1. Objective

The present Certification Regulation refers to the certification procedures applied by BQC for the auditing and certification of Privacy Information Management Systems in accordance with the **ISO/IEC 27701:2019** series or other relevant European or international standards or standard documents. The overall management and issuance of the certificate of compliance meets the requirements of the **ISO/IEC 17021-1:2015** standard, and is based on additional requirements included in **ISO/IEC 27001:2022** (the information security management system standard), **ISO/IEC 27002:2022** (the code of practice for information security audits), **ISO/IEC 27006:2015**, and **ISO/IEC 27006-2:2021** (the requirements and guidance to bodies providing auditing and certification of information security management system), the Hellenic Accreditation System (E.SY.D.) as well as BQC General Certification Regulation.

ISO/IEC 27701:2019 is an extension of the requirements and guidelines defined in **ISO/IEC 27001:2022** for security and privacy management. It is the framework of the management system for the protection of personally identifiable information to demonstrate compliance with data protection regulations, such as the **General Data Protection Regulation (GDPR)**.

In order for an organization to be certified according to ISO/IEC 27701:2019, it must already have a management system in place in accordance with ISO/IEC 27001:2022 (certified or not) or choose its parallel certification based on the two standards for the processing of personal data within an information security management system.

2. Terms – Abbreviations – Definitions

The terms used in this Regulation are in accordance with the terms set forth in §2 of the BQC General Certification Regulation and are in line with the **ISO/IEC 27000:2018** "Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary", **ISO/IEC 27701:2019** "implementing policies that ensure the integrity, confidentiality and availability of information and full compliance with applicable legal requirements for personal data management" and **ISO/IEC 17000:2020**.

Privacy Information Management System (PIMS): part of the management system that focuses on addressing the protection (i.e. employees, customers and partners) of privacy as potentially affected by the processing of PII.

PII controller: natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law

Example: A company that collects financial data of its customers (e.g. payment invoices, financial transactions) in order to make them available to an external partner for the management of its payments

PII processor: natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Example: A company that carries out payment management (accounting services) on behalf of its principal, by processing the data received from its principal

PII controller & processor: natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law and processes those personal data

Example: A company that collects financial data of its customers (e.g. payment invoices, financial transactions), and processes them itself for the purpose of payment

3. Certification Procedure

3.1 Application

Organizations wishing to certify their PIMS address BQC and are informed that the full implementation of the PIMS under certification and the existence of corresponding records for at least two (2) months are required. Then, they fill in the information questionnaire **E050-1** free of charge serving as an application for certification.

3.2 Application Review

After the certification application is returned completed by the organization, it is delivered to the Certification Department, who shall conduct a review of the application (completes **F050-50**) and additional information for the certification, in order to calculate the necessary mandays for the audit and ensure that:

a) the information regarding the applicant organization and its management system is sufficient to conduct the audit,

b) the requirements for certification are clearly defined and documented,

c) any known differences in understanding between the applicant organization and BQC are resolved,

d) BQC has the capacity and ability to perform the certification activities,

e) the requested scope of certification, the facilities of the organization, the time needed to complete audits and other elements that affect the certification activities are taken into account (language, safety issues, risks to impartiality, etc.)

f) the PIMS under Certification is implemented for at least two (2) months.

In case BQC cannot undertake the certification, the reason is documented in the application review form **F050-50**, the organization shall be notified in writing and the process is discontinued.

If BQC can undertake the audit, a Quotation will be prepared by the General Manager of BQC, which is sent to the organization along with the BQC General Certification Regulation to be signed.

To determine the audit program and any later changes, the requirements as described in **F050-50** are taken into account.

- In case of **integrated** certification of **ISO/IEC 27001 and ISO/IEC 27701:2019:**

The duration of the initial audit is the duration resulting from **ISO/IEC 27006:2015** increased by:
20% if the organization is PII processor
30% if the organization is PII controller
50% if the organization is PII controller & processor.
Based on the ISO/IEC 27006-2:2021, the additional audit time for an initial PIMS audit (stage 1 and stage 2) shall be at least:
2,5 days for "PII processors"
3 days for "PII controllers" or
3,5 days for "PII processors & controllers"
The duration of surveillance audits is 1/3 of the duration of the initial audit
The duration of the recertification audit is 2/3 of the duration of the initial audit

- In case **ISO/IEC 27701:2019** is certified **separately** – provided that the ISMS system is already certified:

The duration of the initial audit is the duration of the initial assessment in accordance with ISO/IEC 27001 increased by:
20% if the organization is PII processor
30% if the organization is PII controller
50% if the organization is PII controller & processor.
Based on the ISO/IEC 27006-2:2021, the additional audit time for an initial PIMS audit (stage 1 and stage 2) shall be at least:
2,5 days for "PII processors"
3 days for "PII controllers" or
3,5 days for "PII processors & controllers"
The duration of surveillance audits is 1/3 of the duration of the initial audit
The duration of the recertification audit is 2/3 of the duration of the initial audit

Factors that may affect the duration of an audit: Reduction of audit duration due to the existence of multiple Management Systems

If the organization's management system is integrated and structured to include common responsibilities and processes for more than one standard, then the required mandays are determined according to **IAF MD11:2023**

BQC may accept combined documentation (e.g. for information security, quality, health & safety and environment) provided that the PIMS can be clearly identified as well as its interactions with the other management systems.

Multi-site sampling:

When multi-site sampling is used for the audit of a client management system that covers the same activity at various sites, following the provisions of **IAF MD1:2018**, BQC develops a sampling plan to cover the whole number of documents or scopes, products and departments of the organization as well as all requirements of the Standard. The sampling plan, and the number of facilities which will be audited, follows the methodology below:

- At each audit the headquarters of the organization will be audited.
- For the rest of the facilities, the following apply:
  - Initial Audit: The sample size will be the result of the square root of the rest of the facilities (e.g. Total number of facilities: 4 – 1 Headquarters and 3 more facilities, number of facilities to be audited: 1 +√3 = 1 + 2 = 3).
  - Surveillance Audit: The sample size will be the result of the square root of the rest of the facilities πολλαπλασιασμένο multiplied by a factor of 0.6 (e.g. Total number of facilities: 4 – 1 Headquarters and 3 more facilities, number of facilities to be audited: 1 + √3 × 0.6 = 1 + 1 = 2).
  - Recertification Audit: The sample size should be the same as that of initial audit. However, where the Management System is proven effective for at least 3 years, the sample size will be the result of the square root of the rest of the facilities multiplied by a factor of 0.8 (e.g. Total number of facilities: 4 – 1 Headquarters and 3 more facilities, number of facilities to be audited: 1+ √3 × 0.8 = 1 + 2 = 3).
- During the sample's selection process, at least, the 25% of the facilities shall be chosen randomly.

A sample-based approach for a multiple-site PIMS audit can be applied when the facilities of the organization:

a) all sites are operating under the same PIMS, which is centrally administered and audited and subject to central management review;

b) all sites are included within the client's internal PIMS audit program; and

c) all sites are included within the client's PIMS management review program.

BQC before implementing a sample-based approach for an PIMS audit shall ensure the following:

a) during the initial application review, to the greatest extent possible, the differences between sites are identified so that an adequate level of sampling is determined.

b) a representative number of sites have been sampled, taking into account:

i. the results of internal audits;
ii. the results of management review;
iii. variations in the size of the sites;
iv. variations in the business purpose of the sites;
v. complexity of the information systems at the different sites;
vi. variations in working practices;
vii. variations in activities undertaken;
viii. variations of design and operation of controls;
ix. potential interaction with critical information systems or information systems processing sensitive information;
x. any differing legal requirements;
xi. geographical and cultural aspects;
xii. risk situation of the sites; and
xiii. information security incidents at the specific sites.

c) a representative sample is selected from all sites within the scope of the client's PIMS. The selection shall be based upon judgmental choice to reflect the factors presented above as well as a random element.
d) at the certification audit all facilities that are subject to significant risks are included.
e) the audit program has been designed in the light of the above requirements and covers representative samples of the scope of the PIMS certification within the three-year period, and
f) in the case of a nonconformity being observed (either at the head office or at a single site), the corrective action procedure applies to the head office and all sites covered by the certificate.

3.3 Audit team selection

After the signing of the cooperation agreement by the organization, the Certification Department of BQC, after taking into account the mandays and the overall abilities of the audit team required to conduct the audit, chooses the Audit Team or the Auditor (and Technical Expert, whenever required) to conduct the audit, so as:

- to be familiar with applicable legal regulations and BQC certification procedures.
- to be conversant with the relevant method and documents of audit.
- to have the appropriate technical knowledge of the specific activities for which certification is sought and of the relevant procedures of the organization.
- to have an adequate level of understanding, so as to conduct a reliable evaluation of the supplier's ability to provide products, processes and services on the organization's certification subject.
- be able to communicate effectively, both in writing and orally in the required language.
- be free from any interest, which may compel the team to deviate from an impartial or non-discriminatory manner of action, for example:
  - ➢ members of the audit team or their organization should not have provided consulting services to auditee.
  - ➢ members of the audit team or their organization should not have any previous or planned bond with the auditee.
  - ➢ members of the audit team must not have any relation to a competitive of the auditee.

3.4 Initial Contact with the Auditee

The Lead Auditor of the audit team communicates with the representative of the auditee. Purpose:

- Create communication channels with the auditee.
- Authorization confirmation for the conduct of the audit.
- Application for provision of the necessary documentation of the audited organization (as it is described in §3.5.1 of this Regulation).
- Determination of health and safety rules during the onsite audit.
- Determination for any arrangements for the onsite audit.
- Agreement on the presence of observers and guides for the Audit Team.

The Lead Auditor develops an audit plan **F050-5** for each audit, which is the basis of the agreement for the conduct and scheduling of audit activities.

When informed of the composition of the audit team and the schedule, the audited organization has the right to request in writing within three (3) days upon receiving the audit plan and with proper justification, the replacement of a member or members of the audit team or a change of the audit date. In such cases the Certification Department redefines the Audit Team or the audit schedule and re-informs the audited organization.

If in the assigned audit team there is a technical expert, an interpreter or a trainee, they are not counted as auditors in the calculation of mandays.

If for any reason the organization is unable to follow the audit plan, the organization is obliged to inform the CB. In case that during the opening meeting the auditor realizes that the audit plan cannot be followed

under the responsibility of the organization, the auditor shall postpone the audit.

3.5 Initial Certification Audit

The initial certification audit of a management system is conducted in two stages: the first stage and the second stage.

3.5.1 Stage 1

The first stage of the audit is performed to evaluate the following:

a) the documentation of the management system of the audited organization is reviewed. BQC shall have a sufficient understanding of the design of the PIMS in the context of the client's organization, risk assessment and treatment (including the controls determined), information security policy and objectives and, in particular, of the client's preparedness for the audit. To this end, the audited organization shall send to BQC the documentation for the PIMS that wishes to be certified (at least: information security policy, risk assessment process, information security objectives, change management policy, latest internal audit and management review, corrective actions, list of documents, Statement of Applicability and privacy).

b) the condition of the facilities and the location of the organization are evaluated and interviews with personnel are being conducted to determine its readiness for the second stage of the audit.

c) the condition and understanding of the client regarding the requirements of the standard are reviewed, particularly regarding the identification of key performance issues, processes, the objectives and functioning of the management system.

D) the necessary information regarding the scope of the management system, processes and facilities of the organization and the relevant regulatory and legislative conformity requirements is collected.

e) a focal point is provided for the planning of the 2nd stage of audit, having a sufficient understanding of the management system and the operations of the organization.

f) it is assessed whether internal audits and management reviews are planned and executed and how the level of implementation of the management system justifies if the organization is ready for the 2nd stage of audit.

g) the provision of resources for the 2nd stage of the audit is reviewed and details of the 2nd stage of audit are agreed with the organization.

For information security management systems, the entire 1st stage can be performed offsite, unless otherwise decided.

The findings of the 1st stage are documented in the audit report and are communicated to the organization, including any points that could be recorded during the 2nd stage of audit as non-conformities.

The 1st stage audit report is reviewed by BQC before deciding on proceeding with stage 2 and the adequacy of the audit team selected for the conduct of the 2nd stage is confirmed. This review may be carried out by the Lead Auditor of the 1st stage and recorded in the audit report, provided he/she is competent, unless otherwise decided.

When determining the interval between the 1st and 2nd stage, the organization's need to resolve any problematic points identified during the 1st stage is taken into account, as well as the severity of the findings.

3.5.2 Stage 2

The purpose of the 2nd stage of the audit is to assess the organization's management system and its effectiveness. The 2nd stage of the audit takes place at the premises of the organization and includes at least:

a) information and objective evidence regarding the conformity with all the requirements of the standard or other regulatory document of the applicable management system, as well as the organization's own policies, objectives and procedures;

b) monitoring, measuring, reporting and reviewing of significant objectives and targets;

c) the management system and the performance of the organization regarding the conformity with legal requirements;
d) the operational control of the processes of the organization;
e) the internal audit and management review;
f) top management responsibility and commitment to information security policy and the information security objectives;
g) the relationships between regulatory requirements, policies, objectives and performance targets, any applicable legal requirements, responsibilities, personnel skills, operations, procedures, performance data and conclusions and findings of internal audits;
h) the requirements of standards **ISO/IEC 27001** and **ISO/IEC 27001:2019 (applicable to integrated audit)**;
i) the requirements of standard **ISO/IEC 27701:2019 (applicable to separate audit)**,
j) assessment of information security related risks and if the assessments produce consistent, valid and comparable results if repeated;
k) determination of control objectives and controls based on the information security risk assessment and risk treatment processes;
l) information security management system performance and its effectiveness, evaluating against the information security objectives;
m) correspondence between the determined controls, the Statement of Applicability and the results of the information security risk assessment and risk treatment process and the information security policy and objectives;
n) implementation of controls (according to **Annex D** of **ISO/IEC 27006:2015**), taking into account the external and internal context and related risks, the organization's monitoring, measurement and analysis of information security processes and controls, to determine whether controls are implemented and effective and meet their stated information security objectives; and
o) programs, processes, procedures, records, internal audits and reviews of the PIMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.

Note that if the audited organization has assigned to a subcontractor, part or the entirety of a process – included in the certification scope – it will be audited onsite by the audit team. This onsite audit can be avoided if the implementation and results of this process can be verified by reviewing the records and documents of the implemented Management System.

At least 70% of the total time required to carry out the initial certification audit takes place at the organization's premises.

3.5.3 Conclusions of Initial Certification Audit

The audit team analyzes all the information and objective evidence collected in both stages of the audit, reviews the findings of the audit and arrives at the conclusions of the audit.

3.5.4 Information for Granting of Initial Certification

The information provided by the audit team to the Certification Manager of BQC to take the certification decision shall include, at least, the following:
a) the audit reports;
b) comments on non-conformities and, wherever possible, the corrective actions of the organization;
c) confirmation of the information provided during the review of the application;
d) confirmation that the purpose of the audit has been achieved;
e) a suggestion whether the organization shall be certified or not, along with together with any conditions or remarks.

The Lead Auditor, for each audit he/she undertakes, develops a three-year audit program for a complete certification cycle. The three-year audit program includes the activities that need to be documented in order that the implemented management system complies with the requirements of the relevant standard. Any non-conformities and observations

recorded during the audit are also noted in the program.

The Certification Manager of BQC, makes the certification decision based on the evaluation of the findings and conclusions of the audit and other relevant information (e.g. public information, comments about the audit report by the client).

When during the certification audit major non-conformities are identified, which are not resolved within six (6) months from the last day of the 2nd stage, then the 2nd stage of audit should be repeated before the certification decision is made.

3.6 Surveillance Activities

3.6.1 General

BQC conducts annual surveillance audits to regularly review the organization's departments and operations covered by the purpose of the certified management system, and changes of the organization and its management system.

The surveillance activities include onsite audits to assess whether the organization's management system meets specific requirements, against the standard based on which the certification is granted.

Other surveillance activities may be:

a) questions of BQC to the certified organization, regarding the certification,

b) review of any statements of the organization regarding its operations (e.g. promotional material, website),

c) requests to the client to provide documents and records (on paper or electronic form), and

d) other means of monitoring the performance of the certified organization.

Surveillance audits (1st and 2nd) take place before the expiry of the period of 12 and 24 months respectively, starting from the day of the certification decision.

3.6.2 Surveillance Audit

The surveillance audits are on-site audits, but not necessarily complete audits of the system. They are designed in combination with other surveillance activities (see §3.6.1), so that BQC can maintain confidence that the certified management system continues to meet the requirements between recertification audits. The program of surveillance audits shall include, at least, the following:

a) changes in information security policy,

b) the organization's ability to identify the applicable legal requirements,

c) the implementation and evaluation of compliance with legal and regulatory requirements,

d) the effectiveness of the management system regarding the achievement of the objectives,

e) the progress of pre-designed activities with regard to continuous improvement,

f) the continuous operational control,

g) the review of any changes,

h) the use of logos and / or other references to certification,

i) the audit of files for objections and complaints, where any inability of compliance or failure to meet the certification requirements is recorded along with the actions of the audited organization to investigate the effectiveness of the PIMS, the procedures it implements, and the appropriate corrective measures it takes,

j) maintenance and update of system elements such as information security risk assessment, internal audit, management review and corrective actions,

k) the review of the actions performed for non-conformities identified during the previous audit,

l) communications from external parties as required by the standard **ISO/IEC 27701:2019** and other documents required for certification;

m) areas subject to change;

n) selected requirements of **ISO/IEC 27701:2019**,

o) other selected areas as appropriate.

p) changes to the controls determined, and resulting changes to the Statement of Applicability; and

q) implementation and effectiveness of controls according to the audit program.

The audit report shall include, at the very least, the above, as well as information on the resolve of non-conformities previously recorded, the version of the

Statement of Applicability in force, and any significant changes observed since the previous audit.

3.7 Recertification Activities

3.7.1 General

The recertification audit is carried out before the expiration of the certificate of conformity unless the termination of certification is requested by the organization in writing at least 3 months before the expiry of the certificate of conformity.

If, under the responsibility of the organization, the recertification audit is conducted after the expiration date of the certificate (without documented justification), the audit is considered an audit of initial certification and the rules described in §3.5 are followed.

3.7.2 Planning of Recertification Audit

A recertification audit is designed and conducted to assess the ongoing satisfaction of all the requirements of the relevant standard of the management system or another regulatory document. The purpose of the recertification audit is the confirmation of the continuous compliance and effectiveness of the management system as a whole as well as the continuing relevance and applicability of the scope of certification.

The recertification audit takes into account the performance of the management system during the certification period and includes the review of reports of previous surveillance audits.

The activities of recertification audit shall include the first stage of audit, when there have been significant changes in the system, the client or the operational framework of the management system (e.g. changes in legislation).

In the case of multiple facilities, the audit design shall ensure adequate onsite audits, in order to strengthen the confidence in the certification.

3.7.3 Recertification Audit

The recertification audit includes an onsite audit, which covers the following issues:

a) the effectiveness of the entire management system regarding the internal and external changes, and the continuous relevance and applicability of the scope of certification;

b) the demonstrated commitment to maintaining and improving the effectiveness of the management system, in order to improve the overall performance;

c) whether the operation of the certified management system contributes to the achievement of policies and objectives of the organization;

d) the findings and the effectiveness of the corrective actions recorded throughout the last certification cycle.

If recertification activities are successfully completed prior to the expiration date of the existing certificate, the issue date of the new certificate can be based on the expiry date of the existing certificate. The issue date on the new certificate may be the same as the recertification decision or later.

If the recertification audit has not been completed or any non-conformities are not resolved before the expiry of the existing certificate, then there can be no recommendation for recertification and the validity of the certification shall not be extended. To avoid this, BQC shall notify the organization at least five (5) months prior to the expiration of the certificate, so that the recertification audit can be scheduled at least three (3) months prior to the expiration of the certificate. For each such case, the organization shall be informed of the consequences.

If an organization's existing certificate has expired, BQC may restore the certification, provided that the pending matters of the audit have been resolved within six (6) months. Otherwise, a second-stage audit shall be at least conducted. The date of the recertification certificate shall be the same as the recertification decision or later and the expiration

date will be based on the expiration date of the previous certification cycle.

3.7.4 Information for Granting Recertification

BQC takes decisions on the renewal of certification based on the results of the recertification audit, as well as on the results of the system review during the period of certification validity and any complaints received from users of the certification.

3.8 Main Processes for the Conduct of Audit

3.8.1 Opening Meeting

The opening meeting is convened by the Lead Auditor immediately after the arrival of the Audit Team at the audit site.

Participants:

- From BQC, all members of the audit team
- On the part of the organization, at least the Management Representative and the Chief Information Security Officer of the organization.

Purpose:

- Confirmation of the audit plan
- Introduce the audit team and their roles
- Ensure that all planned audit activities can be performed
- A reference to the way the audit will be conducted
- Confirmation of the communication channels
- Questions of the auditee

CONDUCT OF OPENING MEETING

The following are taken into account:

a) introductions among the attendees and description of their roles;

b) confirmation of certification scope;

c) confirmation of the audit plan (including the type, purpose and criteria of the audit), any changes and other relevant arrangements with the client, such as the date and the time of the closing meeting and interim meetings between the audit team and the client's representative,

d) confirmation of formal communication channels,

e) confirmation that the resources and facilities needed by the audit team are available,

f) confirmation of matters relating to confidentiality and information security,

g) confirmation of work safety, emergency and security procedures for the audit team

h) confirmation of the availability, roles and identity of observers and guides,

i) the method of reporting, including the grading of audit findings,

j) conditions under which the audit may be prematurely terminated,

k) confirmation that the Lead Auditor and the audit team, representing BQC, are responsible for conducting the audit and following the audit plan,

l) confirmation of the status of findings of previous audits,

m) methods and procedures to be during the audit,

n) confirmation of the language to be used during the audit,

o) confirmation that, during the audit, the client will be kept informed of the audit progress,

p) the client is allowed to ask questions.

3.8.2 Role and Responsibility of Guides and Observers

Guides and observers may accompany the audit team with approval of the Lead Auditor, and/or the auditee, if required. They should not influence or interfere with the conduct of the audit. For the observers, any details concerning access, health and safety, environment, security and confidentiality should be arranged with the audited organization. The guides, appointed by the audited organization, should assist the audit team and act on the request of the Lead Auditor or the auditor to which they have been assigned. Their responsibilities include the following:

- assisting the auditors to identify individuals to participate in interviews and confirm the time and location of the interview,
- arranging access to specific locations of the audited organization
- ensuring that rules concerning location-specific arrangements for access, health and safety,

environment, security, confidentiality and other issues are known and respected by the audit team members and observers and any risks are addressed
- witnessing the audit on behalf of the audited organization
- providing clarifications or assisting in collecting information, when required.

Note: The Lead Auditor has the right to ask the organization to change the guide or the observer when proven and repeatedly they deviate from their role and obstruct the work of the audit team.

3.8.3 Audit Conclusions – Completion of Audit Documents

3.8.3.1 Audit Conclusions

During the audit, under the responsibility of the Lead Auditor, the audit team shall evaluate the audit progress and exchange information. The Lead Auditor is responsible, if necessary, to amend the initial audit plan and reassign work between the audit team members. During the audit, the Lead Auditor shall inform the representative of the audited organization for the progress and any points of concern.

The audit team, under the responsibility of the Lead Auditor, shall convene before the closing meeting in order to:
- submit to review the audit findings and other relevant information collected during the audit according to the objectives of the audit
- agree on the conclusions of the audit, taking into account the inherent uncertainty of the audit process,
- agree on the follow-up actions,
- categorize any identified non-conformities,
- confirm the appropriateness of the audit program or identify any modification needed for future audits.

3.8.3.2 Completion of Audit Documents

The Lead Auditor completes the **F050-2** Audit Report, the **F050-52B** Audit Questionnaire, the **F050-51 or F050-51B** Three Year Audit Program and, optionally, the optional **F050-7** Auditor's Note form.

3.8.4 Closing Meeting

Participants:
- From BQC, all members of the audit team
- On the part of the organization, at least the Management Representative and the Chief Information Security Officer of the organization.

Purpose:
- Formalities.
- Declaration of confidentiality and information security.
- Inform the audited organization that the compliance audit, is based on sampling and therefore contains an element of uncertainty.
- Presentation of audit findings.
- Discussion on the audit findings.
- Method and schedule of reporting, including grading of any audit findings.
- Briefing by the Lead Auditor about the procedure for handling non-conformities and the consequence on the client's certification status.
- Schedule for the client to send a plan of corrections and corrective actions for any non-conformities identified during the audit.
- BQC post certification activities.
- Information about the complaint and objection handling process.
- Recommendation on certification.

At the end of the closing meeting, the Management Representative shall sign the audit report **F050-2** and receive a copy of it. In case that he/she refuses to accept the audit findings and therefore to sign the audit report, the Lead Auditor records the disagreement or reservation, and gives a copy of the audit report to the audited organization.

3.9 Granting of Certificate

The positive or negative decision on the issuance of the certificate of conformity is decided by the person defined in the BQC Decision Making Matrix following a recommendation of the Lead Auditor. The decision

evaluates, among other things, the audit report and the documentation of the corrective actions taken to resolve non-conformities recorded during the audit. The decision is communicated to the organization in writing.

The positive or negative decision on certification of the audited organization is taken by the person who has not been involved in the certification process.

The organization is obliged to inform BQC of any change in the version of the Statement of Applicability, which is stated on the certificate of conformity. A certificate of conformity stating an obsolete version of the relevant Statement of Applicability is not valid and shall be withdrawn.

To maintain the validity of the certificate, the organization sends the new version of the Statement of Applicability to BQC. Following, a member of the Certification Department evaluates the changes and decides if further actions are required (e.g. sending additional documentation, conducting an inspection, etc.) before reissuing the certificate of conformity.