of the certification/ registration body.

G.3.7.2. All certificates issued by an accredited certification/ registration body which are within its scope of accreditation should bear the relevant accreditation body's mark. In the case of an organisation requesting a certificate to be issued without an accreditation mark, for the certificate to be regarded as an accredited certificate it shall include the name of the accreditation body and the registration number.

G.3.7.3. In those cases where a certification/ registration body has been accredited by more than one accreditation body, the certificate should bear at least one accreditation mark, as appropriate to suit market needs.

G.3.7.4. The certification/ registration body should have documented procedures for the use of its mark, and for the procedures it is to follow in case of misuse, including false claims as to certification/ registration and false use of certification/ registration body marks.

G.3.7.5. If a certification/ registration body incorrectly claims accredited status for certificates issued before appropriate accreditation has been granted, the accreditation body may require it subsequently to withdraw them.

G.3.7.6. The provisions in clause 3.7.1 of ISO/IEC Guide 62 referring to "certification/ registration mark and logos" and that in clause 3.7.2 referring to a "symbol or logo" are both applicable to marks, logos and symbols.

G.3.7.7. The certification/ registration body should avoid use of the same mark to indicate different systems of conformity certification/ registration (for example product certification/ registration and management system certification/ registration) and should avoid confusion between the meanings of its own marks if there are more than one.

G.3.7.8. A certification/ registration body should have procedures to ensure that certified/ registered organisations do not allow its marks to be used in a way which may be likely to mislead or cause confusion.

3.8 Access to records of complaints to organisations

The certification/ registration body shall require each organisation whose ISMS is certified/ registered to make available to the certification/ registration body, when requested, the records of all complaints and corrective action taken in accordance with the requirements of the ISMS standards or other normative documents.

IAF Guidance

G.3.8.1. This clause deals only with complaints received by the certified/ registered organisation, not by the certification/ registration body.

G.3.8.2. Complaints represent a source of information as to possible nonconformity. On receipt of a complaint the certified/ registered organisation should establish, and where appropriate report on, the cause of the nonconformity, including any predetermining (or predisposing) factors within the organisation's ISMS.

G.3.8.3. During surveillance audits certification/ registration bodies should check where any such nonconformity or failure to meet the requirements of the standard is revealed, that the organisation has investigated its own systems and procedures and taken appropriate corrective action.

G.3.8.4. The certification/ registration body should satisfy itself that the organisation is using such investigations to develop remedial / corrective action, which should include measures for:

- notification to appropriate authorities if required by regulation;
- restoring conformity as quickly as possible;
- preventing recurrence;
- evaluating and mitigating any adverse security incidents and their associated impacts;
- ensuring satisfactory interaction with other components of the ISMS;
- assessing the effectiveness of the remedial / corrective measures adopted.

G.3.8.5. The implementation of the remedial / corrective action should not be deemed to have been completed until its effectiveness has been demonstrated and the necessary changes made in the procedures, documentation and records.

ANNEX 1 SCOPES OF ACCREDITATION

This list of scopes of accreditation is based on the statistical nomenclature for economic activities (NACE Rev. 1) 1994 published by the Commission of European Communities (official Journal L 083 1993).

No	Description	NACE Code
1	Agriculture, fishing	A, B
2	Mining and quarrying	C
3	Food products, beverages and tobacco	DA
4	Textiles and textile products	DB
5	Leather and leather products	DC
6	Wood and wood products	DD
7	Pulp, paper and paper products	DE 21
8	Publishing companies	DE 22.1
9	Printing companies	DE 22.2,3
10	Manufacture of coke and refined petroleum products	DF 23.1,2
11	Nuclear fuel	DF 23.3
12	Chemicals, chemical products and fibres	DG minus 24.4
13	Pharmaceuticals	DG 24.4
14	Rubber and plastic products	DH
15	Non-metallic mineral products	DI minus 26.5,6
16	Concrete, cement, lime, plaster etc	DI 26.5,6
17	Basic metals and fabricated metal products	DJ
18	Machinery and equipment	DK
19	Electrical and optical equipment	DL
20	Shipbuilding	DM 35.1
21	Aerospace	DM 35.3
22	Other transport equipment	DM 34,35.2,4,5
23	Manufacturing not elsewhere classified	DN 36
24	Recycling	DN 37
25	Electricity supply	E 40.1
26	Gas supply	E 40.2
27	Water supply	E 41,40.3
28	Construction	F
29	Wholesale and retail trade; Repair of motor vehicles, motorcycles and personal and household goods	G
30	Hotels and restaurants	H
31	Transport, storage and communication	I
32	Financial intermediation; real estate; renting	J,K 70, K 71
33	Information technology	K 72
34	Engineering services	K 73, 74.2
35	Other services	K 74 minus K 74.2
36	Public administration	L
37	Education	M
38	Health and social work	N
39	Other social services	O