ISOCERT GUIDE

"Certification of management systems "

ISSUE: 1 -2024
DATE OF ISSUE:25.01.2024

1 . INFORMATION ON CERTIFICATION ACTIVITIES AND REQUIREMENTS

ISOCERT is a unit that certifies organizational management systems available to all applicants.

There are no unjustified financial requirements, and access to certification does not depend on the size of the organization or membership in any association or grouping.

ISOCERT activity is financed from business activity.

ISOCERT conducts accounting and statistical reports in accordance with applicable regulations.

Rules for the certification of management systems developed from the last on the basis of the requirements:

- PN-EN ISO / IEC 17021 -1: 2015 "Conformity assessment: Requirements for entities carrying out audits and certification of management systems"
- PN-ISO / IEC 17021-2 "Conformity assessment - Requirements for bodies conducting audits and certification of management systems - Part 2: Requirements for competence to audit andcertify environmental management systems"
- PN-ISO / IEC 17021-3 "Conformity assessment - Requirements for bodies conducting audits and certification of management systems - Part 3: Requirements for competence to audit andcertify quality management systems"
- ISO / IEC TS 17021-10: 2019-11 "Conformity assessment - Requirements for certifications andmanagement systems"
- PN-ISO / IEC 27006: 2021-05 "Information technology. Security techniques. Requirements for entities conducting audit and certification of information security management systems. "
- PN-EN ISO 9001:2015 "Quality management systems - Requirements"
- PN-EN ISO 9000:2006 "Quality Management Systems - Fundamentals and Terminology"
- PN-EN ISO 14001:2015 "Environmental management systems. Requirements and application guidelines. "
- PN-ISO 45001:2018-06 "Occupational health and safety management systems - Requirements and application guidelines”
- PN-EN ISO / IEC 27001:2017-06 "Information technology. Security techniques. Information security management systems. Requirements".
- ISO/IEC 27001:2022 "Information technology. Security techniques. Information security management systems. Requirements".
- EA-7/04 "Compliance with law as part of an accredited certification with respect to ISO 14001:2015‟
- IAF MD1:2023 IAF compulsory document for the audit and certification of multi-site management systems
- IAF MD2:2023 "IAF Mandatory Document on the Transfer of Accredited Certification of Management Systems"
- IAF MD4:2023 "IAF compulsory document on the use of information and communication technologies ("ICT") for conducting audits / evaluations"
- IAF MD5:2023 ”Mandatory document of the IAF regarding the determination of the duration of QMS and EMS audits”
- IAF MD11:2023 ‟IAF compulsory document on the application of ISO / IEC 17021 in audits of integrated management systems”
- IAF MD22:2023 "Application of ISO / IEC 17021-1 in the certification of occupational safety and health management systems
- IAF MD23:2023 ‟Control of Entities operating on Behalf of Accredited Management Systems Certification Bodies”
- IAF ID3:2011 „Informative Document for Management of Extraordinary Events or Circumstances Affecting Abs, CABs and Certified Organizations”.

2. RIGHTS AND OBLIGATIONS OF THE ORGANIZATION

The organization has the right to:

- requesting the change of individual members of the audit team, providing rational justification, for example: of the situation of a conflict of interests, unethical behavior,
- refer to certification in accordance with the principles set out in this guide,

- the use of certification marks, in accordance with the principles set out in this guide,
- requirements from ISOCERT to keep confidential all information related to the certification of the Organization's management system,
- receiving from ISOCERT information on changes in regulations related to certification,
- appeals and complaints, in accordance with the principles set out in this guide,
- extension of its scope specified in the ISOCERT certificate granted by the ISOCERT with the requirements of further reference documents or a new area covered by the system ,
- occurrence of a request for interruption of the certification process, the suspension of the validity of certification, re-evaluation or renew the certification.

The organization applying for certification undertakes that:

- will enable ISOCERT to conduct an initial certification audit within the set time limit.
- will enable ISOCERT to conduct audits in supervision at least once a year, within the deadlines set in the certification documents, with the reservation that the date of the first audit audit after the initial certification should not be later than 12 months from the date of the decision to grant certification.
- will enable ISOCERT to conduct special audits in case of justified doubts as to whether the Organization meets the certification requirements; the occurrence of a serious incident related to health and safety, for example: a serious accident or a serious violation of the law (applies to SMOHS); in the case of extension of the scope of certification at the request of the Organization.
- it will provide the conditions for observers of current audits (e.g. PCA auditors or trainee auditors).
- will maintain a management system compliant with the requirements of the standard, for the compliance with which the certificate was issued.
- will regularly record any complaints and take corrections and/or corrective actions in this regard.
- will notify ISOCERT of any changes that may affect the compliance of the management system, including: legal, commercial, organizational or ownership status, organizational structure and management, the scope of activities covered by the certified management system and places of business, major changes in the system, contact addresses .
- will promptly inform ISOCERT of a serious incident or breach of regulations that requires the involvement of a competent regulatory body (applies to SMOHS)
- will not make or allow to be made any misleading statements regarding its certification.
- will not use or permit the use of the certificate(s) or any part thereof in a misleading manner.
- after suspension or withdrawal of certification, it will cease to use the certificate(s) and ISOCERT marks in all advertising materials containing references to certification, in accordance with ISOCERT's instructions.
- will update all advertising materials in case of limiting the scope of certification.
- will return the certificate(s) issued by ISOCERT within 7 days in the event of a decision to withdraw or limit the scope of certification
- will not allow reference to certification in such a way as to imply that the body certifies a product, service or process.
- will not imply that certification applies to activities that are outside the scope of certification.
- will comply with ISOCERT decisions made in connection with changes in the requirements of the certification process.
- will use the certification mark and refer to certifications only in accordance with the rules set out in the document "Specification and use of the certification mark"

3 . CERTIFICATION PROCESS

In the case of certification of management systems, certification can be implemented in the organization system, that is:

- there is sufficient objective evidence documenting the effective implementation of the system,
- internal audits were carried out,
- management review the system.
- there is sufficient evidence that arrangements for internal audits and management reviews have been implemented, are effective and will continue to be maintained.

3.1. Application for certification

"Application For Certification" is available on the website www.isocert.org.pl .

Filling out the “Application For Certification” and sending it by the Organization to the ISOCERT does not oblige to sign a contract for the ISOCERT certification process.

The completed "Application For Certification" provides ISOCERT with the necessary information to determine:

- the desired scope of certification
- general characteristics of the requesting organization, including its name andaddress (addresses) of its physical locations, determination of the central function,significant aspects of its processes and activities along with the division into locations including information on temporary and virtual branches and all applicable legal obligations,
- confirmation that a single management system is implemented throughout the organization,
- general information relevant to the requested certification area,regarding the applicant organization, such as its activities, human and technical resources, functions and connections in a larger corporation, if such are,
- information on all subcontracted applied processes by organization that mayaffect compliance with requirements,
- standards or other requirements for which the applicant organization isapplying for certification,
- information on uses the present with consultation in regarding the management system.

In addition, in the field of occupational health and safety:

- key hazards and health and safety risks related to processes, the most important hazardous materials, all relevant legal obligations with an indication ofwhat location they relate to
- Information regarding Direct incident of a serious infringement or causing theneed to involve the competent authority governing it
- information on the differences in the operations of each branch
- information on the number of companies (sub) contractors and theiremployees along with the specification of what activities they carry out
- information on accident rates and the incidence of occupational diseases

In addition, in the field of EMS:

- environmental aspects and environmental permits
- confirmations regarding greater sensitivity to the reception of the environment, additional / extraordinary environmental aspects, additional /extraordinary permits / regulations for the sector corresponding to the Organization

Additionally in the scope of ISMS:

- information on the level of security risk information
- actions taken in the organization in connection with the assessment risks
- information on the declaration of use
- information on backup locations, disaster recovery locations, criticality of business sectors, processes and tasks, level of system establishment, infrastructure complexity, outsourcing and supplier dependency, development of IT systems

The "Application For Certification" should also contain information about data that cannot be made available to the certification body because it contains confidential or sensitive information.

ISOCERT considers the "Application for certification" paying particular attention to the aspects of independence, impartiality and elimination of causes of potential conflict of interest. If it is possible to carry out initial certification, ISOCERT prepares and sends an offer/agreement to the Organization for the certification process.

If it is not possible to carry out the certification process, the applicant Organization is informed in writing/by e-mail (depending on the form of submitting the application by the Organization) about the reason for refusing to accept the application.

It is possible to develop an offer without the formal submission of an "Application for Certification" by the organization, based on written or oral information provided by the organization.

Fees related to certification, supervision and re-certification are borne by the certified Organization. Fees depend on the size of the organization, and the price of a given audit is determined depending on the complexity of the organization and other factors applicable in the Organization. The number of auditor-days is calculated according to the rules specified in the detailed instructions for individual certification programs. ISOCERT prepares and sends to the organization an agreement for conducting the certification process, enclosing the document "Specification and use of the certification mark".

3.2. Initial certification audit

Audit starting the certification is carried out in two stages. The dates of the first and second stage of the audit are planned in consultation with the Organization. In the case where the auditor after the 1st stage of the audit determine the possibility of conducting the audit, auditor agrees on a reasonable deadline inconsultation with the certified Organization. It is allowed to carry out the second stage of the audit immediately after the first stage (only in enterprises not exceeding the number of effective 10 employees), taking into account the fact that the objectives of the 1st stage of the audit have been achieved.

3.2.1 I stage of the audit

The 1st stage of the audit includes:

- auditing the organization's documentation,
- assessment of the client's location and location-specific conditions and conducting interviews with the organization's personnel to determine readiness for the second stage of the audit,
- reviewing the organization's status and understanding the requirements of the standard, in particular with regard to the identification of key aspects of the method of operation or significant aspects, processes, objectives and operation of the management system,
- gathering necessary information regarding the scope of the management system, processes, client location and related statutory and legal aspects as well as compliance (e.g. qualitative, environmental, legal aspects of the organization's activities, related risks, etc.),
- conducting a review of the allocation of resources to the second stage of the audit and agreement with the organization of the details of the second stage,
- concentrating on planning the second stage of the audit by achieving a sufficient understanding of the organization's management system and the activity in the location in the context of possible significant aspects,
- assessment of whether internal audits planned and implemented and management reviews and whether the implementation level of the management system justifies the readiness of the body of the agency for the second stage of the audit,
- development of the second stage of the audit plan .

In addition, in the case of ISMS audit, the 1st stage of the audit includes:

- assessment of whether the estimated information security risk (especially in the area of critical risk) properly reflects the scope of the organization's activities and the requirements of ISO 27001,
- check whether the risk assessment includes interfaces with services or activities that do not fully fall under the scope of ISMS and whether they are included in the ISMS framework.

ISOCERT informs in advance about the composition of the team of auditors appointed to conduct the audit. The organization has the right to submit a reservation to the auditors or request additional information about the members of the audit team. From the first stage of the audit, the organization receives "Arrangements from the 1st stage of the audit". After conducting the 1st stage, ISOCERT may, in agreement with the organization, postpone the date of the second stage of the audit or introduce changes in the preparations for the second stage of the audit.
If there are significant changes in the Organization affecting the management system, it may be necessary to repeat the first stage of the audit or its part. The results of the first stage may lead to the postponement or cancellation of the second stage of the initial certification audit.

3.2.2. II stage of the audit

Based on the findings from the first stage of the audit, the leading manager develops the "Audit plan".
The audit plan is sent by the lead auditor to the organization in advance enabling the organization to submit comments before the audit in the organization.
The second stage of the audit begins with the opening meeting. The opening meeting is intended to present the purpose and scope of the audit, an audit plan prepared by the lead auditor should be discussed, generally the activities that will be carried out during the meeting . The opening meeting should be attended by persons responsible for the main functions or processes that will be audited, with the possibility of asking questions directly related to the actions of audit. The leadership of a certified organization should be present at the opening meeting .
The second stage of the audit (in the QMS, EMS, ISMS, OHS, OHSAS and OHS programs) includes at least :

- gathering information and evidence of compliance with the requirements of the relevant management system standard,
- monitoring, measuring, reporting and reviewing achievements in relation to key objectives and tasks (according to the appropriate management system standard),
- management system and the way of acting in terms of compliance with the law,
- operational control of client processes,
- internal audits and management reviews,
- management's responsibility for the organization's policy,

- link between normative requirements, policy, objectives and performance targets (according to the relevant management system standard), applicable legal provisions, responsibilities, staff competences,actions, procedures, performance data and findings and conclusions from internal audits.

In the case of ISMS certification:

- selection of security objectives and security objectives, based on risk assessment and risk management processes
- implementation of security measures, taking into account the effectiveness of the security measures performed by the organizations, to determine whether the security measures are implemented and effective in achieving specific goals
- showing that the analysis for security threats is related to the activities of the client's organization and is suitable for this activity
- determining whether the client's organization procedures regarding the identification, verification and assessment of information-related threats to assets, vulnerabilities and effects and the results oftheir implementation are consistent with the client's organization's policy, objectives and tasks.

Auditors carry out the monitoring of the organization's functioning in accordance with audit plan.

The discrepancies found during the audit are documented on the Charter non-compliance with the reference in terms of the audit criteria (assignment of an appropriate requirement of a standard or other document constituting the basis for certification, and proof and documentation of its existence). In addition, the reference for non-compliance may also be an appropriate item from the organization's SZ documentation.

After the initial certification , in the case of large inconsistencies, the organization's implementation of corrective and corrective actions, including a positive verification of their implementation by the audit team, may not exceed 90 calendar days from the date of non-compliance.

In the case of small inconsistencies, a corrective and corrective action plan is assessed, and if the plan is accepted, the verification of the implemented activities and their effectiveness is carried out at the next audit.

At the end of the audit, the audit team analyzes all information and audit evidence collected during the first and second stage of the audit and reviews the audit findings and reconciles the conclusions.

Then he meets the management and, if appropriate, the persons responsible for the audited functions or processes. In the case of SMOHS, in addition to the representative of the Organization, management members legally responsible for health and safety, personnel responsible for monitoring the health of employees and a representative / and employees responsible for OHS should participate in the closing meeting.

3.2.3 Additional audit

An additional audit is carried out in the case of the occurrence of non-compliance of a large (one or more) certification in the initial audit, in the case of which (verification) of corrective and corrective actions is not possible on the basis of evidence of the actions carried out by the organization.

Depending on the number of inconsistencies and areas concerned, the audit may be full or limited. Decisions are made by the lead auditor.

3.2.4 The conclusions of the initial audit the certification

The lead auditor prepares the "Initial certification audit report".

The report is sent to the organization.

The organization sends comments to ISOCERT to this report.

The absence of such comments means that the organization accept it’s content.

4. GRANTING CERTIFICATION

The decision about granting certification or refusing to certify the organization's management system is taken by ISOCERT, based on:

- opinions and information that is publicly available
- information collected during the initial certification process,
- acceptance of corrective and corrective action plan (for small inconsistencies), corrective and corrective actions carried out and acceptance of evidence for corrective and corrective actions (for large non-compliance)
- verification of documentation regarding the initial certification

The decision must be taken within 90 days from the date of positive verification of corrective and corrective actions or from the date of completion of the audit of the organization (in if there is no inconsistency during the audit).

ISOCERT notifies the organization with a letter about the decision regarding the certification .

In the case of refusal to grant certification, a justification is included in the notifying letter.
Certification is valid for 3 years from the date of the certification decision, unless the accreditation requirements state otherwise. If the expiration date of the certificate is conditioned by accreditation requirements or other ISOCERT requirements, the certificate is valid in accordance with these requirements.

5. ACTIONS IN SUPERVISION

During the certification validity period, ISOCERT carries out surveillance activities.
Activities in surveillance include:

- surveillance audits - assessing that the organization's management system meets the requirementsof the management system standard,
- organization inquiries regarding the aspects of certification,
- browsing the website and promotional materials,
- monitoring of generally available information on the supervised organization,
- requests to provide documents and records from the organization.

The surveillance audit shall include at least:

- internal audits and management reviews,
- verification and effectiveness of the planned actions taken in relation to small inconsistencies identified during the previous audit and observations
- the effectiveness of the actions taken in relation to major non-compliance identified during the previous audit,
- handling complaints,
- the effectiveness of the management system in terms of achieving the organization's goals
- the progress of the planned activity aimed at continuous improvement,
- continuous operational control,
- review of changes,

Surveillance audits are carried out at least once a year. The first surveillance audit after the initial certification should not be later than 12 months from the date of the decision on granting the certification . The decision to maintain the certification is made on the basis of a review of the correctness of the certification process (including surveillance activities), the "audit report" and the positive conclusions of the lead auditor.

6. RE-CERTIFICATION

Re-certification does not require submission of an "Application for certification" by the organization. The recertification audit should be planned and carried out in a way that confirms the continuous fulfillment of all the requirements of the certification program or other normative documents. The audit should be carried out within a timeframe that allows continuity of certification validity.
If there have been significant changes in the management system or in legal requirements concerning the organization, the first stage of the audit is also carried out.
The decision to extend certification or refusing to extend the organization's management system is made by ISOCERT.
Complaints against the organization and the results of the system operation during the certification period are taken into account when making decisions.
If a recertification audit has not been completed or a large non-conformity has not been closed before the certification expires, the decision to extend the certification cannot be taken and the certification cannot be extended.
It is possible to conduct an audit on the basis of an audit recertification audit within 6 months from the date of expiry of certification. In this case, the certificate is issued after making the certification decision, and the validity period of the certification refers to the original validity period.

7. SPECIAL AUDITS

7 .1 Extending the scope of the certification

The scope of certification may be extended at the request of the organization.
If an organization applies for extending the scope of certification to areas of operation or elements of the management system that were not covered by certification, the method and scope of the assessment are specified by ISOCERT.

7 .2 Audits with a short notice period

Audits with a short notice period are carried out in order to:

- investigate complaints,
- in response to changes (affecting the ability of the management system to meet the requirements of

the relevant management system standard),

- further proceedings in the event of the suspension of certification
- To investigate whether the health and safety system performance and its effectiveness have not deteriorated if ISOCERT was informed about, for example, a serious incident related to health and safety (e.g. a serious accident or a serious violation of legal regulations) - applies to SMOHS

ISOCERT undertakes the decision on the need to conduct it .

7.3 Changing the location

The change of location may take place at the request of the organization.
In the case of an organization requesting a change of location, the method and scope of the assessment are determined by ISOCERT.

8 . SUSPENSION CERTIFICATION

Certification may be suspended when:

- the organization's management system is constantly or severely failing to meet the certification requirements, including the requirements for the effectiveness of the management system,
- the organization did not perform corrective and corrective actions resulting from the agreed date discrepancies revealed during audits,
- the organization did not take any action on the agreed date to introduce changes to the SM resulting from a change in the requirements included in the audit categories ,
- the organization does not allow to conduct audits in surveillance or recertification audits with the required frequency,
- the organization voluntarily asked for suspension,
- the organization did not inform ISOCERT about introduction of significant changes to SM,
- the organization does not meet its financial obligations to ISOCERT,
- there are other reasons set out in the requirements or agreed in writing between the organization and ISOCERT.

During the period of certification suspension, the organization may not refer to the certification.
The period of certificate suspension is determined by ISOCERT and cannot be longer than 6 months. ISOCERT shall notify the Organization in writing about the date of suspension of certification .
Certification may be renewed if the organization whose certification has been suspended provides information on the fulfillment of the conditions accompanying the suspension decision.

9 . CERTIFICATION WITHDRAWAL

Certification is revoked if the organization fails to resolve the reasons for suspension of certification within the time limit set by ISOCERT. After revocation of the certification, the organization cannot rely on certification .
After deciding to revoke the certification, ISOCERT terminates the contract and cancels the certification.
ISOCERT notifies the Organization in writing about the date of withdrawal of certification.

10. LIMITING THE CERTIFICATION SCOPE

ISOCERT limits the scope of the organization's certification to exclude those parts that do not meet the requirements. This takes place in the case of a permanent or serious failure to meet the certification requirements to a certain extent of certification .
The scope of certification may be limited :

- as a result of the audit, during which it was found impossible to conduct operations in the full scopeof the certification granted ,
- when the organization did not perform corrective and corrective actions resulting from the agreed date discrepancies revealed during audits,
- at the request of the organization.

ISOCERT notifies the Organization in writing about the deadline for limiting the certification .

11. TRANSFER OF RIGHTS

Transfer of rights from the contract takes place at the request of the organization as a result of changing its legal status.
In the event that the documents that have been changed show (e.g. company registration documents, regulations, procedures etc.) that only the legal status of the organization has changed, ISOCERT may decide to transfer the rights from the contract without an audit.
If the presented documents show that in addition to changes in the legal status other changes have taken place, the decision to transfer the rights may be taken after the audit.

12 . INFORMATION ON CHANGES IN THE ORGANIZATION

The organization should promptly inform ISOCERT of significant changes that affect the ability of the management system to meet the requirements of the standard constituting the basis for certification. These changes may concern, for example:

- legal, commercial, organizational or ownership status,
- organizational and management structure (key managerial, decision-making or technical staff),
- address for contacts and places of business,
- the scope of activity covered by the certified management system,
- major changes in the management system and processes.

13. CHANGES TO CERTIFICATION REQUIREMENTS

ISOCERT informs organizations in writing about changes in certification requirements in advance, enabling changes in organizations. Changes in the certification requirements may concern, for example, changes in management system standards or changes in accreditation requirements. Checking the implemented changes ISOCERT may conduct through surveys, conversations, local visas or audits.

14. REQUIREMENTS FOR MULTILATERAL ORGANIZATIONS

A multi-branch organization should meet the following conditions:

- there is a single management system in the entire organization
- The organization should identify its central function. The central function is part of the organization and should not be subcontracted to an external organization.
- the central function should have organizational rights to define, establish and maintain a single management system.
- a single organization management system should be subject to a centralized management review.
- all branches should be subject to the internal organization's audit program.
- The central function should be responsible for ensuring the collection and analysis of data from all branches and should be able to demonstrate its authority and ability to initiate organizational changesnecessary, among others, but not exclusively in the context of:

- system documentation and changes in the system;
- management reviews;
- complaints;
- assessment of corrective actions;
- planning internal audits and evaluating their results;
- legal and regulatory requirements regarding the applicable norm(s).

15. PRINCIPLES IMPLEMENTATION OF CERTIFICATION PROCESSES IN AN EMERGENCY SITUATION

If, as a result of an emergency, guidelines in a given sector issued by competent authorities or internal regulations of the organization limit the possibility of conducting an on-site audit, or as a result of an emergency, there is a risk to the health / safety of the client or auditor, ISOCERT considers alternative methods of assessing the organization to verify the effectiveness management system of the certified organization. ISOCERT:

- assesses the risk in terms of the possibility of conducting an audit and continuing certification
- analyzes the possibility of using alternative methods to reliably confirm the compliance of the management system with the criteria requirements, alternative places and methods of sampling are identified
- determines the procedure depending on the information held and acquired, constituting the basis for making a decision on certification.
- defines the rules of communication with the certified organization (if it is impossible to establish contact or make the necessary arrangements with the organization, it initiates the process of suspension, withdrawal or termination of certification),
- determines the procedure depending on the type of audit
- develops an audit program that includes deadlines and all information regarding the supervision of the organization,

It is allowed:

- postponement of the audit
- conducting a remote full audit
- conducting a remote partial audit

16. COMPLAINTS AND APPEALS

16.1 Complaints about ISOCERT activities

The organization may submit to ISOCERT a complaint related to the method of conducting the management system certification process, including reservations about the work of auditors.
The person considering the complaint cannot be involved in the subject of the complaint.
ISOCERT shall consider the complaint within 30 days from the date of receipt of the complaint.
The decision on recognizing or rejecting the complaint is made by a person from the ISOCERT management who is not involved in its subject.
ISOCERT determines what actions are to be taken in response to the submitted complaint and inform the person submitting the complaint in writing.

16.2 Appeals

Appeals may concern: decisions in the certification process, supervision over certification including suspensions and withdrawal of certification. Filing an appeal by the organization does not result in any discriminatory actions against the appellant.
Appeals are reviewed by the appeal team appointed by ISOCERT. The team consists of:

- a competent ISOCERT auditor (while maintaining the condition that the auditor appointed to the appeal team did not participate in the certification / verification / audit in the waste management field of the organization submitting the appeal)
- ISOCERT impartiality monitoring committee with the exclusion of the Certification Director (due to the fact that the Certification Director is one of the parties in the Supervisory Committee)

The Certification Director forwards references to the appeal team and all necessary ISOCERT documents and procedures necessary to consider the appea

16.3 Complaints

Complaints may relate to ISOCERT activities (they may relate to the activities of the Organizations operated by ISOCERT or directly to ISOCERT), including breaches of confidentiality and information security.
Complaints about ISOCERT's activities may be submitted to the Polish Center for Accreditation.
In the event of a complaint about the organization's activities supported by ISOCERT, ISOCERT informs the organization to which the complaint relates. ISOCERT requires the organization that received the complaint to determine in response and - when appropriate - report the cause of the complaint. ISOCERT analyzes the problem and verifies the information collected. If a visit to an organization is required for the complaint to be considered, the person conducting the case after agreeing the deadline, makes explanations on the spot (in the organization), developing the report from the findings.
The decision on recognition or non-recognition of the complaint is made by a person from the ISOCERT management who was not involved in the subject of the complaint.
In the event of a complaint about ISOCERT's activities, the complainant is notified of the decision and actions taken in response to the complaint in writing.
In the event of a complaint about the operation of the serviced organization, ISOCERT informs the applicant in writing and the organization concerned about his decision and actions taken in response to the complaint.

17. PUBLIC INFORMATION

ISOCERT maintains and makes publicly available, without request, in all geographical areas in which information about :

- of auditing processes - ISOCERT GUIDE "Certification of management systems", placed on www.isocert.org.pl ("certification " tab)
- processes for granting, refusing, maintaining, extending, suspending, renewing or withdrawingcertification, or extending or limiting the scope of certification - ISOCERT GUIDE "Certification of management systems" , placed at www.isocert.org.pl ("certification" tab)
- types of management systems and certification programs in which it operates - information atwww.isocert.org.pl ("certification" tab)
- use of the ISOCERT name and certification mark - document "Specification and use of the certification mark" placed on www.isocert.org.pl ("certification" tab)
- processes for handling requests for information, complaints and appeals - ISOCERT GUIDE "Certification of management systems" , placed at www.isocert.org.pl ("certification" tab)
- policy of impartiality - Declaration of impartiality, information at www.isocert.org.pl ("certification"tab)

In addition, upon request, ISOCERT provides information about:

- geographical areas in which it operates,
- status of a given certification ,

- name, related normative document, scope and geographical location of a specific certified client.

Other information about organizations that have been certified is confidential.
Access to information about the organization by a third party is possible only with the written consent of the organization.
In any case, the information required by the law on the third party, the organization is informed of the content of the information disclosed (unless the law provides otherwise).

-End-