ORIENTATION FOR CARRYING OUT REMOTE AUDITS - PCA

OBJECTIVE OF THE GUIDANCE

To ensure that all remote auditing activities are conducted in a controlled, secure manner and in accordance with the requirements of the specific Regulations for each scope and / or of Inmetro Ordinance 118: 2015- RGCP.

To ensure that each auditor is aware of the risks and opportunities for assessment within the scope of the remote audit process, including the use of ICT (Information and Communication Technology).

DEFINITIONS

Remote audits - Audits carried out using ICT (Information and Communication Technology)

ICT auditing, in general, means any assessment of company systems, using software and hardware, such as:

- Smartphones,
- Portable devices,
- Portable computer (Laptop),
- Desktop computers,
- Drones,
- Video cameras,
- Wearable technology,
- Artificial intelligence,
- Others.

At Bureau Veritas, remote auditing consists of auditing the client's website only through:

• Online video conference, to share and review documents and interviewing the auditee (s), in real time.

AUDIT APPLICABILITY (TYPES)

Factory audits procedure / Remote complaints handling applies to the following types of audits:

- Initial audits;
- Surveilance audits;
- Recertification audits;
- Extraordinary audits;
- Closing Audit.

Application of remote auditing to any other type of auditing must be agreed and approved by the Technical Management.

AUDIT PLANNING

In planning the audit, the Auditor should consider the use of ICT, as defined above, as well as the Assessment of Risks and Opportunities.

It is important that when sending the plan, it is clear that the audit will be remote and which language will be used in the case of international ones.

The suggested tools are preferably Zoom and Skype.

If the customer has any other tool for remote access and proposes to use it, it can be used.

Important - Test the connection with the auditee (s) the day before the event.

AUDIT PERFORMANCE

The general rules for carrying out the audit remain the same as for traditional auditing.

Start with the opening meeting as already practiced.

Important1 - Use more than one computer / tablet during the evaluation, as it will be possible to complete the report during the event, avoiding rework

AUDIT REPORT

The audit report must have recorded the remote condition and the list of people who participated in the audit. This record can be found in the Information field of Form_017.

ASSESSMENT OF RISKS AND OPPORTUNITIES

Any risk observed, the event must be stopped immediately and the schedule informed. The occurrence will be evaluated to decide how and when the event will be held.

Risks such as:

- Security breach risks

- Loss of data during the event.

- Unstable connection or lack of connection.

- Risks related to breach of confidentiality,

- Lack of confidentiality during the event. The use of security screens, headphones, private rooms is recommended.

- Carry out the evaluation in public places, which is prohibited.

- Recording, PrtSc or equivalent.

- Technical eligibility risk / technical risks,

- Lack of adequate infrastructure;

- Lack or outdated antivirus

- Use of illegal software

- Operational risks,

- Insufficient time;

- Less inquisitive audit (difficulty in accessing the process and documentation)

- Significant organizational changes since the last assessment;

- Risks related to human resources.

- Incomprehension of the auditee (s) about the requests;

- Lack or great difficulty of the auditee (s) with the tool.