Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

Legend: C – Complies, O – Observation, T – To Address at Audit, N – Nonconformity, N/A – Not Applicable

Clause Requirement
2 Normative References *Where does the CB establish the following normative references:* *ISO/IEC 17021-1:2015,Conformity assessment – Requirements for bodies providing audit and certification of management systems—Part 1:Requirements* *ISO/IEC 27001, Information technology – Security techniques – Information security management systems—Overview and vocabulary* *ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5 General requirements **5.1 Legal and Contractual matters** **5.1.1 Legal Responsibility** *Is the certification body a legal entity, or a defined part of a legal entity, such that it can be held legally responsible for all its certification activities? (A governmental certification body is deemed to be a legal entity on the basis of its governmental status).*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.1.2 Certification Agreement *Does the certification body have a legally enforceable agreement for the provision of certification activities to its client?* *Where there are multiple offices of a certification body or multiple sites of a client, does the certification body ensure that there is a legally enforceable agreement between the certification body granting certification and issuing a certificate, and all the sites covered by the scope of the certification?* **An agreement can be achieved through multiple agreements that reference or otherwise link to one another.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

5.1.3 Responsibility for certification decisions

Is the certification body responsible for, and does it retain authority for its decisions relating to certification, including the granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring following suspension, or withdrawing of certification?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

5.2 Management of impartiality

5.2.1 *Does the conformity assessment activities undertaken impartially?*

Is the certification body responsible for the impartiality of its conformity assessment activities and does it not allow commercial, financial or other pressures to compromise impartiality?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

5.2.1 IS 5.2 Conflicts of interests

Does the certification body carry out the following duties without them being considered as consultancy or having potential conflict of interest:

a. *arranging and participating as a lecturer in training courses, provided that, where these courses relate to information security management, related management systems or auditing, certification bodies shall confine themselves to the provision of generic information and advice which is publicly available, i.e. they shall not provide company-specific advice which contravenes the requirements of b) below;*
b. *making available or publishing on request information describing the certification body's interpretation of the requirements of the certification audit standards (see 9.1.3.6)*
c. *activities prior to audit, solely aimed at determining readiness for certification audit; however, such activities shall not result in the provision of recommendations or advice that would contravene this clause and the certification body shall 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 certification audit duration;*
d. *performing second and third-party audits according to standards or regulations other than those being part of the scope of accreditation;*
e. *adding value during certification audits and surveillance visits, e.g. by identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions.*

Does the certification body provide internal information security reviews of the client's ISMS subject to certification?

Furthermore, is the certification body independent from the body or bodies (including any individuals) which provide internal ISMS audit?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
5.2.2 *Does the certification body have top management commitment to impartiality in management system certification activities?* *Does the certification body have a policy that it understands the importance of impartiality in carrying out its management system certification activities, manages conflict of interest and ensures the objectivity of its management system certification activities?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.2.3 *Has the certification body identified, analysed and documented the possibilities for conflict of interests arising from the provision of certification including any conflicts arising from its relationships?* *Where there are any threats to impartiality, does the certification body document and demonstrate how it eliminates or minimizes such threats and document any residual risk?* *Does the demonstration cover all potential sources of conflict of interests identified, whether they arise from within the certification body or from the activities of other persons, bodies or organizations?* I*f a relationship poses an unacceptable threat to impartiality (such as a wholly owned subsidiary of the certification body requesting certification from its parent), is certification provided?* *Does the top management review any residual risk to determine if it is within the level of acceptable risk?* *Does the risk assessment process include identification of and consultations with appropriate interested parties to advise on matters affecting impartiality including openness and public perception?* *Is the consultation with the appropriate interested parties balanced with no single interest predominating?* **Sources of threats to impartiality of the certification body can be based on ownership, governance, management, personnel, shared resources, finances, contracts, training, marketing and payment of a sales commission or other inducement for the referral of new clients, etc.* ***Interested parties can include personnel and clients of the certification body, customers of organizations whose management systems are certified, representatives of industry trade associations, representatives of governmental regulatory bodies or other governmental services, or representatives of non-governmental organizations, including consumer organizations.* ****One way of fulfilling the consultation requirement of this clause is by the use of a committee of these interested parties.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.2.4 *Is there any evidence of the certification body certifying another certification body for its management system certification activities?* SEE NOTE 5.2.2

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.2.5 *Does the certification body or any part of the same legal entity and any entity under the organization control of certification body [see 9.5.1.2, bullet b] offer or provide management system consultancy?* *(This also applies to that part of government identified as the certification body)* **This does not preclude the possibility of exchange of information (e.g. explanation of findings or clarification of requirements) between the certification body and its client.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.2.6 *Does the certification body or any part of the same legal entity and any entity under the organizational control of the certification body offer or provide internal audits to its certified clients? The carrying out of internal audits by the certification body and any part of the same legal entity to its certified clients is a significant threat to impartiality.* *Has the certification body certified a management system on which it provided internal audits within two years following the end of the internal audit?* **SEE NOTE 5.2.3*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.2.7 *Where a client has received management systems consultancy from a body that has a relationship with a certification body, this is a significant threat to impartiality.* *Has the certification body certified a management system within two years following the end of the internal audit?* **SEE NOTE 5.2.3*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.2.8 *Does the certification body outsource audits to a management system consultancy organization?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.2.9 *Are the certification body's activities marketed or offered as being linked with the activities of an organization that provides management system consultancy?* *Does the certification body take action to correct inappropriate claims by any consultancy organization stating or implying that certification would be simpler, easier, faster or less expensive if the certification body were used?* *Does the certification body state or imply that certification would be simpler, easier, faster or less expensive if a specified consultancy organization were used?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.2.10 *Does the certification body use personnel (who have provided management system consultancy, including those acting in a managerial capacity) to take part in an audit or other certification activities if they have been involved in management system consultancy towards the client in question within two years following the end of the consultancy?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.2.11 *Does the certification body take action to respond to any threats to its impartiality arising from the actions of other persons, bodies or organizations?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
5.2.12 *How does the certification body ensure that all personnel, either internal or external or committees, who could influence the certification activities, act impartially and not allow commercial, financial or other pressures to compromise impartiality?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

5.2.13 *Does the certification require personnel, both internal and external, to reveal any situation known to them that may present them or the certification body with a conflict of interests?*
Does the certification body use this information as input to identifying threats to impartiality raised by the activities of such personnel or by the organizations that employ them?
Does the certification body use personnel, either internal or external, that cannot demonstrate that there is no conflict of interest?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

5.3 Liability and financing

5.3.1 *Can the certification body demonstrate that it has evaluated the risks arising from its certification activities?*
Does the certification body have adequate arrangement (e.g. insurance or reserves) to cover liabilities arising from its operations in each of its fields of activities and the geographic areas in which it operates?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

5.3.2 *Has the certification body evaluated its finances and sources of income and demonstrate to the committee specified in 6.2 that initially and on an ongoing basis, commercial, financial or other pressures do not compromise its impartiality?*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

6 Structural requirements

6.1 Organizational Structure and top management

6.1.1 *Has the certification body documented its organizational structure, showing duties, responsibilities and authorities of management and other certification personnel and any committees?*
When the certification is a defined part of a legal entity, does the structure include the line of authority and the relationship to other parts within the same legal entity?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

6.1.2 *Is the certification activities structured and managed so as to safeguard impartiality?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
6.1.3 *Has the certification body identified the top management (board, group of persons or person) having overall authority and responsibility for each of the following:* *a. Development of policies relating to the operation of the body;* *b. Supervision of the implementation of the policies and procedures;* *c. Ensuring impartiality;* *d. Supervision of the finances of the body;* *e. Development of management system certification services and schemes;* *f. Performance of audits and certification, and responsiveness to complaints;* *g. Decisions on certification;* *h. Delegation of authority to committees or individuals, as required, to undertake defined activities on its behalf;* *i. Contractual arrangements;* *j. Provision of adequate resources for certification activities?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
6.1.4 *Does the certification body have formal rules for the appointment, terms of reference and operation of committees involved in the certification activities?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
6.2 Operational control **6.2.1** *Does the certification body have a process for the effective control of certification activities delivered by branch offices, partnerships, agents, franchisees, etc., irrespective of their legal status, relationship or geographical location?* *Does the certification body consider the risk that these activities pose to the competence, consistency and impartiality of the certification body?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

6.2.2 *Does the certification body consider the appropriate level and method of control of activities undertaken including its processes, technical areas of certification bodies' operations, competence of personnel, lines of management control, reporting and remote access to operations including records?*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

7 Resource requirements
7.1 Competence of personnel
7.1.1 General considerations
Does the certification body have processes to ensure that personnel have appropriate knowledge relevant to the types of management systems and geographic areas in which it operates?
Has the certification body determined the competence required for each technical area (as relevant for the specific certification scheme), and for each function in the certification activity?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

7.1.1 IS 7.1.1 General considerations
7.1.1.1 Generic competence requirements
Does the certification body ensure that it has knowledge of the technological, legal and regulatory developments relevant to the ISMS of the client which it assesses?
Does the certification body define the competence requirements for each certification functions as referenced in Table A.1 of ISO/IEC 17021-1?
Does the certification body take into account all the requirements specified in ISO/IEC 17021-1 and 7.1.2 and 7.2.1 of this International Standard that are relevant for the ISMS technical areas as determined by the certification body?
**Annex A provides a summary of the competence requirements for personnel involved in specific certification functions.*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
7.1.2 Determination of competence criteria *Does the certification body have a process for determining the competence criteria for personnel involved in the management and performance of audits and other certification activities?* *Is the competence criteria determined with regard to the requirements of each type of management system standard or specification, for each technical area, and for each function in the certification process?* *Is the output of the process, the documented criteria of required knowledge and skills necessary to effectively perform audit and certification tasks to be fulfilled to achieve the intended results?* **Annex A specifies the knowledge and skills that a certification body shall define for specific functions.* *Are the additional specific competence criteria established for a specific standard or certification scheme (e.g. ISO/IEC TS 17021-2, ISO/IEC TS 17021-3 or ISO/TS 22003) applied?* **The term "technical area" is applied differently depending on the management system standard being considered. For any management system, the term is related to products, processes and services in the context of the scope of the management system standard. The technical area can be defined by a specific certification scheme (e.g. ISO/TS 22003) or can be determined by the certification body. It is used to cover a number of other terms such as "scopes", "categories", "sectors", etc., which are traditionally used in different management system disciplines.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2 IS 7.1.2 Determination of Competence Criteria **7.1.2.1 Competence requirements for ISMS auditing** **7.1.2.1.1 General requirements** *Does the certification body have criteria for verifying the background experience, specific training or briefing of audit team members that ensures at least:* *a. Knowledge of information security;* *b. Technical knowledge of the activity to be audited;* *c. Knowledge of management systems;* *d. Knowledge of the principles of auditing* **Further information on the principles of auditing can be found in ISO 19011.* *e. Knowledge of ISMS monitoring, measurement, analysis and evaluation* *(These above requirements a) to e) apply to all auditors being part of the audit team, with the exception of b), which can be shared among auditors being part of the audit team)* *Is the audit team competent to trace indications of information security incidents in the client's ISMS back to the appropriate elements of the ISMS?* *Does the audit team have appropriate work experience of the items above and practical application of these items (this does not mean that an audit team as a whole shall have enough appreciation and experience to cover the ISMS scope being audited)?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.1.2 Information security management terminology, principles, practices and techniques

Clause Requirement
Does all members of the audit team have the knowledge of: *a. ISMS specific documentation structure, hierarchy and interrelationships;* *b. Information security management related tools, methods, techniques and their application;* *c. Information security risk assessment and risk management;* *d. Processes applicable to ISMS;* *e. The current technology where information security may be relevant or an issue.* **Every auditor shall fulfil a), c) and d).*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.1.3 Information security management system standards and normative documents *Does auditors involved in ISMS auditing have knowledge of:* *a. All requirements contained in ISO/IEC 27001.* *Does all members of the audit team have the knowledge of:* *b. All controls contained in ISO/IEC 27002 (if determined as necessary also from sector specific standards) and their implementation, categorized as:* *1. Information security policies;* *2. Organization of information security;* *3. human resource security;* *4. asset management;* *5. access control, including authorization;* *6. cryptography;* *7. physical and environmental security;* *8. operations security, including IT-services;* *9. communications security, including network security management and information transfer;* *10. system acquisition, development and maintenance;* *11. supplier relationships, including outsourced services;* *12. information security incident management;* *13. information security aspects of business continuity management, including redundancies;* *14. compliance, including information security reviews.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.1.4 Business management practices *Does auditors involved in ISMS auditing have knowledge of:* *a. industry information security good practices and information security procedures;* *b. policies and business requirements for information security;* *c. general business management concepts, practices and the inter-relationship between policy, objectives and result;* *d. management processes and related terminology.* **These processes also include human resources management, internal and external communication*

Clause Requirement
and other relevant support processes.
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.1.5 Client business sector *Does auditor involved in ISMS auditing have the knowledge of:* *a. the legal and regulatory requirements in the particular information security field, geography and jurisdiction(s);* **Knowledge of legal and regulatory requirements does not imply a profound legal background.* *b. Information security risks related to business sector;* *c. Generic terminology, processes and technologies related to the client business sector;* *d. The relevant business sector practices.* *(The criteria a) may be shared amongst the audit team.)*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.1.6 Client products, processes and organization *Do auditors involved in ISMS auditing have knowledge of:* *a. The impact of organization type, size, governance, structure, functions, and relationships on development and implementation of the ISMS and certification activities, including outsourcing;* *b. Complex operations in a broad perspective;* *c. Legal and regulatory requirements applicable to the product or service.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.2 Competence requirements for leading the ISMS audit team *Does audit team leaders fulfil the following requirements, which are demonstrated in audits under guidance and supervision;* *a. Knowledge and skills to manage the certification audit process and the audit team;* *b. Demonstration of the capability to communicate effectively, both orally and in writing.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.3 Competence requirements for conducting the application review

Clause Requirement
7.1.2.3.1 Information security management system standards and normative documents *Does the personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time have knowledge of:* *a. Relevant ISMS standards and other normative documents used in the certification process.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.3.2 Client business sector *Does the personnel conducting the application review to determine the audit team competence required, to select the audit team members and to determine the audit time have knowledge of:* *a. Generic terminology, processes, technologies and risks related to the client business sector.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.3.3 Client products, processes and organization *Does personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time have knowledge of:* *a. Client products, processes, organization types, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing functions.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.4 Competence requirements for reviewing audit reports and making certification decisions **7.1.2.4.1 General** *Does the personnel reviewing audit reports and making certification decisions have knowledge that enables them to verify the appropriateness of the scope of certification as well as changes to the scope and their impact on the effectiveness of the audit, in particular the continuing validity of the identification of interfaces and dependencies and the associated risks?* *Does the personnel reviewing audit reports and making the certification decisions have knowledge of:* *a. Management system in general;* *b. Audit processes and procedures;* *c. Audit principles, practices and techniques.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.4.2 Information security management terminology, principles, practices and techniques *Does the personnel reviewing audit reports and making the certification decisions have knowledge of:* *a. The items listed in 7.1.2.1.2 a), c) and d);* *b. Legal regulatory requirements relevant to information security.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.4.3 Information security management system standards and normative documents *Does the personnel reviewing audit reports and making certification decisions have the knowledge of:* *a. Relevant ISMS standards and other normative documents used in the certification process.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.4.4 Client business sector *Does personnel reviewing audit reports and making certification decisions have knowledge of:* *a. Generic terminology and risks related to the relevant business sector practices.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.2.4.5 Client products, processes and organization *Does personnel reviewing audit reports and making certification decisions have knowledge of:* *a. Client products, processes, organization types, size, governance, structure, functions and relationships.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2 Personnel involved in the certification activities **7.2.1** *Does the certification body have, as part of its own organization, personnel with sufficient competence for managing the type and range of audit programmes and other certification work performed?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.3 Evaluation processes *Does the certification body have documented processes for the initial competence evaluation, and on-going monitoring of competence and performance of all personnel involved in the management and performance audits and other certification activities, applying the determined competence criteria?* *Does the certification body demonstrate that its evaluation methods are effective?* *Is the output from these processes identifies the personnel who have demonstrated the level of competence required for the different functions of the audit and certification process?* *Is competence demonstrated prior to the individual taking the responsibility for the performance of their activities within the certification body?* **A number of evaluation methods that can be used to evaluate competence are described in Annex B.* ***Annex C shows an example of a process flow for determining and maintaining competence.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.1.4 Other considerations Does the certification body have access to the necessary technical expertise for advice on matters directly relating to certification activities for all technical areas, types of management systems and geographic areas in which the certification body operates? Such advice may be provided externally or by certification body personnel.
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2 Personnel involved in the certification activities **7.2.1** *Does the certification body have sufficient, competent personnel for managing and supporting the type and range of audit programmes and other certification work performed?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

7.2.1 IS 7.2 Demonstration of auditor knowledge and experience

Does the certification body demonstrate that the auditors have knowledge and experience through:

a. Recognized ISMS-specific qualification;
b. Registration as auditor where applicable;
c. Participation in ISMS training courses and attainment of relevant personal credentials;
d. Up to date professional development records;
e. ISMS audit witnessed by another ISMS auditor.

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

7.2.1.1 Selecting auditors

In addition to 7.1.2.1, does the criteria for selecting auditors ensure that each auditor:

a. Has professional education or training to an equivalent level of university education;
b. Has at least four years full time practical workplace experience in information technology, of which at least two years are in role or function relating to information security;
c. Has successfully completed at least five days of training, the scope which covers ISMS audits and audit management;
d. Has gained experience in the entire process of assessing information security prior to assuming responsibility for performing as an auditor. This experience should have been gained by participation in a minimum of four ISMS certification audits, including re-certification and surveillance audits, for a total of at least 20 days of which at most 5 days may come from surveillance audits. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting;
e. Has relevant and current experience;
f. Keeps current knowledge and skills in information security and auditing up to date through continual professional development.

Do technical experts comply with criteria a), b) and e)?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

7.2.1.2 Selecting auditors for leading the team

In addition to 7.1.2.2 and 7.2.1.1, does the criteria for selecting an auditor for leading the team ensure that this auditor:

a. Has actively participated in all stages of at least three ISMS audits. The participation shall include initial scoping and planning, review of documentation and risk assessment, implementation assessment and formal audit reporting.

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

7.2.2 *Does the certification body employ, or have access to, a sufficient number of auditors, including audit team leaders, and technical experts to cover all of its activities and to handle the volume of audit work performed?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2.3 *Does the certification body make clear to each person concerned their duties, responsibilities and authorities?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2.4 *Does the certification body have defined processes for selecting, training, formally authorizing auditors and for selecting technical experts used in the certification activity?* *Does the initial competence evaluation of an auditor include a demonstration of applicable personal attributes and the ability to apply required knowledge and skill during audits?* **During the selection and training process described above desired personal behaviour can be considered. These are characteristics that affect an individual's ability to perform specific functions. Therefore, knowledge about the behaviour of individuals enables a certification body to take advantage of their strengths and to minimize the impact of their weaknesses. Desired personal behaviour that is important for personnel involved in certification activities are described in Annex D of ISO/IEC 17021.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2.5 *Does the certification body have a process to achieve and demonstrate effective auditing, including the use of auditors and audit team leaders possessing generic auditing skills and knowledge, as well as skills and knowledge appropriate for auditing in specific technical areas?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2.6 *Does the certification body ensure that auditors (and, where needed, technical experts) are knowledgeable of its audit processes, certification requirements and other relevant requirements?* *Does the certification body give auditors and technical experts access to an up-to-date set of documented procedures giving audit instructions and all relevant information on the certification activities?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2.7 *Does the certification body identify training needs and offer or provide access to specific training to ensure its auditors, technical experts and other personnel involved in certification activities are competent for the functions they perform?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2.8 *Does the group or individual that takes the decision on granting, maintaining, renewing, extending, reducing, suspending or withdrawing certification understand the applicable standard and ISMS certification requirements, and have demonstrated competence to evaluate the audit processes and related recommendations of the audit team?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2.9 *Does the certification body ensure the satisfactory performance of all personnel involved in the audit and certification activities?* *Are there documented procedures and criteria for monitoring and measurement of the performance of all persons involved, based on the frequency of their usage and the level of risk linked to their activities?* *Does the certification body review the competence of its personnel in the light of their performance in order to identify training needs?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2.10 *Does the certification body monitor each auditor considering each type of management system to which the auditor id deemed competent?* *Do they include a combination of on-site observation, review of audit reports and feedback from clients or from the market?* *Are the requirements for documented monitoring procedures documented?* *Is the monitoring designed in such a way as to minimize disturbance to the normal processes of certification, especially from the client's viewpoint?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.2.11 *Does the certification body periodically observe the performance of each auditor on-site? Is the frequency of on-site observations based on the need determined from all monitoring information available?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.3 Use of individual external auditors and external technical experts *Does the certification body require external auditors and external technical experts to have a written agreement by which they commit themselves to comply with applicable policies and procedures as defined by the certification body?* *Does the agreement address aspects relating to confidentiality and to independence from commercial and other interests?* *Does the agreement require the external auditors and external technical experts to notify the certification body of any existing or prior association with any organization they may be assigned to audit?* **Use of an individual or employee of another organization individually contracted to serve as an external auditor or technical expert does not constitute outsourcing.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
7.3.1 IS 7.3 Using external auditors or external technical experts as part of the audit team *Do technical experts work under the supervision of an auditor?* **The minimum requirements for technical experts are listed in 7.2.1.1.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

7.4 Personnel records

Does the certification body maintain up-to-date personnel records, including relevant qualifications, training, experience, affiliations, professional status, competence and any relevant consultancy services that may have been provided?

Does this include management and administrative personnel in addition to those performing certification activities?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

7.5 Outsourcing

7.5.1 *Does the certification body have a process in which it describes the conditions under which outsourcing (which is subcontracting to another organization to provide part of the certification activities on behalf of the certification body) may take place?*

Does the certification body have a legally enforceable agreement covering the arrangements, including confidentiality and conflict of interests, with each body that provides outsourced services?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

7.5.2 *Are decisions for granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing of certification not outsourced?*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

7.5.3 *Does the certification body:*

a. take responsibility for all activities outsourced to another body,

b. ensure that the body that provides outsourced services, and the individuals that it uses, conform to requirements of the certification body and also to the applicable provisions of ISO/IEC 17021 and ISO/IEC 27006, including competence, impartiality and confidentiality, and

c. *Ensure that the body that provides outsourced services, and the individuals that it uses, is not involved, either directly or through any other employer, with an organization to be audited, in such a way that impartiality could be compromised?*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

7.5.4 *Does the certification body have documented procedures for the qualification and monitoring of all bodies that provide outsourced services used for certification activities?*
Does the certification body ensure that records of the competence of auditors and technical experts are maintained?
**For 7.5.1 to 7.5.4, where the certification body engages individuals or employees of other organizations to provide additional resources or expertise, these individuals do not constitute outsourcing provided they are individually contracted to operate under the certification body's management system (see 7.3)*
***For 7.5.1 to 7.5.4, the terms "outsourcing" and "subcontracting" are considered to be synonyms.*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

8 Information requirements
8.1 Publicly information
8.1.1 *Does the certification body maintain (through publications, electronic media or other means), and make public, without request, in all geographical areas in which it operates, information about*
a. audit processes;
b. processes for granting, refusing, maintaining, renewing, suspending, restoring or withdrawing certification or expanding or reducing the scope of certification;
c. types of management systems and certification schemes in which it operates;
d. the use of the certification body's name and certification mark or logo;
e. processes for handling requests for information, complaints and appeals;
f. policy on impartiality.

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

8.1.2 *Does the certification body provide upon request information about:*
a. geographical areas in which it operates;
b. the status of a given certification;
c. the name, related normative document, scope and geographical location (city and country) for a specific certified client.
**In exceptional cases, access to certain information can be limited on the request of the client (e.g. for security reasons)*
**The certification body can also make the information in 8.1.2 public by any means it chooses without request, e.g. on its internet website.*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

8.1.3 *Does the certification body ensure that information provided to any client or to the marketplace, including advertising, is accurate and not misleading?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
8.2 Certification Documents **8.2.1** *Does the certification body provide by any means it chooses certification documents to the certified client?* **8.2.1 IS 8.2 ISMS Certification Documents** *Are certification documents signed by an officer who has been assigned such responsibility?* *Is the version of the Statement of Applicability included in the certification documents?* **A change to the Statement of Applicability which does not change the coverage of the controls of the scope of certification need not require an update of certification document.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
8.2.2 *Do the certification document(s) identify the following:* *a. the name and geographic location of each client whose ISMS is certified (or the geographic location of the headquarters and any sites within the scope of a multi-site certification);* *b. the effective date of granting, expanding or reducing the scope of certification, or renewing certification which shall not be before the date of the relevant certification decisions;* **The certification body can keep the original certification date on the certificate when a certificate lapses for a period of time provided that:* *- the current certification cycle start and expiry date are clearly indicated;* *- the last certification cycle expiry date be indicated along with the date of recertification audit.* *c. the expiry date or recertification due date consistent with the recertification cycle;* *d. a unique identification code;* *e. the standard and/or other normative document, including indication of issue status (e.g. revision date or number) used for audit of the certified client;* *f. the scope of certification with respect to the type of activities, products and services as applicable at each site without being misleading or ambiguous;* *g. the name, address and certification mark of the certification body; other marks (e.g. accreditation symbol, client's logo) may be used provided they are not misleading or ambiguous;* *h. any other information required by the standard and/or other normative document used for certification;* i. *in the event of issuing any revised certification documents, a means to distinguish the revised documents from any prior obsolete documents?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

8.3 Reference to certification and use of marks

8.3.1 *Does the certification body have rules governing any management system certification mark that it authorizes certified client to use?*
Do these rules ensure, among other things, traceability back to the certification body?
Is there no ambiguity, in the mark or accompanying text, as to what has been certified and which certification body has granted the certification?
Has this marks not used on a product nor product packaging nor in any other way may be interpreted as denoting product conformity?
**ISO/IEC 17030 provides additional information for use of third-party marks.*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

8.3.2 *Does certification body not permit its marks to be applied by certified clients to laboratory test, calibration or inspection reports or certificates?*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

8.3.3 *Does certification body have rules governing the use of any statement on product packaging or in accompanying information that the certified client has a certified management system?*
(Product packaging is considered as that which can be removed without the product disintegrating or being damaged. Accompanying information is considered as separately available or easily detachable. Type labels or identification plates are considered as part of the product.)
Does the statement in no way imply that the products, process or service is certified by this means?
Does the statement include reference to:

- *identification (e.g. brand or name) of the certified client*
- *the type of management system (e.g. quality, environment) and the applicable standard;*
- *the certification body issuing the certificate.*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
8.3.4 *Does the certification body through legally enforceable arrangement require that the certified client:* *a. conforms to the requirements of the certification body when making reference to its certification status in communication media such as the internet, brochures or advertising, or other documents;* *b. does not make or permit any misleading statement regarding its certification;* *c. does not use or permit the use of certification document or any part thereof in a misleading manner;* *d. upon withdrawal of its certification, discontinues its use of all advertising matter that contains a reference certification, as directed by the certification body;* *e. amends all advertising matter when the scope of certification has been reduced;* *f. does not allow reference to its management system certification to be used in such a way as to imply that the certification body certifies a product (including service) or process;* *g. does not imply that the certification applies to activities and sites that are outside the scope of certification;* *h. does not use its certification in such manner that would bring the certification body and/or certification system into disrepute and lose public trust.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
8.3.5 *Does the certification body exercise proper control of ownership and does it take action to deal with incorrect references to certification status or misleading use of certification documents, marks or audit reports.* **Such action could include request for correction and corrective action, suspension, withdrawal of certification, publication of transgression and, if necessary, legal action.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
8.4 Confidentiality **8.4.1** *Is the certification body responsible, through legally enforceable agreements, for the management of all information obtained or created during the performance of certification activities at all levels of its structure, including committees and external bodies or individuals acting on its behalf?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

8.4.1 IS 8.4 Access to organizational records

Before the certification audit, does the certification body ask the client to report if any ISMS related information (such as ISMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information?

Does the certification body determine whether the ISMS can be adequately audited in the absence of such information?

If the certification body concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, does it advise the client that the certification audit cannot take place until appropriate access arrangements are granted?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

8.4.2 *Does the certification body inform the client, in advance, of the information it intends to place in the public domain?*

Is all other information, except for information that is made publicly accessible by the client considered confidential?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

8.4.3 *Except as required in ISO/IEC 17021, is information about a particular client or individual disclosed to a third party without the written consent of the client or individual concerned?*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

8.4.4 *Where the certification body is required by law or authorized by contractual arrangements (such as with the accreditation body) to release confidential information to a third party, is the client or individual concerned, unless prohibited by law, notified in advance of the information provided?*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

8.4.5 *Is information about the client from sources other than the client (e.g. complainant, regulators) treated as confidential?*

Is this treatment consistent with the certification body's policy?

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
8.4.6 *Do personnel, including any committee members, contractors, personnel of external bodies or individuals acting on the certification body's behalf, keep all information obtained or created during the performance of the certification body's activities confidential except as required by law?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
8.4.7 *Does the certification body have processes available and use equipment and facilities that ensure the secure handling of confidential information (e.g. documents, records)?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
8.5 information exchange between a certification body and it client **8.5.1 Information on the certification activity and requirements** *Does the certification body provide information and update clients on the following:* *a. a detailed description of the initial and continuing certification activity, including the application, initial audits, surveillance audits, and the process for granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing of certification;* *b. the normative requirements for certification;* *c. information about the fees for application, initial certification and continuing certification;* *d. the certification body's requirements for clients to:* *1. comply with certification requirements;* *2. make all necessary arrangements for the conduct of the audits, including provision for examining documentation and the access to all processes and areas, records and personnel for the purposes of initial certification, surveillance, recertification and resolution of complaints;* *3. make provisions, where applicable, to accommodate the presence of observers (e.g. accreditation assessors or trainee auditor);* *e. documents describing the rights and duties of certified clients, including requirements, when making reference to its certification in communication of any kind in line with the requirements in 8.3;* *f. information on processes for handling complaints and appeals.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
8.5.2 Notice of changes by a certification body *Does the certification body give its certified clients due notice of any changes to its requirements for certification?* *Does the certification body verify that each certified client complies with the new requirements?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
8.5.3 Notice of changes by a certified client *Does the certification body have legally enforceable arrangements to ensure that the certified client informs the certification body, without delay, of matters that may affect the capability of ISMS to continue to fulfil the requirements of the standard used for certification?* *Do these include, for example, changes relating to:* *a. the legal, commercial, organizational status or ownership,* *b. organization and management (e.g. key managerial, decision-making or technical staff),* *c. contact address and sites,* *d. scope of operations under the certified ISMS, and* *e. major changes to the management system and processes.* *Does the certification body take action as appropriate?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9 Process requirements **9.1 Pre-certification activities** **9.1.1 Application** *Does the certification body require an authorized representative of the applicant organization to provide the necessary information to enable it to establish the following:* *a. the desired scope of the certification;* *b. relevant details of the applicant organization as required by the specific certification scheme, including its name and the address(es) of its site(s), its processes and operations, human and technical resources, functions, relationships and any relevant legal obligations;* *c. identification of outsourced processes used by the organization that will affect conformity to requirements;* *d. the standards or other requirements for which the applicant organization is seeking certification;* *e. whether consultancy relating to the management system to be certified has been provided and, if so, by whom.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
9.1.1.1 IS 9.1.1 Application readiness *Does the certification body require the client to have a documented and implemented ISMS which conforms to ISO/IEC 27001 and other documents required for certification?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.2 Application review **9.1.2.1** *Does the certification body conduct a review of the application and supplementary information for certification to ensure that:* *a. the information about the applicant organization and its management system is sufficient to develop an audit programme (see 9.1.3);* *b. any known difference in understanding between the certification body and the applicant organization is resolved;* *c. the certification body has the competence and ability to perform the certification activity;* *d. the scope of certification sought, the site(s) of the applicant organization's operations, time required to complete audits and any other points influencing the certification activity are taken into account (language, safety conditions, threats to impartiality, etc.).*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.2.2 *Following the review of the application, does the certification body accept or decline an application for certification?* *When the certification body declines an application for certification as a result of the review of application, are the reasons for declining an application documented and made clear to the client?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.2.3 *Based on this review, does the certification body determine the competence it needs to include in its audit team and for the certification decision?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
9.1.3 Audit programme **9.1.3.1** *Does an audit programme for the full certification cycle developed to clearly identify the audit activity/activities required to demonstrate that the client's management system fulfils the requirements for certification to the selected standard(s) or other normative document(s)?* *Does the audit programme for the certification cycle cover the complete management system requirements?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.3.1 IS 9.1.3 General *Does the audit programme for ISMS audits take the determined information security controls into account?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.3.2 *Does the audit programme for the initial certification include a two-stage initial audit, surveillance audits in the first and second years following the certification decision, and a recertification audit in the third year prior to expiration of certification?* *(The first three-year certification cycle begins with certification decision. Subsequent cycles begin with the recertification decision (see 9.6.3.2.3))* *Does the determination of the audit programme and any subsequent adjustments consider the size of the client, the scope and complexity of its management system, products and processes as well as demonstrated level of management system effectiveness and the results of any previous audits?* **Annex E provides a flowchart of a typical audit and certification process* ***The following list contains additional items that can be considered when developing or revising an audit programme, they might also need to be addressed when determining the audit scope and developing the audit plan:* - *complaints received by the certification body about the client;* - *combined, integrated or joint audit;* - *changes to the certification requirements;* - *changes to legal requirements;* - *changes to accreditation requirements;* - *organizational performance data (e.g. defect levels, keys performance indicators data);* - *relevant interested parties' concerns.* **If specified by the industry specific certification scheme, the certification cycle can be different form three years.*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.3.2 IS 9.1.3 Audit Methodology *Are the certification body's procedures not presuppose a particular manner of implementation of an ISMS or a particular format for documentation and records?* *Does the certification procedures focus on establishing that a client's ISMS meets the requirements specified in ISO/IEC 27001 and the policies and objectives of the client?* **Further guidance on auditing is given in ISO/IEC 27007.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.3.3 *Is surveillance audits conducted at least once a calendar year, except in recertification years? Is the date of the first surveillance audit following initial certification not more than 12 months from the certification decision date?* **It can be necessary to adjust the frequency of surveillance audits to accommodate factors such as seasons or management systems certification of a limited duration (e.g. temporary construction site).*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.3.3 IS 9.1.3 General preparations for the initial audit *Does the certification body require that a client makes all necessary arrangements for the access to internal audit reports and reports of independent reviews of information security?* *Does the following information at least provided by the client during stage 1 of the certification audit:* *a. general information concerning the ISMS and the activities it covers;* *b. a copy of the required ISMS documentation specified in ISO/IEC 27001 and, where required, associated documentation.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.1.3.4 *Where the certification body is taking account of certification already granted to the client and to audits performed by another certification body, does it obtain and retain sufficient evidence, such as reports and documentation on corrective actions, to any nonconformity?* *Does the document support the fulfilling of the requirements in this part of ISO/IEC 17021?* *Does the certification body, based on the information obtained, justify and record any adjustments to the existing audit programme and follow up the implementation of corrective actions concerning previous nonconformities?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.3.4 IS 9.1.3 Review periods *Does the certification body not certify an ISMS unless it has been operated through at least one management review and one internal ISMS audit covering the scope of certification?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.3.5 *Where the client operates shifts, are the activities that takes place during shift working considered when developing the audit programme and audit plans?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.3.5 IS 9.1.3 Scope of certification *Does the audit team audit the ISMS of the client covered by the defined scope against all applicable certification requirements?* *Does the certification body confirm, in the scope of the client ISMS, that clients address the requirements stated in ISO/IEC 27001, 4.3?* *Do certification bodies ensure that the client's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the scope of certification?* *Do certification bodies confirm that this is reflected in the client's scope of their ISMS and Statement of Applicability?* *Does certification body verify that there is at least one Statement of Applicability per scope of certification?* *Do certification bodies ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to certification and are included in the client's information security risk assessment?* *(An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organizations.)*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.3.6 IS 9.1.3 Certification audit criteria *Do the criteria against which the ISMS of a client is audited be the ISMS standard ISO/IEC 27001? (Other documents may be required for certification relevant to the function performed.)*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.4 Determining the audit time **9.1.4** *Does the certification body have documented procedures for determining the audit time? For each client, does the certification body determine the time needed to plan and accomplish a complete and effective audit of the client's management system?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.4.1 IS 9.4.1 Audit time *Do certification bodies allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or re-certification audit?* *Does the calculation of overall audit time include sufficient time for audit reporting?* *Does the certification body use Annex B to determine audit time?* **Further guidance and examples on audit time calculation are provided in Annex C.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.1.4.2 *In determining the audit time, does the certification body consider, among other things, the following aspects:* *a. the requirements of the relevant ISMS standard;* *b. complexity of the client and its ISMS standard;* *c. technological and regulatory context;* *d. any outsourcing of any activities included in the scope of the ISMS;* *e. the results of any prior audits;* *f. size and number of sites, their geographical location and multi-site consideration;* *g. the risks associated with the products, processes or activities of the organization;* *h. whether audits are combined, joint or integrated.* **Time spent travelling to and from audited sites is not included in the calculation of the duration of the management system audit days.* **The certification body can use the guideline established in ISO/IEC TS 17023 for determining the duration of management system audit when documenting these procedures.* *Where specific criteria have been established for a specific for a specific certification scheme, e.g. ISO/TS 22003 or ISO/IEC 27006, are these applied?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.4.3 *Does the duration of the management system audit and its justification recorded?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.4.4 *Is the time spent by any team member that is not assigned as an auditor (i.e. technical experts, translators, interpreters, observers and auditors-in-training) not count in the above established duration of the management system audit?* **The use of translators and interpreters can necessitate additional time.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.5 Multi-site sampling *Where multi-site sampling is utilized for the audit of a client's management system covering the same activity in various locations, does the certification body develop a sampling programme to ensure proper audit of the management system?* *Is the rationale for the sampling plan documented for each client?* **Where there are multiple sites not covering the same activity sampling is not appropriate.*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.5.1 IS 9.1.5 Multiple sites **9.1.5.1.1** *Where a client organization has a number of sites meeting the criteria from a.) to c.) below, does the certification body consider using a sample-based approach to multiple-site certification audit?* *a. All sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review;* *b. All sites are included within the client organization's internal ISMS audit programme;* *c. All sites are included within the client organization's ISMS management review programme.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.5.1.2 *Does the certification body that uses a sample based approach have procedures in place to ensure the following:* *a. The initial contract review identifies to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined;* *b. A representative number of sites have been sampled by the certification body, taking into account:* *1. the results of the internal audit of the head office and the sites;* *2. the results of the management review;* *3. variations in the size of the sites;* *4. variations in the business purpose of the sites;* *5. complexity of the information systems at the different sites;* *6. variations in working practices;* *7. variations in activities undertaken;* *8. variations of designs and operation of controls;* *9. potential interaction with critical information systems or information systems processing sensitive information;* *10. any differing legal requirements.* *11. Geographical and cultural aspects;* *12. Risk situation of the sites;* *13. Information security incidents at the specific sites.* *c. A representative sample is selected from all sites within the scope of the client organization's ISMS' this selection shall be based upon judgmental choice to reflect the factors presented in item b/above as well as a random element;* *d. Every site included in the ISMS which is subject to significant risks is audited by the certification body prior to certification;* *e. The audit programme has been designed in the light of the above requirements and covers representative samples of the organization scope of the ISMS certification within the three (3) years period;* *f. In the case of a nonconformity being observed, either at the head office or at a single site, the corrective action procedure applies to the head office and all sites covered by the certificate;*

Clause Requirement
Does the audit described in IS 9.1.5 below address the client organization's head office activities to ensure that a single ISMS applies to all sites and delivers central management at the operational level? *Does the audit address all the issues outlined above?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.6 Multiple management systems standards *When certification to multiple management system standard is being provided by the certification body, does the planning for the audit ensure adequate on-site auditing to provide confidence in the certification?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.6.1 IS 9.1.6 Integration of ISMS documentation with that for other management systems *The certification body may accept documentation that is combined (e.g. for information security, quality, health and safety and environment) as long as the ISMS can be clearly identified together with the appropriate interfaces to the other systems.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.1.6.2 IS 9.1.6 Combining management system audits *The ISMS audit may be combined with audits of other management systems, provided that it can be demonstrated that the audit satisfies all requirements for certification of the ISMS.* *Do all the elements important to an ISMS appear clearly and be readily identifiable in the audit reports?* *Is the quality of the audit not adversely affected by the combination of the audits?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.2 Planning audits **9.2.1 Determining audit objectives, scope and criteria** **9.2.1.1** *Are the audit objectives determined by the certification body?* *Does the certification body establish the audit scope and criteria, including any changes, after discussion with the client?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.1.1 IS 9.2.1 Audit objectives *Do the objectives include the determination of the effectiveness of the management system to ensure that the client, based on the risk assessment, has implemented applicable controls and achieved the established information security objectives?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.1.2 *Do the audit objectives describe what is to be accomplished by the audit and include the following?* *a. determination of the conformity of the client's management system, or parts of it, with audit criteria;* *b. evaluation of the ability of the management system to ensure the client organization meets applicable statutory, regulatory and contractual requirements;* ** A management system certification audit is not a legal compliance audit.* *c. evaluation of the effectiveness of the management system to ensure the client organization is continually meeting its specified objectives;* *d. as applicable, identification of areas for potential improvement of the management system.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.1.3 *Does the audit scope describe the extent and boundaries of the audit, such as physical locations, organizational units, activities and processes to be audited?* *Where the initial or re-certification process consists of more than one audit (e.g. covering different sites), does the scope of an individual audit not cover the full certification scope, is the totality of audits consistent with the scope in the certification document?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
9.2.1.4 *Are the audit criteria used as a reference against which conformity is determined, and include the following:* — *the requirements of a defined normative document on management systems;* — *the defined processes and documentation of the management system developed by the client.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.2 Audit team selection and assignments **9.2.2.1 General** **9.2.2.1.1** *Does the certification body have a process for selecting and appointing the audit team, including the audit team leader, taking into account the competence needed to achieve the objectives of the audit and requirements for impartiality?* *If there is only one auditor, does the auditor have the competence to perform the duties of an audit team leader applicable for that audit?* *Does the team have the totality of the competences identified by the certification body as set out in 9.1.2.3 for the audit?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.2.1 IS 9.2.2 Audit team *Is the audit team formally appointed and provided with the appropriate working documents?* *Is the mandate given to the audit team clearly defined and made known to the client?* *(An audit team may consist of one person provided that the person meets all the criteria set out in 7.1.2.1.)*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.2.2.1.2 *In deciding the size and composition of the audit team, does the CAB give consideration to the following:* *a. audit objectives, scope, criteria and estimated time of the audit;* *b. whether the audit is a combined, joint or integrated;* *c. the overall competence of the audit team needed to achieve the objectives of the audit;* *d. certification requirements (including any applicable statutory, regulatory or contractual requirements);* *e. language and culture;* **The team leader of a combined or integrated audit is expected to have in-depth knowledge of at least one of the standards and an awareness of the other standards used for that particular audit.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.2.1.3 *Is the knowledge and skills of the audit team leader and auditors supplemented by technical experts, translators and interpreters?* *Do these team members operate under the direction of an auditor?* *Are translators or interpreters selected such that they do not unduly influence the audit?* **The criteria for the selection of technical experts are determined on a case-by-case basis by the needs of the audit team and the scope of the audit.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.2.1.4 *Are auditors-in-training included in the audit team as participants, provided an auditor is appointed as an evaluator?* *Is the evaluator competent to take over the duties and have final responsibility for the activities and findings of the auditor-in-training?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.2.1.5 *Does the audit team leader, in consultation with the audit team, assign to each team member responsibility for auditing specific processes, functions, sites, areas or activities?* *Do these assignments take into account the need for competence, and the effective and efficient use of the audit team, as well as different roles and responsibilities of auditors, auditors-in-training and technical experts?* *Changes to the work assignments may be made as the audit progresses to ensure achievement of the audit objectives.*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.2.2 Observers, technical experts and guides **9.2.2.2.1 Observers** *Is the presence and justification of observers during an audit activity agreed to by the certification body and client prior to the conduct of the audit?* *Does the audit team ensure that observers do not influence or interfere in the audit process or outcome of the audit?* **Observers can be members of the client's organization, consultants, witnessing accreditation body personnel, regulators or other justified persons.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.2.2 IS 9.2.2 Audit team competence *The requirements listed in Clause 7.1.2 apply. For Surveillance and special audit activities, only those requirements which are relevant to the scheduled surveillance activity and special audit activity apply.* *When selecting and managing the audit team to be appointed for a specific certification audit, does the certification body ensure that the competences brought to each assignment are appropriate?* *Does the team:* *a. have appropriate technical knowledge of the specific activities within the scope of the ISMS for which certification is sought and, where relevant, with associated procedures and their potential information security risks (technical experts may fulfil this function);* *b. have understanding of the client sufficient to conduct a reliable certification audit of its ISMS given the ISMS' scope and context within the organization in managing the information security aspects of its activities, products and services;* *c. have appropriate understanding of the legal and regulatory requirements applicable to the client's ISMS* **Appropriate understanding does not imply a profound legal background.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.2.2.2 Technical experts *Is the role of technical experts during an audit activity agreed to by the certification body and client prior to the conduct of the audit?* *Does technical expert not act as an auditor in the audit team?* *Are technical experts accompanied by an auditor?* **The technical experts can provide advice to the audit team for the preparation, planning or audit.*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.2.2.3 Guides *Is each auditor accompanied by a guide, unless otherwise agreed to by the audit team leader and the client?* *Does the audit team ensure that guides do not influence or interfere in the audit process or outcome of the audit?* **The responsibilities of a guide can include:* *a. establishing contacts and timing for interviews;* *b. arranging visits to specific parts of the site or organization;* *c. ensuring that rules concerning site safety and security procedures are known and respected by the audit team members;* *d. witnessing the audit on behalf of the client;* e. *providing clarification or information as requested by an auditor.* ***Where appropriate, the auditee can also act as a guide.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.3 Audit Plan **9.2.3.1 General** *Does the certification body ensure that an audit plan is established prior to each audit identified in the audit programme to provide the basis for agreement regarding the conduct and scheduling of the audit activities?* **It is not expected that a certification body will develop an audit plan for each audit at a time that the audit programme is developed.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.2.3.1 IS 9.2.3 General *Does the audit plan for ISMS audits take the determined security controls into account?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

9.2.3.2 Preparing the audit plan

Is the audit plan appropriate to the objectives and the scope of the audit?

Does the audit plan include or refer to the following at least:

a. the audit objectives;
b. the audit criteria;
c. the audit scope, including identification of the organizational and functional units or processes to be audited;
d. the dates and sites where the on-site audit activities are to be conducted, including visits to temporary sites, as appropriate;
e. the expected time and duration of on-site audit activities;
f. the roles and responsibilities of the audit team members and accompanying persons, such as observers or interpreters.

**The audit plan information can be contained in more than one document.*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

9.2.3.2 IS 9.2.3 Network-assisted audit techniques

Does the audit plan identify the network-assisted auditing techniques that will be utilized during the audit, as appropriate?

**Network assisted auditing techniques may include, for example, teleconferencing, web meeting, interactive web-based communications and remote electronic access to the ISMS documentation and/or ISMS processes. The focus of such techniques should be to enhance audit effectiveness and efficiency, and should support the integrity of the audit process.*

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

9.2.3.3 Communication of audit team tasks

Are the tasks given to the audit team defined and made known to the client organization, and require the audit team to

a. examine and verify the structure, policies, processes, procedures, records and related documents of the client organization relevant to the management system standard;
b. determine that these meet all the requirements relevant to the intended scope of certification;
c. determine that the processes and procedures are established, implemented and maintained effectively, to provide a basis for confidence in the client's management system;
d. communicate to the client, for its action, any inconsistencies between the client's policy, objectives and targets.

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

9.2.3.3 IS 9.2.3 Timing of audit
A certification body should agree with the organization to be audited the timing of the audit which will best demonstrate the full scope of the organization. The consideration could include season, month, day/dates and shift as appropriate.

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

9.2.3.4 Communication of audit plan
Is the audit plan communicated and the dates of the audit agreed upon, with the client organization in advance?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

9.2.3.5 Communication concerning audit team members
Does the certification body provide the name of and, when requested, make available background information on each member of the audit team, with sufficient time for the client organization to object to the appointment of any particular auditor or technical expert and for the certification body to reconstitute the team in response to any valid objection?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

9.3 Initial certification
9.3.1 Initial certification audit
9.3.1.1 General
Is the initial certification audit of a management system conducted in two stages: stage 1 and stage 2?

State the CB's established policies and procedures: *(To be filled-up by the CB)*

Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.3.1 IS 9.3.1 Initial certification audit **9.3.1.1 IS 9.3.1.1 Stage 1** *In this stage of audit, does the certification body obtain documentation on the design of the ISMS covering the documentation required in ISO/IEC 27001?* *Does the certification body obtain a sufficient understanding of the design of the ISMS in the context of the client's organization, risk assessment and treatment (including the controls determined), information security policy and objectives and, in particular, of the client's preparedness for the audit?* *Does this allow planning for stage 2?* *Is the results of stage 1 documented in a written report?* *Does the certification body review the stage 1 audit report before deciding on proceeding with stage 2 and for selecting the stage 2 audit team members with the necessary competence?* *Does the certification body make the client aware of the further types of information and records that may be required for detailed examination during stage 2?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.3.1.2 Stage 1 **9.3.1.2.1** *Does planning ensure that the objectives of stage 1 can be met?* *Is the client informed of any "on site" activities during stage 1?* **Stage 1 does not require a formal audit plan (see 9.2.3).*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.3.1.2.2 *The objectives of stage 1 are to:* *a. review the client's management system documented information;* *b. evaluate the client's site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for stage 2;* *c. review the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the management system;* *d. obtain necessary information regarding the scope of the management system, including:* *- the client's site(s);* *- processes and equipment used;* *- levels of controls established (particularly in case of multisite clients);* *- applicable statutory and regulatory requirements;* *e. review the allocation of resources for stage 2 and agree the details of stage 2 with the client;* *f. provide a focus for planning stage 2 by gaining a sufficient understanding of the client's management system and site operations in the context of the management system standard or other normative document;* *g. evaluate if the internal audits management reviews are being planned and performed, and that the level of implementation of the management system substantiates that the client is ready for stage*

Clause Requirement
2. **If at least part of stage 1 is carried out at the client's premises, this can help to achieve the objectives stated above.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.3.1.2.3 *Is documented conclusions with regard to fulfilment of the stage 1 objectives and the readiness for stage 2 communicated to the client, including identification of any areas of concern that could be classified as a nonconformity during stage 2?* **The stage 1 output does not need to meet the full requirements of a report (see 9.4.8).*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.3.1.2.4 *In determining the interval between stage 1 and stage 2, is consideration given to the needs of the client to resolve areas of concern identified during stage 1?* *The certification body may also need to revise its arrangements for stage 2.* *If any significant changes would impact the management system occur, does the certification body consider the need to repeat all or part of stage 1?* *Is the client informed that the results of stage 1 may lead to postponement or cancellation of stage 2?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.3.1.3 Stage 2 *Does the purpose of stage 2 is to evaluate the implementation, including effectiveness, of the client's management system?* *Does the stage 2 take place at the site(s) of the client?* *Does it include the auditing of at least the following:* *a. information and evidence about conformity to all requirements of the applicable management system standard or other normative documents;* *b. performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative document);* *c. the client's management system ability and its performance regarding meting of applicable statutory, regulatory and contractual requirements;* *d. operational control of the client's processes;* *e. internal auditing and management review;* *f. management responsibility for the client's policies.*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.3.1.4 Initial certification audit conclusions *Does the audit team analyse all information and audit evidence gathered during stage 1 and stage 2 to review the audit findings and agree on the audit conclusions?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.3.1.2 IS 9.3.1.2 Stage 2 **9.3.1.2.1** *On the basis of findings documented in the stage 1 audit report, does the certification body develops an audit plan for the conduct of stage 2?* *In addition to evaluating the effective implementation of the ISMS, are the objectives of stage 2:* *a. to confirm that the client adheres to its own policies, objectives and procedures.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.3.1.2.2 *To do this, does the audit focus on the client's:* *a. Top management leadership and commitment to information security policy and the information security objectives;* *b. Documentation requirements listed in ISO/IEC 27001;* *c. Assessment of information security related risks and that the assessments produce consistent, valid and comparable results if repeated;* *d. Determination of control objectives and controls based on the information security risk assessment and risk treatment processes;* *e. Information security performance and the effectiveness of the ISMS, evaluating against the information security objectives;* *f. Correspondence between the determined controls, the Statement of Applicability and the results of the information security risk assessment and risk treatment process and the information security policy and objectives;* *g. Implementation of controls, taking into account the external and internal context and related risk, the organization's monitoring measurement and analysis of information security processes and controls, to determine whether controls are implemented and effective and meet their stated information security objectives;* *h. Programmes, processes, procedures, records, internal audits and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and information security policy and objectives.*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4 Conducting audits **9.4.1 General** *Does the certification body have a process for conducting on-site audits?* *Does this process include an opening meeting at the start of the audit and a closing meeting at the conclusion of the audit?* *Where any part of the audit is made by electronic means or where the site to be audited is virtual, does the certification body ensure that such activities are conducted by personnel with appropriate competence?* *Is the evidence obtained during such an audit sufficient to enable the auditor to take an informed decision on the conformity of the requirement in question?* **"On-site" audits can include remote access to electronic site(s) that contain(s) information that is relevant to the audit of the management system. Consideration can also be given to the use of electronic means for conducting audits.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.1 IS 9.4 General *Does the certification body have documented procedures for:* *a. The initial certification audit of a client's ISMS, in accordance with the provisions of ISO/IEC 17021-1;* *b. Surveillance and re-certification audits of a client's ISMS in accordance with ISO/IEC 17021-1 on a periodic basis for continuing conformity with relevant requirements and for verifying and recording that a client takes corrective action on a timely basis to correct all conformities.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.2 IS 9.4 Specific elements of the ISMS audit *Does the certification body, represented by the audit team:* *a) Require the client to demonstrate that the assessment of information security related risks is relevant and adequate for the ISMS operation within the ISMS scope;* *b) Establish whether the client's procedures for the identification, examination and evaluation of information security related risks and results of their implementation are consistent with the client's policy, objectives and targets?* *Does the certification body also establish whether the procedures employed in risk assessment are sound and properly implemented?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.2 Conducting the opening meeting *Is a formal opening meeting, where attendance is recorded, held with the client's management and, where appropriate, those responsible for the functions or processes to be audited?* *Is the purpose of the opening meeting to provide a short explanation of how the audit activities will be undertaken?* *Is the degree of detail consistent with the familiarity of the client with the audit process. Does the opening meeting include the following elements?* *a. introduction of the participants, including an outline of their roles;* *b. confirmation of the scope of certification;* *c. confirmation of the audit plan (including type and scope of audit, objectives and criteria), any changes, and other relevant arrangements with the client, such as the date and time for the closing meeting, interim meetings between the audit team and the client's management;* *d. confirmation of formal communication channels between the audit team and the client;* *e. confirmation that the resources and facilities needed by the audit team are available;* *f. confirmation of matters relating to confidentiality;* *g. confirmation of relevant work safety, emergency and security procedures for the audit team;* *h. confirmation of the availability, roles and identities of any guides and observers;* *i. the method of reporting, including any grading of audit findings;* *j. information about the conditions under which the audit may be prematurely terminated;* *k. confirmation that the audit team leader and audit team representing the certification body is responsible for the audit and shall be in control of executing the audit plan including audit activities and audit trails;* *l. confirmation of the status of findings of the previous review or audit, if applicable;* *m. methods and procedures to be used to conduct the audit based on sampling;* *n. confirmation of the language to be used during the audit;* *o. confirmation that, during the audit, the client will be kept informed of audit progress and any concerns;* *p. opportunity for the client to ask questions.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.3 Communication during the audit **9.4.3.1** *During the audit, does the CAB's audit team periodically assess audit progress and exchange information?* *Does the audit team leader reassign work as needed between the audit team members and periodically communicate the progress of the audit and any concerns to the client?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.3.2 *Where the available audit evidence indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk (e.g. safety), does the audit team leader report this to the client and, if possible, to the certification body to determine appropriate action?* *Does such action include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit?* *Does the audit team leader report the outcome of the action taken to the certification body?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.3.3 *Does the audit team leader review with the client any need for changes to the audit scope which becomes apparent as on-site auditing activities progress and report this to the certification body?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.4 Obtaining and verifying information **9.4.4.1** *During the audit, is information relevant to the audit objectives, scope and criteria (including information relating to interfaces between functions, activities and processes) collected by appropriate sampling and verified to become audit evidence?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.4.2 *Do the methods to collect information include, but not limited to:* *a. interviews;* *b. observation of processes and activities;* *c. review of documentation and records.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
9.4.5 Identifying and recording audit findings **9.4.5.1** *Are audit findings summarizing conformity and detailing nonconformity and supporting audit evidence recorded and reported to enable an informed certification decision to be made or the certification to be maintained?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.5.2 *Are opportunities for improvement identified and recorded, unless prohibited by the requirements of a management system certification scheme?* *Are audit findings which are nonconformities in accordance with 9.1.15 b) and c) not able to be recorded as opportunities for improvement?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.5.3 *Are nonconformities recorded against a specific requirement of the audit criteria, and do they contain a clear statement of the nonconformity and identify in detail the objective evidence on which the nonconformity is based?* *Are nonconformities discussed with the client to ensure that the evidence is accurate and that the nonconformities are understood?* *Does the auditor refrain from suggesting the cause of nonconformities or their solution?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.5.4 *Does the audit team leader attempt to resolve any diverging opinions between the audit team and the client concerning audit evidence or findings, and unresolved points recorded?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.4.6 Preparing audit conclusion *Prior to the closing meeting, does the audit team:* *a. review the audit findings, and any other appropriate information collected during the audit, against the audit objectives;* *b. agree upon the audit conclusions, taking into account the uncertainty inherent in the audit process;* *c. identify any necessary follow-up actions;* *d. confirm the appropriateness of the audit programme or identify any modification required (e.g. scope, audit time or dates, surveillance frequency, competence).*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.7 Conducting the closing meeting **9.4.7.1** *Is a formal closing meeting, where attendance is recorded, held with the client's management and, where appropriate, those responsible for the functions or processes audited?* *Is the purpose of the closing meeting to present the audit conclusions, including the recommendation regarding certification?* *Are nonconformities presented in such a manner that they are understood, and the timeframe for responding agreed?* **"Understood" does not necessarily mean that the nonconformities have been accepted by the client.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.7.2 *Does the closing meeting also include the following elements? Is the degree of detail consistent with the familiarity of the client with the audit process:* *a. advising the client that the audit evidence collected was based on a sample of the information; thereby introducing an element of uncertainty;* *b. the method and timeframe of reporting, including any grading of audit findings;* *c. the certification body's process for handling nonconformities including any consequences relating to the status of the client's certification;* *d. the timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit;* *e. the certification body's post audit activities;* *f. information about the complaint handling and appeal processes.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.7.3 *Is the client given opportunity for questions? Are diverging opinions regarding the audit findings or conclusions between the audit team and the client discussed and resolved where*

Clause Requirement
possible? *Are diverging opinions that are not resolved recorded and referred to the certification body?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.8 Audit report **9.4.8.1** *Does the certification body provide a written report for each audit?* *Does the audit team identify opportunities for improvement without recommending specific solutions?* *Is the ownership of the audit report maintained by the certification body?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.3 IS 9.4 Audit report **9.4.3.1** *In addition to the requirements for reporting in ISO/IEC 17021-1, 9.4.8, does the audit report provide the following information or a reference to it:* *a. an account of audit including a summary of the document review;* *b. an account of the certification audit of the client's information security risk analysis;* *c. deviations from the audit plan (e.g. more or less time spent on certain scheduled activities);* *the ISMS' scope.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.3.2 *Does the audit report have sufficient detail to facilitate and support the certification decision?* *Does it contain:* *a. significant audit trails followed and audit methodologies utilized (see 9.1.3.2);* *b. observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities);* *c. comments on the conformity of the client's ISMS with the certification requirements with a clear statement of nonconformity, a reference to the version of the Statement of Applicability and, where applicable, any useful comparison with the results of previous certification audits of the clients.* *Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report.* *If these methods are used, are these documents submitted to the certification body as evidence to support the certification decision?* *Does information about the samples evaluated during the audit included in the audit report, or in other certification documentation?* *Does the report consider the adequacy of the internal organization and procedures adopted by the client to give confidence in the ISMS?*

Clause Requirement
In addition to the requirements for reporting in ISO/IEC 17021-1, 9.4.8, does the report cover: - *summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS requirements and IS controls;* - *the audit team's recommendation as to whether the client's ISMS should be certified or not, with information to substantiate this recommendation.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.8.2 *Does the audit team leader ensure that the audit report is prepared and responsible for its content?* *Does the audit report provide an accurate, concise and clear record of the audit to enable an informed certification decision to be made and include or refer to the following:* *a. identification of the certification body;* *b. the name and address of the client and the client's management representative;* *c. the type of audit (e.g. initial, surveillance or recertification audit);* *d. the audit criteria;* *e. the audit objectives;* *f. the audit scope, particularly identification of the organizational or functional units or processes audited and the time of the audit;* *g. any deviation from the audit plan and their reasons;* *h. any significant issues impacting on the audit programme;* *i. identification of the audit team leader, audit team members and any accompanying persons;* *j. the dates and places where the audit activities (on site or offsite, permanent or temporary sites) were conducted;* *k. audit findings, reference to evidence and conclusions, consistent with the requirements of the type of audit;* *l. significant changes, if any, that affect the management system of the client since the last audit took place;* *m. any unresolved issues, if identified.* *n. where applicable, whether the audit is combined, joint or integrated;* *o. a disclaimer statement indication that auditing is based on a sampling process of the available information;* *p. recommendation from the audit team;* *q. the audited client is effectively controlling the use of the certification documents and marks, if applicable;* *r. verification of effectiveness of taken corrective actions regarding previously identified nonconformities, if applicable.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.4.8.3 *Does the report also contain:* *a. a statement on the conformity and effectiveness of the management system together with a summary of the evidence relating to:* *- the capability of the management system to meet applicable requirements and expected outcomes;* *- the internal audit and management review process* *b. a conclusion on the appropriateness of the certification scope;* *c. confirmation that the audit objectives have been fulfilled.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.9 Cause analysis of nonconformities *Does the certification body require the client to analyse the cause and describe the specific correction and corrective actions taken, or planned to be taken, to eliminate detected nonconformities, within a defined time?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.4.10 Effectiveness of corrections and corrective actions *Does the certification body review the corrections, identified causes and corrective actions submitted by the client to determine if these are acceptable?* *Does the certification body verify the effectiveness of any correction and corrective actions taken?* *Is evidence obtained to support the resolution of nonconformities recorded?* *Is the client informed of the result of the review and verification?* *Is the client informed if an additional full audit, an additional limited audit, or documented evidence (to be confirmed during future audits) will be needed to verify effective correction and corrective actions?* **Verification of effectiveness of correction and corrective action can be carried out based on a review of documentation provided by the client, or where necessary, through verification on-site. Usually this activity is done by a member of the audit team.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.5 Certification decision **9.5.1 General** **9.5.1.1** *Does the certification body ensure that the persons or committees that make the decisions for granting or refusing certification, expanding or reducing the scope of certification, suspending or restoring certification, withdrawing certification or renewing certification are different from those who carried out the audits?* *Does the individual(s) appointed to conduct the certification decision have appropriate competence?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.5.1 IS 9.5 Certification decision *Is the certification decision based, additionally to the requirements of ISO/IEC 17021-1, on the certification recommendation of the audit team as provided in their certification audit report (see 9.4.3)?* *The persons or committees that take the decision on granting certification should not normally overturn a negative recommendation of the audit team.* *If such a situation arises, does the certification body document and justify the basis for the decision to overturn the recommendation?* *Is the certification not granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective and will be maintained?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.5.1.2 *Is the person(s) [excluding members of committees (see 6.1.4)] assigned by the certification body to make a certification decision employed by, or is under legally enforceable arrangement with either the certification body or an entity under organizational control of the certification body?* *Is a certification body's organizational control one of the following:* *a. whole or majority ownership of another entity by the certification body;* *b. majority participation by the certification body on the board of directors of another entity;* *c. a documented authority by the certification body over another entity in a network of legal entries (in which the certification body resides), linked by ownership or board of director control.* **For governmental certification bodies, other parts of the same government can be considered to be "linked by ownership" to the certification body.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.5.1.3 *Are the persons employed by, or under contract with, entities under organizational control fulfil the same requirements of this part of ISO/IEC 17021 as persons employed by, or under contract with, the certification body?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.5.1.4 *Does the certification body record each certification decision including any additional information or clarification sought from the audit team or other sources?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.5.2 Actions prior to making a decision *Does the certification body have a process to conduct an effective review prior to making a decision for granting certification, or withdrawing of certification, including, that:* *a. the information provided by the audit team is sufficient with respect to the certification requirements and the scope for certification;* *b. for any major nonconformities, it has reviewed, accepted and verified the correction and corrective actions;* *c. for any minor nonconformities, it has reviewed and accepted the client's planned correction and corrective action.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.5.3 Information for granting initial certification **9.5.3.1** *Does the information provided by the audit team to the certification body for the certification decision include, as a minimum:* *a. the audit report;* *b. comments on the nonconformities and, where applicable, the correction and corrective actions taken by the client;* *c. confirmation of the information provided to the certification body used in the application review (see 9.1.2),* *d. confirmation that the audit objectives have been achieved; and;* *e. a recommendation whether or not to grant certification, together with any conditions or observations?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
9.5.3.2 *If the certification body is not able to verify the implementation of corrections and corrective actions of any major nonconformity within 6 months after the last day of stage 2, does the certification body conduct another stage 2 prior to recommending certification?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.5.3.3 *When a transfer of certification is envisaged from one certification body to another, does the accepting certification body have a process for obtaining sufficient information in order to take decision on certification?* **Certification schemes can have specific rules regarding the transfer of certification.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.5.4 Information granting certification *Does the certification body make decisions on renewing certification based on the results of the recertification audit, as well as the results of the review of the system over the period of certification and complaints received from users of certification?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6 Maintaining certification **9.6.1 General** *Does the certification body maintain certification based on demonstration that the client continues to satisfy the requirements of the management system standard?* *Does the certification body maintain a client's certification based on a positive conclusion by the audit team leader without further independent review, provided that:* *a. for any nonconformity or other situation that may lead to suspension or withdrawal of certification, the certification body has a system that requires the audit team leader to report to the certification body the need to initiate a review by appropriately competent personnel (see 7.2.9), different from those who carried out the audit, to determine whether certification can be maintained, and* *b. competent personnel of the certification body monitor its surveillance activities, including monitoring the reporting by its auditors, to confirm that the certification activity is operating effectively?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.2 Surveillance activities **9.6.2.1 General** **9.6.2.1.1** *Does the certification body develop its surveillance activities so that representative areas and functions covered by the scope of the management system are monitored on a regular basis, and take into account changes to its certified client and its management system?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.2.1.2 *Do surveillance activities include on-site audits assessing the certified client's management system's fulfilment of specified requirements with respect to the standard to which the certification is granted?* *Do other surveillance activities include:* *a. enquiries from the certification body to the certified client on aspects of certification,* *b. reviewing any client's statements with respect to its operations (e.g. promotional material, website),* *c. requests to the client to provide documents and records (on paper or electronic media), and* *d. other means of monitoring the certified client's performance.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.2.1 IS 9.2 Surveillance Activities **9.6.2.1.1** *Are surveillance audit procedures consistent with those concerning the certification audit of the client organization's ISMS as described in this international standard?* *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 client organization's operation and to confirm continued compliance with certification requirements. Does the certification body's surveillance audit programme cover the following:* *a. the system maintenance elements which are internal ISMS audit, management review and preventive and corrective action;* *b. communications from external parties as required by the ISMS standard ISO/IEC 27001 and other documents required for certification;* *c. changes to the documented system;* *d. areas subject to change;* *e. selected elements of ISO/IEC 27001;* *f. other selected areas as appropriate*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.2.1.2 *As a minimum, does the certification body review the following as part of surveillance:* *a. the effectiveness of the ISMS with regard to achieving the objectives of the client organization's information security policy,* *b. the functioning of procedures for the periodic evaluation and review of compliance with relevant information security policy;* *c. changes to the controls determined, and resulting changes to the SoA;* *d. implementation and effectiveness of controls according to the audit programme.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.2.1.3 *Does the certification body able to adapt its surveillance programme to the information security issues related to risks and impacts on the client and justify this programme?* *During surveillance audits, does the certification body check the records of appeal and complaints brought before the certification body and where any nonconformity or failure to meet the requirements of certification is revealed, that the client organization has investigated its own ISMS and procedures and taken appropriate corrective action?* *Does a surveillance report contain in particular, any information on clearing of nonconformities revealed previously?* *As a minimum, do the reports arising from surveillance build up to cover in totality the requirements of 9.6.2.1.1 and 9.6.2.1.2 above?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.2.2 Surveillance audit *Are surveillance audits planned together with the other surveillance activities so that the certification body can maintain confidence that the certified management system continues to fulfil requirements between recertification audits?* *Does each surveillance for the relevant management system standard include:* *a. internal audits and management review;* *b. a review of actions taken on nonconformities identified during the previous audit;* *c. treatment of complaints;* *d. effectiveness of the management system with regard to achieving the certified client's objectives;* *e. progress of planned activities aimed at continual improvement;* *f. continuing operational control;* *g. review of any changes;* *h. use of marks and/or any other reference to certification?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.3 Re-certification **9.6.3.1 Recertification audit planning** **9.6.3.1.1** *Are recertification audits planned and conducted to evaluate the continued fulfillment of all of the requirements of the relevant management system standard or other normative document?* *Is this planned and conducted in due time to enable for timely renewal before the certificate expiry date?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.3.1.2 *Does the recertification audit consider the performance of the management system over the period of certification?* *Does the recertification audit include the review of previous surveillance audit reports?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.3.1.3 *Do recertification audit activities have a stage 1 audit in situations where there have been significant changes to the management system, the client, or the context in which the management system is operating (e.g. changes to legislation)?* **Such changes can occur at any time during the certification cycle and the certification body might need to perform a special audit (see 9.6.4), which might or might not be a two-stage audit.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.3.2 Recertification audit **9.6.3.2.1** *Does the recertification audit include an on-site audit that addresses the following:* *a. the effectiveness of the management system in its entirety in the light of internal and external changes and its continued relevance and applicability to the scope of certification;* *b. demonstrated commitment to maintain the effectiveness and improvement of the management system in order to enhance overall performance;* *c. the effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management system?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.3.1 IS 9.6.3 Re-certification Audits *Are recertification audit procedures consistent with those concerning the certification audit of the client organization's ISMS as described in this International Standard?* *Is the time allowed to implement corrective action consistent with the severity of the nonconformity and the risk to the assurance of products or services of the client organization meeting specified requirements?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.3.2.2 *For any major nonconformity, does the certification body define time limits for correction and corrective actions?* *Are these actions implemented and verified prior to the expiration of certification?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.3.2.3 *When recertification activities are successfully completed prior to the expiry date of existing certification, is the expiry date of the new certification based on the expiry date of the existing certification?* *Is the issue date on a new certificate on or after the recertification decision?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.3.2.4 *If the certification body has not completed the recertification audit or the certification body is unable to verify the implementation of corrections and corrective actions for any major nonconformity (see 9.5.2.1) prior to the expiry date of the certification, then is recertification not recommended and the validity of the certification not extended?* *Is the client informed and the consequences explained?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
9.6.3.2.5 *Following expiration of certification, can certification body restore certification within 6 months provided that the outstanding recertification activities are completed, otherwise at least a stage 2 is conducted?* *Is the effective date on the certification on or after the recertification decision and the expiry date based on prior certification cycle?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.4 Special audits **9.6.4.1 Expanding scope** *Does the certification body, in response to an application for extension to the scope of a certification already granted, undertake a review of the application and determine any audit activities necessary to decide whether or not the extension may be granted?* *This may be conducted in conjunction with a surveillance audit.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.4.1 IS 9.6.4 Special cases *Are the activities necessary to perform special audits subject to special provision if a client organization with a certified ISMS makes major modifications to its system or if other changes take place which could affect the basis of its certification?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.4.2 Short-notice audits *It may be necessary for the certification body to conduct audits of certified clients at short notice to investigate complaints or in response to changes or as follow up on suspended clients. In such cases:* *a. describe and make known in advance to the certified clients (e.g. in documents as described in 8.6.1) the conditions under which these short notice visits are to be conducted, and* b. *exercise additional care in the assignment of the audit team because of the lack of opportunity for the client to object to audit team members?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
9.6.5 Suspending, withdrawing or reducing scope of certification **9.6.5.1** *Does the certification body have a policy and documented procedure(s) for suspension, withdrawal or reduction of the scope of certification?* *Does the certification body specify the subsequent actions by the certification body?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.5.2 *Does the certification body suspend certification in cases when, for example:* — *the client's certified management system has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the management system,* — *the certified client does not allow surveillance or recertification audits to be conducted at the required frequencies, or* — *the certified client has voluntarily requested a suspension.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.5.3 *Under suspension, the client's management system certification is temporarily invalid.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.6.5.4 *Does certification body restore the suspended certification if the issue that has resulted in the suspension has been resolve?* *Does failure to resolve the issues that have resulted in the suspension in a time established by the certification body result in withdrawal or reduction of the scope of certification?* **In most cases the suspension would not exceed 6 months.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.6.5.5 *Does the certification body reduce the client's scope of certification to exclude the parts not meeting the requirements, when the client has persistently or seriously failed to meet the certification requirements for those parts of the scope of certification?* *Is any such reduction in line with the requirements of the standard used for certification?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.7 Appeals **9.7.1** *Does the certification body have a documented process to receive, evaluate and make decisions on appeals?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: (*To be filled-up by the AB)*
9.7.2 *Is the certification body responsible for all decisions at all levels of the appeals-handling process?* *Does the certification body ensure that the persons engaged in the appeals-handling process different from those who carried out the audits and made the certification decisions?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.7.3 *Does the certification body ensure submission, investigation and decision on appeals do not result in any discriminatory actions against the appellant?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.7.4 *Does the appeals-handling process include at least the following elements and methods:* *a. an outline of the process for receiving, validating and investigating the appeal, and for deciding what actions are to be taken in response to it, taking into account the results of previous similar appeals;* *b. tracking and recording appeals, including actions undertaken to resolve them;* c. *ensuring that any appropriate correction and corrective action are taken?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
9.7.5 *Is the certification body receiving the appeal responsible for gathering and verifying all necessary information to validate appeal?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.7.6 *Does the certification body acknowledge receipt of the appeal?* *Does the certification body provide the appellant with progress reports and the outcome?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.7.7 *Is the decision to be communicated to the appellant made by, or reviewed and approved by, individual(s) not previously involved in the subject of the appeal?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.7.8 *Does the certification body give formal notice to the appellant of the end of the appeals-handling process?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.8 Complaints **9.8.1** *Is a description of the complaints-handling process publicly accessible?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.8.1 IS 9.8 Complaints *Complains represent a potential incident and an indication to possible nonconformity.*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.8.2 *Does submission, investigation and decision on complaints result in any discriminatory action against the complainant?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.8.3 *Upon receipt of a complaint, does the certification body confirm whether the complaint relates to certification activities that it is responsible for?* *If so, does the certification body deal with it?* *If the complaint relates to a certified client, does examination of the complaint consider the effectiveness of the certified management system?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.8.4 *Is any complaint about a certified client referred by the certification body to the certified client in question at an appropriate time?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.8.5 *Does the certification body have a documented process to receive, evaluate and make decisions on complaints?* *Is this process subject to requirements for confidentiality, as it relates to the complainant and to the subject of the complaint?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.8.6 *Does the complaints-handling process include at least the following elements and methods:* *a. an outline of the process for receiving, validating, investigating the complaint, and for deciding what actions are to be taken in response to it;* *b. tracking and recording complaints, including actions undertaken in response to them;* c. *ensuring that any appropriate correction and corrective action are taken?* **ISO 10002 provides guidance for complaints handling*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.8.7 *Is the certification body receiving the complaint responsible for gathering and verifying all necessary information to validate the complaint?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.8.8 *Whenever possible, does the certification body acknowledge receipt of the complaint?* *Does the certification body provide the complainant with progress reports and the outcome?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.8.9 *Is the decision to be communicated to the complainant made by, or reviewed and approved by, individual(s) not previously involved in the subject of the complaint?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.8.10 *Whenever possible, does the certification body give formal notice of the end of the complaints-handling process to the complainant?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
9.8.11 *Does the certification body determine, together with the client and the complainant, whether and, if so to what extent, the subject of the complaint and its resolution made public?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.9 Client records **9.9.1** *Does the certification body maintain records on the audit and other certification activities for all clients, including all organizations that submitted applications, and all organizations audited, certified, or with certification suspended or withdrawn?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.9.2 *Do records on certified clients include the following:* *a. application information and initial, surveillance and recertification audit reports;* *b. certification agreement;* *c. justification of the methodology used for sampling of sites, as appropriate;* **Methodology of sampling includes the sampling employed to audit the specific management system and/or to select sites in the context of multi-site audit.* *d. justification for auditor time determination (see 9.1.4);* *e. verification of correction and corrective actions;* *f. records of complaints and appeals, and any subsequent correction or corrective actions;* *g. committee deliberations and decisions, if applicable;* *h. documentation of the certification decisions;* *i. certification documents, including the scope of certification with respect to product, process or service, as applicable;* j. *related records necessary to establish the credibility of the certification, such as evidence of the competence of auditors and technical experts?* k. *audit programmes*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
9.9.3 *Does the certification body keep the records on applicants and clients secure to ensure that the information is kept confidential?* *Are records transported, transmitted or transferred in a way that ensures that confidentiality is maintained?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
9.9.4 *Does the certification body have a documented policy and documented procedures on the retention of records?* *Are records of certified clients and previously certified clients retained for the duration of the current cycle plus one full certification cycle?* **In some jurisdictions, the law stipulates that records need to be maintained for a longer time period.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10 Management system requirements for certification bodies **10.1 Options** *Does the certification body establish, document, implement and maintain a management system that is capable of supporting and demonstrating the consistent achievement of the requirements of ISO/IEC 17021?* *In addition to meeting the requirements of Clause 5 to 9, does the certification body implement a management system in accordance with either:* *a. management system requirements in accordance with ISO 9001 (see Clause 10.2); or* *b. general management system requirements (see Clause 10.3).* *Which option has the certification body adopted?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.1.1 IS 10.1 ISMS implementation *It is recommended that certification bodies implement an ISMS in accordance with ISO/IEC 27001. Has the certification body implemented an ISMS in accordance with ISO/IEC 27001?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
10.2 Option A: General management system requirements **10.2.1 General** *Does the certification body establish, document, implement and maintain a management system that is capable of supporting and demonstrating the consistent achievement of the requirements of this part of ISO/IEC 17021?* *Does the certification body's top management establish and document policies and objectives for its activities?* *Does the top management provide evidence of its commitment to the development and implementation of the management system in accordance with the requirements of this part of ISO/IEC 17021?* *Does the top management ensure that the policies are understood, implemented and maintained at all levels of the certification body's organization?* *Does certification body's top management assign responsibility and authority for:* *a. ensuring that processes and procedures needed for the management system are established, implemented and maintained, and* *b. reporting to top management on the performance of the management system and any need for improvement?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.2.2 Management system manual *Have all applicable requirements of this International Standard been addressed either in a manual or in associated documents?* *Does the certification body ensure that the manual and relevant associated documents are accessible to all relevant personnel?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.2.3 Control of documents *Has the certification body established procedures to control the documents (internal and external) that relate to the fulfilment of this International Standard?* *Do the procedures define the controls needed to:* *a. approve documents for adequacy prior to issue,* *b. review and update as necessary and re-approve documents,* *c. ensure that changes and the current revision status of documents are identified,* *d. ensure that relevant versions of applicable documents are available at points of use,* *e. ensure that documents remain legible and readily identifiable,* *f. ensure that documents of external origin are identified and their distribution controlled, and* *g. prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose?* **Documentation can be in any form or type of medium.*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.2.4 Control of records *Has the certification body established procedures to define the controls needed for the identification, storage, protection, retrieval, retention time and disposition of its records related to the fulfilment of this International Standard?* *Has the certification body established procedures for retaining records for a period consistent with its contractual and legal obligations?* *Is access to these records consistent with the confidentiality arrangements?* **For requirements for records on certified clients, see also 9.9*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.2.5 Management review **10.2.5.1 General** *Has the certification body's top management established procedures to review its management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness, including the stated policies and objectives related to the fulfilment of this International Standard?* *Are these reviews conducted at least once a year?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.2.5.2 Review inputs *Does the input to the management review include information related to* *a. results of internal and external audits,'* *b. feedback from clients and interested parties related to the fulfillment of this International Standard,* *c. feedback from the committee for safeguarding impartiality,* *d. the status of corrective actions;* *e. the status of preventive and corrective actions,* *f. follow-up actions from previous management reviews,* *g. the fulfillment of objectives,* *h. changes that could affect the management system, and* *i. appeals and complaints.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*

Clause Requirement
Findings/Comments: *(To be filled-up by the AB)*
10.2.5.3 Review outputs *Do the outputs from the management review include decisions and actions related to* *a. improvement of the effectiveness of the management system and its processes,* *b. Improvement of the certification services related to the fulfillment of this International Standard, and* *c. resource needs* *d. revisions of the organization's policy and objectives?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.2.6 Internal audits **10.2.6.1** *Has the certification body established procedures for internal audits to verify that it fulfils the requirements of this International Standard and that the management system is effectively implemented and maintained?* **ISO 19011 provides guidelines for conducting internal audits.*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.2.6.2 *Is the audit programme planned, taking into consideration the importance of the processes and areas to be audited, as well as the results of previous audits?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.2.6.3 *Are internal audits performed at least once every 12 months?* *Is the frequency of internal audits reduced if the certification body can demonstrate that its management system continues to be effectively implemented according to this International Standard and has proven stability?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*

Clause Requirement
10.2.6.4 *Does the certification body ensure that* *a. internal audits are conducted by qualified personnel knowledgeable in certification, auditing and the requirements of this International Standard,* *b. auditors do not audit their own work,* *c. personnel responsible for the area audited are informed of the outcome of the audit,* *d. any actions resulting from internal audits are taken in a timely and appropriate manner, and* *e. any opportunities for improvement are identified?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.2.7 Corrective action *Has the certification body established procedures for identification and management of nonconformities in its operations?* *Does the certification body also, where necessary, take actions to eliminate the causes of nonconformities in order to prevent recurrence?* *Are corrective actions appropriate to the impact of the problems encountered?* *Do the procedures define requirements for:* *a. identifying nonconformities (e.g. from complaints and internal audits),* *b. determining the causes of nonconformity,* *c. correcting nonconformities,* *d. evaluating the need for actions to ensure that nonconformities do not recur,* *e. determining and implementing in a timely manner, the actions needed,* *f. recording the results of actions taken, and* *g. reviewing the effectiveness of corrective actions?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.3 Option B: General management system requirements in accordance with ISO 9001 **10.3.1 General** *Does certification body establish and maintain a management system, in accordance with the requirements of ISO 9001, which is capable of supporting and demonstrating the consistent achievement of the requirements of this part of ISO/IEC 17021, amplified by 10.3.2 to 10.3.4?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.3.2 Scope *Does the scope of the management system include the design and development requirements for its certification services?*

Clause Requirement
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.3.3 Customer focus *When developing its management system, has the certification body considered the credibility of certification?* *Has the certification body addressed the needs of all parties (as set out in 4.1.2) that rely upon its audit and certification services, not just its clients?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*
10.3.4 Management review *Does the certification body include as input for management review, information on relevant appeals and complaints from users of certification activities and a review of impartiality?*
State the CB's established policies and procedures: *(To be filled-up by the CB)*
Findings/Comments: *(To be filled-up by the AB)*