GUIDELINES ON REMOTE/BLENDED AUDITS

1. Purpose

The purpose of this document is to provide guidelines on processes for conducting remote and blended audits at MSECB, ensuring conformance with International Accreditation Forum (IAF), ISO standards, relevant accreditation body requirements, and other normative documents.

This guideline outlines how MSECB plans, manages, and facilitates remote and blended audits, and is consistent with regulatory frameworks provided below at point 4.

2. Scope

This guideline applies to all remote and blended audit activities conducted by MSECB across all standards, sectors and industries.

3. Definitions

3.1 Remote Audit: An audit conducted using electronic communication and information technology to gather audit evidence, communicate with clients, and conduct interviews remotely.

3.2 Blended Audit: A combination of physical on-site auditing and remote auditing (use of information and communication technology (ICT) techniques).

3.3 Virtual Site: An online environment allowing people from different physical locations to execute processes.

3.4 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.

3.5 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.

3.6 MSECB – Means MSECB as the certification body and includes Subcontractor Key Locations who are authorized to conduct key certification activities.

4. Regulatory Frameworks

4.1 IAF MD4:2025 – IAF Mandatory Document for the Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes.

4.2 IAF MD 5:2023 Determination of Audit Time of Quality, Environmental, and Occupational Health & Safety Management Systems

4.3 IAF ID 3:2011 Management of Extraordinary Events or Circumstances Affecting ABs, CABs and Certified Organizations

4.4 IAF ID 12:2023 Principles on Remote Assessment

4.5 ISO/IEC 17021-1:2015 – Requirements for bodies providing audit and certification of management systems.

4.6 ISO/IEC 17012:2024 – Guidelines for the use of remote auditing methods in auditing management systems

4.7 ISO/IEC 27006-1:2024 – Requirements for bodies providing audit and certification of information security management systems

4.8 ISO/IEC 20000-6:2017 - Requirements for bodies providing audit and certification of service management systems

4.9 Guidelines and directives provided by accreditation bodies.

5. Eligibility for Remote/Blended Audit

Clients must submit remote/blended audit requests to MSECB via email. Upon receipt, MSECB will conduct a risk assessment to determine the level of risk, and the appropriate type of audit based on Annex A. The following elements will be considered for each audit type:

- Available infrastructure of the CB and the client
- Sector in which the client operates
- Type(s) of audit during the certification cycle from initial audit to recertification audit
- Competence of the persons of the CB and the client, who are involved in the remote audit
- Previously demonstrated performance of remote audits for the client
- Scope of certification
- Processes requiring observation not adequately addressed in the audit programme
- Inability to use remote auditing methods due to the nature of the process
- Unknown remote capability of auditee
- Insufficient overall competence of the audit team to conduct audits effectively, using remote methods
- Time loss due to insufficient digitization
- Limited competence or experience in the use of remote auditing technologies
- No provision for an alternative plan in case remote auditing methods fail
- The specific requirements for data protection and information security when digital information is exchanged are not considered
- Inadequate or unreliable technology, i.e. internet connection
- Inability to provide adequate sensory information
- Integrity of audit evidence can be compromised via the use of remote auditing methods

If additional information is required, MSECB will contact the client to gather the necessary details. Once the assessment is complete, MSECB will communicate the decision to the client and finalize the specific arrangements.

Full remote audits may be considered when:

- The organization does not currently maintain an in-person office (a legally registered office where employees report regularly)
- Travel to a client or specific location is not reasonable (safety concerns, travel restrictions, etc.) based on a risk assessment
- 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
- There are unavoidable changes in scheduling for the Auditor (e.g., personal issues, change in business priorities, etc.)
- Any unavoidable changes to the audit schedule (e.g., urgency in completing the audit, specific client personnel working remotely) must be documented in the risk assessment, along with the reasons for the change and its potential impact

Full remote audits cannot be considered when:

- Audit objectives cannot be achieved via a remote audit
- Remote audit is not allowed for a specific standard/scheme

- If the client has a history of a high number of nonconformances on the previous audits
- When no on-site audits have taken place for an extended period of time

Blended audits may be considered when:

- MSECB has confirmed, using a risk assessment[1], that a blended approach is permissible for the scheme and agreed to by the client.
- The outcome of the individual organization's risk assessment has determined the applicable level of risk whether it is low or high as defined on table 1.[2]
- An activity or activities planned for the on-site audit could not be completed, and it is not the best solution to extend the on-site audit.
- A blended audit shall not be permitted if risk assessment identifies an unacceptable threat to the effectiveness of the audit process.

6. Remote and Blended Audit Process

6.1 Audit Planning and Preparation

Before conducting a remote/blended audit, MSECB shall make the necessary audit planning and preparations as follows:

6.1.1 Communicate with the client to determine the feasibility and readiness for a remote/blended audit and the interface for hosting the audit.

6.1.2 Assess the technological infrastructure and capabilities of the client to ensure compatibility and reliability.

6.1.3 Develop an audit plan tailored to the remote/blended audit format, considering factors such as time zones, language barriers, and cultural differences.

6.1.4 Confirm any information that the client needs to make available in advance, e.g. including a list of typical documented information, objective evidence and roles and responsibilities.

6.1.5 Ensure that auditors receive appropriate training and guidance on conducting remote/blended audits effectively.

6.1.6 Audit plans shall make clear that an onsite, remote, or blended approach is being implemented in respect to a given audit activity and contain concise details as to the ICT (reference IAF MD 4:2025 and other normative documents) or other remote method to be used.

6.1.7 When a combination of remote and on-site auditing methods is used, ensure that the plan is clear as to which part of the audit will be remote, which auditors will be remote (if applicable), which auditors are to be on-site and which methods are used by which auditor.

6.1.7 The auditor shall ensure that the audit plan and audit report reference tools that are used to assist remote/blended auditing.

6.1.8 Audit plans and risk assessments will be retained as client records by MSECB.

[1] For ISO/IEC 27001, please refer to requirements of clause 9.1.3.3.
[2] Note 1: For ISO 9001, ISO 14001, and ISO 45001 see IAF MD5
Note 2: For ISO 45001, remote audit activities shall be limited to reviewing documents/records and to interviewing staff and workers. Processes control and OH&S risk control cannot be audited using remote audit techniques.
Note 3: For ISO/IEC 27001 see ISO/IEC 27006-1:2024
Note: 4: For ISO/IEC 20000-1 see ISO/IEC 20000-6

6.2 Conducting the Remote/Blended Audit

During remote/blended audits, MSECB shall:

6.2.1 Utilize secure and reliable communication platforms and technologies for conducting interviews, reviewing documentation, and gathering audit evidence.

6.2.2 Verify the authenticity and integrity of information provided by the client through appropriate means, such as digital signatures or secure file transfer protocols.

6.2.3 Maintain confidentiality and data privacy throughout the audit process, adhering to applicable legal and regulatory requirements.

6.2.3.1 Consider the implications and the commercial sensitivity of data, with agreements to cover the management of recordings or other data transferred during observations at the outset.

6.2.3.2 Recording of interviews and screenshots of documents are usually not permitted.

6.2.3.3 The auditor shall not accept any audit records sent by the client via email or insecure means.

6.2.3.4 Documents made available to the auditor must be discarded or destroyed after the audit is completed, and the auditor may provide confirmation through email for this.

6.2.4 Document all audit activities, findings, and decisions in accordance with established procedures and guidelines.

6.2.4.1 Should an item not be able to be reviewed or complete determination not be able to be made, a record should be made.

6.2.5 For Initial Audits, the results of the Stage 1 Audit shall inform and confirm the ongoing approach (onsite, remote, or blended audit).

6.2.6 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.

6.3 Communication and Reporting

MSECB shall:

6.3.1 Maintain open and transparent communication with the client throughout the remote audit process, addressing any concerns or issues promptly.

6.3.2 Provide clear and concise audit reports detailing the findings, conclusions, and recommendations resulting from the remote audit.

6.3.3 Ensure that audit reports are issued within the agreed-upon timeframe and in compliance with relevant standards and accreditation requirements.

6.3.4 Audit reports clearly state the extent of use of ICT as well as the effectiveness of its use in achieving audit objectives. The report must indicate those processes that could not be audited and should have been audited on-site (if any). This information is important for the decision process and subsequent audits.

6.3.5 Where the activities of the organization are not undertaken at a defined physical location and therefore all activities of the organization are conducted remotely, the audit report shall state that all activities of the organization are conducted remotely.

6.3.6 If virtual sites are included within the scope, the certification documentation shall note that virtual sites are included, and the activities performed at the virtual sites shall be identified.

6.3.7 Communication between the Auditor and the client for sending documents or clarification on issues and corrective management shall be pre-defined and communicated.

6.3.8 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.

6.3.9 Where no activity of the organization within the scope of certification is undertaken at a defined physical location at all, the certificate and the audit report shall state that all activities of the organization are conducted remotely.

Annex A – Risk-Based Audit Approach

Audit Type	High-Risk Approach	Low-Risk Approach
Stage 1	Remote	Remote
Stage 2	Onsite	Onsite
Surveillance 1	Remote	Remote
Surveillance 2	Onsite	Remote
Recertification	Remote	Onsite
Surveillance 1 (post-Recert.)	Onsite	Remote
Surveillance 2 (post-Recert.)	Remote	Remote

Notes:

1. MSECB reserves the right to modify the audit sequence and means of delivery at its sole discretion.
2. Upon client's request, all audits can be conducted onsite regardless of level of risk.
3. For fully remote clients, full remote audits are permissible regardless of level of risk.
4. Auditors may allocate up to:
    a. 20% of the total audit duration for planning and audit report writing for ISO 9001, ISO 14001, ISO 22301, ISO 37001, ISO 20000-1, ISO 13485, ISO 20121.
    b. 30% of the total audit duration for planning and audit report writing for ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 42001.