CERTIFICATION SCHEME

FOR AUDITORS AND LEAD AUDITORS

ISO 37001

Prepared by: Technical Management

Claudio Cesaroni

Approved by: Sole Director

Gian Paolo Venezia

1. PURPOSE AND SCOPE

This document aims to regulate the relationship between AUTENTICERT, operating as a personnel certification body, and individuals requesting voluntary third-party certification for their competencies as Auditor / Lead Auditor for international standards. Personnel certification applies to the individual applying, or to the individual for whom their company is applying, and is not applicable to companies/organizations.

2. GENERAL INFORMATION

For the execution of certification activities, AUTENTICERT carries out the direct assessment of the candidate or on behalf of other selected, qualified, and approved external bodies. The certification bodies must have the premises, equipment (if applicable), tools, and technical personnel to carry out the activity. AUTENTICERT.

AUTENTICERT can certify an unlimited number of people within an organization.

3. DESCRIPTION OF AUDITORS

The professional figure of the Anti-bribery Lead Auditor / Auditor is a person who conducts an audit of the anti-bribery management system. The Lead Auditor / Auditor must be impartial and free from any conflict of interest in relation to their duties. An audit is a systematic, independent, and documented process for obtaining audit evidence (data, statements of fact, or other relevant and verifiable information) and evaluating it objectively, in order to determine the extent to which audit criteria (policies, procedures, or requirements used as a reference for the UNI ISO 37001:2016 standard) are met.

3.1 AUTENTICERT COMMITMENTS

AUTENTICERT guarantees access to its services for candidates, without discrimination of a financial nature or other unnecessary conditions. AUTENTICERT recognizes the importance of impartiality in certification: for this reason, it carries out its activities objectively, avoiding any conflict of interest. In particular, AUTENTICERT undertakes not to use as examiners for the evaluation of candidates individuals who may have a potential conflict of interest. This condition also extends to the examiners of any organization qualified for the evaluation. All functions involved in the personnel certification process comply with the Code of Ethics. Certification is based on the positive evaluation of each candidate based on the results of written and oral tests.

3.2 CANDIDATE COMMITMENTS

By submitting the certification request to Autenticert, the candidate adheres to and accepts the certification scheme, signing the application form, agreeing to all phases of the evaluation, certification, and registration process described below: a) according to the UNI ISO 37001:2025 standard "Anti-bribery Management Systems". b) in the most important international conventions.

To obtain and maintain certification, the applicant must agree to apply all requirements related to the standards required by the certification, additional requirements established by Autenticert and other

conformity assessment bodies, as well as all requirements presented in this document. Candidates are required to comply with the code of ethics.

3.3 SKILLS AND KNOWLEDGE

In addition to the general managerial skills necessary for anti-bribery audit management, it is necessary to possess: - skills in the ability to manage management system audits; - specialized knowledge of ISO 19011 and ISO/IEC 17021-9 standards.

This knowledge must be acquired through training and experience in this field and must be related to: a) according to the UNI ISO 37001:2025 standard "Anti-bribery Management Systems". b) in the most important international conventions. c) in-depth and documented knowledge of legislation (legal, regulatory, and "good practices") for the prevention of active and passive corruption and the management of corporate integrity applicable in the country where the organization's business and commercial activities take place.

4. REFERENCES

All references to undated laws, standards, and Autenticert documents are understood to apply in their latest revision. - Normative references for Audit evaluation: - ISO 19011 - ISO/IEC 17021 - ISO/IEC TS 17021-9:2016 - ISO 37001 - Autenticert references for personnel certification: - ISO/IEC 17024 "General requirements for bodies operating certification of persons" - Certification schemes. Etc.

5. DEFINITIONS

Certification process: Activity by which a certification body determines that a person meets certification requirements, including application, assessment, certification/recertification decision, use of certificates and logo/symbols.

Certification scheme: Further requirements related to the professional specification or competence categories of persons.

Knowledge: Result of the assimilation of information through learning

Skill: Ability to apply knowledge to complete tasks and solve problems

Competence: Proven ability to use knowledge, skills, and personal capabilities in work or study situations and in professional and personal development, which can be exercised with a certain degree of autonomy, e.g. responsibility.

Certification requirements: The set of specific requests, including requirements for methodology, that must be met to obtain or maintain certification.

Scheme owner: Organization responsible for the development and maintenance of the certification scheme. (The organization may be the certification body itself, a governmental authority, or another entity.)

Certificate: Document issued by a certification body, in accordance with the provisions of the International Standard, indicating that the designated person has met the certification requirements.

Qualification: Demonstration of education, training, and work experience, where applicable.

Assessment: Process that evaluates a person's fulfillment of the requirements of the certification scheme.

Examination: Mechanism that is part of the assessment, which measures the candidate's ability, the candidate's competence, by one or more methods; written, oral, practical, and observational, as defined in the certification scheme.

Examiner: Competent person to conduct and evaluate an examination, when the examination requires professional judgment.

Invigilator: Person authorized by the certification body who administers or supervises an examination, but who does not evaluate the candidate's competence.

Personnel: Individuals, internal or external to the certification body, who perform activities for the certification body. (These include committee members and volunteers).

Applicant: Person who has submitted an application to be admitted to the certification process.

Candidate: Applicant who has met the specified prerequisites and has been admitted to the certification process.

Impartiality: Presence of objectivity. Note 1: Objectivity means that conflicts of interest do not exist, or have been resolved in such a way that they cannot negatively influence the subsequent activities of the certification body. Note 2: Other useful terms to convey the element of impartiality are independence, absence of conflict of interest, absence of bias, absence of prejudice, neutrality, fairness, openness, justice, disinterestedness, balance.

Equity: Guarantee of equal opportunities for every candidate in the certification process.

Validity: Demonstration that the assessment measures what it is intended to measure, as defined by the certification scheme.

Reliability: Indicator of the degree to which examination results are stable over time and across different examination locations, different examination formats, and different examiners.

Appeal: Request by the applicant, candidate, or certified person for reconsideration of any decision made by the certification body regarding their desired certification status.

Complaint: Expression of dissatisfaction, other than an appeal, by any individual or organization to a certification body, relating to the activities of the body, or to a certified person, for which a response is expected. NOTE Adapted from ISO/IEC 17000:2004, definition 6.5.

Interested party: Individual, group, or organization affected by the performance of a certified person or the certification body. (Certified person; user of the certified person's services; employer of the certified person; client; government authority).

Surveillance: Periodic monitoring, during the certification period, of the certified person's performance, to ensure conformity with the requirements of the certification scheme.

Examiner: Person who has the competence to develop an examination and, when that examination requires professional judgment of the candidate, to evaluate the result.

Facility/structure/location: Examination center, competence assessment offices, evaluated by the body where certification examinations are conducted under control and according to the body's specific procedures.

Certification Process Review (CPR): Internal examination phase of the certification process to authorize the issuance of the certificate.

6. CERTIFICATION PREREQUISITES

a) Prerequisites: Educational qualification

Auditor: Must hold a higher education diploma in law.

Lead Auditor: Must hold a higher education diploma.

b) Prerequisites: Training

Auditor: Must have a training certificate on the ISO 37001:2016 standard of at least 16 hours, which includes a program with in-depth and documented knowledge of legislation for the prevention of active and passive corruption and corporate integrity management. For those who have already completed a 40-hour course on management systems (in the case of 24-hour courses), it is necessary to have at least a 16-hour course on audit techniques.

Lead Auditor: Must have a training certificate on the ISO 37001:2016 standard of at least 16 hours, which includes a program with in-depth and documented knowledge of legislation for the prevention of active and passive corruption and corporate integrity management. For those who have already completed a 40-hour course on management systems (in the case of 24-hour courses), it is necessary to have at least a 16-hour course on audit techniques.

c) Prerequisites: Total work experience

Auditor:

If holding a secondary education diploma, 3 years of professional experience in the reference role (*responsibility in the management of anti-corruption systems or legal compliance or corporate crimes (and in addition to this, experience as a member of OdV or consultant to Organizations (company/entity) with Legislative Decree 231/2001 or Law 190/2012)).

If holding a degree in Law, 1 year of professional experience in the reference role (* see point above).

Lead Auditor:

3 years of professional experience in the reference role.

*(**) This experience can be acquired as an employee (in industrial or service companies or in public and private entities, with tasks related to the production of goods and services), as well as an independent professional.

7 CERTIFICATION PROCEDURE

a) Criteria for initial certification and recertification

b) Assessment methods for initial certification and recertification. Registration in the Autenticert Personnel Register. Validity

The candidate must demonstrate:

a) - For certification: possession of the required prerequisites (educational qualification, training, total work experience, specific work experience in the sector).

- For recertification: verification of professional updating (minimum 24 hours in the last three years, see point 8.3 c) and continuity of professional activity. The continuity of professional activity implies the need to demonstrate that the candidate continues to exercise their specific professional activity in the field of verification or assessment of conformity to anti-corruption systems in a regular and continuous manner. The candidate must document and demonstrate this continuity with audit records, contracts or letters of appointment, assignments received for audits performed, and continuous training certificates.

b) Passing the exam which will be structured as follows:

TEST OF 50 MULTIPLE-CHOICE QUESTIONS, CONSISTING OF 4 ANSWERS WITH ONLY 1 CORRECT ONE TO BE COMPLETED IN 90 MINUTES.

- **The topics covered by the written test will include:**

Anti-corruption principles

- ISO 37001 requirements
- Organizational context and risk assessment
- Financial and non-financial controls
- Role of leadership and ethical culture
- Planning, implementation, and improvement of the system
- Audit techniques (based on ISO 19011)
- Tecniche di audit (basatesu ISO 19011)
- Nonconformity and corrective action management.

- **CASE STUDY LASTING A MAXIMUM OF 90 MINUTES. The candidate must:**

- Analyze the situation in light of ISO 37001 requirements
- Identify any nonconformities or deficiencies
- Propose corrective actions or recommendations

- If necessary, draft a part of the audit documentation (e.g., a plan, a report, or an investigation sheet).
- **ORAL EXAM OF 4 QUESTIONS LASTING A MINIMUM OF 20 MINUTES AND A MAXIMUM OF 30. The oral questions cover the following areas:**
    1. Knowledge of ISO 37001
    2. Practical application of the standard
    3. Auditor's role and responsibilities
    4. Ethics and professional integrity

The candidate must pass the test and/or the case study and the technical interview with a score of at least 60/100; a) After payment of the required fees, it will be possible to enter the Autenticert personnel register. b) The three-year validity of the certification starts from the certificate issuance date.

c) Surveillance methods and criteria

During the certification validity period, annual maintenance must be considered confirmed as a result of:

- absence of measures by Autenticert against the data subject;

- evidence relating to professional development, 8 hours/year for legislative and jurisprudential matters and for anti-corruption matters, to be documented with certificates or other means;

- absence of complaints from Clients/Directors or other interested parties (the "silence-is-consent" practice applies for specific requests made to Clients at the beginning of the year) or positive management of any complaint received from the Client/Director;

- payment of the annual fee for registration in the Personnel Register in force.

7.1 EXAMINERS AND SUPERVISORS

The exam/evaluation is conducted by competent Autenticert examiners who meet at least the minimum requirements, evaluated by Autenticert or another organization.

They are required to:

- maintain the confidentiality of the exam.

- Conduct the exam evaluation with objectivity.

- Declare any relationship or conflict of interest that could compromise the impartiality of their judgment.

- Comply with this scheme.

The Examination Board is composed of one or more examiners to cover all the competencies required for the process. If the exam is conducted by external personnel, the Examination Board may be supervised, even without prior notice, by personnel authorized by Autenticert. In examination sessions, Autenticert may require the presence of its own supervisors, the DPA, or any other competent authority.

7.2 REPETITION OF THE EXAM

Candidates who do not pass the exam may repeat it by paying the exam repetition fee.

8 CERTIFICATE ISSUANCE

To the candidate who has successfully passed the exam and met all required conditions in accordance with administrative aspects, Autenticert issues the certificate, which demonstrates the person's competence and completes the corresponding register.

The certificate must contain:

- Name of the certifying body

- Name, surname, personal number, date and place of birth of the certified person

- certificate number

- scheme for which it was certified and/or reference to standards/procedures etc.

- start date of validity - end date of validity

- signature of the authorized person

9.1 REGISTRATION IN REGISTERS AND PUBLICATION

Registration in the Autenticert registers takes place after the certificate is issued; and the registration may be accessible on the Autenticert website.

9.2 COMPLETION OF THE REGISTER

The person certified by Autenticert as an Auditor can request to be certified also as a Lead Auditor or/and for other IAF codes after obtaining the certificate.

This request involves the integration of the documentation completed for the previous certification, satisfying the requirements of the next level, and the payment of the established fees.

The evaluation for the candidate's admission occurs through mandatory and time-consuming phases, described in paragraph 7 (Evaluation Process), with the exception of the certification exam.

At the end of these phases, Autenticert will ensure the updating of records with the new information.

The new certificate is issued after the surrender of the old certificate, but the certification date does not change.

9.3 DATA INTEGRITY AND PRIVACY

Autenticert, as the data controller, guarantees that the processing of data of certification candidates is carried out in compliance with EU Regulation 2016/679 and LAW No. 9887, of 10.3.2008 FOR THE PROTECTION OF PERSONAL DATA (Amended by Law No. 48/2012, Official Gazette 53) (Amended by Law No. 120/2014, Official Gazette 160) and other documents related to certification activities. Privacy is guaranteed for all persons participating in the application. Information obtained by personnel working on behalf of Autenticert, including decision-makers, is subject to confidentiality.

10. MAINTENANCE OF CERTIFICATION (SURVEILLANCE)

The validity of the certification during the contractual period of 5 years (starting from the certificate issue date) depends on the positive outcome of the activities after the annual surveillance (the period/date is specified), by Autenticert. To this end, the certified person must provide an annual self-declaration, carried out in application of laws/regulations/procedures (with specific forms prepared by Autenticert), as follows:

- Acceptance of Autenticert's policies and procedures and documentation

- a statement that they are still employed in the field for which they are certified.

- a statement that they have no observations on their work and have an evaluation considered positive, for the field in which they are certified.

The maintenance of the certificate is also subject to the payment of the foreseen annual fees.

11. RECERTIFICATION

Recertification is carried out upon request of the person who renews the contract and proceeds with the process. Renewal is carried out before the certification expires.

Recertification includes, in addition to the documentation submitted for annual maintenance, also:

- Updated CV, dated and signed by the candidate themselves. All other additional documents of activities (training…) carried out after the first application, as well as the list of audits performed during this period.

- update regarding specific work experience carried out in the last 3 years

- professional field update for at least 24 hours over 3 years;

12. CRITERIA FOR SUSPENSION AND REVOCATION OF CERTIFICATION

Causes for suspension:

- Improper use of the certification mark.

- Violation of the Code of Conduct

- Non-payment of obligations

- Failure to meet maintenance/renewal requirements

- Failure to manage complaints

- Formal renunciation of the certificate

Suspension procedures:

- Notification of reasons, revocation conditions, and timelines.

Maximum duration of suspension: 6 months

In the absence of corrective actions: revocation

Effects of suspension:

- Use of the certificate and trademark is prohibited

- Obligation to inform clients if the certificate is decisive

- In case of violation: immediate revocation

Revocation of the certificate:

- Communicated to the Accreditation Body (for accredited registers) and published on Autenticert's website

- No refund of payments made or due

- Possibility of a new certification application after 3 months (resolution of causes)

Suspension of certificate upon request:

- Up to 1 year in case of voluntary interruption of activity

- Resumption of activity: communication and new examination

The evaluation result is communicated in writing by Autenticert.