POLICY FOR AUDIT AND CERTIFICATION PROCESS

1. Purpose

The purpose of this document is to describe the steps and requirements of the MSECB Audit and Certification Process. All auditors and personnel involved in a MS Audit must comply with these requirements.

2. Scope

This policy applies to the entire certification process from auditor assignment to certification issuance and maintenance of such.

3. General Principles

a. All threats to impartiality are taken seriously at MSECB, and all the following need to be avoided:
    i. Auditing a function in an organization for which the auditor has provided consulting services within the past two years;
    ii. Auditing a function in an organization managed by someone with whom the auditor has a family relationship with;
    iii. Auditing an organization that the auditor is a shareholder and/or owns.
b. Potential conflicts of interests shall be reported to MSECB from the auditor, prior to the audit, or as soon as they are revealed. Failure to do so may result in the invalidity of the audit, termination of auditor status and even lawsuits;
c. All MSECB Auditors are expected to comply with the MSECB Code of Ethics;
d. All MSECB Auditors need to sign the 06100-FO5-Confidentiality and Non-disclosure Policy and Engagement before each audit mandate;
e. All MSECB Auditors are expected to share solely the audit documents approved by MSECB;
f. All MSECB Auditors are expected to use and have the specific management system standard while doing audits on behalf of MSECB;
g. Whenever a new standard is published or when the version of a standard is changed, the Compliance Department is responsible to update the audit report template. This must be part of the package when preparing the communication policies of the changes.

4. Stage 1 Audit

The following contains important instructions related to Stage 1 Audit that all MSECB Auditors need to be aware of:

a. Neither an audit plan nor an opening meeting is required for a Stage 1 Audit. The auditor may send them to the client, but MSECB does not require the provision of such evidence or documents;
b. Stage 1 Audit may be conducted completely off-site, if needed. However, if at least part of Stage 1 is carried out at client's premises, this can help to achieve the objectives of Stage 1;
c. The auditors are required to take into account during the audits the requirements derived from clause 9.3.1.2 of ISO/IEC 17021-1;
d. During Stage 1 Audits, auditors are required to use the following methods to obtain information:
    a. Interviews;
    b. Observation of processes and activities;
    c. Review of documentation and records;
e. All nonconformities or findings need to be validated by the auditor before the auditee can be authorized to proceed to the Stage 2 Audit (*see section below related to managing findings*);
f. After completion of the audit, the Stage 1 Audit Report is recommended to be submitted within 24 hours to MSECB;
g. After approval by MSECB, the Stage 1 Audit Report must be shared with the auditee;
h. Stage 2 Audits shall be conducted within 90 days after the last day of the Stage 1 Audit;

i. In case of non-critical findings, the auditee is requested to complete their own internal corrective action plan before the Stage 2 Audit. The auditee is not requested to send this document to MSECB;
j. If the auditor does not recommend the auditee to continue with Stage 2 due to critical findings, the auditee will be given a period of 90 days to address the findings. The auditee shall submit the corrective action plan to MSECB before scheduling Stage 2 Audit by filling 06100-FO10-Corrective Action and Response Form, and the auditor shall pay special attention to it at the next visit. If the corrective action plan is not submitted or approved by MSECB, the Stage 1 Audit shall be repeated.
k. For ISO/IEC 27001 audits, when the certification scope references national and international standards, the auditor shall ensure that the organization has compared all its necessary controls with those in the reference control source(s), to determine that it has not omitted any such reference control in accordance with ISO/IEC 27001:2022, 6.1.3 c). In addition, the auditor must check whether a justification for excluded controls is stated in the SoA in accordance with ISO/IEC 27001:2022, 6.1.3 d).

5. Stage 2 Audit

a. The audit plan is recommended to be submitted to MSECB 1-2 weeks before the audit begins. Once the audit plan is approved, the auditor shall share the audit plan with the client/auditee;
b. An opening meeting is compulsory, and shall contain all of the following elements:
    i. Introduction of participants, including an outline of their roles;
    ii. Confirmation of the certification's scope;
    iii. 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, and interim meetings between the audit team and the client's management;
    iv. Confirmation of formal communication channels between the audit team and the client;
    v. Confirmation of the availability of resources and facilities necessary for the audit team;
    vi. Confirmation of matters related to confidentiality;
    vii. Confirmation of relevant work safety, emergency and security procedures for the audit team;
    viii. Confirmation of the presence, roles and identities of any guides and observers;
    ix. The method of reporting, including any grading of audit findings;
    x. Information about the conditions under which the audit may be prematurely terminated;
    xi. Confirmation that the audit team leader and audit team representing the certification body are responsible for the audit, and shall be in control of executing the audit plan, including audit activities and audit trails;
    xii. Confirmation of the status of the previous audit findings, if applicable;
    xiii. Methods and procedures used to conduct the audit based on sampling;
    xiv. Confirmation of the language to be used during the audit;
    xv. Confirmation that, during the audit, the client will be kept informed of audit progress and any concerns;
    xvi. Opportunity for the client to ask questions.
c. Stage 2 Audit must be conducted onsite. However, off-site audits can be partially performed as well. This can be practical when, for instance, an organization has several sites located far apart from each other, and some of these sites are remote and contain noncritical processes.
d. All major nonconformities need to be validated by the auditor before the auditee can be certified (*see section below related to managing findings*).
e. After completion of the audit, the Stage 2 Audit Report is recommended to be submitted to MSECB as soon as possible, preferably within 3-4 days;
f. After approval by MSECB, the Stage 2 Audit Report must be shared with the auditee when the certification decision is sent.

6. Surveillance and Recertification Audits

a. The audit plan needs to be submitted to MSECB at least 1-2 weeks before the audit begins. Once the audit plan is approved, the auditor shall send the audit plan to the client/auditee;
b. The opening and closing meetings are required for surveillance or recertification audits;
c. Surveillance and recertification audits must be conducted onsite[2]. However, off-site audits can be partially performed as well;
d. All major nonconformities need to be validated by the auditor before the auditee's certification can be maintained (*see section below related to managing findings*);
e. After completion of the audit, the surveillance or recertification audit report must be submitted to MSECB as soon as possible, preferably within 3-4 days;
f. After approval by MSECB, the surveillance or recertification audit report must be shared with the auditee.

7. Managing Findings

a. If no findings were discovered during the audit, the auditee may be certified/continue certification by MSECB shortly after the audit without any additional procedures;
b. If any findings were discovered, the Annex A – Nonconformity Report of the Audit Report shall be filled out by the auditor and auditee. The auditor shall evaluate the adequacy of the proposed correction and corrective actions:
    i. If the correction and corrective actions are deemed to be adequate, the auditor will approve these correction and corrective actions and issue clearance in the respective 'Nonconformity Report' and submit it to MSECB;
    ii. If the correction and corrective actions are deemed to be inadequate, the auditor will reject these correction and corrective actions and require the auditee to propose other correction and corrective actions. This will need to be performed until all findings have correction and corrective actions validated by the auditor.
c. If, during the audit, only non-critical findings (minor nonconformities) are revealed, the auditor may recommend certification once adequate correction and corrective actions have been approved for each finding;
d. If, during the audit, critical findings (major nonconformities) are discovered, the auditor cannot recommend certification. The auditee will have to go through a specific process to validate that all critical findings (major nonconformities) have been adequately resolved before the auditor is able to recommend certification. This process may include a follow-up audit, depending on the scale and number of the major nonconformities.
e. Findings discovered during the audit shall not be shared in writing with the client until the Closing Meeting. Findings may be discussed verbally with the client during the end-of-day meeting, but this shall not allow the client to make any changes/updates to their management systems until the audit is completed and audit conclusions have been shared in writing.