GENERAL TERMS AND CONDITIONS FOR CERTIFICATION CONTRACTS

An integral part of the certification contracts concluded with the management systems certification body of INCERT EOOD

CONTENTS

1. Introduction 1
2. Types of management systems and certification schemes 1
3. Application for certification 1
4. Transfer of accredited certification 1
5. Audit process 2
6. Audits of management systems 2
6.9. Special audits – scope extension and unscheduled audits 3
7. Actions in case of extraordinary events or circumstances 3
8. Conducting remote audits 4
9. Information regarding payments 5
10. Decisions related to certification 6
11. Nonconformities 6
12. Reference to certification and accreditation 7
13. Consideration of complaints and appeals 8
14. Provision of information upon request 9
15. Privacy Policy 9
16. Impartiality policy 9
17. Announcement of changes by a certified client 10
18. Announcement of changes by the certification body 10
19. Disclaimer 10
19.1. It should be borne in mind that any audit is based on an assessment of a sample of the client's management system, and therefore 100% compliance with the requirements is not guaranteed. 10
20. Anti-bribery management system (ABMS) certification only 10
- End - 10

1. Introduction

1.1. The General Terms and Conditions for Certification Contracts provide information about the certification process of the certification body of INCERT EOOD.

1.2. The certification body for management systems at INCERT EOOD must comply with ISO/IEC 17021-1 and other standards and mandatory documents related to certification. When planning and conducting audits, the certification body also applies the guidance of ISO 19011:2026, insofar as it does not contradict these requirements.

1.3. The client, not the certification body, is responsible for maintaining its management system and achieving its objectives, and the certification body is responsible for assessing sufficient objective evidence of conformity with the requirements of the specific standard on which to base the decision to grant or refuse certification.

1.4. These General Terms and Conditions are an integral part of the certification contract concluded between INCERT EOOD and the Client. Each client undertakes to comply with them by signing a certification contract.

2. Types of management systems and certification schemes

2.1. The certification body for management systems is a separate structure in the legal entity INCERT EOOD, registered under the Commercial Law of Bulgaria, with registered office and address of management Sofia, 45 Kalimantsi Str., Office 3 and EIK 205511883.

2.2. The certification body for management systems of INCERT EOOD offers certification to the following management systems and certification schemes:

2.2.1. Quality Management Systems (QMS);

2.2.2. Environmental Management Systems (EMS);

2.2.3. Occupational Health and Safety Management Systems (OHSMS);

2.2.4. Information Security Management Systems (ISMS);

2.2.5. Road Traffic Safety Management Systems (RTSMS);

2.2.6. Food Safety Management Systems (FSMS);

2.2.7. Anti-bribery Management Systems (ABMS).

3. Application for certification

3.1. Each potential client completes an Application for Certification. The application is completed online via the certification body's website www.incert.bg; where necessary, a member of staff of the certification body assists in completing it.

3.2. The application for certification shall provide the certification body with the necessary information regarding:

3.2.1. the desired scope of certification;

3.2.2. appropriate details of the applicant organisation as required by the specific certification scheme, including the name and address(es) of its locations, its processes and activities, human and technical resources, functions, relationships and any applicable legal obligations;

3.2.3. identification of all processes outsourced by the organisation that affect compliance with certification requirements;

3.2.4. the standards or other requirements for which the applicant organisation wishes to be certified and whether consultancy services related to the management system to be certified have been used and, if so, by whom.

3.3. A representative of the certification body shall review the completed application and any additional information related to the certification to ensure that:

3.3.1. the information on the applicant organisation and its management system is sufficient to develop an audit program;

3.3.2. all identified differences between the certification body and the applicant organisation are resolved (e.g. inaccurate or incomplete information is obtained which does not allow for a decision to be taken);

3.3.3. the certification body has the necessary competence and ability to perform the certification activities;

3.3.4. the desired scope of certification, the locations where the applicant organisation operates, the audit duration, and other issues affecting certification are taken into account (e.g. language, safety conditions, threats to impartiality, etc.)

3.4. If necessary, an employee of the certification body shall contact the representative of the potential client for clarifications and additional information.

3.5. A competent person in the certification body decides to accept or reject the application. If the application is accepted, it is submitted to prepare an offer and a draft contract.

3.6. The certification application may be rejected if the certification body cannot meet the requirements specified above. In this case, a motivated written response is sent to the client, stating the reasons for the refusal.

3.7. If the application for certification is accepted, an audit program is developed for the client, which determines the audits, duration, the scope of certification, audited sites, etc. Based on the approved audit program for the specific client, a price offer and a draft contract are prepared. They are sent to the client, together with the current General Terms and Conditions for Certification Contracts, which are an integral part of the contract. The certification procedure starts after signing a contract.

3.8. When certification of an integrated management system is requested in the application, the client shall provide information to the certification body to determine the level of integration of the system.

3.9. If it is confirmed that the system is "fully integrated", the audit program, including the audit time, is developed taking into account this circumstance (it may lead to the planning of fewer audit days).

3.10. During Stage 1 of the initial on-site audit, the audit team conducts a planning session to confirm that the system is "fully integrated".

3.11. If the audit team cannot confirm this, it may be recommended to increase the audit time and renegotiate the conditions under which the certification will take place.

3.12. All offers for certification of integrated management systems and the relevant contracts shall explicitly state whether the audit program and audit time are defined for a "fully integrated system".

4. Transfer of accredited certification

4.1. "Transfer" (or "transfer") of certification means the recognition of an existing and valid management system certification issued by one accredited certification body by another accredited certification body to issue its certificate.

4.2. Only organisations already certified by another certification body accredited by an accreditation body that is a signatory of IAF/MLA level 3, and where levels 4 and 5 are applicable, may be eligible for transfer of certification. A list of accreditation services signatories to the IAF/MLA is available at http://www.iaf.nu/.

4.3. Only valid certification can be transferred. Certification known to be withdrawn or invalid cannot be subject to a transfer.

4.4. If the certification has been granted by a certification body that is no longer operational, or whose accreditation is no longer valid, or has been terminated or withdrawn, the transfer must be completed within six months from the date of expiry of the accreditation (or its termination or withdrawal) or before the expiry of the certification, whichever is earlier. In such cases, before accepting the transfer, the certification body of INCERT EOOD notifies its accreditation body, under whose accreditation it intends to issue the certificate.

4.5. Prospective clients wishing a transfer of certification shall complete the relevant section in F 03-01 Application for Certification, enclosing copies of the documents specified in the application.

4.6. For a transfer of certification to be accepted, the following conditions must be met at the same time, which are confirmed by the certification body of INCERT at the pre-transfer review stage:

4.6.1. The following documents must be available:

- The last valid certificate issued;
- Stage 2 report of the initial audit or the last recertification audit (which is applicable);
- Report from the latest surveillance (if applicable);
- Evidence that all nonconformities described in the reports have been closed or correction/corrective action plans have been approved;
- Audit Program in the certification cycle, provided by the certification body that issued the certificate (if available);

4.6.2. The certification subject to transfer is valid, i.e. not suspended, which is proven by checking in reliable public registers (public register of the Accreditation Service, IAF CertSearch) or by contacting the certification body that has issued the certificate.

4.6.3. The certification body of INCERT must have valid accreditation for the relevant certification scheme and the relevant scope (NACE code/s or technical areas, as applicable), which are within the scope of the multilateral agreement to which our accreditation body is a signatory.

4.6.4. The certification body that issued the certificate must have valid accreditation for the relevant certification scheme and the relevant scope (NACE code/s or technical areas, as applicable), which are within the scope of the multilateral agreement to which its accreditation body is a signatory.

4.6.5. The site for which a transfer is sought shall have a valid accredited certification.

4.6.6. Until the date of the transfer request, the audit program of the certification body which has issued the certificates has been implemented, which is proven by a review of the submitted report and audit program.

4.6.7. All major nonconformities have been closed as of the review date.

4.6.8. For all minor nonconformities, a corrective action plan has been approved as of the review date.

4.6.9. The complaints and the actions taken on them are acceptable.

4.6.10. Information is available on the legal requirements applicable to the client scope of certification and the reasons for seeking a transfer.

4.7. INCERT may request a pre-transfer visit before the completion of the pre-transfer review if:

4.7.1. Not all major nonconformities have been closed as of the review date.

4.7.2. Not all minor nonconformities have an approved corrective action plan at the review date.

4.7.3. It cannot be confirmed that the complaints and their action are acceptable.

4.8. After completing the pre-transfer review, the client is informed in writing about the result. In case of a positive result, an audit programme is developed for the client, including the audits that are to be performed in the current certification cycle. The client is provided with an offer and a draft contract for the transfer of certification, and a transfer decision may be taken only after the client signs the contract. After the decision to transfer the certification is taken, it is the responsibility of the certification body of INCERT EOOD to notify the certification body which issued the certificate.

4.9. In case it is decided that the transfer is not acceptable, the client may be provided with an offer as a new client with a start of a new certification cycle. In all cases, the client is informed in writing about the reasons for accepting or refusing to perform a transfer of certification.

4.10. After each decision for certification transfer, the client is issued a certificate. The date of issue is the date of the decision to transfer the certification. The date of validity of the certificate is the same as the expiry date of the certificate issued by the previous certification body.

4.11. Global ACI-TECH-3-002 (M)[1] requires accredited certification bodies to cooperate by exchanging information in the certification transfer process. The same document obliges the certification body that issued the certificate not to suspend or withdraw the client's certification without justified reasons.

5. Audit process

5.1. Management system certification is a way to ensure that an organisation has implemented and applies a management system for aspects related to its activities, products and services in accordance with its policy and the requirements of the relevant international management system standard. Certification is independent proof that the management system of an organisation conforms to the specified requirements, is capable of consistently achieving its stated policy and objectives and is effectively implemented.

5.2. Certification activities are the individual activities from the review of the application to the completion of certification. They also include audits of an organisation's management system. Audits are a systematic, independent and documented process for obtaining objective audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled (e.g. the applicable management system standard, certification requirements, etc.)

5.3. The audit program for the initial certification cycle includes an initial two-stage audit, surveillance in the first and second years and a recertification audit after the third year but before the certification expires.

Additionally, it is possible to conduct special audits, e.g. at the request of a certified client to extend the scope of certification or based on received complaints or grievances. All audits are conducted on dates agreed in advance with the client. All audits are performed by competent auditors and technical experts who have been assessed and approved by the certification body.

5.4. The certification body shall also apply procedures to ensure that auditors perform their duties impartially and objectively and maintain confidentiality.

5.5. Audits are conducted on-site at the client, remotely (see section 8) or by a combination of both methods – for example when part of the audit team works on-site and another part participates remotely, or when a virtual location is audited. The method for each audit is determined by the certification body in the audit programme on the basis of a risk assessment and of the ability of the method to achieve the audit objectives, taking into account the available information and communication technologies (ICT). Where these General Terms and Conditions state that an audit is conducted on-site, this does not exclude the use of remote audit methods for parts of the audit, where permissible under section 8.

6. Audits of management systems

6.1. The certification activities start with an initial audit carried out in two stages.

Initial audit stage 1

6.2. Stage 1 of the initial audit must take place no later than six months after signing the certification contract. After this period, it is necessary to submit a new application for certification.

6.3. The audit is conducted on-site at the client premises, and only in exceptional limited cases, it is allowed to conduct it outside the client's site, including as a remote audit (see 8.7).

6.4. The objectives of the stage 1 audit are:

- to review the documented information about the client management system;
- to assess the specific conditions of the client and conduct interviews with the client's staff to determine the level of preparation for stage 2 audit;
- to review the client's condition and understanding of the requirements of the applicable standard (s), especially about the identification of the most important results or significant aspects, processes, objectives and the functioning of the management system;
- to gather the necessary information on the scope of the management system, including the locations of the client's organisation, the processes and the technical means used, the established levels of control (especially in the case of different locations) and the applicable legal requirements established by a regulatory or other competent state body.
- To review the allocation of resources for the Stage 2 audit and agree with the client on the details of the Stage 2 audit;
- to plan stage 2 audit after sufficient understanding of the client's management system and its functioning on-site in the conditions of the requirements

[1] Global ACI-TECH-3-002 (M) "Mandatory Document for the Transfer of Accredited Certification of Management Systems", version 1.0 of 10.07.2026, applicable from 28.08.2026. Replaces IAF MD 2 (in the previous version of this document – IAF MD 2:2017; latest edition IAF MD 2:2023).

of the applicable management system standard (s) and other normative documents have been achieved;

- to assess whether the internal audits and management review have been planned and performed and whether the degree of implementation of the management system demonstrates that the client organisation is ready for stage 2 audit.
- to confirm with the client the scope of certification (including the correct wording);

6.5. The specific objectives of the Stage 1 audit for Food Safety Management Systems (FSMS) are to focus on the planning of Stage 2 of the audit by gaining an understanding of the organisation's FSMS and of the organisation's state of readiness for Stage 2 of the audit by reviewing the extent to which:

- the organisation has identified the prerequisite programs that are appropriate for its activities (e.g. regulatory requirements, customers and the certification scheme),
- FSMS includes adequate processes and methods for identification and assessment of hazards to food products of the organisation and appropriate selection and categorisation of control measures (combinations),
- FSMS includes adequate processes and methods for identification and application of the relevant food safety legislation;
- FSMS is developed to achieve the food safety policy of the organisation,
- the implementation of the FSMS program gives the right to proceed with the audit procedures (stage 2),
- the programs for validation of the measures for control, the inspection of activities and improvement comply with the requirements of BDS EN ISO 22000:2018;
- the FSMS documents and agreed measures are applied to carry out the internal exchange of information and communication with the respective suppliers, customers and stakeholders, and
- there is some additional documentation that needs to be reviewed and/or information to be obtained in advance.
- When an organisation has implemented externally developed combined control measures, during Stage 1, a review of the FSMS documentation is done to determine whether the combination of control measures is suitable for the organisation, whether it has been developed following the requirements of BDS EN ISO 22000:2018, and kept up to date.
- When collecting information on compliance with the regulations, the availability of the relevant permits is also checked.
- Non-compliant documentation is identified in the summary of compliance of the documents.
- The report identifies "areas of concern" that could be classified as nonconformities during the stage 2 audit. Stage 2 of the initial audit cannot start until any major areas of concern in the system documents have been satisfactorily resolved.

6.6. Initial audit stage 2

6.6.1. Stage 2 of the initial audit must take place no later than six months after Stage 1. If stage 2 is not conducted within this period, a new stage 1 must be conducted.

6.6.2. The stage 2 audit aims to evaluate the implementation, including the effectiveness, of the client's management system. The stage 2 audit is carried out on-site at the client according to an audit plan agreed in advance with the client. For clients with more than one site, the audit should cover the full scope of all sites and each site separately, where applicable.

6.6.3. The audit team analyses all information and evidence gathered during the stage 2 audit, reviews the findings, and formulates the audit conclusions documented in an audit report.

6.7. Surveillance

6.7.1. Following the certification, the certification body shall plan and perform a series of surveillance activities to ensure that the management system consistently meets the requirements of the applicable standard and that the certification requirements are met.

6.7.2. Surveillance activities include on-site audits to verify the compliance of the certified client management system with the requirements set out in the applicable standard to which the certification is granted.

6.7.3. The surveillance activities are planned so that the characteristic areas and functions that are within the scope of the certified client's management system are subject to regular monitoring and to take into account changes in the organisation and its management system, as well as complaints received, findings from previous audits, incidents that have occurred and changes in the client's regulatory and operational environment.

6.7.4. Surveillance audits shall be carried out at least once in a calendar year, except in recertification years. The date of the first surveillance audit following initial certification shall not be more than 12 months from the date of the certification decision. Unless otherwise justified, the second surveillance audit in a certification cycle is conducted no later than 24 months after the date of the certification decision.

6.7.5. Surveillance audits are not necessarily complete system audits and are planned so that the certification body can maintain confidence that the certified management system continues to comply with the certification requirements between two audits.

6.7.6. Each surveillance is conducted on-site according to a pre-agreed with the client audit plan. The audit team analyses all information and evidence gathered during the audit, reviews the findings, and formulates the audit conclusions documented in an audit report.

6.7.7. In this order, the surveillance is planned and conducted after the recertification audit and after a certification transfer.

6.8. Recertification audits

6.8.1. Recertification audits are planned and conducted in due time to allow timely recertification before the certificate expiry date.

6.8.2. 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 the applicability of the scope of certification.

6.8.3. The recertification audit is carried out according to an audit plan agreed with the client, on-site at the client. For clients with more than one site, the audit should cover the full scope of all sites and each site separately, where applicable.

The audit team analyses all the information and evidence collected during the audit, reviews the findings and formulates the audit conclusions in a report.

6.8.4. Recertification audits are conducted before the expiry of the certification. All corrections and corrective actions for major nonconformities must be implemented by the client and verified by the certification body before the expiry of the certification.

6.8.5. When all recertification activities have been successfully completed before the expiry of the existing certification, a decision on recertification is taken. The date of issue of the new certificate is the date following the expiry date of the existing certification, and the new certificate is valid until the expiry date of the existing certification plus three years.

6.8.6. If the recertification audit has not been completed or the certification body is unable to verify the effectiveness of the corrections and corrective actions for any major nonconformity before the expiry of the existing certification, no decision on recertification is taken. The client is informed in writing of the results and the consequences.

6.9. Special audits – scope extension and unscheduled audits

6.9.1. Scope extension audits may be conducted outside the approved audit programme, or during a scheduled surveillance audit or recertification audit. The audit report must contain sufficient information regarding the extended scope to justify a decision to extend the scope of certification.

6.9.2. The certification body may conduct unscheduled or unannounced audits of certified clients to investigate complaints, or in response to changes, or as follow-up on clients with suspended certification. In these cases, the certification body plans the audit in the same way as a surveillance audit is planned, but taking into account the objectives, scope and criteria for the specific unscheduled audit.

6.10. The specific objectives of FSMS audits are:

- To assess the effective implementation (identification and selection, if permitted) of the management of food safety hazards (this includes hazard analysis and critical control points (HACCP), as defined in the scheme);
- To assess the effective management of the interrelated processes of the FSMS;
- To assess system ability to meet applicable statutory and regulatory requirements;
- To assess the organization’s use of an effective risk-based approach to products and processes and management of change;
- To assess whether the requirements of the scheme and of the organization, if any, are met;
- To verify that the certification scope is appropriate to the activities of the orgnisation and audit sampling is representative.

7. Actions in case of extraordinary events or circumstances

7.1. "Extraordinary event or circumstance" is a circumstance that is beyond the control of the organisation (certification body, client), also called "force majeure",

etc. These include but are not limited to hostilities, riots, strikes, political instability, geopolitical tensions, terrorism, crime, pandemics, floods, earthquakes, malicious intrusions into computer systems, and other natural or man-made disasters.

7.2. These actions shall be applied if deemed necessary due to extraordinary events or circumstances or when requested by a specific certified organisation affected by an extraordinary event or circumstance that temporarily prevents the certification body from conducting scheduled on-site audits client's premises.

7.3. The certification body assesses the client's current and expected future situation. It identifies alternative short-term methods for evaluating the organisation to ensure that the management system's effectiveness is maintained.

7.4. To assess the current and future situation with the client and to make decisions about the necessary actions, the certification Body collects information in the following areas, as applicable:

- When the organisation will be able to function normally;
- When the organisation will be able to manufacture products or provide services within the scope of certification;
- Will the organisation use alternative sites for production and/or distribution; If so, are these sites included in the scope of certification or will they need to be further assessed;
- Whether the available products meet customer requirements or the organisation will have to agree permissible deviations with its customers;
- If the organisation is certified under the schemes ISMS, EMS and/or OHSMS, i.e. a scheme that requires emergency preparedness and response capability or a contingency plan, has the organisation implemented the plan and has it been effective?
- Will some of the implemented processes/services or products be outsourced? If so, how will the certified organisation control the activities of these other organisations;
- To what extent is the functioning of the management system affected;
- Has the certified organisation made an impact assessment;
- For organisations with more than one site, is it possible to identify alternative sites as part of the audit sample;

7.5. If the risk of continuing certification is low and based on the information gathered, the certification body allows alternative short-term assessment methods to verify the continued effectiveness of the management system.

7.6. These alternative short-term methods include reviewing records by the certification body without a site visit to determine the effectiveness of the system and compliance with certification requirements (short-term only) and include the following documents:

- Minutes of management reviews;
- Records of corrective actions,
- Records from internal audits;
- Records of tests/inspections, etc. (if applicable).

7.7. The certification body informs the client in writing about its decision stating at least the following:

- Result of the assessment and possible follow-up;
- Indication of the maximum period for which the alternative short-term assessment method may be applied before the certification is suspended or revoked.
- The criteria for the reinstatement of normal surveillance activities (at least - the possibility of access to the affected sites), including the method and timing of activities and assessments to restore normal activities.
- Proposed amendments to the organisation's audit program;

7.8. Any deviations from the accreditation requirements and the certification body procedures must be justified and documented. All plans for temporary deviation from the requirements must be agreed upon in advance with the accreditation service.

7.9. If contact with the organisation cannot be established, the usual procedures for suspension and revocation of certification are followed.

7.10. In developing alternative short-term assessment methods, the certification body shall take into account the following limitations:

7.10.1. First surveillance

Based on sufficient evidence collected under items 7.4 – 7.6 above, which gives confidence that the certified management system is effective, the first surveillance may be postponed for a period not longer than six months, i.e. up to 18 months from the date of initial certification.

Otherwise, the certification must be suspended or the scope reduced.

7.10.2. Subsequent surveillance

The requirement of clause 9.1.3.3 of BDS EN ISO/IEC 17021-1:2015 applies, namely "Surveillance audits shall be conducted at least once a calendar year, except in recertification years."

There may be specific circumstances through which the certification body justifies the determination of the period for subsequent surveillance. If an organisation is forced to suspend operations for a limited period (less than six months), the certification body may postpone an audit planned for the closure period until the organisation resumes operations. The organisation must inform the certification body when activities resume so that the audit can be planned and conducted without delay.

7.10.3. Recertification Audits

Based on sufficient evidence gathered under items 7.4 – 7.6 above to give assurance that the certified management system is effective, the certification may be extended for a period not exceeding six months. The recertification audit must be carried out within this period. Otherwise, a new initial audit must be performed. The validity of the renewed certification must be based on the initial certification cycle.

All deviations from approved audit programs must be justified, documented and made available upon request by the accreditation body.

7.11. If an extraordinary event or circumstance occurs during an audit (on-site or remote), the lead auditor reviews the situation with the client and a decision is taken whether the audit is interrupted, rescheduled or continued (e.g. with a change of the method or of the audit plan). Changes to the audit plan are agreed with the client and documented, and where the audit objectives cannot be achieved, this and the reasons for it are stated in the audit report.

8. Conducting remote audits

8.1. Remote audits[2] are "activities carried out in any place other than the location of the audited entity, regardless of distance." The term corresponds to “remote audit method” as per ISO 19011:2026, 3.4 and ISO/IEC TS 17012:2024. A remote audit may cover the whole audit or only part of it and may be combined with an on-site audit; it is also applicable to virtual locations (see 8.9).

8.2. Use of ICT (information and communication technologies)[3] is "the use of technologies for the collection, storage, retrieval, processing, analysis and transmission of information. ICT includes software (communication software or operating system) and hardware such as laptops, desktops, drones, video cameras, wearable technology, artificial intelligence, etc. The use of ICT is suitable for both on-site and remote audits. "

8.3. Methods and tools used in remote audits

8.3.1. Teleconferencing, including audio, video and data sharing, but limited to mobile and desktop computers;

8.3.2. Telephone interviews;

8.3.3. review of documents and records by remote access in real-time or by e-mail;

8.3.4. Providing visual and audio access to facilities (e.g. remote or potentially dangerous sites), e.g. by drones or cameras installed on moving remote-controlled robots or carried by the organisation's staff working on-site in direct video/audio contact with the auditor/audit team member.

8.4. Remote activities (i.e., exchanging information between the client's representatives and the audit team) must be performed in real-time.

8.4.a. The objective of remote auditing techniques should be to enhance audit effectiveness and efficiency, and to support the integrity of the audit process.

8.5. Criteria for using remote audit

The certification body may allow remote audits after assessing the presence/absence of the following circumstances:

- Travel to the client's physical location is not suitable due to objective reasons related to risks to the lives and health of the teams, imposed travel restrictions, etc.
- The number of sites within the scope of the system is difficult to evaluate in a reasonable time using traditional audit methods.
- The client systematically applies a database management system in which records and data can be viewed regardless of where they are created.
- The audit is for minimal extension of the scope.

[2] Ref. ISO 19011:2026 Guidelines for auditing management systems, Annex A.1

[3] Ref. Global ACI-TECH-3-003 (M) Mandatory Document for the Use of ICT for Conformity Assessment Purposes (formerly IAF MD 4:2018, Issue 4)

- There is evidence of the conformity of the client's location from previous on-site audits.
- The certification body assessed the risk associated with conducting a remote audit for the specific client as low.
- The certification body has an auditor (s) who have performed previous on-site audits and are well acquainted with the client's management system and practices.
- The remote audit investigates complaints received by the certification body for the certified organisation.

8.6. A remote audit may not be performed in any of the following circumstances:

- In case of major nonconformities or a large number of nonconformities (five or more) in a previous on-site audit at the client;
- In the initial stage 2 audit (except for the case for ABMS under 8.7), for a scope extension (except for a minimal extension – see 8.5) or for adding a new site to the scope;
- When we do not have a lead auditor who has already performed an on-site audit of the specific client, or the same lead auditor does not have the competence to perform a remote audit.
- When the client's on-site audit has not been conducted for an extended period (e.g. at one of the sites in organisations with more than one site);
- When significant changes have occurred in the audited organisation;
- When a regulatory act or certification scheme requires a mandatory on-site audit.

Where an interpreter is needed for a remote audit, he/she participates under the same ICT, information security and confidentiality requirements as the audit team members, and additional time is provided in the audit plan where necessary.

8.7. Types of audits that may be planned and conducted as a "remote audit":

- Stage 1 of the initial audit (limited to small clients, with justification);
- Stage 2 of the initial audit (limited to the certification of ABMS, where sampling of sites is not allowed; applicable only to additional sites with an identical scope, different from the central function, provided that a sufficient number of sites are visited to ensure confidence in the audit conclusions – the rationale must be documented).
- Surveillance;
- Recertification Audit;
- Audit to assess the effectiveness of corrective actions;
- **All types of ISMS audits, if the client does not conduct activities at physical sites.**

8.8. No reduction in audit time or audit duration due to ICT use is allowed.

8.9. Audits of Virtual Locations

8.9.1. A virtual location audit is considered a remote audit.

8.9.2. A virtual location is a location where the organisation performs work or provides a service using an online environment that allows individuals, regardless of their physical location, to run processes (i.e., organisations with online operating systems where all processes can be performed by staff at different locations/addresses or in the internal software environment of the organisation).

8.9.3. Situations where processes must be performed at a physical location, such as a warehouse, production site, testing laboratory, installations or product repairs, cannot be audited as virtual sites. An example of such a virtual site is a development organisation in which all employees work remotely, for example in a cloud environment.

8.9.4. If there is a virtual site in the scope of certification, it must be indicated as "virtual" on the certificate.

8.9.5. In ISMS certification, if the client does not perform activities at physical sites, the certificate shall state that all activities within the scope are conducted remotely.

8.10. In accordance with Global ACI-TECH-3-003 (M), [4]the certification body applies procedures to determine the level of remote audits that can be used when auditing the client's management system.

8.11. The procedures include the analysis and assessment of risks associated with the use of remote audits for a specific client, taking into account the following factors:

a) the available infrastructure of the Certification Body and the client;

b) the sector in which the client operates;

c) the type(s) of audit during the certification cycle—from initial certification to recertification audit;

d) the competence of the personnel from both the Certification Body and the client involved in the remote audit;

e) previously demonstrated outcomes from remote audits for the client;

f) the scope of certification;

g) the ability of the remote audit to achieve the audit objectives, including the availability and reliability of ICT at the client and at the certification body, the level of confidence in the evidence obtained and the applicable regulatory and certification scheme requirements.

8.12. The analysis is conducted prior to performing a remote audit. The analysis and justification for using remote audits during the certification cycle are documented.

8.13. The audit plan and audit report shall include information if remote audit activities were conducted.

8.14. Remote audits cannot be used if the risk assessment identifies unacceptable risks to the effectiveness of the audit process.

8.15. The risk assessment is reviewed before each audit within the certification cycle to ensure its continued applicability.

8.16. The successful conduct of a remote audit is a joint responsibility of the client and the audit team. Before the audit, the client and the certification body agree on the ICT used and the method of remote access to documents, records and sites, the information security and confidentiality measures, as well as the actions in case of loss of connection or technical problems (e.g. use of an alternative technology, rescheduling of part of the audit or adding time). Where necessary, a preliminary check of the connection and the platform is carried out.

8.17. During a remote audit, the client provides a suitable environment free of background noise and disturbances and, where necessary, plans or layouts of the remote locations. Screenshots and recordings are made only under the conditions of 15.6. Microphones and cameras are switched off during breaks to protect confidentiality.

9. Information regarding payments

9.1. We understand that our source of income is our clients who pay for the certification, which could be perceived as a potential threat to our impartiality. From our point of view, the clients do not pay for the issuance of a certificate but the services of the certification body of INCERT EOOD for conformity assessment and certification maintenance activities.

9.2. A certificate is issued according to the certification procedures and after confirming the compliance of the implemented and assessed system with the requirements of the respective standard.

9.3. The certification body for management systems of INCERT EOOD does not collect fees for reviewing certification applications.

9.4. Fees due by each client related to the provision and maintenance of certification are specified in their contract with the certification body for management systems of INCERT EOOD.

9.5. The annual fees include performing all certification maintenance activities, including conducting audits following the audit program. The basis for determining the annual fees is the duration of the audits, calculated in man-days required for the audit.

9.6. During the certification cycle, additional fees may be agreed upon between the certification body and the client for the performance of activities not provided for in the initial certification program, e.g. reissue of a certificate, closing of major nonconformities at the site at the client.

9.7. Payment terms and consequences of late payment

9.7.1. The annual fees are paid in advance, against an invoice, within the term set in the certification contract. By exception, with the agreement of the certification body, the audit may be performed before payment – in that case the fee is paid within 10 days after the last day of the audit. In both cases, no certificate is issued or reissued until the amount due has been paid.

9.7.2. If a payment is not made on time, the certification body sends the client an e-mail reminder with an additional term of 14 days.

9.7.3. If the amount is not paid within 30 days after the due date – or earlier, if the surveillance audit cannot be performed within the required timeframe because of the non-payment – the certification is suspended for up to 3 months (item 10.4). The status "suspended" is shown in the public register at www.incert.bg and in IAF CertSearch, and the client may not refer to the certification or use the certification marks.

9.7.4. If, within the suspension period, the client pays all amounts due and the

[4] Global ACI-TECH-3-003 (M) "Mandatory Document for the Use of Information and Communication Technology (ICT) for Conformity Assessment Purposes", version 1.0 of 10.07.2026, applicable from 28.08.2026. Replaces IAF MD 4:2025 (Issue 3) – the text was transferred without changes in substance.

missed audit (if any) is performed, the certification is restored without changing the validity of the certificate.

9.7.5. If the amounts due are not paid by the end of the suspension period, the certification is withdrawn (item 10.5) and the certification contract is terminated with the notice of withdrawal. The client owes the fees for the activities performed and the statutory interest for late payment. New certification is possible only after the outstanding amounts are paid and a new initial audit is performed.

10. Decisions related to certification

10.1. The following main categories of decisions can be taken in connection with certification:

- to continue with stage 2 audit (after stage 1 audit);
- to grant certification (after stage 2 audit);
- to extend or reduce the scope of certification;
- to continue the certification (after surveillance);
- for recertification (after a recertification audit);
- for temporary suspension, reinstatement or withdrawal of the certification;
- for transfer of certification.

10.2. Certificates are issued based on a certification decision and a recertification decision. Certificates are valid for three years (36 months minus one day) from the date of the certification decision. When a certificate needs to be reissued during the certification cycle (e.g. after an audit and a decision to extend the scope of certification, a change in the site address, etc.), it shall be reissued with its original validity, indicating the date on which it was reissued.

10.3. Recertification decisions are taken based on the results of the recertification audit, the review of the system for the certification cycle, and the complaints received from users of certification.

10.4. Certification may be suspended by a written decision of the manager of the certification body for one or more of the following reasons:

- the certified client management system permanently or seriously does not meet the requirements for certification, including the requirements related to the effectiveness of the management system;
- established nonconformities are not closed within the terms agreed with the client;
- the certified client does not allow performing supervisory audits and recertification audits with the required frequency;
- the certified client is misusing the certification or certification marks.
- the certified client has not paid a fee due within the term under item 9.7.3.

10.5. Certification may be withdrawn for one or more of the following reasons:

- the certified client does not want to renew their certification.
- the certified client wishes to terminate their certification; in this case, the client must notify the certification body in writing.
- the certified client terminates its activity.
- the certified client has not fulfilled the conditions for restoring the certification after suspension.
- the certified client has not paid the amounts due by the end of the suspension period (item 9.7.5).

10.6. When certifying integrated management systems, if certification under only one of the standards is subject to suspension, reduction or withdrawal, the certification body shall investigate and document the impact of these actions on the certification under the other management system standards and take action.

10.7. In the case of multisite organisations, if a major nonconformity is raised at a stage 2 audit or a recertification audit at one of the sites, no certification decision may be taken for the whole organisation until the organisation provides evidence that corrective actions have been taken at all sites within the scope of certification.

10.8. In the above case, the certification body will not accept that the "problematic" site be excluded from the scope of certification and that a decision be taken to grant certification only for the remaining sites.

10.9. After certification, if any of the sites within the scope of certification does not meet the certification requirements, this leads to suspension/withdrawal of the certification of the entire organisation and all its sites.

10.10. When certifying an OHSMS, the client is obliged to inform without delay the certification body about any accident related to health and safety at work or violation of the regulatory requirements in the field of OHS, which also imply actions by the state control authorities. The certification body may request a special audit to examine whether the management system has not been compromised and is functioning effectively. The certification body shall keep records of the results of this survey.

10.11. Based on information about accidents or violations of legal requirements, requiring the involvement of state control bodies, which is submitted by the client or directly provided to the audit team during a special audit, the certification body must decide on the necessary actions, including actions for suspension or withdrawal of certification, when it has been demonstrated that the OHSMS does not significantly comply with the certification requirements.

10.12. In case there are specific legal requirements that the organisation does not comply with, the organisation must be able to demonstrate that it is implementing a compliance plan within a specified period, supported by a written agreement with the control body (or other documents according to the specific requirements). Successful implementation of this plan should be a priority within the OHSMS.

10.13. In exceptional cases, the certification body may decide to grant certification, but only after receiving sufficient objective evidence that the organisation's OHSMS (all three conditions must be met simultaneously):

- is able to achieve the required compliance by fully implementing the above plan within the deadline set therein,
- includes all OHS hazards and risks to workers and other personnel, and that there are no activities, processes or situations that can or could lead to significant occupational diseases or accidents, and
- there are sufficient control mechanisms to ensure that during the transition period, any OHS risks are reduced and controlled.

10.14. The certification body may limit the scope of a client's certification to exclude from the scope activities that do not meet the certification requirements if the client systematically or to a large extent fails to meet the certification requirements for that part of the scope.

10.15. These decisions are taken by the certification body manager, documented and communicated to the client, and the decision is kept in the client's file. Upon request, the certification body provides information on the status of the certification of any client.

11. Nonconformities

11.1. Any nonconformities found during an audit are categorised as minor or major. The classification criteria are defined in 11.2 and 11.3 and are applied consistently in all audits. Each nonconformity is described clearly, stating the requirement, the objective evidence and why the requirement is not fulfilled.

11.2. A minor nonconformity is a failure to fulfil a requirement, as a result of which:

- The effect of non-compliance is likely to have a negligible impact on the activities and efficiency of the management system, processes or results of processes, activities, products, waste and sources of pollution (in EMS), systems and procedures.
- it is unlikely to reduce the ability to ensure effective process management;
- is unlikely to lead to delivering a non-compliant product/service to the customer.

11.3. A major nonconformity is a failure to fulfil a requirement where:

- A system document is missing or is not complied with at all, or the requirements of one or more of the clauses of the management system standard against which the audit is performed are not fulfilled/maintained.
- The effect of non-compliance is likely to reduce the ability to use the product or the safe use of the product or service.
- There is a significant impact on the activities and efficiency of the management system, processes or results of processes, activities, products, waste and sources of pollution (in EMS), systems and procedures.
- It is very likely to lead to delivering a non-compliant product/service to the customer.
- Several minor nonconformities with the same clause of the standard, which, taken as a whole, indicate that the requirements of the clause are not being met.

11.4. Each nonconformity is documented in a separate Nonconformity Report (F 05-24), which is accepted by a client representative. If several unfulfilled requirements are found under one clause of the audited standard, they are combined into one nonconformity (e.g. described with sub-items). It is not permissible to have several nonconformities in one audit under the same clause.

11.5. The client must take action on any nonconformities found by performing a root cause analysis to determine the most appropriate corrective action and ensure that the corrective action is performed and effective.

11.6. For all minor nonconformities, the client must submit to the audit team proposals for corrective actions, which need to be approved as appropriate by the

lead auditor in order to proceed with a decision to grant or renew certification.

11.7. All major nonconformities must have corrections and corrective actions that have been reviewed, accepted and verified by the CB to proceed with a decision to grant or renew certification (applicable to initial audits and recertification audits).

11.8. For all surveillance, all major nonconformities must be closed or their significance reduced to "minor" within 90 days of the last day of the audit. The lead auditor determines whether corrections and corrective actions are verified on-site or by documents and records the decision and the reasons in the report. If the nonconformity is not closed or reduced to “minor” within this period, the certification is suspended in accordance with section 10.

11.9. The time taken to take corrective action must be commensurate with the risks:

- for QMS - risks for the quality of products and services;
- for EMS - the risks for the environment;
- for OHSMS - risks for people;
- for ISMS - the risks for the security of the Information;
- for FSMS - the risks to food safety;
- for RTSMS - the risks for RTS;
- for ABMS – the bribery risks;

11.10. If, during an audit, a risk of causing significant damage to people or property is identified, the lead auditor must require immediate appropriate action by the client, incl. suspension of the audit until the risk has been eliminated or reduced to acceptable limits.

11.11. If, during an audit, a member of the audit team identifies a nonconformity with a legal requirement, it is raised as a major nonconformity when: a) the organisation has not identified the requirement or has not evaluated its compliance with it and has not taken action; b) the breach is systematic or ongoing; or c) the breach creates a direct risk to human health and safety, the environment, food safety or information security. In other cases (e.g. the organisation has itself identified the breach and is implementing a plan to remedy it with a responsible person and a deadline), a minor nonconformity is raised. Nonconformity with a legal requirement is reported to the client as soon as possible.

11.12. For audits of integrated management systems, if non-compliance with one of the audited standards is found, the lead auditor must consider the impact of this non-compliance on maintaining compliance with the requirements of the other audited standards.

11.13. For multisite organisation audits, where nonconformities are found at one of the sites in the scope (whether during an internal audit or a third party audit), it is necessary to examine the extent to which other sites are affected by the same nonconformity. The certification body requires the organisation to review these nonconformities and determine whether or not they indicate a common problem throughout the management system.

11.14. If it is confirmed that the nonconformity affects the entire management system, the corrective action must be performed and verified both at the central function and at the individual affected sites. If the opposite is confirmed (i.e. the nonconformity is local), the organisation must be able to present to the certification body a justification for limiting the scope of implementation of the corrective actions.

12. Reference to certification and accreditation

12.1. "Reference to the certification status" is made by using the certificates and the certification marks provided by the certification body for the relevant certification scheme, as well as by referring to the certification in text. Reference in text form is considered and treated as equivalent to the use of a certification mark.

12.2. When certified clients refer to the status of their certification in the media, including the Internet, brochures and promotional materials and other documents, they must do so following these General Terms and Conditions.

12.3. The certified client must not make or allow to be made any misleading claims relating to its certification.

12.4. The certified client must not use or allow the use of the certificate or parts thereof misleadingly.

12.5. Upon withdrawal of the certification, the client must immediately discontinue the reference to certification.

12.6. When the scope of certification is reduced, the client must promptly update their documents/promotional materials in which they refer to the certification.

12.7. A certified client must not allow reference to the certification of its management system to be used in a manner that misleads that the certification relates to a product (including service) or process.

12.8. The certified client must not imply that the certification relates to activities and sites outside the scope of the certification.

12.9. A client that operates on more than one site and/or has different certification scopes for different sites must develop and implement procedures to ensure that it informs its customers if they purchase goods and services outside the accredited scope of certification.

12.10. The certified client must not use their certification in a way that could damage the reputation of the certification body and/or the certification system and compromise public confidence in it.

12.11. The certification body provides all certified clients with certificates and certification marks (separate for each management system). In addition, it records all valid certificates in a public register, available at the website of the certification body - www.incert.bg.

12.12. The certificates and certification marks are the property of the certification body of INCERT EOOD. The certification body provides them for use for the time for which the client has a valid certification for a specific standard or scope.

12.13. The certification body provides its certified clients with the following certification marks[5]:















12.14. The clients of the certification body at INCERT EOOD must comply with the following requirements when referring to their certification and the use of certificates and certification marks:

12.14.1. Applicable to the certification of all types of management systems:

- reference to certification shall be made for the scope of the certification and the period of its validity;
- where reference is made to the status of certification without use of the certification mark, the client must indicate the registration number of the certificate;
- certified clients may use the certification mark in reports, offers, brochures with instructions (against the name of the organisation, not the product), letterheads, correspondence, training materials, etc., following the areas and scope of the issued certificate;
- the certification mark may not be assigned or provided for use to users, suppliers or other third parties who are not part of the structure of the certified organisation;
- the certification mark must be used without change in form, content and proportions, in black and white or in the original colours, and must be legible and intelligible;
- the certification mark of INCERT EOOD may not be affixed on laboratory test reports, calibration or control protocols, or certificates issued by the certified client;
- when a certified organisation, together with its logo, uses the certification mark of INCERT EOOD, then the certification mark of INCERT EOOD is smaller than those of the logo of the organisation;
- the certification mark of INCERT EOOD cannot be used independently without the client's logo.

[5] Images are for information only. Clients receive high-quality files with the certification marks intended for printing.

12.14.2. Applicable to the certification of all types of management systems except FSMS:

- it is not allowed to place the certification mark on a product or on a product packaging that is visible to consumers or used in a manner that may be construed as a mark of conformity of the product or in a manner that may mislead the consumer. On the product packaging6 or accompanying information7, it is permissible to put a text containing the name of the certified client, the type of management system and the applicable standard and the name of the certification body that issued the certificate;

12.14.3. Applicable only to the certification of FSMS:

- Clients are not allowed to use the certification mark on the product nor the product packaging. Product packging in this context refers to all product packaging, both primary packaging (which contains the product) and any outer or secondary packaging.
- It is forbidden to use any statement on the product packaging that the client has a certified FSMS. This includes all product packaging, both primary packaging (which contains the product) and any outer or secondary packaging.

12.15. Applicable to all clients who have certification under the accreditation of the Bulgarian Accreditation Service Executive Agency (BAS EA):

12.15.1. Certified clients must comply with BAS EA requirements to use the accreditation symbol and reference to the accreditation.

12.15.2. Accredited certificates issued by the certification body of INCERT EOOD in no way imply that BAS EA or any other institution approves the product or service.

12.15.3. Reference to the accreditation in text form is considered and treated as equivalent to the use of an accreditation symbol.

12.15.4. Certified clients can use the accreditation symbol of BAS EA to refer to the accreditation of the certification body of INCERT EOOD when this is strictly limited to the scope certified by the certification body within its accreditation. In this case, the certified clients must use the accreditation symbol together with the certification mark of the certification body of INCERT EOOD.

12.15.5. It is forbidden to place an accreditation symbol/accreditation reference on advertising materials and business cards of the staff of the certified clients, regardless of whether they are related to the certified management system.

12.15.6. It is forbidden to place an accreditation symbol /accreditation reference on products or packaging of a product that is visible to consumers or otherwise that could be interpreted as indicating the conformity of the product.

12.15.7. The certification mark of INCERT EOOD in combination with the accreditation symbol of BAS EA cannot be placed on protocols of laboratory tests, protocols of calibration or control, or certificates issued by certified clients.

12.15.8. The accreditation symbol of BAS EA cannot be used without the certification mark of the certification body of INCERT EOOD.

12.15.9. The accreditation symbol of BAS EA cannot be larger than the certification mark or the client's logo.

12.15.10. Together, the accreditation symbol of BAS EA and the certification mark of INCERT EOOD may be displayed as follows (example image):





12.15.11. The certification body monitors compliance with the requirements by:

- reviewing the activities of the certified client at each audit (surveillance or recertification);
- requiring actions (e.g. corrections and corrective actions, unplanned audits) in case of violations, e.g. based on available public information or complaints about misuse of certificates and certification marks, etc.

12.15.12. Failure to comply with these requirements may lead to suspension of certification, withdrawal of certification, notification of the violation, including taking action under applicable law.

13. Consideration of complaints and appeals

13.1. The certification body for management systems of INCERT EOOD applies a procedure for reviewing and taking action on all received appeals and complaints.

13.2. Appeals can be submitted by certified clients who request a revision of a decision of the certification body related to the certification process, e.g. a decision to grant, suspend, withdraw a certificate, etc. All stakeholders may file complaints (clients, their clients and consumers, institutions, public organisations, etc.). Complaints are related to dissatisfaction related to the activities of the certification body.

13.3. Appeals are submitted in writing (on paper or by e-mail) to the manager of INCERT EOOD in the capacity of secretary of the Impartiality Committee. The client receives a written confirmation that the appeal has been registered and a notification of the forthcoming actions and the time limits for its consideration.

13.4. The appeal is reviewed by an Appeals Committee. The specific composition of the Appeals Committee, including its chairman and members, is determined by an Order of the Chairman of the Impartiality Committee for each individual case, taking into account the nature and character of the appeal. The Committee includes at least the following categories of experts:

- Lead auditor(s) in the certification schemes under which the client who filed the appeal is certified - selected from the Register of Approved Lead Auditors/Auditors/Technical Experts;
- Legal expert;
- Technical expert in the scope of client certification - selected from the Register of Approved Lead Auditors/Auditors/Technical Experts;

13.5. The Appeals Committee consists of an odd number of members and a minimum of three persons.

13.6. In determining the composition of the Appeals Committee, the presence of combined competence in management systems, the legal and technical aspects of the appeal and ensuring impartiality are leading. Persons who have carried out audits or who have taken certification decisions, as well as other persons for whom a threat to impartiality may be identified, may not participate in the Appeals Committee - e.g. persons representing the appellant or their competitors.

13.7. The Appeals Committee is competent to:

- to rule with a separate decision on each registered appeal, solely on issues related to a decision to grant, maintain, suspend, withdraw or limit the scope of certification of management systems;
- to rule on the justification of the submitted appeal;
- In case the appeal is justified, the decision of the Appeals Committee should give unambiguous instructions to the manager of the certification body. The instructions are binding on the manager of the certification body.

13.8. No forms of discriminatory action against the appellant are allowed.

13.9. In examining and deciding on the appeal, the Committee shall be guided by the applicable standards and operating procedures, the information and documents provided in the case file, and consider the results of previous similar appeals (if applicable). The Committee may request additional documents and information from the Parties and independent experts to take an objective and reasoned decision.

13.10. The Appeals Committee shall respect confidentiality, which shall be guaranteed by signing individual declarations of professional secrecy, independence, and impartiality.

13.11. The deadline for a decision by the Appeals Committee is 30 (thirty) days from the date of receipt of the appeal.

13.12. The decisions of the Appeals Committee are final and not subject to appeal to the certification body.

13.13. In cases where the objector is not satisfied with the decision of the Appeals Committee, they may apply to the accreditation body and/or to the court.

13.14. In case the appeal is accepted as justified, the manager of the certification body, in implementing the decision, is obliged to take correction in respect of the specific client, as well as preventive actions to prevent the recurrence of the nonconformity.

13.15. The manager of INCERT EOOD sends the appellant a copy of the decision of the Appeals Committee within three days from its receipt. In addition, the manager of INCERT EOOD monitors the implementation of the decision and reports at a meeting of the Impartiality Committee.

13.16. Complaints are submitted in writing (on paper or by e-mail) to the manager of the certification body of INCERT EOOD. Each complaint must contain at least the following:

- Names and contacts of the complainant;
- Description of the circumstances on which the complaint is based;
- The request.

13.17. The complainant receives a written confirmation that the complaint has been registered.

13.18. The manager of the certification body reviews the subject of the complaint to confirm whether the complaint is related to the certification activities for which the certification body is responsible. If the complaint is outside the scope of the

[6] The packaging of the product is anything that can be removed without compromising the integrity of the product or damaging it.

[7] Accompanying information is that which is available separately or is easy to tear off. Labels or identification plates are considered part of the product.

certification activities for which the certification body is responsible, the manager of the certification body shall notify the complainant.

13.19. If the complaint is within the scope of the certification activities for which the certification body is responsible, the manager of the certification body shall proceed with the complaint by determining the order in which it will be considered.

13.20. All complaints are reviewed within one month of their registration, and a decision on the justification of the complaint is taken within the same period. Extension of the term is allowed in situations requiring additional time for investigation. The complainant is notified of this in writing.

13.21. The consideration of all received complaints is carried out in compliance with confidentiality. No forms of discriminatory action against the complainant are allowed. All decisions and actions in connection with a received complaint are taken/executed only by persons who have not participated in the activity related to the subject of the complaint.

13.22. Complaints related to the activity of the certification body

The manager of the certification body appoints a working group to review each complaint. If necessary, competent external experts may be involved. The working group collects, summarises and analyses all the circumstances of the complaint and makes a proposal for a decision on the merits, applying the evidence that has been considered. The manager of the certification body gets acquainted with the proposal for a decision and prepares a written decision on the merits of the complaint.

13.23. Complaints related to the activity of certification body staff (own and external)

The manager of the certification body makes a written decision on the merits by examining the circumstances, requesting information from the direct supervisor, if necessary, may request written information from the employee involved in the complaint, setting a deadline for its submission (not more than five days).

13.24. Complaints related to the activity of certified clients of the certification body or those in the process of certification

All complaints in this category are considered in terms of the efficiency of the certified management system. The manager of the certification body informs the certified client about the received complaint and assigns the lead auditor, who performed the last audit of the certified client or approved for audit of a client in the process of certification, to study and analyse the complaint providing the available information.

13.25. The lead auditor uses appropriate research methods, e.g. performing a special on-site audit (subject to additional payment), examining the complaint during a scheduled on-site audit (if deadlines allow), requesting written information from the client, checking documents available at the certification body, holding meetings for establishing the facts of the complaint.

13.26. Notwithstanding the actions taken, within three weeks of the registration of the complaint, the lead auditor has to analyse and summarise the information available and collected in the course of the examination and propose a decision on the merits, enclosing evidence that has been examined.

13.27. The manager of the certification body gets acquainted with the proposal for decision and prepares a written decision on the merits of the complaint.

13.28. Informing the complainant

The decision on the merits of the complaint is sent to the complainant within one month of the registration of the complaint, unless the term for its examination has been extended, in which case the complainant is informed of this in writing before the expiry of the one-month term.

13.29. Taking actions and evaluating their effectiveness

In case the complaint is justified, the manager of the certification body shall take decisions for further actions in compliance with the procedures of the certification body and the applicable legislation.

13.30. If the complaint is justified and it refers to a certified client that is not complying with the General Terms and Conditions for Certification Contracts, the certification body may decide to suspend temporarily, withdraw or limit the scope of certification.

13.31. If the complaint is justified and it refers to a client in the process of certification by the certification body and non-compliance with the General Terms and Conditions for Certification Contracts is established, the certification body may decide to refuse to grant certification, to renew certification or to extend the scope of certification.

13.32. Each year, at the management review, the deputy manager of the certification body prepares and submits a report on the received complaints and their actions.

13.33. Records are kept of correspondence and all decisions and actions that have been taken.

13.34. The manager of the certification body controls the implementation of the actions taken on the received complaints.

13.35. The manager of the certification body shall discuss with the complainant and the certified client (as applicable) whether and to what extent the complaint and the decision taken may be made public.

14. Provision of information upon request

14.1. The certification body for management systems at INCERT EOOD provides upon request information on the status of a specific certification. A check on the status of a particular certification can be made on the certification body website in the "Certificate Verification" section.[8] It is necessary to enter the unique number of the certificate in the search field to obtain information about the client, scope of certification, sites within the scope, certification standards, and the status of the certification (e.g. "valid", "terminated", etc.)

14.2. An inquiry can also be sent in writing to office@incert.bg or through the contact form on the website www.incert.bg, and the inquiry must contain the registration number of the certificate for which information is requested.

14.3. If the certificate is valid, the certification body for management systems at INCERT EOOD confirms its validity and provides information about the client's name, the relevant certification standard, the scope of certification and the sites within the scope.

14.4. In case the registration number does not indicate a valid certificate, the answer to the request confirms that there is no valid certificate with the indicated registration number.

15. Privacy Policy

15.1. The certification body for management systems at INCERT EOOD understands the importance of maintaining confidentiality in the certification process and takes all necessary measures to ensure its protection at all levels in the organisation and every stage.

15.2. All Information accessed by the certification body staff during the certification process is considered a professional secret and shall be used only for mutually agreed purposes.

15.3. Access to the reports prepared as a result of an audit is given to the client, the certification body of INCERT EOOD and the representatives of the accreditation service (when applicable). Information related to a specific client is not provided to a third party without the client's prior written consent. When the certification body for management systems at INCERT EOOD is obliged to provide information considered a professional secret to a third party (e.g. in response to a court order or at the request of the accreditation body), the client shall be notified in advance in writing of the information which will be provided.

15.4. The employees of the certification body for management systems at INCERT EOOD and all members of the Impartiality Committee declare in writing that they will keep the professional secret related to all information received or created during the activities of the certification body. The certification body provides and uses appropriate technical means and facilities to ensure the security of confidential information.

15.5. Only the information in the issued certificate is public and can be freely provided by both parties.

15.6. Photographs, audio and video recordings and screenshots during an audit (on-site or remote) are made only after prior agreement with the client and in compliance with its security and safety rules. They, as well as copies of documents and records obtained during the audit, are kept as confidential information and are destroyed when no longer needed for certification purposes.

16. Impartiality policy

16.1. The certification body for management systems at INCERT EOOD has adopted a policy of impartiality, which is published on its website www.incert.bg. Decisions of the certification body of management systems are based only on objective evidence of compliance (or non-compliance) established during the audit. These decisions are not influenced by other interests or by other parties.

16.2. The certification body applies a procedure for managing risks to impartiality, including having established an Impartiality Committee, through which impartiality in the certification process is ensured to the fullest extent. The staff of the certification body (internal and external) and the members of the Committee sign declarations of impartiality and confidentiality and must declare any conflict of interest before each audit in which they are engaged, or without delay when they identify a threat to the impartiality of the audit process.

16.3. Before each audit, the client is informed of the names of the audit team members (auditors and technical experts), as well as of the participation of inter-

[8] https://incert.bg/proverka-na-sertifikat/

preters and observers (e.g. representatives of the accreditation body or a witnessing auditor of the CB). The client may refuse to accept a specific auditor in the audit. The refusal must be made in writing, stating the reasons for this.

16.4. Client employees or client representatives (e.g. consultants) must also report the existence of relationships (professional or personal) with INCERT auditors or employees engaged in the certification process that could jeopardise the impartiality of the certification process.

16.5. The participation of observers is agreed with the client before the audit. Observers and guides appointed by the client accompany the audit team but do not participate in the audit as auditors or technical experts and do not influence its conduct.

17. Announcement of changes by a certified client

17.1. Each client is obliged to immediately notify the certification body of any circumstances that may affect the ability of the management system to continue to comply with the requirements of the selected certification standard. This includes at least the following circumstances:

17.1.1. changes in the legal, commercial and organisational status or change in the ownership of the organisation;

17.1.2. changes in organisation and management (e.g. key personnel such as managers, decision-makers or technical staff);

17.1.3. changes in contact address and location (site);

17.1.4. changes in the scope of activities performed within the certified management system;

17.1.5. essential changes in the management system and the processes;

17.1.6. incidents and extraordinary events that significantly affect the management system or compliance with legal requirements (e.g. serious accidents and incidents, information security incidents, inspections or sanctions by control authorities).

17.2. The certification body must review and analyse the changes and notify the client of the necessary actions.

18. Announcement of changes by the certification body

18.1. The certification body shall provide its clients with information on any changes to the certification requirements. Changes may be required in the event of changes in regulatory requirements, applicable standards and procedures, or body policies.

18.2. In case of a change in the General Terms and Conditions for Certification Contracts, the current version is published on the website www.incert.bg, incl. information in the News section. In accordance with the provisions of the certification contract, clients are obliged to keep themselves informed of the changes through the indicated website - www.incert.bg. In case of changes, the clients must get acquainted with them and make sure that they fulfil the changed requirements that affect them, so as not to jeopardise the validity of their certification.

18.3. If other changes are required (e.g. a new version of a management system standard is published and a transition period for adapting the systems to the new requirements is forthcoming), the certification body notifies all its certified clients in writing within a reasonable time, indicating the necessary actions on their part and how compliance with the changed requirements will be confirmed by the certification body.

19. Disclaimer

19.1. It should be borne in mind that any audit is based on an assessment of a sample of the client's management system, and therefore 100% compliance with the requirements is not guaranteed.

19.2. Clients use the services of the certification body of INCERT EOOD to assess the degree of compliance of their management system with the standard of their choice, and the certification body of INCERT EOOD is not responsible for the day-to-day management of the system.

19.3. In this sense, if a product or service offered by clients of INCERT EOOD leads to damages or losses for users of their products or services, no fault can be attributed to INCERT EOOD and no claims for compensation of damages or losses may be brought against it.

20. Anti-bribery management system (ABMS) certification only[9]

20.1. An ABMS certification may be requested by any organization, regardless of the size and nature of its activity. The ABMS certification application is separate from the general application and contains specific information necessary to make a decision to provide a certification offer.

20.2. When reviewing an application for certification, in addition to the information provided by the client, the certification body also conducts its own "independent investigation", by checking public sources and registers in order to understand the context, business model and related risks of bribery (e.g. Commercial Register and Register of NGOs, Register of Administrative Structures, Transparency International Corruption Perception Index, website of the Audit Chamber, website of KPCONPI, CAIS EOP, and others, as applicable).

20.3. The certificate is issued to the legal entity and includes all sites, branches, activities and processes performed by the organization. Exclusion of processes or personnel for the territory of one country is not allowed.

20.4. Any organization that has been certified or is in the process of being certified under an ABMS certification scheme must inform the certification body without delay if it finds itself in a critical situation that could compromise the validity of the system's certification (e. g. news of public interest, crisis or investigations/lawsuits related to cases of bribery and/or corruption).

20.5. The organization must promptly inform the certification body of any case of bribery that may have involved personnel of the organization, and inform the certification body of the follow-up action it has taken, including root cause analysis and corrective actions.

20.6. If the certification body receives information from the organization itself or from other sources that the organization is suspected of involvement in a corruption-related scandal or is a party to legal prosecution, the certification body will immediately conduct an investigation.

20.7. In these cases, the public will be informed by the certification body through a publication on the authority's website that this particular situation is "subject to an assessment in relation to specific events".

20.8. After analysis, the certification body takes action (e. g. archiving the investigation/assessment, implementing actions provided for in the certification requirements, increasing the frequency of audits, etc.) based on the adequacy of the organization's response/reaction.

20.9. It is the certification body's policy not to certify an ABMS through an integrated management system audit.

20.10. The certification body accepts combined documentation (e. g. ABMS and QMS) only if the ABMS can be clearly delineated, together with appropriate interrelationships with other management systems.

20.11. An ABMS audit could be combined with audits of other management systems provided the audit fulfills all the requirements regarding the ABMS certification. The audit report must contain all the necessary information to make a decision related to the certification. Audit quality should not be compromised as a result of combining audits.

21. Specific to the Certification of Information Security Management Systems (ISMS)

21.1. References or cross-references to other national and international standards are permissible in ISMS certificates of conformity only if:

a) the organization has mapped all its necessary controls against those in the source of the reference controls to ensure that no reference control required by ISO/IEC 27001:2022, clause 6.1.3 c), has been omitted;

b) for excluded reference controls, justification is provided in the Statement of Applicability (SoA) as per ISO/IEC 27001:2022, clause 6.1.3 d).

21.2. Reference standards for controls may be based on ISO/IEC 27001:2022, Annex A, or on standards that include controls for information security.

21.3. Certificates of conformity in such cases shall state that the set of controls used in the Statement of Applicability is provided solely as a reference for the relevance of including or excluding controls in the ISMS and is not used for conformity assessment.

21.4. The CB's procedures do not prescribe a specific method for implementing ISMS or a specific format for documentation and records. The certification process focuses on verifying that the client's ISMS meets the requirements specified in ISO/IEC 27001, as well as the client's policies and objectives.

21.5. Organizations may develop their own necessary controls or select them from any sources. It is possible for an organization to be certified against ISO/IEC 27001 even if none of its controls are from those listed in Annex A of ISO/IEC 27001:2022.

- End -

[9] The conditions under item 20 take precedence over all other general provisions contained in this document.