	Procedure	Document No.	P-01
		Version	16.00
	Application, Audit and Certification	Date of Issue	Jul 01, 2018

Reviewed & Approved by	Name	Designation	Signature	Date
	Kaushal Goyal	Managing Director		Jul 01, 2018

Revision History

Version	Date	Description	Remarks
1.00	Mar 01, 2008	Original release as per standard ISO/ IEC 17021	
2.00	Mar 01, 2009	Based on the inputs from document review by NABCB for FSMS	
3.00	Nov 01, 2009	To include EMS and OHSAS	
4.00	Mar 01, 2010	Para 4.5, 4.6 revised.	
5.00	Nov 01, 2010	Revised para 4.2b, 4.2h, 4.3.1, 4.5c, 4.6.2.1(2), 4.6.2.2(2) and added 4.2m based on document review by JAS-ANZ	
6.00	Jan 20, 2012	Para 4.2i, 4.3.1, 4.3.3a revised	
7.00	Apr 01, 2012	Modified for transition to 17021:2011	
8.00	Aug 22, 2013	To include EnMS	
9.00	Nov 02, 2015	Modified for transition to 17021:2015	
10.00	Apr 01, 2016	Modified to include requirements as per ISO 50003:2014	
11. 00	Aug 12, 2016	Based on the inputs from document review by NABCB for EnMS .	
12. 00	Oct 06, 2016	Modified as part of Corrective action on the NCs raised by DAC & JAS-ANZ	
13.00	Oct 16, 2017	Defined Renewal process, in case the client has been certified by other CB	
14.00	Nov 15, 2017	Reviewed and revised.	
15.00	Mar 01, 2018	Revised to address the requirements of ISO/IEC 27001	
16.00	Jul 01, 2018	Revised based on IAF MD22:2018	

1.0 Purpose

To lay down a procedure for application, initial audit & certification, surveillance and re-certification of management systems.

2.0 Scope

QMS, EMS, OHSAS, FSMS, EnMS, ISMS and other related management systems

3.0 Responsibility & Authority

Manager Audit

4.0 Policy & Procedure

4.1 Pre-certification activities

4.1.1 Application

KBS requires an authorized representative of the applicant organization to provide the necessary information in form F-01 to including the following:

a) the desired scope of the certification;
b) relevant details of the applicant organisation 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 organisation that will affect conformity to requirements;
d) the standard or other requirements for which the applicant organisation is seeking certifications;
e) whether consultancy relating to the management system to be certified has been provided and, if so, by whom.
f) Identification of the key hazards and OH&S risks associated with processes, the main hazardous materials used in the processes, and any relevant legal obligations coming from the applicable OH&S legislation.
g) Details of personnel working on, as well as working away from the organisation's premises.

4.1.1.1 Application Readiness(ISMS)

KBS requires the client to have a documented and implemented ISMS which confirms to ISO 27001 and other documents required for certification.

4.1.2 Application Review

Audit Manager conducts a review of the application and supplementary information in form F-02 to ensure that:

a) the information about the applicant organisation and its management system is sufficient to develop an audit programme;

b) any known difference in understanding between KBS and the applicant organisation is resolved;
c) KBS has the competency and ability to perform the certification activity;
d) The scope of certification sought, the site (s) of the applicant organisation '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.)

Following the review of the application, Audit Manager takes the decision to either accepts or declines the application for certification. If the application is declined as a result of the review of application, the reasons for declining an application are documented and made clear to the client.

Based on this review, Audit Manager determines the competences it needs to include in its audit team and for the certification decision and recorded in Form F-02. Proposal is sent for customer approval and signature in Form F-03.

4.1.3 Audit Programme

Audit Manager develops an audit programme F-16 for the full certification cycle to clearly identify the audit activity (ies) required to demonstrate that the client's management system fulfills the requirements for certification to the selected standard (s) or other normative document (s). The audit programme for the certification cycle cover the complete management system requirements.

The audit programme for the initial certification includes 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 the certification decision. Subsequent cycles begin with the recertification decision. The determination of the audit programme and any subsequent adjustments is carried out based on the size of the client organization, 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. In addition, the followings are considered when developing or revising an audit programme:

- Complaints received by KBS about the clients;
- Combined, integrated or joint audits
- Changes to the certification requirements;
- Changes to legal requirements;
- Changes to accreditation requirements;
- Organizational performance, data (e.g. defect levels, key performance indicators data);
- Relevant interested parties' concerns.

Surveillance audits are conducted at least once a calendar year, except in recertification years. The date of the first surveillance audit following initial certification shall not be more than 12 months from the certification decision date.

The frequency of surveillance audits is adjusted to accommodate factors such as seasons or management system certification of a limited duration (e.g. temporary construction site).

Where KBS is taking account of certification or other audits already granted to the client and to audits performed by another certification body, it obtains and retains sufficient evidences, such as reports and documentation on corrective actions, to any nonconformity. The documentation shall support the fulfilling the requirements of ISO / IEC/ 17021. Based on the information

obtained, KBS justifies and records any adjustments to the existing audit programme and follow up the implementation of corrective actions concerning previous nonconformities.

Where the client operates shifts, the activities that take place during shift working are considered when developing the audit programme and audit plans.

4.1.3.1 General (ISMS)
The audit programme for ISMS audits take the determined information security controls into account.

4.1.3.2 Audit Methodology (ISMS)
KBS procedures do not presuppose a particular manner of implementation of an ISMS or a particular format for documentation and records. 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.

4.1.3.3 General preparation for the initial audit (ISMS)
KBS require that a client makes all necessary arrangements for the access to internal audit reports and reports of independent reviews of information security. At least the following information shall be 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 documented specified in ISO/IEC 27001 and where required, associated documentation.

4.1.3.4 Review periods (ISMS)
KBS do 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.

4.1.3.5 Scope of certification(ISMS)
The audit team audit the ISMS of the client covered by the defined scope against all applicable certification requirements. KBS confirm, in the scope of the client ISMS, that clients address the requirements stated in ISO/IEC 27001, 4.3.

KBS 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. KBS confirm that this is reflected in the client's scope of their ISMS and Statement of Applicability. KBS verify that there is at least one Statement of Applicability per scope of certification.

KBS 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.

4.1.3.6 Certification audit criteria (ISMS)
The criteria against which the ISMS of a client is audited is ISMS standard ISO/IEC 27001. Other documents may be required for certification relevant to the function performed

4.1.4 Determining audit time

KBS has documented procedure P-13 (including 13A, 13B) for determining audit time, and for each client Audit Manager determines the time needed to plan and accomplish a complete and

effective audit of the client's management system. The audit time determined, and the justification for the determination, is recorded.

In determining the audit time, Audit Manager considers, among other things, the following aspects:

a) The requirements of the relevant management system standard;
b) Complexity of the client and its management system;
c) Technological and regulatory context;
d) Any outsourcing of any activities included in the scope of the management system;
e) The results of any prior audits;
f) Size and number of sites, their geographical locations and multi-site considerations;
g) The risks associated with the products, processes or activities of the organisation;
h) Whether audits are combined, joints 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 duration of the management system audit and its justification is recorded in F-02.

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) shall not count in the above established duration of the management system audit.

The use of translators and interpreters may necessitate additional time.

For OHSAS: If the client provides services at another organization's premises, KBS verifies that the client's OH&SMS covers these offsite activities (notwithstanding the OH&SMS obligations of the other organization). In determining the time to be spent for audit, KBS considers to audit periodically any organization site where these employees work. Whether all sites are to be audited depends on various factors such as OH&S risks associated with the activities therein performed, contract agreements, being certified by another accredited CAB, internal audit system, statistics on accidents and near misses. The justifications for such decision are recorded.

4.1.4.1 Audit time
KBS allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or recertification audit. The calculation of overall audit time include sufficient time for audit reporting.

4.1.5 Multi-site sampling

Where multi-site sampling is utilized for the audit of a client's management system covering the same activity in various geographical locations, Audit Manager develops a sampling programme to ensure proper audit of the management system as per procedure P-10 (for QMS, EMS, OHSAS FSMS, ISMS) & P-10 A (for EnMS). The rationale for the sampling plan is documented for each client.

When there are multiple sites not covering the same activity sampling is not undertaken.

4.1.6 Multiple management systems standards

When certification to multiple management system standards is being provided by KBS, the planning for the audit ensure adequate on-site auditing to provide confidence in the certification.

4.2 Planning audits

4.2.1 Determining audit objectives, scope and criteria

9.2.1.1 The audit objectives are determined by Audit Manager. The audit scope and criteria including any changes, are established after discussion with the client.

The audit objectives describe what is to be accomplished by the audit and include the following:

a) Determining of the conformity of the client's management system, or parts of it, with audit criteria;
b) Determination of the ability of the management system to ensure the client meets applicable statutory, regulatory and contractual requirements;

c) Determination of the effectiveness of the management system to ensure the client can reasonably expect to achieving its specified objectives;
d) As applicable, identification of areas for potential improvement of the management system.

The audit scope describes the extent and boundaries of the audit, such as sites, 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), the scope of an individual audit may not cover the full certification scope, but the totality of audits is consistent with the scope in the certification document.

The audit criteria used as a reference against which conformity is determined, and include:

- The requirements of a defined normative document on management systems;
- The defined processes and documentation of the management system developed by the client.
- *to ensure the client meets applicable statutory, regulatory and contractual requirements,*

The OH&SMS include activities, products and services within the organization's control or influence that can impact the organization's OH & SMS performance.

Temporary sites, for example, construction sites are covered by the OH&SMS of the organization that has control of these sites, irrespective of where they are located.

4.2.1.1 Audit objectives (ISMS)
The audit 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.

4.2.2 Audit team selection and assignments

4.2.2.1 General

The audit team, including the audit team leader is selected and appointed taking into account the competence needed to achieve the objectives of the audit. If there is only one auditor, the auditor has the competence to perform the duties of an audit team leader applicable for that audit. The audit team has the totality of the competences identified by KBS.

In deciding the size and composition of the audit team, consideration is given to the following:

a) audit objectives, scope, criteria and estimated time of the audit;
b) whether the audit is a combined, integrated or joint audit;
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;

For combined or integrated audit team leader having in-depth knowledge of at least one of the standard and an awareness of the other standards used for that particular audit is appointed.

The necessary knowledge and skills of the audit team leader and auditors are supplemented by technical experts, translators and interpreters who operate under the direction of an auditor. Where translators or interpreters are used, they are 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.

Auditors-in-training may be included in the audit team as participants, provided an auditor is appointed as an evaluator. The evaluator be competent to take over the duties and have final responsibility for the activities and findings of the auditor-in-training.

The audit team leader, in consultation with the audit team, assigns to each team member responsibility for auditing specific processes, functions, sites, areas or activities. Such 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.

4.2.2.1 Audit team

The audit team is formally appointed and provided with the appropriate working documents. The mandate given to the audit team is 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 .
9.2.2.2 Audit team competence (ISMS)
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 the certification body shall ensure that the competences brought to each assignment are appropriate. 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.

4.2.2.2 Observers, technical experts and guides

The presence and justification of observers during an audit activity is to be agreed to by the certification body and client prior to the conduct of the audit. The audit team ensures 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.

The role of technical experts during an audit activity is agreed by KBS and client prior to the conduct of the audit. A technical expert does not act as an auditor in the audit team. The technical experts are accompanied by an auditor. The technical experts can provide ad vice to the audit team for the preparation, planning or audit.

Each auditor is accompanied by a guide, unless otherwise agreed to by the audit team leader and the client. Guide(s) are assigned to the audit team to facilitate the audit. The audit team ensures that guides do not influence or interfere in the audit process or outcome of the audit.

The responsibilities of a guide 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 the guide.

4.2.3 Audit Plan

4.2.3.1 General

Audit Manager ensures that an audit plan (F-05) is established for each audit identified in the audit programme to provide the basis for agreement regarding the conduct and scheduling of the audit activities. This audit plan is based on policies and procedures defined by KBS.

4.2.3.2 Preparing the audit plan

The audit plan appropriate to the objectives and the scope of the audit is prepared. The audit plan at least includes or refers to the following:

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 will be conducted, including visits to temporary sites and remote auditing activities, where appropriate;
e) the expected 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 and audit schedule (F-06) contains the above information.

4.2.3.3. Communication of audit team tasks

The tasks given to the audit team is defined and made known to the client organization, and requires 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,
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, and
d) communicate to the client, for its action, any inconsistencies between the client's policy, objectives and targets (consistent with the expectations in the relevant management system standard or other normative document) and the results.

4.2.3.4 Communication of audit plan

The audit plan is communicated, and the dates of the audit are agreed upon, in advance, with the client organization.

4.2.3.5 Communication concerning audit team members

Audit Manager provides 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 to reconstitute the team in response to any valid objection.

4.2.3.6 General (ISMS)

The audit plan for ISMS audits take the determined information security controls into account.

4.2.3.6 Network-assisted audit techniques (ISMS)

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 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.

4.2.3.7 Timing of audit (ISMS)

KBS 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.

4.3 Initial certification

4.3.1 Initial certification audit
4.3.1.1 General

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

4.3.1.2 Stage 1 audit

Planning shall ensure that the objective of stage-1 can be met and the client is informed of any "on site" activities during stage 1. Stage 1 does not require a formal audit plan.

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 the stage 2 audit;
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) collect necessary information regarding the scope of the management system, including :
    - the client 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 audit and agree with the client on the details of the stage 2 audit;
f) provide a focus for planning the stage 2 audit 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 and management reviews are being planned and performed, and that the level of implementation of the management system substantiates that the client is ready for the stage 2 audit.

*** EnMS:** The stage 1 audit includes followings in addition to above

a) confirmation of scope and boundaries of the EnMS for certification
b) review of a graphical or narrative description of the organizations facilities, equipment, systems and processes for the identified scope and boundaries;
c) confirmation of the number of EnMS effective personnel, energy sources, significant energy uses and annual energy consumption, in order to confirm the audit duration;
d) review of the documented results of the energy planning process;
e) review of a list of the energy performance improvement opportunities identified as well as the related objectives, targets and action plans.

ISMS

In stage 1 audit, KBS obtain documentation on the design of the ISMS covering the documentation required in ISO/IEC 27001.

KBS obtains a sufficient understanding of the design of the ISMS in the context of the client organization, risk assessment and treatment (including the controls determined), ISMS policy and objectives, and, in particular, of the client organization's preparedness for the audit.

The results of the stage 1 audit is documented in a written report. KBS review the stage 1 audit report before deciding on proceeding with the stage 2 and for selecting the stage 2 audit team members with the necessary competence.

KBS makes the client aware of the further types of information and records that may be required for detailed examination during the stage 2 audit.

At least part of the stage 1 audit is carried out at the client's premises to achieve the objectives stated above. In case the audit team is familiar with the client's premises and systems, the on-site may be exempted.

Documented conclusions with regard to fulfilment of the stage 1 objectives and the readiness for stage 2 are communicated to the client in form F-06, including identification of any areas of concern that could be classified as a non-conformity during stage-2.

In determining the interval between stage 1 and stage 2, consideration is given to the needs of the client to resolve areas of concern identified during the stage 1 audit. KBS may also need to revise its arrangements for stage 2. If any significant changes, which would impact the management system, occur, KBS consider the need to repeat all or part of the stage 1. The client is informed that the results of stage 1 may lead to postponement or cancellation of stage 2.

4.3.1.3 Stage 2

The purpose of the stage 2 audit is to evaluate the implementation, including effectiveness, of the client's management system. The stage 2 audit takes place at the site(s) of the client. It includes at least the following:

a) information and evidence about conformity to all requirements of the applicable management system standard or other normative document;
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 meeting 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;

***** EnMS: During the Stage 2 audit, KBS gather the necessary audit evidence to determine whether or not energy performance improvement has been demonstrated prior to making a certification decision. Confirmation of energy performance improvement is required for granting the initial certification.

ISMS

On the basis of findings documented in the stage 1 audit report, KBS develops an audit plan for the conduct of the stage 2 audit. In addition to evaluating the effective implementation of the ISMS, the objectives of the stage 2 is to confirm that the client organization adheres to its own policies, objectives and procedures. To do this, the audits 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 ISMS 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 ISMS

policy and objectives;

g) implementation of controls (see Annex D), taking into account external and internal context and related risks, the organisation'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 management decisions and the ISMS policy and objectives.

4.3.1.4 Initial certification audit conclusions

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

4.4 Conducting audits

4.4.1 General

On-site audits process includes 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, Audit Manager ensures that such activities are conducted by personnel with appropriate competence. The sufficient evidence are obtained during audit to enable the auditor to take an informed decision on the conformity of the requirement in question.

On-site audit can include remote access to electronic site(s) that contain(s) information that is relevant to the audit of the management system. Consideration is also given to the use of electronic means for conducting audits.

For EnMS: Auditor collects and verifies audit evidence related to energy performance, which includes as a minimum energy planning (all sections), operational control, monitoring measurement and analysis. For classifying nonconformities for ISO 50001, the definition of major non conformity for EnMS is used as under:

"nonconformity that affects the capability of the management system to achieve the intended results such as follows- a) audit evidence that energy performance improvement was not achieved; b) a significant doubt that effective process control is in place; c) a number of minor nonconformities associated with the same requirements or issue demonstrating a systemic failure"

Specific elements of the ISMS audit

Audit team:

a) require the client organization to demonstrate that the assessment of 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 risks and the results of their implementation are consistent with the client's policy, objectives and targets.

Audit team also establish whether the procedures employed in risk assessment are sound and properly implemented.

4.4.2 Conducting the opening meeting

A formal opening meeting is held with the client's management and, where appropriate, those responsible for the functions or processes to be audited as per D-15. The purpose of the opening meeting, which is usually conducted by the audit team leader, is to provide a short explanation of how the audit activities will be undertaken. The degree of details is consistent with the familiarity of the client with the audit process and considers the following:

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 bo dy is responsible for the audit and shall be in control of executing the audit plan includin g 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.

4.4.3 Communication during the audit

During the audit, the audit team periodically assesses audit progress and exchanges information. The audit team leader reassigns work as needed between the audit team members and periodically communicates the progress of the audit and any concerns to the client.

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), the audit team leader reports this to the client and, if possible, to the certification body to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit. The audit team leader reports the outcome of the action taken to the certification body.

The audit team leader reviews with the client any need for changes to the audit scope, wh ich becomes apparent as on-site auditing activities progress and report this to the certificat ion body.

4.4.4 Obtaining and verifying information

During the audit, information relevant to the audit objectives, scope and criteria (including information relating to interfaces between functions, activities and processes) is to be collected by appropriate sampling and verified to become audit evidence.

Methods to collect information include, but are not limited to:

a) interviews;
b) observation of processes and activities;
c) review of documentation and records.

For OHS, the audit team interview the following personnel:

- *the management with legal responsibility for Occupational Health and Safety,*
- *employees' representative(s) with responsibility for Occupational Health and Safety,*
- *personnel responsible for monitoring employees' health, for example, doctors and nurs es. Justifications in case of interviews conducted remotely shall be recorded,*
- *managers and permanent and temporary employees;*
- *managers and employees performing activities related to the prevention of Occupation al Health and Safety risks, and*
- *contractors' management and employees.*

The audit team ensures adequate balance between review of documents and records and the evaluation of the OH&SMS implementation during operational activities (e.g. site tour of f acilities and other work sites) to ensure that an adequate audit of the effectiveness of the O H&SMS is undertaken.

4.4.5 Identifying and recording audit findings

Audit findings summarizing conformity and detailing nonconformity and its supporting audit evidence are recorded and reported to enable an informed certification decision to be made or the certification to be maintained.

Opportunities for improvement may be identified and recorded. Audit findings, which are non-conformities, are not recorded as opportunities for improvement.

A finding of nonconformity is recorded against a specific requirement of the audit criteria, containing a clear statement of the nonconformity and identifying in detail the objective evidence on which the nonconformity is based. Nonconformities are discussed with the client to ensure that the evidence is accurate and that the nonconformities are understood. The auditor however refrains from suggesting the cause of nonconformities or their solution. *In case any ongoing or potential non-compliances are identified in relation to relevant regulatory requirements, the non-compliances are immediately communicated to the organization being audited for immediate action. Certificate is granted only after confirming compliance with initial and ongoing legal requirements. During each surveillance and re-assessment, Audit team verify the management of legal compliance based on the demonstrated implementation of the system and not rely on planned or expected results. Any deliberate or consistent non-compliance with legal requirements may lead to suspension, or withdrawal of the certificate.* The audit team leader attempts to resolve any diverging opinions between the audit team and the client concerning audit evidence or findings, and unresolved points are recorded.

4.4.6 Preparing audit conclusions

Under the responsibility of the audit team leader and prior to the closing meeting, the audit team:

a) reviews the audit findings, and any other appropriate information collected during the audit, against the audit objectives and audit criteria and classify the nonconformities;

b) agree upon the audit conclusions, taking into account the uncertainty inherent in the audit process;
c) agree any necessary follow-up actions;
d) confirm the appropriateness of the audit programme or identify any modification required (e.g. scope of certification, audit time or dates, surveillance frequency, audit team competence).

4.4.7 Conducting the closing meeting

A formal closing meeting, where attendance is recorded, is held with the client's management and, where appropriate, those responsible for the functions or processes audited as per D-15. The purpose of the closing meeting, which normally conducted by the audit team leader, is to present the audit conclusions, including the recommendation regarding certification. Any non-conformities are presented in such a manner that they are understood, and the timeframe for responding is agreed.

The closing meeting also includes the following elements. The degree of detail is 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 post audit activities of KBS;
f) information about the complaint handling and appeal processes.

The client is given opportunity for questions. Any diverging opinions regarding the audit findings or conclusions between the audit team and the client are discussed and resolved where possible. Any diverging opinions that are not resolved are recorded and referred to KBS.

For OH&SMS: The organization representative are requested to invite the management legally responsible for occupational health and safety, personnel responsible for monitoring employees' health and the employees' representative(s) with responsibility for occupational health and safety to attend the closing meeting. Justification in case of absence is recorded.

4.4.8 Audit report

KBS provides a written report for each audit to the client. The audit team may identify opportunities for improvement but do not recommend specific solutions. KBS maintain ownership of the audit report.

The audit team leader ensures that the audit report is prepared and is responsible for its content. The audit report provides an accurate, concise and clear record of the audit to enable an informed certification decision to be made and includes or refers to the following:

a) identification of KBS as 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 or special audits);
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; any deviation from the audit plan and their reasons;
g) any significant issues impacting on the audit programme;
h) identification of the audit team leader, audit team members and any accompanying persons;
i) the dates and places where the audit activities (on site or offsite, permanent or temporary sites) were conducted;
j) audit findings, reference to evidence and conclusions, consistent with the requirements of the type of audit;
k) significant changes, if any, that affect the management system of the client since the last audit took place;
l) any unresolved issues, if identified.
m) where applicable, whether the audit is combined, joint or integrated;
n) a disclaimer statement indicating that auditing is based on a sampling process of the available information;
o) recommendation from the audit tea
p) the audited client is effectively controlling the use of the certification documents and marks, if applicable;
q) verification of effectiveness of taken corrective actions regarding previously identified nonconformities, if applicable.

* For EnMS, the audit report also include a) scope and boundaries of the EnMS being audited b) statement of achievement of continual improvement of the EnMS and energy performance improvement with audit evidence to support the statements.

The report also contains:

a) a statement on the conformity and the 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.

ISMS

The audit report provide the following information or a reference to it:

a) an account of the 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);

d) the ISMS' scope.

The audit report includes sufficient detail to facilitate and support the certification decision. It contains:

a) significant audit trails followed, and audit methodologies utilized;

b) observations made, both positive (e.g. noteworthy features) and negative (e.g. potential

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 client.

Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report. If these methods are used, these documents are submitted to KBS as evidence to support the certification decision. Information about the samples evaluated during the audit is included in the audit report, or in other certification documentation.

The report considers the adequacy of the internal organization and procedures adopted by the client to give confidence in the ISMS.

The report also covers:

- a 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.

For OH&SMS: Audit reports contain a statement on the conformity and the effectiveness of the organization's OH&SMS together with a summary of the evidence with regards to the capability of the OH&SMS to meet its compliance obligations.

It is made clear that KBS auditors are not inspectors of the OH&S regulator. Auditors don't' provide "statements" or "declarations" of legal compliance. Nevertheless, they do "verify the evaluation of legal compliance" in order to assess conformity with the applicable OH&SMS standard.

Accredited certification of an OH&SMS as fulfilling the requirements in an OH&SMS standard cannot be an absolute and continuous guarantee of legal compliance but neither can any certification or legal scheme guarantee ongoing legal compliance. However, an OH&SMS is a proven and effective tool to achieve and maintain legal compliance and provides top management with relevant and timely information on the organisation's compliance status.

4.4.9 Cause analysis of nonconformities

KBS requires 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. The proposed corrective action along with correction action needs to be provided with 30 days of the NC while in case of Major non-conformities, this time limit is 60 days.

4.4.10 Effectiveness of corrections and corrective actions

KBS reviews the corrections, identified causes and corrective actions submitted by the client to determine if these are acceptable. KBS verifies the effectiveness of any correction and corrective actions taken. The evidence obtained to support the resolution of nonconformities is recorded. The client is informed of the result of the review and verification. The client is 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 documented information provided by the client, or where necessary, through verification on-site. Usually this activity is done by a member of the audit team.

4.5 Certification decision

4.5.1 General

Certification Manager makes decisions for granting or refusing certification, expanding or reducing the scope of certification, suspending or restoring certification, withdrawing certification or renewing certification after the technical review of the report by an independent person who had not been part of the team. In case Certification Manager or technical reviewer is part of the audit team, another person appointed by MD takes decision. The individual (s) appointed to conduct the technical review and certification decision have appropriate competence including in the technical area/sector and may be supplemented by a technical expert.

Certification Manager records each certification decision including any additional information or clarification sought from the audit team or other sources.

ISMS

The certification decision is based on the certification recommendation of the audit team as provided in their certification audit report in addition to the following requirements.

The persons or committees that take the decision on granting certification do not normally overturn a negative recommendation of the audit team. If such a situation does arise, KBS document and justify the basis for the decision to overturn the recommendation.

Certification is 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 are to be maintained.

4.5.2 Actions prior to making a decision

Each report is reviewed by a technical reviewer appointed by the certification Manager having competence prior to making decision for granting certification, expanding or reducing the scope of certification, renewing, suspending or restoring, 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 plan for correction and corrective actions

The Certification decision is made as per procedure P-09 and recorded in form F-19.

4.5.3 Information for granting initial certification

The information provided by the audit team to KBS for the certification decision includes, as a minimum,

a) the audit reports including all forms identified in F-18,
b) comments on the nonconformities and, where applicable, the correction and corrective actions taken by the client,
c) confirmation of the information provided to KBS used in the application review and confirmation that the audit objectives have been achieved;
d) a recommendation whether or not to grant certification, together with any conditions or observations.

If KBS 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, KBS conducts another stage 2 prior to recommending certification.

When a transfer of certification is envisaged from another certification body, KBS has defined the process in procedure P-11 for obtaining sufficient information in order to take a decision on certification.

For OH&SMS:

An OH&SMS standard requires a commitment to comply with legal requirements. Accredited certification of an organization's OH&SMS indicates conformity with the requirements of the applicable OH&SMS standard and includes a demonstrated and effective commitment to compliance with applicable legal requirements.

The organization must be able to demonstrate it has achieved compliance with its applicable legal requirements through its own evaluation of compliance prior to the KBS granting certification.

The control of legal compliance by the organization is an important component of the OH&SMS assessment and remains the responsibility of the organization.

Certification of an OH&SMS as fulfilling the requirements in an OH&SMS standard confirms that the OH&SMS has been shown to be effective in achieving its policy commitments including fulfilment of legal compliance obligations and provides the foundation and support for an organization's continued legal compliance.

Accredited certification of an OH&SMS as fulfilling the requirements in an OH&SMS standard cannot be an absolute and continuous guarantee of legal compliance but neither can any certification or legal scheme guarantee ongoing legal compliance. However, an OH&SMS is a proven and effective tool to achieve and maintain legal compliance and provides top management with relevant and timely information on the organisation's compliance status.

KBS grants certification only after confirming compliance with legal OH&S requirements or if an organization is able to demonstrate it has activated an implementation plan to achieve full compliance within a declared date, supported by a documented agreement with the regulator, wherever possible for the different national conditions. The successful implementation of this plan is considered as a priority within the OH&SMS.

In order to maintain the confidence of interested parties and stakeholders in the above attributes of the accredited certification of an OH&SMS, KBS ensure that the system has demonstrated

effectiveness before granting, maintaining or continuing certification.

In exceptional cases, KBS may still grant certification after confirming that the organisation's OH&SMS:

- *is capable of achieving the required compliance through full implementation of the above implementation plan*
- *has addressed all hazards and OH&S risks to workers and other exposed personnel and that there are no activities, processes or situations that can or may lead to a serious injury and/or ill health, and*
- *during the transitional period has put in place the necessary actions to ensure that the OH&S risk is reduced and controlled.*

The OH&SMS can act as a tool for dialogue between the organisation and its OH&S regulators and form the basis for a trusting partnership, replacing historical adversarial "them and us" relationships. OH&S regulators and the public should have confidence in organizations with an accredited OH&SMS standard certificate and be able to perceive them as being able to constantly and consistently manage their legal compliance

4.5.4 Information for granting recertification

KBS makes 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.

4.6 Maintaining certification

4.6.1 General

KBS maintains certification based on demonstration that the client continues to satisfy the requirements of the management system standard. It maintains a client's certification based on a positive conclusion by the audit team leader without further independent review and decision, provided that:

a) for any major nonconformity or other situation that may lead to suspension or withdrawal of certification, KBS has a system that requires the audit team leader to report to it the need to initiate a review by appropriately competent personnel, different from those who carried out the audit, to determine whether certification can be maintained, and
b) competent personnel of KBS monitor its surveillance activities, including monitoring the reporting by its auditors, to confirm that the certification activity is operating effectively.

Where, any points/issues are raised by the technical reviewer (independent reviewer), the letter of continuation is issued only after the issues/ points have been cleared.

For OHS&SMS: If the facilities and work areas are subject to closure, the OH&S risk may change and new risks may emerge. KBS audit team verifies that the management system continues to meet the OH&SMS standard and to be effectively implemented in respect of the closed facilities and work areas. In case f not meeting the requirements, the certificate may be suspended.

4.6.2 Surveillance activities

4.6.2.1 General

KBS has developed its surveillance activities so that representative areas and functions covered by the scope of the management system are monitored on a regular basis, and takes into account changes to its certified client and its management system.

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. Other surveillance activities may include

a) enquiries from KBS 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 certified client to provide documented information (on paper or electronic media), and
d) other means of monitoring the certified client's performance.

Surveillance activities (ISMS)

Surveillance audit procedures are consistent with those concerning the certification audit of the client's ISMS.

The purpose of surveillance is to verify that the approved ISMS continues to be implemented, to consider the implications of change to that system initiated as a result of changes in the client's operation and to confirm continued compliance with certification requirements. Surveillance audit programmes cover at least:

a) the system maintenance elements such as information security risk assessment and control maintenance, internal ISMS audit, management review 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 requirements of ISO/IEC 27001;
f) other selected areas as appropriate.

As a minimum, every surveillance by KBS review the following:

a) the effectiveness of the ISMS with regard to achieving the objectives of the client's information security policy;
b) the functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations;
c) changes to the controls determined, and resulting changes to the SoA;
d) implementation and effectiveness of controls according to the audit programme.

KBS is able to adapt its surveillance programme to the information security issues related to risks and impacts on the client and justify this programme.

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

During surveillance audits, KBS check the records of appeals and complaints brought before KBS and, where any nonconformity or failure to meet the requirements of certification is revealed, that the client has investigated its own ISMS and procedures and taken appropriate corrective action.

A surveillance report contains, in particular, information on clearing of nonconformities revealed previously and the version of the SoA and important changes from previous audit.

4.6.2.2 Surveillance audit

Surveillance audits are on-site audits, but are not necessarily full system audits, and are planned together with the other surveillance activities so that KBS can maintain confidence that the certified management system continues to fulfill requirements between recertification audits.

Each surveillance for the relevant management system standard includes:

a) internal audits and management review,
b) a review of actions taken on nonconformities identified during the previous audit,
c) complaints handling,
d) effectiveness of the management system with regard to achieving the certified client's objectives, and the intended results of the respective management system (s);
e) progress of planned activities aimed at continual improvement,
f) continuing operational control,
g) review of any changes, and
h) use of marks and/or any other reference to certification.
i) compliance with legal requirements

*** EnMS:** During the surveillance audits, KBS review the necessary audit evidence to determine whether or not continual energy performance improvement has been demonstrated.

4.6.3 Recertification

4.6.3.1 Recertification audit planning

The purpose of the recertification audit is to confirm the continued conformity and effectiveness of the management system as a whole, and its continued relevance and applicability for the scope of certification. A recertification audit is planned and conducted to evaluate the continued fulfilment of all of the requirements of the relevant management system standard or other normative document. This is planned and conducted in due time to enable for timely renewal before the certification expiry date.

The recertification activities include the review of previous surveillance audit reports and consider the performance of the management system over the most recent certification cycle. In case the client has been certified by other CB and applies for renewal to KBS, the stage 1 audit will be carried out if the previous audit reports are not available for review.

Recertification audit activities may need to have a stage 1 audit in situations where there have been significant changes to the management system, the organisation, 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 KBS may perform a special audit, which might or might not be a two-stage audit.

4.6.3.2 Recertification audit

The recertification audit includes 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 (s).

For any major nonconformity, KBS defines the time limits for correction and corrective actions. These actions shall be implemented and verified prior to the expiration of certification.

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

If KBS 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 prior to the expiry date of the certification, then recertification shall not be recommended, and the validity of the certification shall not be extended. The client shall be informed, and the consequences shall be explained.

Following expiration of certification, KBS can restore certification within 6 months provided that the outstanding recertification activities are completed. The effective date on the certificate is on or after the recertification decision and the expiry date is based on prior certification cycle.

* EnMS: During the recertification audit, KBS reviews the necessary audit evidence to determine whether or not continual energy performance improvement has been demonstrated prior to making a recertification decision. The recertification audit also takes into account any major change in facilities, equipment, systems or processes. Confirmation of continual energy performance improvement is required for granting the recertification. Energy performance improvement can be affected by changes in facilities, equipment, systems or processes, business changes, or other conditions that result in a change or a need to change the energy baseline.

ISMS
Recertification audit procedures shall be consistent with those concerning the certification audit of the client organization's ISMS as described in this International Standard.

The time allowed to implement corrective action shall be consistent with the severity of the nonconformity and the associated information security risk.

4.6.4 Special audits
4.6.4.1 Expanding scope

KBS, in response to an application for extension to the scope of a certification already granted, undertakes a review of the application and determines any audit activities necessary to decide

whether or not the extension may be granted. This may be conducted in conjunction with a surveillance audit.

4.6.4.2 Short-notice audits

It may be necessary for KBS to conduct audits of certified clients at short notice or unannounced to investigate complaints, or in response to changes, or as follow up on suspended clients. In such cases
a) KBS describes and makes known in advance to the certified clients, the conditions under which these short notice visits are to be conducted, and
b) KBS exercises additional care in the assignment of the audit team because of the lack of opportunity for the client to object to audit team members.

For OH&SMS: Independently from the involvement of the competent regulatory authority, a special audit may be necessary in the event that KBS becomes aware that there has been a serious incident related to occupational health and safety, for example, a serious accident, or a serious breach of regulation, in order to investigate if the management system has not been compromised and did function effectively. KBS documents the outcome of its investigation.

4.6.4.3 Special cases(ISMS)
The activities necessary to perform special audits are 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.

4.6.5 Suspending, withdrawing or reducing the scope of certification

KBS has a policy and documented procedure(s) P-09 for suspension, withdrawal or reduction of the scope of certification, and has specified the subsequent actions by it (KBS).

KBS suspends 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.
- ✓ *the client deliberately or consistently non-comply with legal requirements*

Under suspension, the client's management system certification is temporarily invalid.

KBS restore the suspended certification if the issue that has resulted in the suspension has been resolved. Failure to resolve the issues that have resulted in the suspension in a time established by KBS results in withdrawal or reduction of the scope of certification. In most cases the suspension does not exceed 6 months.

KBS reduces 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. Any such reduction is in line with the requirements of the standard used for certification.

FOR OH&SMS: Information on incidents such as a serious accident, or a serious breach of regulation necessitating the involvement of the competent regulatory authority, provided by the

certified client or directly gathered by the audit team during the special audit, provide grounds for KBS to decide on the actions to be taken, including a suspension or withdrawal of the certification, in cases where it can be demonstrated that the system seriously failed to meet the OH&S certification requirements. Such requirements are part of the contractual agreements between the KBS and the organization.

4.7 Use of Certificate, Certification Logo and Accreditation Mark

(1) Certification Manager ensures that KBS complies with the conditions for use of Accreditation Mark.
(2) Customer's use of certificate and certification logo is controlled in accordance with Procedure P-12.

5.0 Records

- Records identified in Assessment Reports Package [F-18]
- List of Certified Customers [F-20]