RECTO SOLUTIONS PVT. LTD.

ADDRESS: A2/544-B, Shiva Arcade, Acharya Niketan, Mayur Vihar Ph-1, Delhi - 110091, INDIA

GUIDELINES FOR AUDITING OF MANAGEMENT SYSTEMS

DOC.: RSPL/AG/01

Issue No.: 01

Date of Issue: 01-Sep-2023

STATUS OF AMENDMENTS

Amendment No.	Date of amendment	Clause	Page No.	Brief Description of amendment	Amendment approved by

TABLE OF CONTENTS

1. INTRODUCTION

This document is intended to provide guidance to the RSPL personnel conducting management systems audits of its clients for certification to Quality Management Systems (QMS) ISO 9001:2015 Standard / Environmental Management Systems (EMS) ISO14001:2015 Standard / Food Safety Management Systems (FSMS) ISO 22000:2018 Standard / Occupational Health & Safety Management System ISO 45001:2018 Standard, Information Security Management Systems (ISMS) ISO/IEC 27001:2022 and Educational Organization Management System (EOMS) 21001:2018 as applicable to the client.

2. SCOPE

This document provides guidance for personnel responsible for planning, carrying out, and documenting audits of clients' management systems e.g. quality, environmental, occupational health & safety, Information Security Management Systems and food safety management systems. The document covers the following areas and other related requirements on the follow-up of corrections, corrective, preventive, or improvement actions, as applicable. In addition, it describes the competence criteria that the audit team should meet.

a) The Certification Process
b) Code of Conduct
c) Auditors' Responsibilities
d) Initial Certification Audit i.e. Stage-1 and Stage-2 Audit
e) Conduct of Surveillance & Recertification Audit
f) Procedures for Reporting

3. PURPOSE

The purpose of this document is to:

- ✓ Harmonize and to provide guidance on auditing management systems of clients' organization;
- ✓ Help the RSPL develop their auditing procedures;
- ✓ Assist auditors and auditees in preparing for, facilitating and responding to audits.

4. REFERENCES

4.1. ISO 19011:2011: Guidelines for Auditing Management Systems

4.2. ISO/IEC 17021-1:2015: Conformity assessment —Requirements for bodies providing audit and certification of management systems: — Part 1: Requirements

4.3. ISO/IEC TS 17021-2: Conformity assessment —Requirements for bodies providing audit and certification of management systems: — Part 2: Competence requirements for auditing and certification of environmental management systems

4.4. ISO/IEC TS 17021-3: Conformity assessment —Requirements for bodies providing audit and certification of management systems: Part 3: Competence requirements for auditing and certification of quality management systems

4.5. ISO/IEC TS 17021-10:2018: Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 10: Competence requirements for auditing and certification of occupational health and safety management systems

4.6. ISO/TS 22003:2013: Food safety management systems –Requirements for bodies providing audit and certification of food safety management systems

4.7. ISO/IEC 27006:2015: Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

5. THE CERTIFICATION PROCESS

5.1. The Certification process consists of the following key stages:

a) Receipt of Enquiries,
b) Preparation of Quotations,
c) Client's Application for Certification,
d) Initial Certification Audit i.e. Stage-1 and Stage-2 Audit,
e) Surveillance Audit, and
f) Recertification Audits

5.2. Enquiries are received in several forms, by telephone, letter or facsimile. If they fall within RSPL scope of accreditation by UAF or others – these result in the sending out of an Information Brochure pack, including an application form to be completed for the purpose of providing a quotation of fees for certification based upon the information made available to be submitted to the client for acceptance.

5.3. Upon acceptance of the fee quotation, the client completes and submit the "Application Form for Certification" together with the Application fee upon receipt of which Technical Coordinator verifies the relevant details of the client's application with the fee quotation and completes a supplementary Application/Contract Review including allocation of the scope sector of the clients activities coming under the applied scope of registration with the original Questionnaire to check that there is no discrepancy.

5.4. Initial Certification Audit
The initial certification audit of a management system is normally conducted in two stages: Stage-1 and Stage-2 audit.

5.4.1. Stage-1 Audit

5.4.1.1. The Stage-I audit is performed to:

a) Review the client's management system documented information against the requirements of the relevant ISO 9001 / ISO 14001 / ISO 22000 / ISO 45001 / ISO/IEC 27001 / EOMS 21001 Standard;
b) Evaluate the client's site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for stage-2 audit;
c) Review the client's status and understanding regarding requirements of the relevant standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the management system;
d) Obtain necessary information regarding the scope of the relevant management system, including:
- ✓ The client's site(s);
- ✓ Processes and equipment used;
- ✓ Levels of controls established (particularly in case of multisite clients);
- ✓ Applicable statutory and regulatory requirements;

e) Review the allocation of resources for stage 2 audit and agree the details of stage 2 audit with the client;
f) Provide a focus for planning Stage -2 audit by gaining a sufficient understanding of the client's management system and site operations in the context of the relevant 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 relevant management system substantiates that the client is ready for stage 2 audit.

5.4.1.2. A report on the documentation of the relevant management system with regard to fulfilment of the Stage-1

requirements and the readiness for Stage-2 audit will be communicated to the client, including identification of any areas of concern that could be classified as nonconformity during stage 2 audit.

5.4.1.3. It is expected that the relevant management system has been in place for at least about three months before the Stage-1 audit is considered.

5.4.1.4. A period of two to three weeks is normally recommended between Stage-1 and Stage-2 visits but the certification audit is to be scheduled on a mutually convenient date upon client's intimation of readiness and the number of days required to resolve the areas of concern identified during Stage-1 audit.

5.4.2. Stage-2 Audit

5.4.2.1. Planning for Stage-2 audit

5.4.2.1.1. Stage-2 audit is only undertaken on effective closure by the client's areas of the concerns raised during the Stage-1 audit. In some cases, depending on the outcome of the Stage-1 audit, there may be needed to amend the previously done application/contract review.

Planning for Stage-2 audit normally includes:

- **a)** Dates for audit/assessment;
- **b)** Required number of audit man-days;
- **c)** Constitution of audit/assessment team, including Technical Expert, if required;
- **d)** Location(s)/site(s) of audit

5.4.2.1.2. Stage-2 audits are scheduled on dates agreed with the client during the Stage-1 audit. Client is advised of the above details in advance for his confirmation and acceptance including the audit team members.

5.4.2.1.3. A detailed Audit Plan, giving the allocation(s) of the audit, name of audit team members, Technical Expert (if required) and the time schedules for various audit activities/departments/processes is forwarded to the client in advance together with the agreed traveling arrangements.

5.4.2.1.4. The audit Team Leader is responsible for the detailed planning, organizing and execution of the audit plan. The audit plan is based upon the competence of the audit team members and audit man-days requirements after the application/contract review and as per the outcome of Stage-1 review and is designed to verify the relevant clauses/requirements of the applicable standard and give the appreciate areas of the client's organization.

5.4.2.2. Purpose of Stage-2 Audit

The purpose of the Stage-2 is to evaluate the implementation, including effectiveness, of the client's management system relevant to applicable ISO 9001 / ISO 14001 / ISO 22000 / ISO 45001 / ISO/IEC 27001 / EOMS 21001 standard or any other management system. The Stage-2 audit is normally take place at the site(s) of the client. The Stage-2 audit includes the auditing of at-least of the following:

- **a)** Information and evidence about conformity to all requirements of the applicable management system standard or other normative documents;
- **b)** Performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative documents)
- **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;
g) Scope of activities is also to be verified for various products items, processes covered and verified for the implementation with records references as required.

5.4.3. Initial Certification Audit Conclusion

5.4.3.1. After conducting Stage-1 and Stage-2 audit, the audit team is required to analyse all information and audit evidence gathered during Stage-1 and Stage-2 audit to review the audit findings and agree on the audit conclusions.

5.4.3.2. All the objective evidence of compliance and any non-compliance identified with the requirements of the relevant management system standard are required to be brought to the attention of the auditee and noted on the report format by the auditors. At the end of assessment, these are to be discussed along with the improvement suggestions (if any) and the client's management representative is asked to sign the report acknowledging that he understands and accepts the findings.

5.4.3.3. The assessment is concluded with a "Closing Meeting" in which the Team Leader presents the findings and makes recommendations, either for certification to the applicable management system standard or otherwise with a requirement for a verification audit in case of non-conformances having been identified.

5.4.3.4. In case non-conformances are identified during the audit, RSPL will provide a detailed report to the client and request the client to complete the correction and corrective action plan (CAP) in detail, including proposed time frame for effective implementation of the corrective actions. The client must submit the completed correction and corrective action plan within 21 days of completion of the audit visit. The organisation has a maximum of 30 days from the last day of the audit to provide evidence of effective correction and corrective action. Verification may require an on-site visit or a desktop review of documents, depending on the seriousness of the Non-conformance. During initial certification, failure to effectively close a non-conformance may trigger a repeat of the Stage-2 audit. For any existing certification, failure to close a non-conformance may result in the withdrawal of the organisation's certification approval.

5.4.3.5. Each certified client is required to undergo a surveillance audit at minimum intervals of one year, during the term of validity of its certification. The continual conformance of the client's organization management system with the relevant certification standard is verified by auditing selected elements of the applicable management system at each visit besides verification of the effective action for the suggested improvement during the previous audit.

5.4.3.6. Auditors are required to complete the audit reports in a precise and accurate manner. The justification for non-inclusion of any element as per the management system standard e.g. Design & Development etc. (e.g. ISO-9001) should be carefully verified and recorded in the audit report.

6. CODE OF CONDUCT

6.1. Auditors should understand that they are visiting the client's organization as representatives of RSPL and their conduct must reflect professional and ethical standards of the highest order. Auditors are expected to:
a) Be smartly dressed and well groomed;
b) Be calm and polite during communication;
c) Be well prepared and objective in conducting the audits ensuring effective time management;
d) Be direct and decisive;
e) Seek objective evidence of compliance and non-compliance;

f) Use only RSPL documents and formats;

Auditors are required to declare a denial of their involvement in providing consultancy or professional interest of any company before undertaking an auditing assignment in the client's organization. Auditors are not expected to:

a) Correspond directly with the client unless authorized by Recto Solutions Pvt. Ltd.

b) Offer advice that may be interpreted as consultancy to the client's organization being assessed.

7. AUDITORS' RESPONSIBILITY

7.1. For each assessment a Team Leader (TL) is nominated who is responsible for the management of the audit and observes the performance and conduct of each of the auditor and/or Observers/Technical Expert present on behalf of RSPL.

7.2. The Team Leader is responsible for planning and conduct of the audit. Team Leader is also responsible for ensuring that all relevant information concerning the assessment is reported.

7.3. Team Leader shall allocate tasks to each member of the audit team and Team Leader shall ensure that the members of the team are fully prepared and capable of undertaking the auditing functions professionally and effectively. Assessment recommendations are arrived at by the audit team at the pre-closing meeting where the Team Leader will debrief all the auditors. The final report & recommendation, however, shall be decided by the Team Leader himself.

7.4. During the planning phase of the auditing process, the Team Leader and other members may prepare individual audit check lists for evaluating the relevant management system elements assigned to them. These lists should be filled up in a manner as to provide evidence of an in-depth probe into quality systems. These should also bring out evidence of both positive and negative findings about the client's applicable management systems.

7.5. The Team Leader should ensure that the completed check lists and rough notes of each auditor are attached to the audit reports before forwarding the same to RSPL.

8. AUDIT PLANNING/PREPARATION

8.1. Audit Plan Matrix

The team has to prepare in advance a matrix of the elements of the relevant management system standard against the departments/functions to be audited. Matrix should have judicious cross reference to the auditees' activities.

8.2. Audit Programme

8.2.1. After ascertaining the geographical location of various departments and functions of the client's organization and their quantum of work, the Team Leader should allocate time and auditing function to each auditor, including allocation of technical experts, if any, for critical areas of the auditees' activities in the Audit Plan. The Team Leader is required to discuss the Audit Plan with the Audit Team members and the Technical Experts, during Audit Team briefing before the commencement of the Audit.

8.2.2. Audit Plan and composition of Audit Team details are advised to the client's management and its representative in advance for their acceptance and the same is explained in details at the time of opening meeting.

8.3. Check list/Recording of Observations/Use of RSPL Audit Report Documents & Formats

The Team Leader should advise the team members to prepare their individual check lists relating to their assigned audit areas/functions. This check list should be based on the type of industry/NACE Codes and the Scope of Management System Certification. Further, it may also be based upon the criticality of the function/product/process and it's bearing on the

relevant management systems e.g. Quality/Environment/Occupational Health & Safety/Information Security/Food Safety.

Assessment checklists for all the schemes of certification viz. ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 22000:2018, ISO/IEC 27001:2022 and ISO 21001:2018 standards are provided with these guidelines for the guidance of the auditing personnel.

8.4. Guidance Documents

8.4.1. Audit team members should study sector/technical area specific guidance materials well before the audit. Based on this, clauses/requirements of the applicable management system standard which become critical because of the peculiar requirements of the sector specific industry should also be identified.

8.4.2. RSPL normally arranges, where necessary, sector or technical area specific guidance including checklists or briefing notes relevant to the auditing of industry scope/sectors as per IAF Code Classification with the assistance of the technical experts or from any other sources e.g. internet, in that field. RSPL has maintained adequate database of technological information, applicable legal requirements, processes, environmental aspects and impacts and occupational, health & safety information in respect of various sectors and technical areas for the assistance and guidance for its personnel involved in certification activities.

8.5. Audit Scope

8.5.1. If the scope covers installation & commissioning activities, the planning matrix should include onsite verification. If the client's certification scope includes design & development requirements, special care is to be taken in earmarking the team member with experience in design & development. Further the team leader should ensure that adequate amount of time is allotted for this function.

8.5.2. The Team Leader should confirm the scope of certification applied for, with the client, during the opening meeting. In the event an amended scope involving a major addition or change to the original scope is proposed by the client, the Team Leader should seek instructions from RSPL office before proceeding for the assessment, as an amended scope may require additional audit man-days or sector scope competence. Minor changes in the scope of certification may, however, be accepted for assessment and reported, accordingly.

9. AUDIT EXECUTION

9.1. Time Management

Good planning by preparation of Audit Plan Matrix, RSPL Programme sheet and check lists prior to the commencement of the audit will ensure that team does not waste any time during the execution of the audit. An itinerary will be prepared by RSPL for each audit giving tentative time schedule, covering clauses/requirements of the relevant management system standard and name of the auditor for guidance of audit team and auditee. This will be issued 7 to 10 days in advance. In case of integrated management system audit common clauses/requirements may be suitably clubbed under a single auditor to avoid duplication of effort.

9.2. Check on Interface Activities

Good planning and thorough preparation by detailed study of the various functions/departments of the client's organization will ensure that its interface activities are covered. While conducting audit in one department/function, do not see it in isolation, but See with which other functions, it is inter-related/inter-dependent/interacting. It is essential that we look into these areas/interfaces during our audits.

9.3. In-depth Probing/Questioning

Auditors should seek objective evidence of compliance of each audit function with the relevant management system

standards and scope of certification by in-depth verification of the related documents, operations and processes (e.g. note an instrument in production area with calibration sticker duly affixed and check its calibration status in Calibration laboratory. Note down particulars of an operator who is not performing as per work instructions and look for his training records in HRD) and seek objective evidence. This should be compared with the relevant clause of the management system standard in order to arrive at Non-conformities (NCs). This should be agreed to by the auditee during the execution of Audit. In case of ISO 9001 Quality Management Systems certification audit, any clause/requirement being considered not applicable to the client's operations, a suitable explanation is required to justify the exclusion of the clause/requirement of the standard from the audit in the audit report.

9.4. Audit Trail

Audit plan for each auditee function relevant to the clauses of the required certification standard should provide for audit to be conducted in a logical sequence, consistent with the flow of work rather than leap forging. For example, in case of ISO 9001 standard, auditors nominated for production areas may cover in one sequence planning, issue of material, preparation of material, machine shop, fabrication, assembly and final inspection. When auditing Q.C./Inspection/Testing department, verify the calibration status of the monitoring and measuring equipment from the Calibration Department.

10. CONDUCTING AUDITS

10.1. General

The Team Leader and other audit team members will ensure that due caution are exercised in complying with the following requirements when conducting management systems audits. The following process for conducting on-site audits has been established by RSPL. The process normally 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 to be made by electronic means or where the site to be audited is virtual, such activities will be conducted by a competent auditor deputed by RSPL. The auditor is required to ensure that the evidence obtained during such an audit is sufficient to take an informed decision on the conformity of the requirement in question.

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

10.2. Conducting of Opening Meeting

A formal Opening Meeting will be conducted by the Audit Team Leader with the client's management and, where appropriate, those responsible for the functions or processes to be audited. The purpose of the opening meeting is to provide a short explanation of how the audit activities will be undertaken. The detail of explanation during the opening meeting should be consistent with the familiarity of the client with the audit process and the following points are required to be addressed:

- **a)** Introduction of 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 such as room, transport, tea, lunch, etc. are available;
- **f)** Confirmation of matters relating to confidentiality;
- **g)** Confirmation of relevant work safety, emergency and security procedures for the audit team;
- **h)** Confirmation of the availability, roles and identities of any guides and Observers;
- **i)** The method of reporting, including any grading of audit findings;

j) Information about the conditions under which the audit may be prematurely terminated;
k) Confirmation that the audit team leader and audit team representing the certification body (RSPL) is responsible for the audit and will be in control of executing the audit plan including audit activities and audit trails;
l) Confirmation of the status of findings of the previous review or audit, if applicable;
m) Methods and procedures to be used to conduct the audit based on sampling;
n) Confirmation of the language to be used during the audit;
o) Confirmation that, during the audit, the client will be kept informed of audit progress and any concerns;
p) Opportunity for the client to ask questions.

10.3. Auditing Process

10.3.1. The audit of the management system is to be conducted against the requirements of the applicable management system standard (ISO 9001 / ISO 14001 / ISO 22000 / ISO/IEC 27001 / ISO 45001 / ISO 21001 etc.) on a sampling basis by covering all the clauses/requirements of the relevant management system standard and other normative requirements. The assessment is concerned with establishing that the client's documented Management System is well established and implemented in accordance with the requirements of the applicable management system standard i.e. ISO 9001 / ISO 14001 / ISO 22000 / ISO/IEC 27001 / ISO 45001 / ISO 21001 etc. The audit should also include a verification of the legal/statutory requirements applicable to the client's products and/or services and its compliance in the client's organization.

10.3.2. The Audit team accompanied by the company's representative shall start their audit in the designated areas/processes/functions at random by selecting a feature relevant to the appropriate requirement of the applicable management system standard against which the client's organization is to be audited, and proceed according to the audit programme ensuring that the audit takes account of all requirements of applicable management system standard(s) and any other applicable normative document. The team members shall keep in mind the possibility that some elements may overlap over more than one department's functions.

10.4. Communication during the audit

10.4.1. During the audit, the audit team is required to periodically assess audit progress and exchange information. The audit team leader may reassign work as needed between the audit team members and periodically communicate the progress of the audit and any concerns to the client's management representative.

10.4.2. Where the available audit evidence indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk (e.g. safety), the audit team leader is required to report this to the client's management representative and, if possible, to the CEO of RSPL 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 is required to report the outcome of the action taken to the CEO of RSPL.

10.4.3. The audit team leader is required to review with the client's management representative any need for changes to the audit scope which becomes apparent as on-site auditing activities progress and report this to the CEO of RSPL.

10.5. Obtaining and verifying information

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

10.5.2. The following methods are required to be used to obtain information, but may not be limited to:
a) Interviews;

b) Observation of processes and activities;
c) Review of documentation and records.

10.6. Identifying and recording audit findings

10.6.1. Audit findings summarizing conformity and detailing nonconformity are required to be identified, classified and recorded to enable an informed certification decision to be made or the certification to be maintained.

10.6.2. Opportunities for improvement may be identified and recorded, unless prohibited by the requirements of the applicable management system certification scheme. Audit findings, however, which are nonconformities, are not required to be recorded as opportunities for improvement.

10.6.3. A finding of nonconformity is required to be recorded against a specific requirement, and it must contain a clear statement of the nonconformity, identifying in detail the objective evidence on which the nonconformity is based. Nonconformities are required to be discussed with the client's management to ensure that the evidence is accurate and that the nonconformities are understood. The auditor however is required to refrain from suggesting the cause of nonconformities or their solution.

10.6.4. The audit team leader is required to attempt to resolve any diverging opinions between the audit team and the client concerning audit evidence or findings, and unresolved points shall be recorded.

10.7. Preparing audit conclusions

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

a) Review the audit findings, and any other appropriate information obtained 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 for future audits (e.g. Scope of certification, audit time or dates, surveillance frequency, audit team competence).

10.8. Conducting the closing meeting

10.8.1. A formal closing meeting, where attendance is to be recorded, to be held with the client's management and, where appropriate, those responsible for the functions or processes audited. The purpose of the closing meeting, usually conducted by the audit team leader, is to present the audit conclusions, including the recommendation regarding certification. Any nonconformity observed during the audit is to be presented in such a manner that they are understood, and the timeframe for responding is to be agreed.

NOTE *"Understood" does not necessarily mean that the nonconformities have been accepted by the client.*

10.8.2. The following elements are also to be included in the closing meeting:
a) Advising the client that the audit evidence obtained 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 corrective action plan (CAP) for correction and corrective action for any nonconformities identified during the audit;
e) The certification body's post audit activities;

f) Information about the complaint and appeal handling processes.

10.8.3. The client is to be given opportunity for questions. Any diverging opinions' regarding the audit findings or conclusions between the audit team and the client is required to be discussed and resolved where possible. Any diverging opinions that are not resolved are to be recorded and referred to RSPL, the certification body.

10.9. Audit report

10.9.1. RSPL, the certification body will provide a written report for each audit to the client. The audit team may identify opportunities for improvement but will not recommend any specific solutions. The ownership of the audit report lies with RSPL, the certification body.

10.9.2. The audit team leader is required to ensure that the audit report is prepared and is responsible for its content. The audit report must provide an accurate, concise and clear record of the audit to enable an informed certification decision to be made and it must include the following:

a) Identification of the certification body;
b) The name and address of the client and the client's 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;
g) Any deviation from the audit plan and their reasons;
h) Any significant issues impacting on the audit programme;
i) Identification of the audit team leader, audit team members and any accompanying persons;
j) The dates and places where the audit activities (on site or offsite, permanent or temporary sites) were conducted;
k) After stage-1 Audit findings (ISO 9001 / ISO 14001 / ISO 22000 / ISO/IEC 27001 / ISO 45001 / ISO 21001) (see 10.6), reference to evidence and conclusions, consistent with the requirements of the type of audit;
l) Significant changes, if any, those affect the management system of the client since the last audit took place;
m) Any unresolved issues, if identified;
n) Where applicable, whether the audit is combined, joint or integrated;
o) A disclaimer statement indicating that auditing is based on a sampling process of the available information;
p) Recommendation from the audit team
q) The audited client is effectively controlling the use of the certification documents and marks, if applicable;
r) Verification of effectiveness of taken corrective actions regarding previously identified nonconformities, if applicable;
s) A statement on the conformity and the effectiveness of the management system together with a summary of the evidence relating to:
  i. The capability of the management system to meet applicable requirements and expected outcomes;
  ii. The internal audit and management review process;
t) A conclusion on the appropriateness of the certification scope;
u) Confirmation that the audit objectives have been fulfilled.

10.10. Cause analysis of nonconformities

The client is required to analyse the cause and describe the specific correction and corrective actions taken, or planned to be taken, to eliminate detected nonconformities and submit a Corrective Action Plan (CAP), within a defined time, which is normally within 2 weeks.

10.11. Effectiveness of corrections and corrective actions

10.11.1. The certification body will review the corrections, identified causes and corrective actions submitted by the client to determine if these are acceptable. The certification body will verify the effectiveness of any correction and corrective actions taken. The evidence obtained to support the resolution of nonconformities will be recorded. The client will be informed of the result of the review and verification. The client will be 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.

10.11.2. 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.

10.12. Recommendation by Audit Team

10.12.1. Non-grant of Certification: In the event of there being non-conformities which are considered to render the management system deficient and inoperable, a recommendation for certification should not be made. Depending upon the extent and nature of deficiencies, a recommendation for a supplementary audit for verification of corrective actions or reassessment may be made. A client **will not be recommended for grant of certification unless it has demonstrated effective implementation** of the requirements of the applicable management system standard particularly an Internal Audit programme and the Management Review process. The audit team leader is required to ensure that non-compliances and matters of concern are recorded in the Executive Summary of the audit report and the Non-conformities are reported in the non-conformance format. These should be recorded objectively and precisely.

10.12.2. Where recommendation for certification to the applicable management system standard was not being granted, the audit team leader will discuss further action with the client. Such action is left to the audit team leader's discretion and may be anything from a "follow-up action" in areas of non-compliance to a total re-assessment depending on the severity of the deficiencies.

10.12.3. In the case of a 'follow-up' action (limited re-assessment) the Team Leader will agree on a re-visit date with the client and be responsible for drafting the re-assessment programme, based on the non-compliances raised. The Team Leader MUST state the duration of the limited re-assessment i.e. 1 audit man-day or 2 audit man-days in his recommendation and the maximum time limit will be approx. 60 days from the date of conduct of the audit.

10.12.4. Right to Appeal against Non-granting of Certification

In case when the audit team's recommendation is for non-grant of certification, the client must be advised of their **"RIGHT TO APPEAL"** and availability of information about the complaint handling and appeal processes on the RSPL web sites. The client is required to submit its appeal within 14 days in writing to the CEO of RSPL, the certification body. The CEO will refer the appeal to the Expert Committee which will constitute a separate Appeals Panel. The Appeals Panel decision will be final.

10.12.5. Recommendations for Certification

10.12.5.1. In the event of nonconformities being identified in respect of the implementation of any clause/requirement of the applicable management system standard, a recommendation for certification is to be made subject to a Corrective Action Plan (CAP) being submitted within 2 weeks and corrective actions being verified onsite and closed out through a special visit within 30 days of the audit date, or as decided by CEO of the certification body.

10.12.5.2. In case when "opportunities for improvement" have been raised and recorded during the certification audit, the actions, as applicable, are verified for the effectiveness at the subsequent audit visit.

11. CERTIFICATION DECISION

11.1. General

RSPL, the certification bodies always ensure that the persons or committees that make the decisions for granting or refusing certification, expanding or reducing the scope of certification, suspending or restoring certification, withdrawing certification or renewing certification are different from those who carried out the audits. RSPL also ensure that the individual(s) appointed to conduct the certification decision have appropriate competence.

The person(s) assigned by RSPL to make a certification decision are either employed by, or are under legally enforceable arrangement with these certification bodies. These persons have to fulfil the same requirements as persons employed by, or under contract with these certification bodies.

RSPL maintain record of each certification decision including any additional information or clarification sought from the audit team or other sources.

11.2. Actions Prior to Making a Decision

RSPL conduct an effective review prior to making a decision for granting certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing of certification, on the basis of:

- **a)** The information provided by the audit team is sufficient with respect to the certification requirements and the scope for certification;
- **b)** Any major nonconformities, it has reviewed, accepted and verified the correction and corrective actions;
- **c)** Any minor nonconformities it has reviewed and accepted the client's plan for correction and corrective action.

11.3. Information for granting initial certification

11.3.1. The information provided by the audit team to RSPL, for the certification decision must include, as a minimum:

- **a)** The audit report;
- **b)** Comments on the nonconformities and, where applicable, the correction and corrective actions taken by the client;
- **c)** Confirmation of the information provided by the client to RSPL which was used in the application (contract) review;
- **d)** Confirmation that the audit objectives have been achieved;
- **e)** A recommendation whether or not to grant certification, together with any conditions or observations.

11.3.2. If RSPL 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, the certification body will conduct another Stage-2 prior to recommending certification.

11.4. Information for granting recertification

RSPL make decisions on renewing certification based on the results of the recertification audit, as well as the results of the review of the applicable management system over the period of certification and complaints received from users of certification.

12. MAINTAINING CERTIFICATION

12.1. RSPL maintain client's certification based on demonstration that the client continues to satisfy the requirements of the applicable management system standard. Client's certification is maintained on the basis of a positive conclusion by the audit team leader without further independent review and decision, provided that:

there is no any major nonconformity or other situation that may lead to suspension or withdrawal of certification and need to initiate a review by competent personnel, different from those who carried out the audit, to determine whether certification can be maintained;

Competent personnel of the certification body monitor its surveillance activities'; including monitoring the reporting by its auditors, to confirm that the certification activity is operating effectively.

12.2. Surveillance Activities

12.2.1. RSPL conduct its surveillance activities so that representative areas and functions covered by the client's scope of the applicable management system certification scheme are monitored on a regular basis, and take into account changes to its certified client and its management system.

12.2.2. Surveillance activities normally include on-site auditing of the certified client's management system's fulfilment of specified requirements with respect to the applicable standard to which the certification is granted. Other surveillance activities may include:

- **a)** Enquiries from the certification body to the certified client on aspects of certification;
- **b)** Reviewing any certified 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);
- **d)** Other means of monitoring the certified client's performance.

12.3. Surveillance Audit

Surveillance audits are on-site audits, but are not necessarily full system audits, and are normally planned together with the other surveillance activities so that the certification body can maintain confidence that the client's certified management system continues to fulfil requirements between recertification audits. Each surveillance audit for the relevant management system standard normally 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;
- **h)** Use of certification marks and/or any other reference to certification.

12.4. Recertification

12.4.1. Recertification audit planning

12.4.1.1. 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/scheme or other normative document. This is being planned and conducted in due time to enable for timely renewal before the certificate expiry date.

12.4.1.2. The recertification activity normally includes the review of previous surveillance audit reports and considers the performance of the management system over the most recent certification cycle.

12.4.1.3. Recertification audit activities may need to have a Stage-1 in situations where there have been significant changes to the client's management system, the organization, or the context in which the management system is operating (e.g. changes to legislation).

NOTE: *Such changes can occur at any time during the certification cycle and the certification body might need to perform a special audit, which might or might not be a two-stage audit.*

12.4.2. Recertification Audit

12.4.2.1. 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).

12.4.2.2. For any major nonconformity, the client is required to submit Corrective Action Plan (CAP) within 2 weeks and corrective actions being verified onsite and closed out through a special visit within 30 days of the audit date, or as decided by CEO of the certification body. These actions are required to be implemented and verified prior to the expiration of certification.

12.4.2.3. When 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 will be on or after the recertification decision.

12.4.2.4. In case RSPL could not complete the recertification audit or the 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 will not be recommended and the validity of the certification will not be extended. The client will be informed and the consequences will also be explained.

12.4.2.5. Following expiration of certification, RSPL can restore certification within 6months provided that the outstanding recertification activities are completed, otherwise at least a Stage-2 will be conducted. The effective date on the certificate will be on or after the recertification decision and the expiry date shall be based on prior certification cycle.

12.4.3. Special Audits

12.4.3.1. Expanding scope

RSPL, in response to an application from the certified client for expanding the scope of a certification already granted, will undertake a review of the application and determine if any audit activities necessary to decide whether or not the extension may be granted. This may be conducted in conjunction with a surveillance audit.

12.4.3.2. Short-Notice Audits

If in case it is necessary for the RSPL 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, then in such cases RSPL:

a) Will describe and make known in advance to the certified clients the conditions under which such audits will be conducted; and

b) Will exercise additional care in the assignment of the audit team because of the lack of opportunity for

the client to object to audit team members.

12.4.4. Suspending, withdrawing or reducing the scope of certification

12.4.4.1. RSPL normally suspends certification in cases when, for example:

a) The client's certified management system has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the management system.

b) The certified client does not allow surveillance or recertification audits to be conducted at the required frequencies;

c) The certified client has voluntarily requested a suspension.

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

12.4.4.3. RSPL restores 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 the certification body will result in withdrawal or reduction of the scope of certification.

NOTE: *In most cases, the suspension would not exceed six months.*

12.4.4.4. RSPL can reduce the scope of certification to exclude the parts not meeting the requirements, when the certified client has persistently or seriously failed to meet the certification requirements for those parts of the scope of certification. Any such reduction will be in line with the requirements of the applicable standard used for certification.

13. PERFORMANCE EVALUATION

13.1. Performance Evaluation of Audit Team Members

The Audit Team Leader will evaluate each member/observer as per the need/guidance from RSPL office of his team against the various parameters. The performance reports should be forwarded separately to the CEO of RSPL and these will be treated confidentially. The Reporting Auditor may suggest any training need, where necessary.

13.2. Performance Evaluation of Auditor / Leaders

The performance of Team Leaders will be verified through Witness Audits independently by Senior Lead Auditors nominated by CEO of RSPL, who will report on the Auditor's performance. Each Auditor's performance is normally verified once a year, and that of Lead Auditor once in 3 years.

13.3. Performance Evaluation of Trainee Auditors

a) All auditors who are qualified as an approved Lead Auditor/Assessor for ISO 9001 / ISO 14001 / ISO 22000 / ISO/IEC 27001 / ISO 45001 / ISO 21001 and fulfilled the other qualification and knowledge & skills criteria for empanelment of external auditors are required to obtain auditing experience for 20 audit man-days before qualifying them for assignment as an audit team member for that management system in which he/she qualified as Lead Auditor/Assessor on behalf of RSPL.

b) The requisite audit experience is obtained through attachment with audit teams for conduct of third party audits of management systems including documentation review, certification and surveillance audits.

c) Trainee auditors are assigned for working strictly under the direction and supervision of the assigned Team Leader and do not undertake any audit function, independently, during training.

d) The Team Leader is responsible for ensuring that the Trainee Auditor is guided and trained in the methodology and practical conduct of all aspects of auditing of a management system as per ISO 9001 / ISO 14001 / ISO 22000 / ISO/IEC 27001 / ISO 45001 / ISO 21001 standards.

e) The Team Leader is required to assess the understanding and performance of the 'Trainee Auditor' under his

supervision and report on his compliance with the various attributes and skills as per RSPL Performance Report including recommendation for desirable corrective actions, training and improvement.

f) The performance report is required to be forwarded for each audit by the Team Leader in respect of each Trainee Auditor for review by the RSPL office and record. The Trainee Auditor will be advised of any deficiencies and requirement of training in specific area for improvement in his performance.

g) Upon completion of the requisite man-days of auditing, overall performance of the 'Trainee Auditor' is evaluated to confirm his up gradation to the Audit Team Member's grade or recommend further training, if necessary.

h) The up gradation of 'Trainee Auditor' will be duly recorded and his name entered in the RSPL list of Approved Auditors.

14. Technical Experts

Technical Experts (TE) are selected for a specific technical area/sector and assigned as and when required. Their appointment as Technical Expert is based on their Technical/Professional Qualification, Industry experience, knowledge& skills and expertise in that specific technical area. Their expertise is also verified during the audit in that technical area.

Annex. 1: Assessment Checklist for Quality Management Systems (ISO 9001:2015)

4. Context of the organization

- ✓ Has the organization determined the external and internal issues that are relevant to the organization's purpose and the achievement of customer satisfaction and the organization's strategic direction?
- ✓ Does the organization have a way of reviewing and monitoring these on a regular basis?
- ✓ Has the organization determined the needs and expectations of interested parties that are relevant to the Quality Management System (QMS)?
- ✓ Has the scope of the QMS been determined taking into account the external and internal issues, interested parties and the organization's products and services?
- ✓ Has the organization QMS been established including the processes needed and their sequence and interaction?
- ✓ Have the criteria for managing these been established together with responsibilities, methods, measurements and related performance indicators needed to ensure the effective operation and control?

5. Leadership

- ✓ Has the organization's top management taken accountability for the effectiveness of the QMS?
- ✓ Have the policy and objectives for the QMS, which are compatible with the strategic direction of the organization, been established and communicated?
- ✓ Have the objectives been established at relevant departmental and individual levels with the business?
- ✓ Have the requirements for the QMS been integrated into the business processes and have management promoted awareness of the process approach?
- ✓ Have customer requirements and applicable statutory and regulatory requirements been determined, met and communicated throughout the organization?
- ✓ Have the risks and opportunities that are relevant to the QMS been established?
- ✓ Has the organization established and communicated the responsibilities and authorities for the effective operation of the QMS?

6. Planning

- ✓ Have the risks and opportunities that need to be addressed to give assurance that the QMS can achieve its intended result(s) been established?
- ✓ Has the organization planned actions to address these risks and opportunities and integrated them into the system processes?
- ✓ Is there a defined process for determining the need for changes to the QMS and managing their implementation?

7. Support

- ✓ Has the organization determined and provided the resources needed for the establishment, implementation, maintenance and continual improvement of the QMS (including people, environmental and infrastructure requirements)?
- ✓ If monitoring or measuring is used for evidence of conformity of products and services to specified requirements, has the organization determined the resources needed to ensure valid and reliable monitoring and measuring of results?
- ✓ Has the organization determined the knowledge necessary for the operation of its processes and achievement of conformity of products and services and implemented a lessons learnt process?
- ✓ Has the organization ensured that those persons who can affect the performance of the QMS are competent on the basis of appropriate education, training, or experience or taken action to ensure that those persons can acquire the necessary competence?
- ✓ Has the documented information required by the standard and necessary for the effective implementation and operation of the QMS been established?

8. Operation

- ✓ Is there a defined process for the provision of products and services that meet requirements defined by the customer?

- ✓ When changes are planned are they carried out in a controlled way and actions taken to mitigate any adverse effects?
- ✓ Are any outsourced processes managed and controlled?
- ✓ Is there a defined process for reviewing and communicating with customers in relation to information relating to products and services, enquiries, contracts or order handling?
- ✓ Is there review conducted prior to the organization's commitment to supply products and services?
- ✓ If the organization design and develop products or services, are these processes established and implemented in line with the requirements of the standard?
- ✓ Does the organization ensure that externally provided processes, products, and services conform to specified requirements?
- ✓ Does the organization have criteria for the evaluation, selection, monitoring of performance and re-evaluation of external providers?
- ✓ Is the provision of products and services carried out in controlled conditions? which include:
  - The availability of documented information that defines the characteristics of the products and services?
  - The availability of documented information that defines the activities to be performed and the results to be achieved?
  - Monitoring and measurement activities at appropriate stages to verify that criteria for control of processes and process outputs, and acceptance criteria for products and services, have been met?
  - The people carrying out the tasks are competent?
- ✓ Does the organization have effective methods of ensuring traceability during the operation process?
- ✓ Where property belonging to customers or external providers is used in the provision of the product or service, is this controlled effectively?
- ✓ If there is a requirement for post-delivery activities associated with the products and services such as warranty, maintenance services, recycling or final disposal, are these defined and managed?
- ✓ Are any nonconforming process outputs managed so as to prevent their unintended use?

9. Performance evaluation

- ✓ Has the organization determined:
  - What needs to be monitored and measured and
  - The methods for monitoring, measurement, analysis and evaluation, to ensure valid results?
- ✓ Has it established when the results from monitoring and measurement shall be analysed and evaluated?
- ✓ Have methods of monitoring customer perceptions of the provision of products and services been established?
- ✓ Has it determined the need or opportunities for improvements within the QMS and how these will be fed into management reviews?
- ✓ Has the organization established a process for an internal audit of the QMS?
- ✓ Has an approach to perform management reviews been established and implemented?

10. Improvement

- ✓ Has the organization determined and selected opportunities for improvement and implemented the necessary actions to meet customer requirements and enhance customer satisfaction?
- ✓ Has the organization determined appropriate processes for managing nonconformities and the related corrective actions?
- ✓ Has the organization decided on how it will address the requirement to continually improve the suitability, adequacy, and effectiveness of the QMS?

Annex. 2: Assessment Checklist for Environmental Management Systems (ISO 14001:2015)

4. Context of the organization

- ✓ Has the organization undertaken a review to determine fully the external and internal issues that are relevant to establishing the context of the organization?
- ✓ Has the organization undertaken a review to identify interested parties, to understand their needs and expectation and which of these, if any, they will adopt as a compliance obligation?
- ✓ Has the organization determined the boundaries and applicability of the Environmental Management System (EMS)?
- ✓ Has the organization established an environmental management system?

5. Leadership

- ✓ Has top management demonstrated its commitment to establishing an EMS and effective leadership in the continual improvement of the system?
- ✓ Has the organization established an environmental policy?
- ✓ Has the organization assigned responsibilities and authorities in respect of the EMS?

6. Planning

- ✓ Does the organization follow a process that determines risks and opportunities?
- ✓ Have the risks and opportunities been considered with regard to the context of the organization and the needs and expectations of interested parties?
- ✓ Has the organization identified and evaluated its environmental aspects and impacts, and identified the risks and opportunities associated with adverse and beneficial impacts?
- ✓ Has the organization determined and have access to its compliance obligations and determined how these apply?
- ✓ Has the organization established an action plan to address the identified risks and opportunities and determined how these specifically apply to the organization?
- ✓ Does the organization have plans in place to achieve environmental objectives?

7. Support

- ✓ Has the organization provided adequate resources (including human, technological and financial) for the establishment, implementation, maintenance and continual improvement of the EMS?
- ✓ Has the organization taken the necessary steps to determine the competence of persons, undertaking work under its control, which can affect EMS performance?
- ✓ Has the organization promoted awareness of environmental management; so that all those working under the organization's control are aware of the requirements as associated with their work0 and have they determined their competence requirements?
- ✓ Has the organization planned, implemented and maintained a communication process operating internally and externally taking into account compliance obligations and ensuring consistency with information generated by the EMS?
- ✓ Has the organization established, maintained and sufficiently controlled documented information as required by the standard and as determined necessary by the organization?

8. Operation

- ✓ Has the organization determined planned and implemented control of the processes to meet the requirements of the EMS?
- ✓ Has the organization considered the life cycle perspective where appropriate when procuring products and services, designing its products and services, communications with contractors and end users?
- ✓ Has the organization established and implemented a process specifying how it will respond to a potential environmental emergency situation?

9. Performance evaluation

- ✓ Has the organization determined details, methods and frequency of areas of operation that need to be monitored, measured, analysed and evaluated in order to establish the performance and effectiveness of the EMS?
- ✓ Has the organization established and implemented a process to evaluate the organization's level of conformances with its compliance obligations, recording the results?
- ✓ Has the organization established, implemented and maintained an EMS internal audit program and documented evidence of the results?
- ✓ Has the organization undertaken management reviews of the EMS, does the output of the review include opportunities to improve the integration of the EMS in to other business processes if needed?

10. Improvement

- ✓ Does the organization react effectively to any nonconformity identified within its EMS and maintain documented information where appropriate?
- ✓ Does the organization continually improve its EMS to enhance its environmental performance?

Annex. 3: Assessment Checklist for Occupational Health & Safety Management Systems (ISO 45001:2018)

4. Context of the organization

- ✓ Has the organization undertaken a review to determine fully the external and internal issues that are relevant to establishing the context of the organization?
- ✓ Has the organization undertaken a review to identify interested parties, to understand their needs and expectation and which of these, if any, they will adopt as a compliance obligation?
- ✓ Has the organization determined the boundaries and applicability of the Occupational Health & Safety Management System (OH&SMS)?
- ✓ Has the organization established an Occupational Health & Safety Management System?

5. Leadership

- ✓ Has top management demonstrated its commitment to establishing an OH&SMS and effective leadership in the continual improvement of the system?
- ✓ Has the organization established an OH&SMS policy?
- ✓ Has the organization assigned responsibilities and authorities in respect of the OH&SMS?

6. Planning

- ✓ Does the organization follow a process that determines risks and opportunities?
- ✓ Have the risks and opportunities been considered with regard to the context of the organization and the needs and expectations of interested parties?
- ✓ Is a comprehensive risk assessment programme following a hierarchy of control measures and covering all activities in place?
- ✓ Is a risk control action plan in place to deal with those risks not judged to be acceptable?
- ✓ Are legal and other requirements which apply to all activities identified and the relevant documents are held?
- ✓ Are overall plans and objectives in place for achieving OH&SMS policy?
- ✓ Are arrangements in place for ensuring that there are sufficient knowledge, skills and experience available to manage OH&SMS issues effectively?
- ✓ Are operational plans for implementing risk controls in place?
- ✓ Are operational plans for implementing legal and other requirements in place?
- ✓ Are operational control activities in place for ensuring that OH&SMS policy is implemented and effectively managed?
- ✓ Are arrangements in place for measuring, auditing and reviewing OH&SMS performance to identify any shortfalls and implementing necessary corrective and preventive actions?
- ✓ Are arrangements in place for implementing, monitoring and reviewing corrective and preventive actions?

7. Support

- ✓ Has the organization provided adequate resources (including human, technological and financial) for the establishment, implementation, maintenance and continual improvement of the OH&SMS?
- ✓ Has the organization taken the necessary steps to determine the competence of persons, undertaking work under its control, which can affect OH&SMS performance?
- ✓ Has the organization promoted awareness of OH&SMS management; so that all those working under the organization's control are aware of the requirements as associated with their work and have they determined their competence requirements?
- ✓ Has the organization planned, implemented and maintained a communication process operating internally and externally taking into account compliance obligations and ensuring consistency with information generated by the OH&SMS?
- ✓ Has the organization established, maintained and sufficiently controlled documented information as required by the standard and as determined necessary by the organization?

8. Operation

- ✓ Has the organization determined planned and implemented control of the processes to meet the requirements of the OH&SMS?
- ✓ Has the organization considered the life cycle perspective where appropriate when procuring products and services, designing its products and services, communications with contractors and end users?
- ✓ Is a top manager allocated with full responsibility for OH&S throughout the organization?
- ✓ Is there clear responsibility in the management structure?
- ✓ Is there clear accountability in the management structure?
- ✓ Is there clear delegation of authority in the management structure?
- ✓ Are any necessary resources allocated?
- ✓ Are all personnel working for, or on behalf of, the organization aware of their individual responsibilities?
- ✓ Are all personnel working for, or on behalf of, the organization aware of their responsibility to others who may be affected by the activities they control?
- ✓ Are all personnel working for, or on behalf of, the organization aware of the consequences of their action or inaction?
- ✓ Are a training, awareness and competence assessment programme in place for personnel working under its control?
- ✓ Is a retraining and refresher training programme in place?
- ✓ Is a system for effective, open two-way communication of OH&SMS information in place with all interested parties?
- ✓ Are specialist (in-house or external) advice/services made available, where appropriate?
- ✓ Workers (including contractors) and external interested parties are fully involved and consulted
- ✓ Is an adequate documentation system in place?
- ✓ Is a system in place for ensuring documents are kept up to date and relevant?
- ✓ Are contingency plans in place for emergencies, including arrangements for evacuating the site, liaison with the emergency services and start-up following an emergency?
- ✓ Is emergency response takes into account the needs of relevant interested parties and is periodically tested?

9. Performance evaluation

- ✓ Has the organization determined details, methods and frequency of areas of operation that need to be monitored, measured, analysed and evaluated in order to establish the performance and effectiveness of the OH&SMS?
- ✓ Has the organization established and implemented a process to evaluate the organization's level of conformances with its compliance obligations, recording the results?
- ✓ Has the organization established, implemented and maintained an OH&SMS internal audit program and documented evidence of the results?
- ✓ Has the organization undertaken management reviews of the OH&SMS, does the output of the review include opportunities to improve the integration of the OH&SMS in to other business processes if needed?

10. Improvement

- ✓ Does the organization react effectively to any nonconformity identified within its EMS and maintain documented information where appropriate?
- ✓ Does the organization continually improve its OH&SMS to enhance its Occupational health & safety performance?

Annex. 4: Assessment Checklist for Food Safety Management Systems (ISO 22000:2018)

4. Context of the organization

4.1. Understanding the Organization

- ✓ How does the organization determine and document its external and internal issues that are relevant to its food safety management system?
- ✓ How are these issues reviewed and updated periodically?

4.2. Understanding the Needs and Expectations of Interested Parties:

- ✓ What methods does the organization use to identify and assess the needs and expectations of interested parties relevant to the food safety management system?
- ✓ How does the organization monitor and keep updated on changes in the needs and expectations of interested parties?

4.3. Scope of the Food Safety Management System:

- ✓ How does the organization define the scope of its food safety management system?
- ✓ How is the scope communicated and documented within the organization?

4.4. Establishing the Context:

- ✓ How does the organization establish, review, and update the context of the organization, including internal and external issues, and the needs and expectations of interested parties?
- ✓ How is this information used to ensure the effectiveness of the food safety management system?

4.5. Legal and Regulatory Requirements:

- ✓ How does the organization identify and monitor applicable legal and regulatory requirements related to food safety?
- ✓ How are changes in legal and regulatory requirements communicated and incorporated into the food safety management system?

4.6. Strategic Direction and Objectives:

- ✓ How is the organization's strategic direction integrated into the food safety management system?
- ✓ How are food safety objectives established to align with the organization's strategic direction?

4.7. Risk Management:

- ✓ How does the organization identify and assess risks and opportunities related to the context of the organization and the food safety management system?
- ✓ What actions are taken to address these risks and opportunities?

4.8. Communication:

- ✓ How does the organization ensure effective internal and external communication relevant to the food safety management system?
- ✓ How is information about the context of the organization and the food safety management system communicated to interested parties?

4.9. Monitoring and Review:

- ✓ How does the organization monitor, measure, analyze, and evaluate the performance of the food safety management system in the context of the organization?
- ✓ How are the results of these evaluations used to make informed decisions and drive continual improvement?

5. Leadership

5.1. Commitment to Food Safety:

- ✓ How does top management demonstrate its commitment to ensuring the effectiveness of the food safety management system?
- ✓ In what ways does top management communicate the importance of meeting food safety requirements to the entire organization?

5.2. Policy Development:

- ✓ How is the food safety policy established, reviewed, and communicated within the organization?
- ✓ How does the food safety policy align with the organization's overall objectives and strategic direction?

5.3. Roles, Responsibilities, and Authorities:

- ✓ How are roles, responsibilities, and authorities defined and communicated at all levels within the organization?
- ✓ How does top management ensure that individuals have the necessary competence to fulfill their roles in relation to food safety?

5.4. Integration with Business Processes:

- ✓ How does top management integrate the food safety management system into the organization's business processes?
- ✓ In what ways is food safety considered in decision-making processes throughout the organization?

5.5. Resource Allocation:

- ✓ How does top management ensure that adequate resources are allocated for the establishment, implementation, maintenance, and continual improvement of the food safety management system?
- ✓ How are resource needs assessed and adjusted based on changes in the organization's context?

5.6. Communication:

- ✓ How does top management ensure effective communication both within the organization and with external interested parties regarding food safety matters?
- ✓ How are communication channels established to promote awareness and understanding of food safety responsibilities?

5.7. Setting Objectives:

- ✓ How are food safety objectives established and aligned with the overall strategic goals of the organization?
- ✓ How does top management ensure that objectives are measurable, monitored, and reviewed for effectiveness?

5.8. Review of the Food Safety Management System:

- ✓ How does top management conduct reviews of the food safety management system to ensure its continuing suitability, adequacy, and effectiveness?
- ✓ In what ways are the results of these reviews used to drive improvement and enhance food safety performance?

5.9. Promoting a Culture of Food Safety:

- ✓ How does top management promote a culture that emphasizes the importance of food safety throughout the organization?
- ✓ What measures are in place to encourage employees to report food safety concerns without fear of reprisal?

5.10. Demonstrating Leadership in Crisis and Emergency Situations:

- ✓ How does top management demonstrate leadership during crisis or emergency situations that may impact food safety?
- ✓ How are contingency plans developed and tested to ensure preparedness for such situations?

6. Planning

6.1. Hazard Analysis:

- ✓ How does the organization conduct hazard analysis to identify and evaluate potential hazards relevant to food safety?
- ✓ How frequently is the hazard analysis updated to account for changes in processes, products, or other relevant factors?

6.2. Determining the Scope of the Food Safety Management System:

- ✓ How is the scope of the food safety management system determined, documented, and communicated within the organization?
- ✓ What considerations are taken into account when defining the boundaries of the food safety management system?

6.3. Setting Food Safety Objectives:

- ✓ How are food safety objectives established, considering the organization's strategic direction and the results of the hazard analysis?
- ✓ How are these objectives communicated and monitored within the organization?

6.4. Risk Assessment and Treatment:

- ✓ How does the organization identify and assess risks and opportunities related to food safety?
- ✓ What actions are taken to address identified risks and opportunities, and how are they integrated into the food safety management system?

6.5. Legal and Regulatory Compliance:

- ✓ How does the organization ensure awareness of and compliance with applicable legal and regulatory requirements related to food safety?
- ✓ How are changes in legal and regulatory requirements monitored and incorporated into the food safety management system?

6.6. Emergency Preparedness and Response:

- ✓ How is emergency preparedness and response addressed within the food safety management system?
- ✓ How are procedures established and tested to ensure the organization is prepared to respond to potential emergencies affecting food safety?

6.7. Communication Planning:

- ✓ How does the organization plan and manage internal and external communication regarding food safety?
- ✓ What mechanisms are in place to ensure effective and timely communication in the event of a food safety incident?

6.8. Resource Planning:

- ✓ How does the organization plan for and allocate resources necessary for the effective implementation and maintenance of the food safety management system?
- ✓ How is resource planning adjusted based on changes in the organization's activities, products, or services?

6.9. Monitoring and Measurement Planning:

- ✓ How does the organization plan and implement the monitoring, measurement, analysis, and evaluation of its food safety performance?
- ✓ How are these activities used to ensure the effectiveness of the food safety management system?

6.10. Continual Improvement Planning:

- ✓ How does the organization plan for continual improvement of the food safety management system?
- ✓ What measures are in place to track and review progress toward objectives and targets?

7. Support

7.1. Resource Provision:

- ✓ How does the organization determine and provide the necessary resources to establish, implement, maintain, and continually improve the food safety management system?
- ✓ How is the adequacy of resources assessed, and how are adjustments made based on changes in the organization's context?

7.2. Competence and Training:

- ✓ How are the competence requirements for personnel involved in the food safety management system identified and documented?
- ✓ What mechanisms are in place to ensure that personnel have the necessary competence through education, training, and experience?

7.3. Awareness:

- ✓ How does the organization ensure that personnel are aware of the relevance and importance of their activities and how they contribute to the achievement of food safety objectives?
- ✓ What methods are used to promote awareness of food safety among employees?

7.4. Communication:

- ✓ How is internal and external communication related to the food safety management system planned and executed?
- ✓ How does the organization ensure that relevant information is communicated to, and from, external interested parties?

7.5. Documented Information Control:

- ✓ How is documented information (e.g., policies, procedures, records) controlled to ensure its availability and suitability for the food safety management system?
- ✓ How are changes to documented information managed, and how is the latest version communicated to relevant personnel?

7.6. Documented Information Accessibility:

- ✓ How does the organization ensure that documented information required for the food safety management system is available to those who need it?
- ✓ What measures are in place to prevent unauthorized access to sensitive documented information?

7.7. Monitoring and Measuring Equipment:

- ✓ How does the organization ensure that monitoring and measuring equipment used for food safety purposes is calibrated, maintained, and controlled?
- ✓ What procedures are in place to address out-of-specification equipment?

7.8. Infrastructure:

- ✓ How does the organization ensure that the infrastructure necessary for the operation of the food safety management system is identified, maintained, and fit for its intended purpose?
- ✓ How are changes in infrastructure evaluated for their potential impact on food safety?

7.9. Work Environment:

- ✓ How is the work environment managed to ensure it does not compromise food safety?
- ✓ What considerations are given to factors such as hygiene, temperature control, and cleanliness within the work environment?

7.10. External Communication:

- ✓ How does the organization manage external communication related to the food safety management system, including with customers, regulators, and other interested parties?
- ✓ What measures are in place to ensure accurate and timely communication with external stakeholders?

8. Operation

8.1. Operational Planning and Control:

- ✓ How does the organization plan and control its processes to meet the requirements of the food safety management system?
- ✓ What measures are in place to ensure effective control and monitoring of critical control points (CCPs) identified in the hazard analysis?

8.2. Prerequisite Programs (PRPs):

- ✓ How are prerequisite programs identified and implemented to create a hygienic environment and prevent food safety hazards?
- ✓ How are PRPs monitored and updated based on changes in the organization's processes or products?

8.3. Handling of Potentially Unsafe Products:

- ✓ How does the organization handle products that may be potentially unsafe due to deviations from critical limits or other factors?
- ✓ What procedures are in place for segregating and disposing of products that do not meet food safety requirements?

8.4. Emergency Preparedness and Response:

- ✓ How is emergency preparedness and response addressed within the operational processes to ensure the continuity of food safety?
- ✓ How are employees trained and equipped to respond to food safety emergencies?

8.5. Traceability and Recall:

- ✓ How does the organization ensure traceability of products throughout the food supply chain?
- ✓ What procedures are in place for initiating and conducting product recalls when necessary?

8.6. Supplier Control:

- ✓ How are suppliers evaluated and controlled to ensure they meet the necessary food safety requirements?
- ✓ What measures are in place to address and manage potential risks associated with the supply chain?

8.7. Monitoring and Measurement of Processes:

- ✓ How are the processes within the food safety management system monitored, measured, and evaluated for effectiveness?
- ✓ What performance indicators are used to assess the performance of operational processes?

8.8. Validation of Control Measures:

- ✓ How does the organization validate control measures to ensure they are effective in controlling identified food safety hazards?
- ✓ What records are maintained to demonstrate the validation of control measures?

8.9. Food Safety System Updates:

- ✓ How does the organization manage updates and changes to the food safety management system, including changes in processes, products, or regulations?
- ✓ How are employees informed and trained regarding changes in food safety procedures?

8.10. Handling of Nonconforming Products:

- ✓ How does the organization handle products that do not conform to food safety requirements?
- ✓ What procedures are in place for identifying, segregating, and addressing nonconforming products?

9. Performance evaluation

9.1. Monitoring and Measurement of Processes:

- ✓ How does the organization monitor and measure its processes to ensure the effective operation of the food safety management system?
- ✓ What indicators and metrics are used to assess the performance of key processes?

9.2. Monitoring and Measurement of Food Safety Objectives:

- ✓ How are food safety objectives monitored, measured, and evaluated for achievement?
- ✓ What mechanisms are in place to track progress toward food safety objectives?

9.3. Internal Audits:

- ✓ How does the organization plan and conduct internal audits of the food safety management system?
- ✓ How are audit findings documented, communicated, and addressed for continual improvement?

9.4. Evaluation of Compliance:

- ✓ How does the organization evaluate its compliance with legal and regulatory requirements related to food safety?
- ✓ What procedures are in place to address instances of non-compliance?

9.5. Management Review:

- ✓ How does top management conduct reviews of the food safety management system to ensure its continuing suitability, adequacy, and effectiveness?
- ✓ In what ways are the results of management reviews used to drive improvement?

9.6. Data Analysis:

- ✓ How does the organization analyze data collected from monitoring and measurement activities to identify trends, opportunities for improvement, and areas of concern?
- ✓ What actions are taken based on the analysis of data?

9.7. Customer Feedback and Complaints:

- ✓ How does the organization collect, analyze, and respond to customer feedback and complaints related to food safety?
- ✓ How are trends in customer feedback used to enhance food safety performance?

9.8. Corrective Actions:

- ✓ How does the organization identify and address nonconformities and take corrective actions to prevent recurrence?
- ✓ What measures are in place to verify the effectiveness of corrective actions?

9.9. Continual Improvement:

- ✓ How does the organization promote a culture of continual improvement in relation to the food safety management system?
- ✓ In what ways are employees encouraged to contribute ideas for improvement?

9.10. Communication of Results:

- ✓ How are the results of performance evaluations communicated within the organization?
- ✓ What measures are in place to ensure that relevant information is shared with appropriate stakeholders?

9.11. Documentation of Performance:

- ✓ How is the performance of the food safety management system documented, including records of monitoring, measurement results, internal audits, and management reviews?
- ✓ How are these documents maintained and made available for relevant personnel?

10. Improvement

10.1. Nonconformity and Corrective Action:

- ✓ How does the organization identify and document nonconformities within the food safety management system?
- ✓ What is the process for determining the causes of nonconformities and implementing corrective actions?

10.2. Root Cause Analysis:

- ✓ How does the organization conduct root cause analysis when addressing nonconformities and implementing corrective actions?
- ✓ How is the effectiveness of corrective actions verified to ensure the nonconformity does not recur?

10.3. Preventive Action:

- ✓ How does the organization identify potential nonconformities and take preventive actions to avoid their occurrence?
- ✓ How is the effectiveness of preventive actions assessed and documented?

10.4. Continuous Improvement Initiatives:

- ✓ How does the organization encourage and manage initiatives for continuous improvement within the food safety management system?
- ✓ In what ways are employees involved in suggesting and implementing improvements?

10.5. Review of the Food Safety Management System:

- ✓ How often does top management conduct reviews of the food safety management system?
- ✓ How are the results of management reviews used to drive continual improvement?

10.6. Monitoring of Improvement Activities:

- ✓ How does the organization monitor and measure the effectiveness of improvement activities?
- ✓ What metrics and indicators are used to assess the success of implemented improvements?

10.7. Review of Customer Feedback:

- ✓ How does the organization review and analyze customer feedback for opportunities to improve food safety performance?
- ✓ In what ways are customer suggestions considered in the improvement process?

10.8. Employee Training and Development:

- ✓ - How does the organization provide training and development opportunities for employees to enhance their skills and knowledge related to food safety?
- ✓ - How is the impact of training programs assessed?

10.9. 9. **Documentation of Improvement Activities:

- ✓ How are improvement activities documented within the food safety management system?
- ✓ What records are maintained to demonstrate the planning, implementation, and results of improvement initiatives?

10.10. Communication of Improvement:

- ✓ How is information about improvements in the food safety management system communicated within the organization?
- ✓ In what ways is success and progress in improvement initiatives shared with relevant stakeholders?

10.11. Feedback Mechanisms:

- ✓ How does the organization gather feedback from employees at various levels regarding the effectiveness of improvement initiatives?
- ✓ What mechanisms are in place to address and respond to employee feedback?

Annex. 5: Assessment Checklist for Educational Organization Management Systems (ISO 21001:2018)

4. Context of the organization

- ✓ The organization shall determine external and internal issues that are relevant to its purpose, its social responsibility and its strategic direction, and that affect its ability to achieve the intended outcomes of its EOMS?
- ✓ The organization shall monitor and review information about these external and internal issues.
- ✓ Has the scope of the EOMS been determined taking into account the external and internal issues, interested parties and the organization's services?

4.1. Understanding the needs and expectations of interested parties

- ✓ The interested parties that are relevant to the EOMS?
- ✓ The relevant requirements of these interested parties?
  The interested parties should be
  — Learners;
  — Other beneficiaries;
  — staff of the organization

5. Leadership

Top management shall demonstrate leadership and commitment with respect to the EOMS by:

- ✓ Being accountable for the effectiveness of the EOMS?
- ✓ Ensuring that the educational organization policy and educational organization objectives are established and are compatible with the context and strategic direction of the organization?
- ✓ Ensuring that the resources needed for the EOMS are available?
- ✓ Communicating the importance of effective educational organization management and of conforming to the EOMS requirements?
- ✓ Engaging, directing and supporting persons to contribute to the effectiveness of the EOMS?
- ✓ Ensuring that learners' educational requirements, including special needs, are identified and addressed?
- ✓ Supporting the sustainable implementation of the educational vision and related educational concepts?

6. Planning

- ✓ Have the risks and opportunities that need to be addressed to give assurance that the EOMS can achieve its intended result(s) been established?
- ✓ Has the organization planned actions to address these risks and opportunities and integrated them into the system processes?
- ✓ Is there a defined process for determining the need for changes to the EOMS and managing their implementation?

7. Support

- ✓ Has the organization determined and provided the resources needed for the establishment, implementation, maintenance and continual improvement of the EOMS (including people, environmental and infrastructure requirements)?
- ✓ The organization shall retain appropriate documented information as evidence of fitness for purpose of monitoring and

measurement resources?

- ✓ The organization shall determine and provide the resources needed to ensure valid and reliable results when monitoring or measuring is used to verify the conformity of products and services to requirements?
- ✓ Has the organization ensured that those persons who can affect the performance of the EOMS are competent on the basis of appropriate education, training, or experience or taken action to ensure that those persons can acquire the necessary competence?
- ✓ Has the documented information required by the standard and necessary for the effective implementation and operation of the EOMS been established?

8. Operation

The organization shall plan, implement and control the processes needed to meet requirements for the provision of educational products and services and to implement the actions determined by:

- ✓ Determining requirements for the educational products and services?
- ✓ Determining the resources needed to achieve conformity to the educational product and service requirements?
- ✓ Determining and keeping documented information to the extent necessary?
- ✓ Ensuring appropriate and accessible teaching methods and learning environments?
- ✓ Defining criteria for learning assessment?
- ✓ Conducting learning assessment?
- ✓ Defining and conducting improvement methods?
- ✓ Facilitate a team environment with adequate resources to support individual learners to meet their optimal potential?
- ✓ Allowing enrolment in two distinct programs or educational organizations?
- ✓ Does the organization have effective methods of ensuring traceability during the operation process?
- ✓ Where property belonging to customers or external providers is used in the provision of the product or service, is this controlled effectively?
- ✓ If there is a requirement for post-delivery activities associated with the products and services such as warranty, maintenance services, recycling or final disposal, are these defined and managed?
- ✓ Are any nonconforming process outputs managed so as to prevent their unintended use?

9. Performance evaluation

- ✓ Has the organization determined:
  - What needs to be monitored and measured and
  - The methods for monitoring, measurement, analysis and evaluation, to ensure valid results?
- ✓ Has it established when the results from monitoring and measurement shall be analyzed and evaluated?
- ✓ Have methods of monitoring customer perceptions of the provision of products and services been established?
- ✓ Has it determined the need or opportunities for improvements within the EOMS and how these will be fed into management reviews?
- ✓ Has the organization established a process for an internal audit of the EOMS?
- ✓ Has an approach to perform management reviews been established and implemented?

10. Improvement

- ✓ Has the organization determined and selected opportunities for improvement and implemented the necessary actions to meet customer requirements and enhance customer satisfaction?
- ✓ Evaluate the need for action to eliminate the causes of the Nonconformity, in order that it does not recur or occur elsewhere?
- ✓ The organization shall continually improve the suitability, adequacy and effectiveness of the EOMS, taking into account

relevant research and best practices?

The organization shall consider the results of analysis and evaluation, and the outputs from management review, to determine if there are needs or opportunities that shall be addressed as part of continual improvement?

Annex. 6: Assessment Checklist for Information Security Management Systems (ISO/IEC 27001:2022)

4. Context of the organization

4.1. Understanding the Organization:

- ✓ How does the organization determine and document its external and internal issues that are relevant to its information security management system (ISMS)?
- ✓ How are these issues reviewed and updated periodically?

4.2. Understanding the Needs and Expectations of Interested Parties:

- ✓ What methods does the organization use to identify and assess the needs and expectations of interested parties relevant to the ISMS?
- ✓ How does the organization monitor and keep updated on changes in the needs and expectations of interested parties?

4.3. Scope of the ISMS:

- ✓ How does the organization define the scope of its ISMS?
- ✓ How is the scope communicated and documented within the organization?

4.4. Establishing the Context:

- ✓ How does the organization establish, review, and update the context of the organization, including internal and external issues, and the needs and expectations of interested parties?
- ✓ How is this information used to ensure the effectiveness of the ISMS?

4.5. Legal and Regulatory Requirements:

- ✓ How does the organization identify and monitor applicable legal and regulatory requirements related to information security?
- ✓ How are changes in legal and regulatory requirements communicated and incorporated into the ISMS?

4.6. Strategic Direction and Objectives:

- ✓ How is the organization's strategic direction integrated into the ISMS?
- ✓ How are information security objectives established to align with the organization's strategic direction?

4.7. Risk Management:

- ✓ How does the organization identify and assess risks and opportunities related to the context of the organization and the ISMS?
- ✓ What actions are taken to address these risks and opportunities?

4.8. Communication:

- ✓ How does the organization ensure effective internal and external communication relevant to the ISMS?
- ✓ How is information about the context of the organization and the ISMS communicated to interested parties?

4.9. Monitoring and Review:

- ✓ How does the organization monitor, measure, analyze, and evaluate the performance of the ISMS in the context of the organization?
- ✓ How are the results of these evaluations used to make informed decisions and drive continual improvement?

5. Leadership

5.1. Commitment to Information Security:

- ✓ How does top management demonstrate its commitment to information security within the organization?
- ✓ In what ways is this commitment communicated to all levels of the organization?

5.2. Information Security Policy:

- ✓ How is the information security policy developed, approved, and communicated within the organization?
- ✓ How does the policy align with the organization's strategic direction and applicable legal and regulatory requirements?

5.3. Roles, Responsibilities, and Authorities:

- ✓ How are roles, responsibilities, and authorities for information security defined and communicated at all levels within the organization?
- ✓ How does top management ensure that individuals have the necessary competence to fulfill their roles in relation to information security?

5.4. Integration with Business Processes:

- ✓ How does top management integrate information security into the organization's business processes?
- ✓ In what ways is information security considered in decision-making processes throughout the organization?

5.5. Resource Allocation:

- ✓ How does top management ensure that adequate resources are allocated for the establishment, implementation, maintenance, and continual improvement of the ISMS?
- ✓ How are resource needs assessed and adjusted based on changes in the organization's context?

5.6. Communication:

- ✓ How does top management ensure effective communication both within the organization and with external interested parties regarding information security matters?
- ✓ How are communication channels established to promote awareness and understanding of information security responsibilities?

5.7. Setting Objectives:

- ✓ How are information security objectives established and aligned with the organization's strategic direction?
- ✓ How does top management ensure that objectives are measurable, monitored, and reviewed for effectiveness?

5.8. Management Reviews:

- ✓ How often does top management conduct reviews of the ISMS?
- ✓ In what ways are the results of these reviews used to make informed decisions and drive continual improvement?

5.9. Promoting a Culture of Information Security:

- ✓ How does top management promote a culture that emphasizes the importance of information security throughout the organization?
- ✓ What measures are in place to encourage employees to report information security concerns without fear of reprisal?

5.10. Demonstrating Leadership in Information Security Incidents:

- ✓ How does top management demonstrate leadership during information security incidents or breaches?
- ✓ What measures are in place to ensure a swift and effective response to incidents?

6. Planning

6.1. Risk Assessment:

- ✓ How does the organization conduct a risk assessment to identify and evaluate information security risks?
- ✓ What criteria are used to assess the impact and likelihood of identified risks?

6.2. Risk Treatment:

- ✓ How does the organization determine and apply risk treatment measures to address identified information security risks?
- ✓ How are risk treatment decisions documented and communicated?

6.3. Statement of Applicability (SoA):

- ✓ How is the Statement of Applicability (SoA) developed and maintained?
- ✓ How does the organization ensure that the SoA accurately reflects the controls selected for the ISMS?

6.4. Objectives and Planning to Achieve Them:

- ✓ How are information security objectives established, considering the results of the risk assessment?
- ✓ How does the organization plan to achieve these objectives?

6.5. Legal and Regulatory Requirements:

- ✓ How does the organization identify and monitor applicable legal and regulatory requirements related to information security?
- ✓ How are changes in legal and regulatory requirements assessed and incorporated into the ISMS?

6.6. Information Security Policy:

- ✓ How is the information security policy aligned with the organization's business objectives and the results of the risk assessment?
- ✓ In what ways is the policy communicated to relevant stakeholders?

6.7. Resource Allocation:

- ✓ How does the organization allocate resources for the implementation, maintenance, and continual improvement of the ISMS?
- ✓ How is the adequacy of resources assessed and adjusted based on changes in the organization's context?

6.8. Documentation and Control of Information:

- ✓ How does the organization plan for the creation, update, and control of documented information within the ISMS?
- ✓ What measures are in place to ensure the availability and confidentiality of information?

6.9. Incident Response Planning:

- ✓ How is incident response planning addressed within the organization's information security planning?
- ✓ What procedures are in place to respond to and manage information security incidents?

6.10. Communication Planning:

- ✓ How does the organization plan and manage internal and external communication regarding information security?
- ✓ What mechanisms are in place to ensure effective and timely communication in the event of an information security incident?

6.11. Change Management:

- ✓ How does the organization plan for and manage changes that could affect the information security requirements of the ISMS?
- ✓ What processes are in place to assess and control changes?

7. Support

7.1. Resource Provision:

- ✓ How does the organization determine and provide the necessary resources to establish, implement, maintain, and continually improve the ISMS?
- ✓ How is the adequacy of resources assessed, and how are adjustments made based on changes in the organization's context?

7.2. Competence and Training:

- ✓ How are the competence requirements for personnel involved in the ISMS identified and documented?
- ✓ What mechanisms are in place to ensure that personnel have the necessary competence through education, training, and experience?

7.3. Awareness:

- ✓ How does the organization ensure that personnel are aware of the relevance and importance of their activities as they relate to information security?
- ✓ What methods are used to promote awareness of information security responsibilities among employees?

7.4. Communication:

- ✓ How is internal and external communication related to the ISMS planned and executed?
- ✓ How does the organization ensure that relevant information is communicated to, and from, external interested parties?

7.5. Documented Information Control:

- ✓ How is documented information (e.g., policies, procedures, records) controlled to ensure its availability and suitability for the ISMS?
- ✓ How are changes to documented information managed, and how is the latest version communicated to relevant personnel?

7.6. Documented Information Accessibility:

- ✓ How does the organization ensure that documented information required for the ISMS is available to those who need it?
- ✓ What measures are in place to prevent unauthorized access to sensitive documented information?

7.7. Monitoring and Measurement Equipment:

- ✓ How does the organization ensure that monitoring and measurement equipment used for information security purposes is calibrated, maintained, and controlled?
- ✓ What procedures are in place to address out-of-specification equipment?

7.8. Infrastructure:

- ✓ How does the organization ensure that the infrastructure necessary for the operation of the ISMS is identified, maintained, and fit for its intended purpose?
- ✓ How are changes in infrastructure evaluated for their potential impact on information security?

7.9. Work Environment:

- ✓ How is the work environment managed to ensure it does not compromise information security?
- ✓ What considerations are given to factors such as physical security, access controls, and other aspects of the work environment?

7.10. External Communication:

- ✓ How does the organization manage external communication related to the ISMS, including with customers, regulators, and other interested parties?
- ✓ What measures are in place to ensure accurate and timely communication with external stakeholders?

8. Operation

8.1. Access Control:

- ✓ How are access controls implemented to ensure that only authorized individuals have access to information and information processing facilities?
- ✓ How is access reviewed and updated regularly?

8.2. Incident Management:

- ✓ How is incident management addressed within the ISMS operation?
- ✓ What procedures are in place for reporting, responding to, and learning from information security incidents?

8.3. Cryptographic Controls:

- ✓ How does the organization implement cryptographic controls to protect sensitive information?
- ✓ Are cryptographic keys managed securely, and is their usage monitored?

8.4. Security of Systems and Equipment:

- ✓ How are systems and equipment secured to prevent unauthorized access and protect against information security threats?
- ✓ Are security patches and updates regularly applied to systems and software?

8.5. Information Security Monitoring:

- ✓ How does the organization monitor information security events, including intrusion detection and prevention?
- ✓ What measures are in place to detect and respond to security breaches?

8.6. Operational Planning and Control:

- ✓ How is operational planning and control addressed within the ISMS?
- ✓ What mechanisms are in place to ensure that information security controls are effective in day-to-day operations?

8.7. Supplier Relationships:

- ✓ How are information security requirements defined and communicated to suppliers?
- ✓ How does the organization ensure that suppliers adhere to information security requirements?

8.8. System Acquisition, Development, and Maintenance:

- ✓ How does the organization address information security in the acquisition, development, and maintenance of information systems?
- ✓ What measures are in place to ensure that security requirements are considered throughout the system life cycle?

8.9. Vulnerability Management:

- ✓ How does the organization manage vulnerabilities in information systems?
- ✓ What processes are in place for identifying, assessing, and mitigating vulnerabilities?

8.10. Information Security in Change Management:

- ✓ How does the organization ensure that information security is considered in change management processes?
- ✓ What measures are in place to assess and manage the impact of changes on information security?

8.11. Information and Communication Technology (ICT) Security Policies:

- ✓ How are security policies for information and communication technology (ICT) defined, documented, and communicated?

- ✓ How does the organization ensure adherence to these policies?

8.12. Asset Management:

- ✓ How does the organization manage information assets throughout their lifecycle?
- ✓ What procedures are in place for identifying, classifying, and protecting information assets?

9. Performance evaluation

9.1. Monitoring and Measurement of Information Security Performance

- ✓ How does the organization monitor and measure the performance of the ISMS against planned objectives and targets?
- ✓ What indicators and metrics are used to assess the effectiveness of information security controls?

9.2. Internal Audits:

- ✓ How does the organization plan and conduct internal audits of the ISMS?
- ✓ How are audit findings documented, communicated, and addressed for continual improvement?

9.3. Evaluation of Compliance:

- ✓ How does the organization evaluate its compliance with legal, regulatory, and contractual requirements related to information security?
- ✓ What procedures are in place to address instances of non-compliance?

9.4. Management Reviews:

- ✓ How often does top management conduct reviews of the ISMS?
- ✓ In what ways are the results of management reviews used to make informed decisions and drive continual improvement?

9.5. Analysis of Data:

- ✓ How does the organization analyze data collected from monitoring and measurement activities to identify trends, opportunities for improvement, and areas of concern?
- ✓ What actions are taken based on the analysis of data?

9.6. Incident Response Effectiveness:

- ✓ How does the organization assess the effectiveness of its incident response procedures?
- ✓ What measures are in place to continually improve incident response capabilities?

9.7. Customer Feedback and Satisfaction:

- ✓ How does the organization collect, analyze, and respond to customer feedback related to information security?
- ✓ How are trends in customer feedback used to enhance information security performance?

9.8. Effectiveness of Corrective and Preventive Actions:

- ✓ How does the organization measure the effectiveness of corrective actions taken in response to incidents or non-conformities?
- ✓ What measures are in place to assess the success of preventive actions?

9.9. Continual Improvement Initiatives:

- ✓ How does the organization encourage and manage initiatives for continual improvement within the ISMS?
- ✓ In what ways are employees involved in suggesting and implementing improvements?

9.10. Communication of Results:

- ✓ How are the results of performance evaluations communicated within the organization?
- ✓ In what ways is success and progress in meeting information security objectives shared with relevant stakeholders?

9.11. Documentation of Performance:

- ✓ How is the performance of the ISMS documented, including records of monitoring, measurement results, internal audits, and management reviews?
- ✓ How are these documents maintained and made available for relevant personnel?

10. Improvement

10.1. Nonconformity and Corrective Action:

- ✓ How does the organization identify and document nonconformities within the ISMS?
- ✓ What is the process for determining the causes of nonconformities and implementing corrective actions?

10.2. Root Cause Analysis:

- ✓ How does the organization conduct root cause analysis when addressing nonconformities and implementing corrective actions?
- ✓ How is the effectiveness of corrective actions verified to ensure the nonconformity does not recur?

10.3. Preventive Action:

- ✓ How does the organization identify potential nonconformities and take preventive actions to avoid their occurrence?
- ✓ How is the effectiveness of preventive actions assessed and documented?

10.4. Continuous Improvement Initiatives:

- ✓ How does the organization encourage and manage initiatives for continuous improvement within the ISMS?
- ✓ In what ways are employees involved in suggesting and implementing improvements?

10.5. Review of the ISMS:

- ✓ How often does top management conduct reviews of the ISMS?
- ✓ How are the results of management reviews used to drive continual improvement?

10.6. Monitoring of Improvement Activities:

- ✓ How does the organization monitor and measure the effectiveness of improvement activities?
- ✓ What metrics and indicators are used to assess the success of implemented improvements?

10.7. Review of Customer Feedback:

- ✓ How does the organization review and analyze customer feedback for opportunities to improve information security performance?
- ✓ In what ways are customer suggestions considered in the improvement process?

10.8. Employee Training and Development:

- ✓ How does the organization provide training and development opportunities for employees to enhance their skills and knowledge related to information security?
- ✓ How is the impact of training programs assessed?

10.9. Documentation of Improvement Activities:

- ✓ How are improvement activities documented within the ISMS?
- ✓ What records are maintained to demonstrate the planning, implementation, and results of improvement initiatives?

10.10. Communication of Improvement:

- ✓ How is information about improvements in the ISMS communicated within the organization?
- ✓ In what ways is success and progress in improvement initiatives shared with relevant stakeholders?

10.11. Feedback Mechanisms:

- ✓ How does the organization gather feedback from employees at various levels regarding the effectiveness of improvement initiatives?
- ✓ What mechanisms are in place to address and respond to employee feedback?