ADDITIONAL RULES FOR THE CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS

Original Copy

Revision Register:

Date	Edit.	Rev.	Edit for	Issued	Approved
01/08/2016	1	0	First emission	QM	ADM
14/11/2016	1	1	Integration	QM	ADM
06/08/2018	1	2	Updating standard	QM	ADM
23/05/2019	1	3	Updating reference standard	QM	ADM
29/03/2021	1	4	Updating reference standard	QM	ADM
09/01/2023	1	5	Updating ISO 27001:2022	QM	ADM
03/06/2024	2	0	Integration Requirements ISO 27001:2022	QM	ADM

Distribution	*Signature:*
☑ Verified copy	
☐ Unverified copy	

1. GENERAL

The present Rules define the additional procedures, not as substitute, applied by QS for certification of information security management systems in comparison to what is already defined in the QS General Rules for the certification of Management Systems, last version in force.

QS issues the certification in accordance with requirements of standard ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/AMD 2020 to Organizations whose Management System has been recognized in accordance with the requirements ISO/IEC 27001:~~2013~~ 2022.

In addition, upon request, QS can carry out conformity assessments of a Information Security Management System according to other normative documents of reference and, if appropriate, issue the certification (ISO/IEC 27002, ISO/IEC 27010, ISO 22301:2012).

In addition; ISO/IEC 27001:2022/Amd 1:2024, requires organisations to actively assess and address the implications of climate change in their operations and strategic planning.

For such cases should also be considered any specific regulations/guidelines of QS.

1.1 TERMS AND DEFINITIONS:

For the specific terminology concerning information security management systems QS generally apply terms defined in Standards ISO/IEC ~~27001:2013~~ 27001:2022, ISO/IEC 27006:2015/AMD 2020 and ISO/IEC 27000:2018

1.2 ACRONYMS:

- ISMS : Information Security Management System

- SoA (Statement of Applicability) equivalente a Dichiarazione di Applicabilità (DdA)

2. REFERENCE STANDARD/REQUIREMENTS FOR CERTIFICATION

To get certification by QS, a ISMS meet initially and over time the requirements of ISO 27001 last version in force and the additional ones required by Accreditation Bodies.

The applicable regulations as reference for ISMS, in addition to the basic standards already defined in the QS general rules and QS Manual, are:
- ISO/IEC 27000:2018 —Information technology - Security techniques - Information security management systems - Overview and vocabulary
- ISO/IEC 27001:2013/Cor2:2015 "Information technology - Information technology – Security techniques – information security management systems - Requirements"
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection -- information security management systems -- Requirements
- Guidelines ISO/IEC 27002:~~2013~~ 2022—Information technology- Security techniques – Code of practice for information security controls",
- Guidelines ISO/IEC 27003:2017 - Information technology -- Security techniques -- Information security management systems -- Guidance
- ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
- Guidelines ISO/IEC 27005:~~2018~~ 2022—Information Information security, cybersecurity and privacy protection — Guidance on managing information security risks
-ISO/IEC 27006:2015/AMD 2020 Information Technology - Security techniques - Requirements for bodies
-ISO/IEC 27007:~~2017~~ 2020 providing audit and certification of information security management systems Information technology -- Security techniques -- Guidelines for information security management systems auditing
- ISO/IEC 27017:2015 Information technology -- Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 Information technology -- Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

The system is intended fully operational when, in addition to the provisions of the QS General rules for the certification of management systems, have been undertaken actions that give guarantee to apply an appropriate process of assessment and treatment of risks that produces consistent results, valid and comparable of confidentiality, integrity and availability of information covered by the scope of the ISMS and coherently with the company context.

3. CERTIFICATION PROCEDURE

In addition to what is established by point 10 of the QS General Rules, together with the certification application form, or immediately later, the Organization shall provide the following documentation to QS:

- General information about ISMS and scope application/associated risks;
- SoA - Statement of Applicability (QS reserves during the audit to assess the appropriateness of the controls applied by the Organization).
- the main characteristics and applicable regulations of the provided products/services for the correct application of information security

The above documents are evaluated by QS for the conformity with the reference standard and with the requirements of these Rules

To start the certification procedure, the company shall:

- have an operating management system in accordance with ISO/IEC ~~27001:2013~~ 27001:2022 at any particular requirements established for types of process/service;
- describe this system in specific documented information
- have made at least one cycle of internal audits and one management review that covers the purpose of ISMS Certification

During of the certification process, the organization shall keep in consideration the following particular provisions and requirements:

The standard lists in sections from 4 to 10 (included) a series of mandatory requirements for ISMS, which cannot be subject to exclusion therefore.

Furthermore in Appendix A of the standard (dedicated to controls and to related control objectives) it lists the possible controls to be applied in the context of the specific ISMS, depending upon the results of the risk assessment and treatment processes;

Therefore the controls described in Appendix A, are not required for all systems, but they shall be selected by the organization responsible for the ISMS using documented criteria that show that the company is aware about their real needs and risks (according their own context); thus the controls deemed truly necessary and thus "mandatory" in the context of the specific ISMS are identified by the Organization at SoA document, where shall be indicated and justified any exclusion.

In addition to what is established in the QS General Rules, the company shall comunicate to QS:

- any confidential or particular information that may not be available during the inspection being not authorized to communicate them to third parties (es. mandatory law). (QS reserves the right to assess whether the system can be verified properly even without the availability of such data. If QS will consider that this situation may affect the effiency of the audit, QS will try to reach an agreement with the Organization; If the agreement will be not reached, the certification process cannot be started. Such an agreement may consist in the fact that the Organization authorize the audit team to access information, confidential or sensitive data, only for the time of the audit and in accordance with specified arrangements)
- any need based on the context and company operating procedures, which some processes/requirements shall be examined through network-assisted auditing techniques (eg. remote access to documented information, web-based interactive communications, teleconferencing, etc.). Using these techniques must be agreed during the audit planning. QS

reserves the right not to use such audit techniques in the case that found that may put at risk the efficiency and effectiveness of the audit as well as the integrity of the audit process.

The cost of certification activity is proportional to the number of man-days (m/d) necessary to the evaluation of the ISMS and the level of complexity/criticality/risks, sites etc, with reference to Annex ISO/IEC 27006 document last version in force.

The total number of persons doing work under the organization's control for all shifts within the scope of the certification is starting point for determination of audit time.

The planning of audits will be decided in consultation with the organization taking into consideration the most appropriate time to verify better the certification scope (according sites, seasons, months, days shifts etc)

3.1 OUTSOURCING AND TEMPORARY SITES

Ove l'Organizzazione abbia deciso di allocare dei processi che impattano sulla sicurezza delle informazioni all'esterno della stessa Organizzazione, le attività di Audit potranno essere estese presso tali outsourcer, al fine di verificare l'efficacia dell'ISMS anche presso tali Organizzazioni.

If the organization has decided to allocate processes that impact on the security of information outside the Organization itself, the audits will be extended at those outsourcers, in order to verify the effectiveness of the ISMS at these organisations

The audits at suppliers of the organization can take place within the initial Audit and/or at the periodic maintenance surveillance audits.

The choice of conducting such audits will depend on the influence of outsourcing on the information security management System, whose relevance will be dictated by the analysis and risk evaluation and assessments of the Lead Auditor.

The ownership of the effectiveness of the management information system will remain in the organization. The unavailability of such suppliers to be audited, will void the possibility to certify the applicant organization.

3.1.2 SHARED SITES / CO-WORKING SITES

n the event that the organization shares its site and infrastructure management with other entities/organization, it:

- shall identified in the purpose of the ISMS this situation and consider it as part of the evaluation and treatment of risks;

- shall have identified their interfaces to manage the site and infrastructure with other identities;

- shall demonstrate to apply an appropriate level of control, on the site and on infrastructures, also in order to improve.

3.2 CERTIFICATION: INITIAL AUDIT STAGE 1

The Stage 1 audits must be conducted entirely at the client organization.

Beyond what is specified in section 10.6 of the QS General RULES, the additional audit objectives of Stage 1 are:

- obtain a sufficient understanding of the implementation of the ISMS in the Organization context (internal and external context), of the risk assessment of the security of information and the planning and control of risk (treatment)

- verify the completeness and conformity of the documentation of ISMS, politics and objectives of information security.

Among the documents specified in the standard, in particular is required the definition of the scope and limitations, ISMS documented informations of objectives and the policy, documents related to evaluation and treatment and risk methodology (and related procedures and controls supporting

the ISMS), the Statement of Applicability, and documented procedures necessary for the Organization to ensure the effective planning , operation and control of their information security processes and to describe how to measure the effectiveness of controls.

In the above documents shall be clearly shows the scope of the ISMS and the latter's physical boundaries (sites of the organization included in the ISMS) and logical (systems and users covered by the ISMS albeit physically not in the sites).

The audit team shall verify the customer's defined the scope of the ISMS Certification observes all applicable certification requirements. The purpose of the ISMS shall meet the requirements of ISO/IEC 27001 point 4.3.

The audit team shall examine that information security risk assessment and risk treatment properly reflect the activity of the client and extend the limits of its activities, as defined in the scope of certification. The audit team should confirm that this is reflected in the ISMS in the statement of applicability.

The audit team should ensure that interfaces with services or activities that are not fully under the management system are addressed within the management systems and are included in the client's information security risk assessment. (example: sharing facilities such as computer systems, databases and communication systems or outsourcing of business function with other organization)

The result of the examination of the documentation is shown, together with the findings of the initial visit, in a separate report, issued at the conclusion of the audit. Any deficiencies and gaps in the documentation can disrupt the process, in the opinion of the audit team, until their resolution.

After the audit QS sends a report identifying company gaps, or, in case of positive assessment, it suggests continuing certification activities. Resolved these gaps, the audit team plan the audit stage 2, communicating to the Organization the audit plan, with details of the sites and process etc. to assess.

The results of stage 1 audit will be sent to QS by the audit team. QS, by its technical managers that have not partecipated to the audit, will review the audit documentation of Stage 1 before deciding on proceeding with Stage 2 and after this evaluation will decide if the audit team members have the necessary compentence to continue the Stage 2 or if to change one or all the memebr of the audit team.

3.2 CERTIFICATION: INITIAL AUDIT STAGE 2

In addition to the provisions of the QS General Rules last version in force, the audit team should ensure the effective implementation of the ISMS confirming that the customer comply and apply effectively their policy, objectives, and procedures; that the client evaluate, adequately to the certification scope, risks related to information security.

The audit team has infact the objectives to verify:

- leadership commitment for the implementation and application of appropriate policies and objectives for information security considering the purpose of their certification scope and the associated risks (the effectiveness and the address given by the leadership to ISMS shall be traceable also in the programs, procedures, internal audits, recordings and management reviews)
- that the Statement of Applicability (SoA) and the ISMS documentation ISMS is appropriate to the company reality and to the requirements of the standard
- taht the analysis of security threats is adapted to the Organization's processes and produces valid and comparable results
- that the organization has established adequate and proper procedures for the identification, analysis, evaluation and treatment of risks to information security, and that the application of the operating controls is congruent with the policy, objectives and targets defined by the organisation itself;
- measurements of effectiveness of controls is consistent and matching to SoA and the results obtained by the process treatment risks are comparable to the security policy and objectives

- that performance of ISMS is effective with respect to objectives, namely that the ISMS set is relevant and appropriate with respect to the Organization's activities and threats, vulnerabilities and impacts identified.

3.3 SURVEILLANCE AUDIT

The certified organization is required to communicate to QS Quality Services any changes to the document SoA ("*Statement of Applicability").*

The purpose of surveillance audit is:
to ensure that the approved management system continues to be implemented, to consider the implications of changes to the system as a result of changes applied by the customer and to confirm continuos compliance with the certification requirements.

Each surveillance audit is related to elements of the ISMS: it always includes, in principle, certain fixed elements of the ISMS according to norm (sections 4 to 10 and paragraph A. 18) plus additional elements according the specific context/situation of the company.
In addition to the provisions of the QS General Rules last version in force, the audit team should verify as minimum requirements:
- updates of documented information (eg. SoA) and system modifications from the previous assessme
- the maintenance of system elements such as evaluation and risk control, performing a management review and internal audit
- maintaining the certification scope, internal and external communicatio
- the effectiveness of the ISMS with regard to achieving the objectives of the common security of customer information
- the effectiveness of the ISMS with regard to achieving the objectives of the information security policy
- the effectiveness and operation of the procedures for the periodic assessment and review of compliance with legislation and regulations information security
- any change of controls and any change in results in SoA
- implementation and effectiveness of the controls according to the audit program
- records of any complaints or requests between the certification/recertification and subsequent surveillance audit, non-conformities found by the customer on your ISMS and their corrective actions
- registrations of any claims or requests that occurred between the certification/re-certification and the subsequent verification of surveillance, non-conformity detected by the customer on their ISMS and corrective actions
- any changes to other areas of the system

Each of the surveillance audits is related to parts of the ISMS: It always includes, in principle, some fixed elements of the ISMS according to the norm (sections 4 to 10 and paragraph A. 18) plus further elements; However, in the case of any "additional" surveillance audits, the fixed items cited may not be subject to verification by the audit team; However altogether the surveillance audits of the three-year period cover at least once the entire ISMS.

4. INTEGRATED AUDITS

QS admits carrying out audits about ISMS integrated with other management systems (quality, safety, or environment) as long as the Information security system is clearly identified and it meets every requirement of the reference standard. Companies wishing to combine their IS management system with existing management system (e.g. quality system) can benefit from a coordinated assessment program. For the requirements of application and calculation of combined audit, please refer to the QS General Rules.

5. CERTIFICATION OF "MULTI-SITE" ORGANIZATION

The multi-site sampling approach is considered possible, where organizations that require it operates in different sites but with similar processes and activities under the supervision and coordination of a central entity.

In addition to that specified in the QS General Rules, QS specifies that the multisite sampling is applicable only under the following conditions:
a) all sites with similar processes
b) all sites operate under one centralized and verified information security management system;
c) all sites are included in the ISMS internal audits and management reviews schedules leadership.
d) at least one internal audit was conducted on all sites during two years prior to certification;
e) shall be individuated all the complexity of the information systems at each site and the treatment
f) internal audits of all sites must be in accordance with ISO/IEC 27001;
g) the findings emerged from the audits of individual sites should be considered indicative of the whole system must be implemented the fix accordingly

Sampling shall always provide for the assessment of the effectiveness of security controls and responsibilities of leadership the main operative headquarter, plus a sample of sites allowing, in a reasonable period and in any case before recertification, coverage of the entire organization.

After certification, an internal audit shall be performed at each site during the three-year period of certification;

The non-conformities found in various sites during the audits, will be subject to a process of improvement applied to all sites of the organization.
The possible persistence of noncompliance, involves the withdrawal of certification to the entire organization, not only at the individual site audited.

6. CERTIFICATION DOCUMENT

The certification documents may reference national and international standards as source(s) of control set for controls that are determined as necessary in the organization's Statement of Applicability in accordance with ISO/IEC 27006:2015/AMD 2020 6.1.3.
The reference of certification documents shall be clearly stated as being only a control set source for controls applied in the Statement of Applicability (SoA) and not a certification thereof.

7. TRANSITION PROCESS to the edition ISO 27001:2022

As dictated by IAF MD 26:2022 'Transition requirements for ISO/IEC 27001:2022', it is expected:

- **FOR INITIAL CERTIFICATIONS**: as of 1 November 2023, companies will only be able to apply to be certified in accordance with the new ISO/IEC 27001:2022 (i.e. initial certifications in accordance with ISO/IEC 27001:2013 are permitted until 31 October 2023)

- **FOR EXISTING CERTIFICATIONS**: organizations already certified before October 2023 in accordance with ISO/IEC 27001:2013 (or UNI ISO/IEC 27001:2017) will have until 31 October 2025 to complete the transition to the new 2022 edition.

All certifications in accordance with ISO/IEC 27001:2013 will expire/will be revoked at the end of the transition period (31 October 2025).

MODALITY

IAF MD 26 allows transitional audits to be carried out during an already scheduled surveillance or re-certification audit or during an audit additional to the normal certification cycle.

The transition audit may not be documentary, but must include a field review of the new or modified technological controls applied by the organization. However, remote audits are generally permitted if they ensure the achievement of audit objectives.

The transition audit should include at least the following:

- verification of compliance with the 2013 edition (possible closure of findings from previous audits)

- gap analysis of ISO/IEC 27001:2022, as well as the need for changes to the client's ISMS;

- updating the Statement of applicability (SoA);

- staff competence and awareness

- updating the risk treatment plan;

- the implementation and effectiveness of new or modified controls chosen by the client according to its context.

TRANSITION AUDIT DURATION

Also according to IAF MD 26, the transition audit will have to be a minimum of 0.5 man-days in addition to the previously accepted offer, when the transition is carried out during a surveillance audit or as a separate audit. The increase of this audit time will however depend on the size of the company and risk of the activities. QS will issue a revised offer for the transition audit.

It is specified that when the certification document is updated because the client has only successfully completed the transition audit, the deadline of its current certification cycle will not be changed.