REGULATIONS REGARDING THE ISSUE AND MAINTENANCE OF MANAGEMENT SYSTEM CERTIFICATION (REG 01)

ATTACHMENT 3 – ADDITIONAL PROVISIONS FOR THE ISSUE AND MAINTENANCE OF CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS) ACCORDING TO UNI CEI ISO/IEC 27001:2017 STANDARD.

This document integrates, for the indicated specific sections, the Regulations regarding the issue and maintenance of the certification (REG 01).
In the event of ambiguous instructions these Regulations shall prevail and in the event of further doubts reference shall be made to UNI CEI ISO/IEC 27001:2017 reference standard.

2. SCOPE AND AREA OF APPLICABILITY
These Regulations define the relationships between CERTIQUALITY SRL - hereinafter referred to as the Institute - and the Organizations that intend to achieve and have registered the Certification of their Information Security Management System according to ISO/IEC 27001 reference Standard.
The enforcement of these Regulations is supervised by the Committee for Safeguarding Impartiality, appointed by the Institute's Board of Directors, which include members from all parties interested in Certification.

The CERTIQUALITY Certificate is the document whereby the Institute certifies that the requesting Organization employs a Management System complying with the reference standard.
The certification can be issued for the whole information system of the company or for specific areas and applications having a particular criticality.
The certificate always contains the applicable version of the Statement of Applicability.

3. DEFINITIONS
For the specific terms concerning information security management systems, the definitions provided in UNI CEI ISO/IEC 27001:2017 reference standard and ISO/IEC 27006:2015 standard shall apply.

4. GENERAL CONDITIONS
4.2 For the Certification procedure to be started by the Institute, the requesting Organisation shall:
- document and implement a management system that complies with the UNI CEI ISO/IEC 27001:2017 Standard with any specific prescriptions defined for given types of process/service;
- have carried out at least one senior management review and one internal audit on the ISMS covering the certification scope,
- accept the rules set forth by these Regulations and the conditions communicated by the Institute.

4.4 The Certification exclusively concerns the compliance of the management systems with the ISO/IEC 27001 Standard; the abidance by the laws in force is the exclusive responsibility of the certificated Organization.

5. PROCEDURE FOR THE CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEM
5.1 Request of Certification offer/Certification application and acceptance of the offer.
Those organizations wishing to obtain certification shall request a Certification offer to the Institute by filling an application form in its entirety and then sending it with the required documentation.

The offer by the Institute includes the examination of the submitted documentation, with a verification of the completeness and accuracy of general information and on-site verifications depending on the characteristics and complexity of the information system which is the subject of the ISMS (*Information Security Management System*).
The acceptance of the offer finalizes the contractual relationship between the parties and it involves also the acceptance of the provisions set out in the reference standard as well as in these Regulations, and subsequent modifications, available on the website: www.certiquality.it

5.2 Certification issue
5.2.1 Following the acceptance of the offer, the Institute agrees with the Organisation the period for conducting the audit. Acceptance of the contract does not constitute either a direct or an indirect obligation to certify by Certiquality.
Before the audit the Organisation shall inform the Institute or the auditor appointed for the audit if it deems that one or more documents of the ISMS cannot be made available for the audit. The Institute evaluates whether if it is possible to conduct a full audit to the reference standard also in the absence of such documents. In these cases the certification scope will only include the audited processes.
The initial certification audit is conducted in two stages:
- stage 1, at the Organisation's premises, is aimed at understanding the structure of the ISMS system, assessing the risks and treatments (determined controls included) as well as the Organisation's degree of preparation for the execution of stage 2.
- stage 2, at the Organisation's premises, is aimed at assessing the implementation and effectiveness of the ISMS system.

5.2.2 Before the Stage 1 audit the Organisation shall:
- make the general information related to the ISMS and area of applicability as well as the documentation required by the ISMS available to the auditor of the Institute,
- indicate to the auditor any needs for which the documental assessment shall be carried out in a place different than the site which is the subject of the certification.

5.2.4 At the end of Stage 1, the audit team sets the dates for stage 2.

No more than three months may pass between stage 1 and stage 2; after this period, the Stage 1 audit must be repeated.

Certiquality evaluates exceptional cases where there are conditions to maintain the results of Stage 1 valid.

During Stage 1 the audit team carries out an examination of the documentation of the ISMS of the Organization, that shall be constituted by the following documents:

a) documented statements about the policy and objectives of the ISMS;
b) area of applicability of the ISMS;
c) procedures and controls supporting ISMS;
d) description of the risk assessment method;
e) risk assessment report;
f) risk handling plan;
g) documented procedures necessary for the Organisation to ensure the effective planning, operation and control of its information security processes and to describe how to measure the effectiveness of controls;
h) the records required by the ISO/IEC 27001;
i) Statement of Applicability.

Stage 2 audit is aimed at:

- confirming that the Organisation works in accordance with its procedures and objectives:
- Confirming that the ISMS complies with the requirements of the UNI CEI ISO/IEC 27001:2017 standard.

During stage 2 the Organisation shall demonstrate that the ISMS set out is relevant and adequate to the activity of the Organisation and to the identified threats, vulnerability and impacts.

During the audit the Organisation shall also demonstrate to have a management system able to ensure compliance with the laws and regulations applicable to information security.

In exceptional cases Stage 1 and Stage 2 can be carried out consecutively. At the end of the first part of audit the auditor, on the basis of the evidences collected, confirms if the audit can continue with the second stage or not.

5.2.8 Multi-site companies

Certiquality can apply the sampling system of sites if the company meets the following requisites:

- all the sites work within the same ISMS, centrally administered and verified, that is subject to a review by the central Senior Management;
- all the sites are included in the internal audit plan of the internal ISMS;
- all the sites are included in the Senior Management review plan.

External sites – Temporary sites

In case of activities undertaken in a continual way and with specific personnel at sites "external" to the Organisation, the time for the on-site audit of a sample of these "worksites" shall be scheduled.

Furthermore the company shall declare if there are other temporary sites, that is sites not listed in the certificate where for a set period of time the activities included in the certificate subject are carried out.

The need for verifying these sites and therefore extending the sampling shall be assessed and reasons recorded within the calculation of the audit duration.

The assessment includes the risk that a non-conformity originated in a temporary site may cause a lack in the ISMS of the company.

6. VALIDITY OF THE MANAGEMENT SYSTEMS CERTIFICATION

The Certification issued by CERTIQUALITY is subject to periodical surveillance, to be carried out at least at an annual frequency, as well as to the full review of the Management System to be carried out every three years. The certificate issued shows the 3-year expiration date.

7. RIGHTS AND DUTIES OF THE CERTIFIED ORGANISATION

7.3 The certified Organisation shall inform Certiquality of any modification made to the *"Statement of Applicability*" document.

8. CERTIFICATION SUSPENSION

9. CERTIFICATION REVOCATION

10. WAIVER TO THE CERTIFICATION

11. CONFIDENTIALITY

12. FINANCIAL CONDITIONS

13. LIABILITY

14. APPEALS

15. DISPUTES

16. COMPLAINTS