MSECB

POLICY ON REMOTE AUDIT

1.   Purpose

MSECB uses remote audit techniques to supplement the traditional on-site audit activities when appropriate. This policy establishes the minimum requirements to allow use of remote audit techniques.

This policy provides guidance on how MSECB plans, manages, and facilitates remote audits, and is consistent with IAF MD 4:2018, IAF ID 3:2011 and IAF ID 12:2015.

2.   Scope

This policy document is applicable to remote audits conducted by MSECB in order to complement traditional oversight techniques.

3.   Definitions

3.1 Remote Audit: The facilitation of audit of a client from a location other than the physical location of the client.

3.2 Virtual site: An online environment allowing persons from different physical locations to execute processes.

3.3 Electronic documented information: All documented information used in demonstrating conformity to the relevant standard and/or requirements maintained and available via electronic means from any site or location, regardless of where the work is completed.

3.4 ICT – Stands for "*Information and Communication Technologies*". ICT refers to technologies that provide access to information through telecommunications. This includes the internet, wireless networks, cell phones, and other communication mediums.

4.   Criteria for initiating a remote audit

Remote audit can be used at MSECB's discretion, but the accreditation body has to be informed about this and receive proper justification. MSECB and the client are aware of the risks and opportunities of the information and communication technologies used and the impacts that they may have on the validity and objectivity of the information gathered.

Remote audit may be considered for use when:

- Travel to a client or specific location is not reasonable (safety concerns, travel restrictions, etc.);
- It is difficult for MSECB to completely audit the number of sites to be audited within its timeframe;
- MSECB has determined the client's business risk has a low risk level;
- An activity or activities planned for the on-site audit could not be completed, and it is not the best resolution to extend the on-site audit;
- The situation requires the audit team to come back for a follow up audit, but another visit is not feasible within a short period of time;

For initial audits that are conducted remotely, a verification visit is requested.

The remote audit may be less suitable when the client has a history of nonconformance at the location being audited.

Remote audit cannot be used for the following circumstances:

- Audit objectives could not be achieved via remote audit;
- Client has changed location and/or address;

06000-PO4-MSECB Policy on Remote Audit
Owner: SCM
Classification: Public | ACL: MSECB
Status: Released

Approver: SBOD
Approval date: 2022-10-01
Version: 2.1
Page 2 of 3

- Remote audit is not allowed for a specific standard/scheme;
- MSECB has determined the client's business risk has a moderate to high risk level.

5.   Remote audit planning and scheduling

The first step for MSECB is to determine whether the client is a viable candidate for remote audit. MSECB has in place the following criteria to determine eligibility:

- The client permits and accommodates remote audit activities (e.g. readily accessible electronic documented information);
- The client has virtual meeting capabilities, including audio and video, aptitude, and resources (on-site IT, personnel, and tools);
- The client can provide a representative that is capable of communicating in the same language as the auditor;
- The designated auditor has the capability and aptitude to conduct the remote audit in the chosen medium of the remote audit;
- The client has a list of activities, areas, information, and personnel available to be involved in the remote audit.

MSECB and the client shall plan/define prior to the remote audit the following:

- The audit plan and documentation to be available during remote audit;
- The certification scope;
- The list of activities, areas, information, and personnel to be involved in the remote audit;
- A plan on how to review the information that cannot be shared remotely (e.g. confidential information). MSECB will define how this will be dealt with (e.g. follow up audit);
- The interface (e.g. Go-To-Meeting, Zoom, etc.), for hosting the audit;
- Granting security and/or profile access to the auditor;
- Testing interface compatibility between the auditor and the client;
- Considering the use of webcams, cameras, etc.;
- Time zone management to coordinate reasonable and mutually agreeable convening times.

6.   Conduct remote audit

- Should an item not be able to be reviewed or complete determination not be able to be made, a record should be made;
- The audit should be facilitated in quiet environments whenever possible to avoid interference and background noise (i.e., speakerphones);
- Both parties should make their best effort to confirm what was heard, stated, and read throughout the audit;
- All remote audits shall be concluded with a summary, review of the events, issues of concerns, clarification of issues, non-conformities, and expectations;
- The records required for the remote audit are the same as records required when the audit is conducted on site;
- The auditor shall not accept any audit records send by the client via email or other means;
- The auditor shall not video-record any communication during the audit;
- Both parties need to take appropriate measures to safeguard data confidentiality in any format;
- If MSECB audit team concludes that the audit objectives cannot be achieved at any time during the remote audit, the remote audit activity will be terminated, and an on-site audit will have to be planned.

7.   Post audit activities

- Findings need to be drafted by the remote audit team members and submitted to the client in a timely manner for each session for review and acknowledgement, prior to closure of non-conformities;

06000-PO4-MSECB Policy on Remote Audit
Owner: SCM
Classification: Public | ACL: MSECB
Status: Released

Approver: SBOD
Approval date: 2022-10-01
Version: 2.1
Page 3 of 3

- The audit report should include the details of the records reviewed and any findings. Both parties should make their best efforts to confirm what was heard, stated, and read throughout the audit;
- Report to include % of Information and Communication Technology (ICT) used during the audit and its effectiveness to meet audit objectives (e.g. virtual meetings, documents and records with remote access, etc.);
- Communication between the Auditor and the client for sending documents or clarification on issues and corrective management shall be pre-defined and communicated;
- The auditor shall specify the information that couldn't be shared remotely (e.g. confidential information) in the audit report, so it is considered in the next audit;
- Virtual sites included in the scope and activities performed at the virtual sites shall be included in the audit report;
- The treatment of non-conformities, continuing approval of certification should follow the same processes that are utilized for on-site audits.
- In case any audit records which contain confidential information are shared with the auditor via email or any other means, the auditor agrees to destroy all the confidential audit records from their laptops/cloud once the audit process is completed.