CONTENTS

1.	**Purpose and effective date**	**2**
2.	**Scope**	**2**
3.	**Terms and definitions**	**2**
4.	**Responsibility**	**3**
5.	**Control of the regulation**	**3**
6.	**Certification procedure**	**3**
6.1	**General information**	**3**
6.2	**Audit procedure and audit programme**	**4**
6.3	**Start of the certification procedure**	**4**
6.4	**Pre-audit**	**4**
6.5	**Stage 1 audit (Initial review of documentation + initial audit)**	**4**
6.6	**Stage 2 audit (for an initial audit of the management system or certification audit)**	**5**
6.7	**First issue of certification and renewals**	**6**
6.8	**Surveillance audit**	**6**
6.9	**Renewal audit**	**7**
6.10	**Special audits or unscheduled audits or a reduction in the scope of certification**	**7**
6.10.1	**Reduction in the scope of certification (if any)**	**7**
7.	**Register of certified organisations**	**7**
8.	**Referencing the certification Use of the certificate and mark**	**7**
9.	**Suspension of certification**	**7**
10.	**Withdrawal/cancellation of certification**	**7**
11.	**Complaints handling and management of disclosures from customer organisations and interested parties**	**7**
12.	**Documentation or documented information of the management system and and accessibility for TÜV Italia srl audits**	**8**
13.	**Changes to the management system**	**8**
14.	**Changes to the certification system rules**	**8**
15.	**Special requirements for organisations already certified by another body**	**8**
16.	**Confidentiality**	**8**
17.	**Appeals**	**8**
18.	**Complaints against TÜV Italia**	**8**
19.	**Disputes**	**8**
20.	**Financial conditions**	**8**

Description of changes	*Reference to the Technical Regulation RT-37 rev.01 "Requirements for accreditation with the purpose of flexible accreditation, Department of Certification and Audit Bodies". ISO/IEC 27701 extension reference and ISO/IEC 27006:2015/Amd 1:2020*

	Department	**Date**	**Name**	**Signature**
Prepared by:	CTSSI	2021-06-21	Antonio Bagiolini	*Document unsigned, as approved by the TÜV Italia srl digital management system*
Checked by:	T&QM	2021-06-25	Stefano Parini	
Checked by:	RQA	2021-06-25	Luca Boniardi	
Approved by:	MDBA	2021-06-25	Andrea Coscia	

1. Purpose and effective date

The purpose of this document is to supplement the General Regulation for the Certification of Management Systems (RGSG) adopted by TÜV Italia s.r.l. (TÜV Italia), for the specific purposes of certifying Information Security Management Systems (ISMS).
This regulation will come into effect on the date indicated in the heading.

2. Scope

This regulation applies to activities to certify information security management systems (ISMS), carried out under ACCREDIA accreditation, according to the international standard ISO/IEC 27001, and to guidelines referable to the standard, within the context of SSI flexible accreditation.
It does not prejudice the application of any other regulations on additional certification schemes for which the organisation may be certified by TÜV Italia and/or by other Certification Bodies.
The following are applicable reference standards for ISMS certification:

- ISO/IEC 27001:2013 “Information technology – Security techniques – information security management systems - Requirements”, or the Italian version UNI CEI EN ISO/IEC 27001:2017, considered herein as equivalent, in terms of the description of requirements, and identified as "the Standard".
- ISO/IEC 27006:2015 “Information Technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems”
- Norma ISO/IEC 27006:2015+ISO/IEC 27006:2015/Amd 1:2020 “Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems — Amendment 1”
- UNI CEI EN ISO/IEC 17021-1:2015 ”Conformity assessment - Requirements for bodies providing audit and certification of management systems”
- ISO/IEC 27002:2013 “Information technology- Security techniques – Code of practice for information security controls”, or its Italian version UNI CEI EN ISO/IEC 27002:2017.
- 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”.
- Norma ISO/IEC/ 27701:2019 “Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines”

The following documents issued by the certification body ACCREDIA, available at www.accredia.it are also a mandatory reference for accreditation:

- Regulation on the accreditation of Certification and Audit Bodies RG-01
- Regulation on the accreditation of management system Certification Bodies RG-01-01
- Technical Regulation RT-37 rev.01 “Requirements for accreditation with the scope of flexible accreditation, Department of Certification and Audit Bodies”
- Circular no. 02/2018 “Information on accreditation for the ISO/IEC 27001:2013 certification scheme, with supplementation of ISO/IEC 270XX:20YY “Information Technology, Security techniques, Code of practice”
- Circular no. 01/2019 “Accreditation of the ISO/IEC 27001:2013 certification scheme, with the supplementation of ISO/IEC 27017:2015 and ISO/IEC 27018:2014 - Information Technology, Security techniques, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”
- Circolare n.10/2019 “Provisions about ISO/IEC 27701 accreditation”
- Other Provisions and Regulations on accreditation
- For specific information about activities carried out under ACCREDIA accreditation, see www.accredia.it or www.tuv.it, to view the accreditation certificate with related attachments.

3. Terms and definitions

The terminology used in these regulations corresponds to the following standards:

- ISO/IEC 27000:2018 “Information technology - Security techniques - Information security management systems - Overview and vocabulary”.
- UNI EN ISO 9000:2015 "Quality management systems - Fundamentals and vocabulary";
- UNI CEI EN 45020:2007: "Standardization and related activities - General vocabulary".

- UNI CEI EN ISO/IEC 17000:2005 “Conformity assessment - Vocabulary and general principles”

The following acronyms are used in this regulation, in particular:
- ISMS (Information Security Management System)
- SoA (Statement of Applicability)

For the definitions:

- Deficiency (CA)
- Nonconformity (NC)
- Observation (OBS)
- Comment (COM)

see the RGSG.

4. Responsibility

The contents of section 4 of the RGSG will apply.

5. Control of the regulation

These rules are available to interested parties at https://www.tuvsud.com/it-it . Organisations can request a copy in printed or digital format.
The contents of section 5 of the RGSG will also apply.

6. Certification procedure

6.1 General information

The contents of section 6.1 of the RGSG will apply, with the following additions:

- In sections 4 and 10, the Standard includes a number of mandatory requirements for ISMS, that cannot be excluded.
- Appendix A (standard)" (on controls and related control objectives, called "Annex A" in the original version of the standard), lists the possible controls to adopt for the specific ISMS, based on the results of risk assessment and treatment processes; therefore the controls described in "Appendix A" are not all mandatory for the ISMS, but are selected by the organisation responsible for the ISMS using documented criteria that take into account its actual needs; the controls actually considered necessary and which are therefore "mandatory" for the specific ISMS are identified by the organisation in the SoA, where any exclusions must be indicated and justified.
- Based on the above, TÜV Italia, as a certification body for ISMS, assesses the documentation and implementation of all requirements of sections 4 to 10 (included), as well as the controls in "Appendix A", which the organisation declared applicable in the SoA; TÜV Italia may assess the adequacy of the organisation's choices.
- In conducting its audits, TÜV Italia also examines the existence and consistency of connections among various parts of the ISMS, such as: the policy, risk assessment results, general and specific objectives, risk treatment strategies, responsibilities, programmes. procedures, internal security reviews, etc.
- Regarding compliance with statutory requirements (legal provisions, regulations, directives, etc.), the general principle is that the maintenance and assessment of conformity to these statutory requirements falls under the responsibility of the organisation managing the ISMS; TÜV Italia merely carries out random checks to obtain assurance that the ISMS is effective from this point of view and that – in the case of any nonconformity regarding the statutory requirements – the organisation will take appropriate corrective actions.
- The organisation may manage information networks that are under the control of a single ISMS but are in different geographical areas or at multiple sites. In this situation, TÜV Italia may issue a single certificate, but may decide to audit each site or sample some sites and only audit those sites (TÜV Italia takes this decision based on specific requirements and recommendations in the current editions of ISO/IEC 27006 and ISO/IEC 17021-1, and in the Regulations issued by ACCREDIA).
- Certification according to ISO/IEC 27001 may be supplemented by ISO/IEC 27017 and ISO/IEC 27018, on request of the Organisation, if the scope of the management system includes the provision of cloud services, and if personal data are processed according to this procedure. In this case, the certification may be supplemented by ISO/IEC 27017 alone, or in conjunction with ISO/IEC 27018, but may not be supplemented by ISO/IEC 27018 alone.
- Certification according to ISO/IEC 27001 can also be supplemented by ISO/IEC 27701, extending the scope to the latter to the perimeter of Privacy Management [Privacy Information Management System]. The standard, being an extension of ISO/IEC 27001, must take into account the ISO/IEC 27002. Therefore, the application of ISO/IEC 27701 cannot stand alone, but must be based on the application of the above standards.

- In particular, the supplemented procedure may be carried out both for new certification, and in the case of ISO/IEC 27001 certification already in effect, provided it has been issued by TÜV Italia (otherwise, prior transfer to TÜV Italia is requested).

6.2 Audit procedure and audit programme

The contents of section 6.2 of the RGSG will apply, with the following additions:

When applying for certification, the organisation is required to notify whether it intends opting to not give the audit team access to documents containing information considered confidential or sensitive (for example information on personnel, customers, suppliers, intellectual property, national security); in this case, TÜV Italia will assess whether the information it can access is sufficient for the purposes of assessing the ISMS; if the information is not sufficient, the organisation and TÜV Italia must reach - where possible - an agreement on procedures to access all information which is essential for assessing the ISMS; if an agreement cannot be reached, the certification procedure cannot be started. This agreement may entail the organisation authorising the audit team to access confidential or sensitive information only for the time of the audit, and according to procedures that have been agreed on.

In the event of multiple management systems (referred to more than one certifiable standard), the audit may be conducted for the issue of certification, provided that all requirements of the reference standard for the ISMS have been met, and moreover, all documented information is available, conforming to the above requirements, and the interfaces with the other management systems have been identified.

6.3 Start of the certification procedure

The contents of section 6.3 of the RGSG will apply, with the following additions:

The audit duration, whether involving a single site or several sites that come under the scope of the ISMS, will be determined by TÜV Italia based on the requirements of the current edition of ISO/IEC 27006.
For multisite and integrated audits, reference is made to the documents IAF MD 1 and IAF MD 11 respectively.
In the case of audits whose criteria are extended to the codes of practice included in the scope of flexible accreditation (e.g. ISO/IEC 27017 and/or ISO /IEC 27018, and/or 27701), the audit duration will be determined also based on relevant Accredia Provisions.

6.4 Pre-audit

The contents of section 6.4 of the RGSG will apply.

6.5 Stage 1 audit - (Initial review of documentation + initial audit)

The contents of section 6.5 of the RGSG will apply, with the following additions: The stage 1

audit will be conducted entirely at the Organisation.

a) Control of ISMS documentation (1st phase of stage 1)
ISMS documentation is always controlled, with limitations, if any, due to reasons of confidentiality indicated in section 6.2.
ISMS documentation means:

- the documents referred to in the Standard with the term "documented information"
- the list of statutory requirements applicable to the ISMS is included in the stage 1 report (RI02). The signature on the stage 1 report provides evidence of the Organisation's written declaration of conformity to these requirements.

The documents referred to in the standard include, in particular, documents on the risk assessment and treatment, the Statement of Applicability, and the policies and procedures for information security.
In addition, these documents must include a clear reference to the scope of the IMSI, as well as the physical "scope" (the organisation's sites included in the ISMS), and logical scope (the systems and equipment covered by the ISMS even if not physically present at the sites). Any interfaces / interactions with services or activities that are not fully included in the scope must be identified and included in the risk assessment (for example this might be the case for computers or telecommunication systems shared with other organisations).
The purpose of the documentation review is to establish, first and foremost, that documentation is complete, i.e. it meets all requirements of the Standard and this regulation; the documentation must also be clear, i.e. it must leave no doubt about its interpretation, all its parts must be consistent and it must be easily legible.

b) Initial audit (2nd phase of stage 1)

The initial audit will always be conducted and consists of an audit at the site (or sites) of the organisation.
It enables TÜV Italia to better understand:

- the size and characteristics of the organisation's ISMS;
- the extent of the organisation's suitability to undergo the certification procedure;
- the applicability of legal requirements and regulations on information security;
- the type of experience required of the team appointed to conduct the stage 2 audit;
- the number of people who will be needed for the stage 2 audit.

The initial audit will also enable the organisation to further review the following aspects (if not already solved for example during any pre-audits as indicated in section 6.4):

- details of the certification procedure;
- more specific planning of the times necessary to achieve certification;
- the exact definition of the scope of the ISMS;
- the identification of any deficiencies in the adoption of the ISMS.

To achieve these purposes, during the initial audit, the audit team will assess the extent to which the following fundamental points of the Standard have been met:

- the requirements of sections 4 to 10;
- the requirements of paragraph A.18.

For each of these requirements, the ISMS must have been implemented, and the corresponding records must be available.
The outcome of the documentation review must be indicated, together with the results of the initial audit, in a specific report, which will be issued after completion of the stage 1 audit. A copy of the report is also given to the organisation; if necessary, the report can be explained to the customer during a direct meeting held with the customer. If the implementation of the ISMS is defective, the customer will be informed in the report.
If the documentation review identifies any deficiencies (CA), the organisation must correct them before the stage 2 audit; if any deficiencies (CA) in the documentation still exist at the time of the stage 2 audit, the immediate issue of the certificate will be prevented, and a post-audit will be necessary.
TÜV Italia will review the stage 1 report to decide whether the conditions exist to proceed with the stage 2 audit, and to assess whether any specific expertise is required for the stage 2 audit team. If there are deviations from the information notified by the organisation, when making the offer, TÜV Italia may assess the need to change its price proposal.

6.6 Stage 2 audit (for an initial audit of the management system or certification audit)

The contents of section 6.6 of the RGSG will apply, with the following additions:

At the time of the stage 2 audit, the organisation's ISMS must be operative; in particular, the organisation must have defined objectives for information security that are measurable and - where applicable - quantified, it must have conducted a documented management review and a complete cycle of internal audits according to the requirements in section 9 of the Standard, and, lastly, it must comply with the requirements in sections 8 and 11 of this regulation.
The audit is conducted based on an audit plan designed to take account of the outcome of activities already carried out (stage 1 audit), giving importance to aspects of the ISMS that are most significant (the assessment of information security risks and related importance of results, the selection of control objectives and controls based on the risk assessment results, review of the effectiveness of the ISMS and measurement of the effectiveness of controls, adoption of controls, etc.); in general, the plan will include all the requirements of the applicable standard. However, it is possible for the plan to not include any requirements that were found to have been met in full during the stage 1 audit.
The organisation will be informed of the plan before the audit.
The purpose of the certification audit is to ensure that the ISMS has been put in place in accordance with relevant documentation (policy, procedures, instructions, SoA, legal requirements, any other statutory requirements, programmes, etc.), effectively, and that it meets the requirements of the reference standard.
The audit team also assesses whether:

- top management's leadership is committed and effective;
- the needs of parties concerned - including legal obligations - have been duly considered and inspire information security objectives;
- the analysis carried out on security risks is adequate for the organisation's processes;
- the organisation has established adequate procedures to identify, review and assess information security

risks, and whether the adoption of operating controls is consistent with the policy, objectives and targets defined by the organisation;
- documentation conforms to the standard;
- the measurement of the effectiveness of controls is consistent.

The purpose of the audit is also to ensure that interfaces with services or activities that are entirely or partially outside the scope of the ISMS have been considered and therefore included in the information security risk assessment.

In the case of certification extended to ISO/IEC 27017 and ISO/IEC 27108, certification may only be issued after an audit has been conducted at the organisation's site(s) concerned, and in particular all data centers where servers managing the cloud will be located, must be audited.
If the Data Centers used for cloud activities are outsourced with suppliers that have ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018 certification accredited and recognised at an MLA level, it is not necessary to add the audit time for these sites. In all other cases, the time must be added for the "De visu" audit of sites operating through outsourcing. In the case of sites where it is not possible to conduct a direct audit (e.g. suppliers such as AWS, AZURE), additional time shall be used at the central site to assess the contractual and operating controls concerning these suppliers. This last requirement is only applicable in the case of Data Centers with TIER III or TIER IV certification.

In the case of certification extended to ISO/IEC 27701, it will also be necessary to verify whether the organization periodically carries out periodically vulnerability assessment / penetration test, and the mode of execution.

The extension to ISO/IEC 27701 is not allowed for organizations that use services provided in "cloud" mode, without the support of ISO/IEC 27017:2015 and ISO/IEC 27018.

6.7 First issue of certification and renewals

The contents of section 6.7 of the RGSG will apply, with the following additions:

- The certificate will indicate the Statement of Applicability (SoA) with the date, edition and/or revision.
- Moreover, the certificate shall also be re-issued during the surveillance stage, indicating new references to the SoA, if the SoA indicates that the coverage of controls in Appendix A of the standard has changed.
- If certification is extended to the codes of practice included in TÜV Italia's SSI flexible accreditation scope (e.g. ISO/IEC 27017, ISO/IEC 27108 and 27701), reference must be made to these codes in the certificate.

6.8 Surveillance audit

The contents of section 6.8 of the RGSG will apply, with the following additions:

Each of the surveillance audits refers to parts of the ISMS: in general, the audit always includes some set parts of the ISMS according to the Standard (sections 4 to 10 and paragraph A.18) plus additional parts; however in the case of "additional" surveillance audits (see Section 6.10 of this document), the audit team may decide to not audit the set parts referred to above; however, in general, three-year surveillance audits cover the entire ISMS at least once.

At the time of this audit, the organisation's ISMS must provide evidence of the management review and a cycle of internal audits having been carried out at least annually, according to the requirements in section 9 of the Standard.
As a minimum requirement, besides indications in the RGSG, the surveillance audit reviews:
- the effectiveness of the ISMS in achieving the objectives established in the information security policy;
- the functioning of procedures for the periodic assessment of legal and regulatory conformity;
- the actions taken for nonconforming situations identified in the previous audit;
- any changes in the coverage of controls indicated in Appendix A of the standard, and consequent changes to the Statement of Applicability;
- the implementation and effectiveness of controls according to the audit programme;
- the handling of complaints made by parties concerned to TÜV Italia;

- the audit programme based on changes taking place (including context aspects, risks, legal aspects, requests or disclosures from parties concerned);
- appropriate use of the certificate.

6.9 Renewal audit

The contents of section 6.9 of the RGSG will apply.

At the time of this audit, the organisation's ISMS must provide evidence of the management review and a cycle of internal audits having been carried out according to the requirements in section 9 of the Standard.

6.10 Special audits or unscheduled audits or a reduction in the scope of certification

The contents of section 6.10 of the RGSG will apply.

6.10.1 Reduction in the scope of certification (if any)

TÜV Italia has the right to reduce the scope of the certification to exclude parties that do not meet requirements, if the organisation has failed, persistently or seriously, in meeting the certification requirements concerning parts of the scope of certification. This reduction will be consistent with the requirements of the standard used for the certification.

7. Register of certified organisations

The contents of section 7 of the RGSG will apply.

8. Referencing the certification. Use of the certificate and mark

The contents of section 8 of the RGSG will apply.
For management systems that are only certified in accordance with the Standard, the following mark will apply, subject to updates:

Note: in the case of additional certification of the management system obtained through TÜV Italia a specific mark may be sent - if available. This will also refer to the other schemes for which certification was obtained.

9. Suspension of certification

The contents of section 9 of the RGSG will apply.

10. Withdrawal/cancellation of the certification

The contents of section 10 of the RGSG will apply.

11. Complaints handling and management of disclosures from customer organisations and interested parties

The contents of section 11 of the RGSG will apply.
Moreover, the organisation shall specifically indicate in its complaints handling procedure, the procedures for:

- Any notices to the authorities, if required by regulations.
- Reassessment of the information security risk.
- Assessment of interactions with other parts of the ISMS.

12. Documentation, or documented information of the management system and accessibility for TÜV Italia srl audits

The contents of section 12 of the RGSG will apply.
If the information contained in system documentation and audit reports is such that it cannot be distributed in a controlled manner to TÜV Italia or to third parties, the organisation must formally notify TÜV Italia of the reasons why controlled distribution cannot take place.

13. Changes to the management system

The contents of section 13 of the RGSG will apply.

14. Changes to the certification system rules

The contents of section 14 of the RGSG will apply.

15. Special requirements for organisations already certified by another body

The contents of section 15 of the RGSG will apply.

16. Confidentiality

The contents of section 16 of the RGSG will apply.

17. Complaints (or Appeals)

The contents of section 17 of the RGSG will apply.

18. Complaints against TÜV Italia

The contents of section 18 of the RGSG will apply.

19. Disputes

The contents of section 19 of the RGSG will apply.

20. Financial conditions

The contents of section 20 of the RGSG will apply.