F

0.1 Approval and Issue

Reviewed by : **Technical Advisory Committee**

Approved by : **Chief Executive Officer**

Note:

1. Management Representative is responsible for issue and distribution of this document including amendments.

2. Holder of this copy is responsible for incorporation of all the amendments and currency of the document.

0.2 Amendment Record

Amendment No.	Date of Amendment	Nature of Amendment	Page Ref.
1	01-11-2016	New Requirements of ISO27006:2015	At relevant places
2	30.08.2021	Aligned with ISO 27006:2015 amd 2020	At relevant places

1.0 Purpose and Scope

The purpose of this document is to establish procedures for the assessment of organizations having applied for ISMS Certification.

This document has been prepared to achieve the following objectives:

a) To ensure uniformity in assessing organizations seeking certification against ISO/IEC 27001 under the STQC ISMS Certification scheme. This shall include all stages of the assessment starting from evaluation of the Information Security Management System documentation provided by the organization, Assessment stage 1, Assessment stage 2, and surveillance assessments.
b) To ensure adequate control on the assessments to be carried out.
c) To ensure uniform methods of reporting during and after the assessment, to both the organization and STQC.
d) To serve as training document to new assessors.

2.0 Responsibility

Chief Executive Officer	Assignment of the Assessment Team.
Team Leader (ISMS Lead Assessor)	Responsible for the entire assessment process (including corrective action follow-up) up to and including making the final recommendation for certification.
ISMS Assessors	Responsible for carrying out assessment as per task allocated by the Team Leader.
Technical Experts	Responsible for advising the Team Leader and ISMS Assessors on technical issues.
Operations personnel	Responsible for co-ordinating activities during all stages of the assessment process and to provide necessary support to the assessment team when required.

3.0 Associated Documents

ITCERT/D01	-	IT Manual
ISMS/D01	-	Product Manual - ISMS
ISMS/P01	-	Application handling
ISMS/P03	-	ISMS Assessment Team Competence
ISMS/F01	-	ISMS Checklist Preliminary Evaluation for Adequacy
ISMS/F02	-	ISMS Checklist for Assessment
ISMS/F04	-	Nonconformity Report
ISMS/F06	-	Certification Process Data Sheet
ISMS/F07	-	ISMS Assessment Report
ISMS/F08	-	Assessor Notes

4.0 Definitions

For the purpose of this document the definitions contained in clause 1.3 of Doc ITCERT/D01 shall apply.

5.0 Resources

For the purpose of the activities defined in this document, the personnel resources are identified in Doc ITCERT/D03.

6.0 Procedure

The process of ISMS assessment starts after the positive conclusion of the successful application review, and initial document review if any (ISMS/P01) and the selection and assignment of an ISMS Assessment Team (ISMS/P03).

The Assessment Team performs the assessment of the organisation's ISMS in two stages at the organisation's site(s), unless an alternative approach is justified, e.g. in case of the assessment of very small organisations.

The ISMS assessment can be combined with assessments of other management systems. All elements important to the ISMS will appear clearly and readily identifiable in the assessment reports.

The ISMS assessment is done in two stages (assessment stage 1 and assessment stage 2) each covering four phases as follows:

- Phase I Planning
- Phase II Preparation
- Phase III Performance
- Phase IV Report, follow-up and Close out

6.1 *Assessment stage 1*

The objectives of assessment stage 1 are to provide a focus for planning assessment stage 2 by gaining an understanding of the ISMS in the context of the organisation's security policy and objectives.

In assessment stage 1, the assessment team performs a detailed review of the applicant’s ISMS documentation for ensuring compliance with all applicable requirements of ISO/IEC 27001.
Assessment stage 1 is not restricted to the document review, but includes sufficient understanding of the design of the ISMS in the context of client organization, policy, objectives, risk assessment and treatment (Statement of Applicability of controls), client’s readiness for the audit and verification of the organization's implementation of the procedures for internal audit and management review.

The results of assessment stage 1 are documented in a written report that is communicated to the organization.
If non-compliances are observed, the organization will have to carry out necessary corrective actions prior to assessment stage 2.

The Certification Body will review the report for deciding on proceeding with assessment stage 2 and, if applicable, for selecting new or additional assessment team members with the necessary competence.

6.1.1 Assessment stage 1 - Phase I, Planning

Planning at this stage involves reaching an agreement between the organization and the Team Leader and his/her team concerning the date on which assessment stage 1 will be performed and also to make arrangements for access to internal audit reports, reports of independent security review as well all the relevant document required.. As general rule, assessment stage 1 will take place at the premises of the organization. This has the advantage that the organization is not required to submit its confidential system documentation to the outside. By visiting the organization, the assessment team will get a feeling for the particular structure and culture of that organization. In case of small size organizations, the detailed review of the ISMS documentation could take place at the offices of the Certification body, provided that the organization agrees.

Assessment stage 1 will require, depending on the size of the organization, from 1 to 4 day effort by the ISMS Assessment Team. However audit efforts may be increased on the recommendation of Head operations/ LA.

6.1.2 Assessment stage 1 - Phase II, Preparation

The preparation for assessment stage 1 consists of Assessment Team briefing and Assessment Plan drawing-up. Assessment plan shall clearly address Audit scope, objectives and criteria, including any changes and agreed with the client. The audit plan also identify the network-assisted auditing techniques (such as Video/audio conferencing etc) that will be utilized during the audit, as appropriate.

The audit objectives shall be addressed as follows:

a) Determination of the conformity of the client management system, or parts of It to audit criteria;

b) Evaluation of the ability of the management system to ensure that client organisation meets applicable statutory, regulatory and contractual reqts

c) Evaluation of the effectiveness of the management system to ensure the client organization based on the risk assessment has implemented applicable controls and is continually meeting its specified ISMS objectives;

d) As applicable, identification of areas for potential improvement of the management system

In case of initial or re-certification audits consisting of more than one audit the audit scope of individual audit may not cover the full scope but the all audits combined shall address the full scope of audit.

The Team Leader briefs the team on the following:

- Audit Scope and objectives, type, structure, and IT infrastructure of the organization
- Conclusions from document review for Adequacy
- Expected areas of interest and concern
- Possible legislative issues
- Allocation of activities to the team members
- Assessment stage 1 methodology.

The briefing can be done in writing or by holding a meeting.

The Team Leader prepares an assessment plan (schedule) for assessment stage 1. The plan shall include at least the following:

- Name, address, and contact person of the organization
- Date and place of the assessment stage 1
- Names of the members of the Assessment Team and possible observers
- Programme, approximate time schedule, and allocation to team members
- The programme shall at least contain the following:
  - Brief opening meeting
  - Tour of the premises (if applicable)
  - Presentation by the organization of structure, IT infrastructure, and documentation
  - Documentation review
  - Verification of procedures and records concerning system audit considerations
  - Verification of procedures and records concerning security reviews
  - Team meeting to prepare for the closing meeting closing meeting.

The Team Leader ensures that the assessment plan is communicated to the organization and the team members. The organization shall be explicitly requested whether objections exist to any of the proposed team members and possible observers. In case of objections, the Certification body shall seek adequate replacements.
A copy of the assessment plan and related correspondence is kept in the client file.

6.1.3 Assessment stage 1 - Phase III, Performance

This phase is not designed to be a compliance audit. It is, in effect, a detailed and on-the-spot information gathering and confirmation exercise. However, if non-compliances are observed they must be brought to the attention of the organization for corrective action.

The assessment activities are conducted by:

- Listening to the company presentation of its organizational structure, management set-up, IT infrastructure, and structure of the documented ISMS,
- Discussion and observation of actual practice,
- Review of the documented ISMS,
- Verification of internal audit and management review practices. It is ensured that at-least one complete cycle of internal audit and management review covering the entire scope is completed by the client.

As such, it is essential that the team members establish good communications and relationship with the organization's personnel in order to be able to rapidly but accurately understand the situation regarding the adequacy of the ISMS, both documented and implemented.

Opening Meeting

The Team Leader conducts the opening meeting of assessment stage 1. It should be held fairly informally. The organization's top management is not necessarily present at this meeting, but Information Security management and staff should attend. The purpose is to:

- Introduce the team and establish the credentials of the team members,
- Emphasise confidentiality of information and practices to be seen
- Explain the assessment methodology and the purpose of this visit,
- Establish the need for open communication,
- Confirm the scope of the activities covered by the ISMS,
- Answer any questions that the organization may have at this stage.
- Provide a focus for planning Stage-2 by gaining sufficient understanding of the client's management system and site operations in context of the management system standards or other normative documents.

Tour of the premises

The first action after the opening meeting is a brief visit under guidance of the organization's personnel to the premises, especially the computer room and the offices where IT facilities are used. This visit should give the Assessment Team an impression of the physical and environmental security as implemented by the organization.

Conduct of the assessment

The Assessment Team reviews in detail the following documentation:

- Scope (for ensuring consistency in line with Business processes) The audit scope shall describe the extent and boundaries of the audit such as sites, organizational units and processes to be audited. It shall 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. Certification bodies shall confirm that this is reflected in the client's scope of their ISMS and Statement of Applicability. The team shall verify that there is at least one Statement of Applicability per scope of certification.

It is also checked 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.

- Criteria : the audit criteria shall be used as reference against which conformity is determined such as ISO 27001.
- Description of the organization and its IT infrastructure
- Information security Risk Analysis (in line with business activities within the scope and SOA)
- Information Security Policy and objectives as a commitment of Top Management to ISMS
- Statement of Applicability
- Management responsibilities for information security
- Evaluate that Internal audits and Management Reviews are planned and performed
- Determination of control objectives and Levels of controls established (including multisite operations)
- Applicable regulations and the organization's compliance measure
- ISMS procedures and working instructions
- Interfaces with services/activities that are not under the scope of ISMS

and verifies the conformance of the documented management system with the requirements of ISO/IEC 27001.

The Assessment Team verifies records concerning system audit considerations and security reviews.

The Assessment Team interviews appropriate personnel of the organization to obtain answers to possible questions and to receive additional information if required. Areas where non-compliances appear to exist shall be examined in detail in order that the Assessment Team may accurately understand the situation.

Detailed notes shall be taken (form ISMS/F08) to ensure that observations are correctly reported on completion of assessment stage 1.

Team Management

An ISMS assessment is usually carried out by a team of more than one ISMS Assessor and possibly Technical Experts. The team encompasses all required skills, knowledge and experience for the specific organization under assessment. To ensure that the assessment achieves its objectives and is carried out in a professional manner, the Team Leader shall exercise management skills.

He/she must ensure that:

- Regular team meetings are held to co-ordinate the activities,
- The timing of the schedule is followed,
- Team members execute their assigned tasks.

On completion of the assessment activities, the Team Leader shall assemble the team to review all observations and decide upon any non-compliance that require the organization's attention for further development. Also the allocation of resources for Stage-2 may be discussed. All Assessment Team members will be involved in this preparation for the closing meeting. However, the team meeting is led by the Team Leader who is empowered to make final decisions.

Closing Meeting

The purpose of the closing meeting is to present to the organization a verbal report of the observations made during the assessment stage 1. The following subjects shall be covered:

- Thanks for hospitality and co-operation,
- Emphasize confidentiality of information and practices seen,
- (Re-) Explanation of the assessment methodology and purpose of this visit,
- Confirmation of the scope of the activities covered by the ISMS,
- Detailed explanation of any areas of concerns that could be classified as Non-conformity during Stage-2,
- General summary of the overall state of compliance and preparedness for assessment stage 2,
- Subsequent steps to be taken in the assessment process,
- Answering any questions that the organization may have.

6.1.4 Assessment stage 1 - Phase IV, Report, follow-up and close out

The Team Leader shall prepare a formal documented report that will provide the organization with objective evidence of the non-conformance identified and act as the basis for investigation and action.

The report shall cover in detail:

- Organization name, site, activities, IT infrastructure, scope of ISMS
- Assessment Team names and functions in team
- Assessment stage 1 date, place and actual assessment schedule
- Summary of assessment results
- Major/Minor Nonconformity to be indicated in Assessment results overview list (minor =partial compliance, major = no compliance). No separate Nonconformities are to be made.
- Summary of position concerning assessment stage 2.

The report shall be concise, clear, and unambiguous in its statements.

The Team Leader issues the report to the organization and, if appropriate, requests evidence of corrective action to be provided within three months from the date of the report. The organization shall be informed that delay in providing corrective action will result in the Certification body having to repeat assessment stage 1 and charge for costs accordingly. The decision of the lead assessor shall be final based on the business activities and IT infrastructure of the client. Upon receiving the evidence of corrective action, the Team Leader draws up a summary report of the actions taken by the organization and his/her conclusions regarding the readiness of the organization for assessment stage 2.

The RM/Operational person independent of the audit will review the report on assessment stage 1 and possible corrective action summary report for deciding on proceeding with assessment stage 2 and shall confirm if the stage 2 audit team members have the necessary competence; this may be done by the auditor leading the team that conducted the stage 1 audit if deemed competent and appropriate. The organization shall be informed in writing of the decision The client is informed that the result of Stage-1 may lead to postponement or cancelation of Stage-2.

6.2 *Assessment stage 2*

The objectives of assessment stage 2 are:
- To confirm that the organization adheres to its own policies, objectives and procedures.
- To confirm that the ISMS conforms to the requirements of ISO/IEC 27001 and is effective in achieving the organization's policy objectives.

Where any part of the audit is made by electronic means or where the site to be audited is virtual, CB shall ensure that such activities are conducted by personnel with appropriate competence.

6.2.1 Assessment stage 2 - Phase I, Planning

The Team Leader, having gained an intimate understanding of the organization's activities and actual and potential significant issues relating to the Information Security as well as a clear knowledge of the structure and development of the documented ISMS, shall plan assessment stage 2. The previously issued assessment quotation shall be reviewed against the information obtained in assessment stage 1 and shall be confirmed or, if appropriate, revised.

The review shall consist of:
- Re-evaluation of the skills required in the Assessment Team,
- Re-evaluation of the number of days allocated for assessment stage 2,
- Re-evaluation of manpower and travel costs.

The Operational person prepares a confirmation of the quotation or drafts a new quotation. The final quotation is reviewed by the Chief Executive Officer and, after approval, submitted to the organization.

6.2.2 Assessment stage 2 - Phase II, Preparation

The Team Leader drafts an assessment plan for the conduct of assessment stage 2 on the following basis:
- The requirements of ISO/IEC 27001
- Product Manual - ISMS (ISMS/D01)
- ISMS Assessment Procedure (this procedure)
- Report on assessment stage 1
- Corrective action summary report (if applicable).

- Use of network assisted auditing techniques (such as teleconferencing, web-based etc.) where applicable.

- Team leader agrees 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

The structure of the assessment plan/schedule is similar to the assessment plan for assessment stage 1 described above under 6.1.2. In case assessment stage 2 takes more than one day, the assessment plan shall foresee in a feedback meeting with the organization's representative at the end of each day. The feedback meeting serves to inform the organization's representative of the assessment progress and possible non-compliances observed. The closing meeting shall be planned on the last day of the assessment.

The Team Leader ensures that the assessment plan is communicated to the organization and the team members. The organization shall be explicitly requested whether objections exist to any of the proposed team members and possible observers. In case of objections, the Certification body shall seek adequate replacements.
A copy of the assessment plan and related correspondence is kept in the client file.

If applicable, the Team Leader will inform the organization in writing of the further types of information and records that are required for detailed inspection during assessment stage 2.

The Team Leader decides on holding a team briefing detailing assignment of specific tasks to audit team members. This could be necessary if new members have been assigned to the team; however, the Team Leader could provide individual briefings.

6.2.3 Assessment stage 2 - Phase III, Performance

Opening Meeting

The Team Leader conducts the opening meeting of assessment stage 2. This is a formal meeting at which the organization's (top) management should be present as well as Information Security management and representatives of information owners.

The purpose of the opening meeting is to:
- Introduce the team and establish the credentials of the team members,
- Confirm the role of lead auditor and audit team memebers
- Confirm confidentiality of information and practices to be seen
- Confirm the scope of the activities covered by the ISMS,
- Explain the assessment methodology,
- Confirm the assessment plan/schedule, and logistics for the following:
  . Availability of managers and staff to be interviewed
  . Roles and Availability of guides/ observers
  . Availability of documentation
  . Working space for the Assessment Team

. Suitability of the time schedule, including arrangements for breaks and meals and any changes required
- confirmation of the communication channels and language to be used during audit

- Emphasize that assessment is based on sampling,
- Confirmation of the relevant work safety, emergency and security procedures of the audit team
- information about the conditions under which the audit may be prematurely terminated.
- Explain manner of reporting, grading of findings and requirements for corrective action,
- Status of previous audit findings where applicable
- Confirm the place and time of the, audit debriefing (to report the progress) meetings and closing meeting,
- Answer any questions that the organization may have at this stage,
- Thank for participating in the opening meeting.

Team Management

An ISMS assessment is usually carried out by a team of more than one ISMS Assessor and possibly Technical Experts. The team encompasses all required skills, knowledge and experience for the specific organization under assessment. To ensure that the assessment achieves its objectives and is carried out in a professional manner, the Team Leader shall exercise management skills. He/she must ensure that:

- Regular meetings are held to co-ordinate the team activities and to provide feedback to the representative of the organization and review the audit progress and communicate any concerns.
- The timing of the schedule is followed,
- Team members execute their assigned tasks and any changes required in the assigned tasks and reassignment of activities as required.

Conduct of the assessment

The assessors in the team usually act as individuals splitting up to assess different areas of the organization. Each assessor is to be accompanied by a guide assigned by the organization who facilitates movement around the premises. Technical Experts in the team accompany assessors; they do not operate independently.

The assessment will focus on the organization's:

1) Analysis of information security related risks and the resulting design of the ISMS.
2) Statement of Applicability;
3) Objectives and targets derived from this process;
4) Top Management leadership and commitment for the information security policy and objectives;
5) Performance monitoring, measuring, reporting and reviewing against the objectives and targets;
6) Client’s management system ability and its performance regarding meeting applicable statutory, regulatory and contractual requirements
7) Internal audits and management reviews;

8) Links between the policy, the results of information security risk assessments, risk treatment (consistency, adequacy, soundness, implementation and effectiveness of Risk Assessment process), objectives and targets, responsibilities, programmes, procedures, performance data, and security reviews and effectiveness of ISMS.
9) Operational control objectives and controls and its implementation of the client processes.

Conformance to the requirements of ISO 27001

In order to provide confidence that the organization is consistent in establishing and maintaining procedures for the identification, examination and evaluation of information security related threats to assets, vulnerabilities and impacts on the organization, the Assessment Team will consider the following factors:

a) It is for the organization to define the criteria by which information security related threats to assets, vulnerabilities and impacts on the organization are identified as significant, and to develop procedure(s) for doing this.
b) The Assessment Team will require that the organization demonstrate that the analysis of security related threats is relevant and adequate for the operation of the organization.
c) Any observed inconsistency between the organization's policy, objectives and targets and its procedure(s) or the results of their implementation will be reported by the Assessment Team as non-compliance.

The Assessment Team will establish whether the procedures employed in risk analysis are sound and properly implemented. If an information security related threat to assets, or a vulnerability and or an impact on the organization is identified as being significant, it shall be managed within the ISMS.

The maintenance and evaluation of legal compliance is the responsibility of the organization. The Assessment Team will restrict itself to checks and samples in order to establish confidence that the ISMS functions in this regard. The Assessment Team will verify that the organization has evaluated legal and regulatory compliance and can show that action has been taken in cases of non-compliance with relevant regulations.

The Assessment Team interviews appropriate personnel of the organization to receive information on implementation of the ISMS. Evidence shall be collected through these interviews as well as through examination of documents and records and observation of activities and conditions. Conducting the interviews and verifying documentation and records may be supported by means of questionnaires drawn up by the Assessment Team for the particular assessment.

Detailed notes shall be taken (form ISMS/F08) to ensure that observations are correctly reported on completion of Assessment stage 2.
Areas where non-compliances appear to exist shall be examined in detail in order that the Assessment Team may accurately understand the situation.

Assessment observations of non-compliances

The proper treatment of observations of non-compliances is critical in any assessment. Assessment Team members shall make sincere efforts to state observations of non-compliances in a non-controversial and unbiased manner. The observations shall be stated clearly, unambiguously, and shall be based on supportive data and facts. The consent of the organization's representative should be sought regarding the data and facts leading to the non-compliance.
The non-compliances may be of the following types:

1) Adequacy and relationship of risk analysis, Statement of Applicability, objectives and targets, management responsibility, and design of the ISMS and their apparent non-compliance in actual practice.
2) Conditions that need corrective actions or which otherwise may result in non-compliance with the stated policies and practices.
3) Conditions for which compliance status cannot be ascertained e.g. due to lack of objective evidence.

Detailed notes shall be taken (form ISMS/F08) to ensure that observations (positive and negative) are correctly reported. An observed non-compliance is reported by raising a Nonconformity Report (ISMS/F04). The Nonconformity report shall include the following aspects:

- Exact observation of the facts
- Where it was found
- What was found
- Why it is a Nonconformity
- Reference to the clause of the standard or ISMS document.

Two categories of non-compliances are distinguished as follows:

- Major,
- Minor.

A Nonconformity should be classified MAJOR in the following situation:

- The absence of, or the failure to implement or maintain a required ISMS element, or objective evidence of a situation that would raise significant doubts as to the capability of the organization to achieve its Information Security policy and objectives. Too many minor non-compliances observed at one location of the organization and belonging to the same element of the standard or the ISMS constitute a major non-compliance.

A Nonconformity should be classified MINOR in the following situation:

- A single observed lapse or imperfection or weakness in fulfilling a requirement specified in the standard or the ISMS.

The following shall be ensured while raising Nonconformity reports:

a) The department, area, or functional unit where the non-compliance is noticed shall be made aware of the facts by the assessor before leaving the area.
b) It is preferable to raise a Nonconformity report on the spot. However, the issue might be too complex to do this and could require discussion with the team members before the report is formulated.
c) Non-compliances may be observed against more than one clause of the standard and/or the ISMS documentation. However, for the purpose of

accounting of the assessment results only the clause of the standard against which the non-compliance is most justified shall be identified in the appropriate column of form ISMS/F04. Possible other clauses shall be mentioned in text of the Nonconformity report.

d) Nonconformity reports are not classified as major or minor until the Assessment Team has discussed the issues during the team's preparation for the closing meeting.
e) Copies of Nonconformity reports shall be marked 'preliminary' and shall be handed over by the Team Leader to the organization's representative during the feedback meeting at the end of each assessment day.
f) The final decision on raising Nonconformity reports and their classification as major or minor shall be taken by the Assessment Team during the preparation for the closing meeting.

Preparation for the closing meeting

The Assessment Team shall review all collected assessment evidence to determine whether the ISMS conforms to the requirements of certification standard and the organization's policies, objectives and procedures.
The following applies during the team meeting:

- The Team Leader co-ordinates the meeting.
- Only members of the Assessment Team, including Technical Experts and possible observers appointed by the Certification body, shall be present.
- The team shall ensure that non-compliances are documented in a clear, concise and unambiguous manner and are supported by verifiable facts and data.
- The team classifies each Nonconformity report as major or minor.
- The Team Leader is empowered to make final decisions.
- Audit team based on the audit findings agrees and finalises the audit conclusions and any follow-up actions.
- Team leader confirms the appropriateness of the audit program and any changes in the same inn future audits.

Closing Meeting

The purpose of the closing meeting is to formally present the observations and conclusions agreed by audit team of the assessment to the organization.
The following applies to the closing meeting:

- The closing meeting is chaired by the Team Leader.
- An attendance list shall be circulated for completion by the participants.
- The Team Leader thanks the organization for hospitality and co-operation.
- Confidentiality of information and practices seen is emphasized.
- The scope of the activities covered by the ISMS is confirmed.
- The assessment method and its limitations (audit evidences are based on sampling) shall be explained.
- Non-compliances shall be presented and briefly explained, preferably by the assessors who observed the relevant facts and data.
- The Team Leader presents a summary, conclusions and the recommendation regarding certification.

- The Assessment Team answers any questions that the organization may have.
- The Team Leader explains the assessment reporting procedure.
- The Team Leader explains the requirements for corrective actions the timeframe for the client to present a plan for correction and corrective actions for any non-conformity identified during the audit.
- The Team Leader ensures that all Nonconformity reports are signed for receipt.
- Post audit activities of CB
- The team leader explains about the complaint and appeal handling processes.
- The client is given opportunity for questions. Any diverging opinion regarding the audit findings or conclusions between the audit team and client shall be discussed and resolved, if possible. The diverging opinions which can not be resolved shall be recorded and referred to Certification body.

6.2.4 Assessment stage 2 - Phase IV, Report, follow-up and close out

The Team Leader shall prepare a formal documented report of the assessment. The report shall cover in detail:

- Organization name, site, activities, IT infrastructure, scope of ISMS
- Assessment Team names and functions in team
- Assessment stage 2 date(s), place(s) and actual assessment schedule
- Any deviations from the audit plan & their reasons
- Any significant issues impacting on the audit programme
- A disclaimer statement indicating that auditing is based on sampling process of the available information
- Audited client is effectively controlling the use of certification documents and marks, if applicable
- Summary of assessment results including client's risk assessment and document review (as applicable).
- Recommendation of the audit team concerning certification
- Audit trails followed, positive (Strength) and negative (improvement opportunities) observations, comments on conformity and detailed description of non-compliances.
- Verification of the corrective actions regarding previously identified non-conformities, if applicable.

The report shall be concise, clear, and unambiguous in its statements.

Whenever audit team leader based on audit evidences determine that the audit objectives may not be achieved, the same is reported to the client and CB for appropriate action, which may include modification or reconfirmation including changes to audit plan, scope and objectives. The change of scope where applicable is discussed and confirmed with the audit client.

The Team Leader issues the report to the organisation and, requests for Root cause analysis and evidence of corrective action to be provided within two months from the date of the report or as deemed adequate by

the lead assessor depending on the business activities and IT infrastructure. The Team Leader shall announce that major non-compliances require on-site verification.

The organisation shall be informed that delay in providing corrective action will result in the Certification body having to repeat assessment stages 1 and 2 and charge for costs accordingly.

Upon receiving the evidence of corrective action and, if applicable, on-site verification of major non-compliances, the Team Leader draws up a summary report of the actions taken by the organisation. If the organisation does not close the raised issues within the reasonable timeframe & efforts of CB , certificate will be refused.

In case the CB is not able to verify the implementation of corrections and corrective actions of any major nonconformity within six months after the last day of stage-2, the certification body shall conduct another Stage-2 prior to recommending certification.

The Team Leader forwards the reports on assessment stages 1 and 2 including possible corrective action summary reports to the Certification Committee for decision on certification.

A three years Audit programme is prepared and maintained in client files by CB.