CONTENTS

Description of the revision	References to ISO/IEC 20000-1:2018 and its requirements (sections 2, 3, 6)

	Department	Date	Name	Signature
Prepared by:	CTSSI	2019-10-30	Danilo Diomede	*Document unsigned, as approved by the TÜV Italia srl digital management system*
Checked by:	BUM- RES	2019-10-30	Sara Brandimarti	
Checked by:	T&QM	2019-10-30	Stefano Parini	
Approved by:	RDBA	2019-10-30	Andrea Coscia	

1. Purpose and effective date of this document

The purpose of this document is to supplement the RGSG for the Certification of Management Systems (RGSG) adopted by TÜV Italia s.r.l. (TÜV Italia), for the specific purposes of certifying Information Technology - Security Management Systems (hereinafter “SMS”).
These rules will come into effect on the date indicated in the heading.

2. Field of application

These rules apply to the certification of service management systems carried out with ACCREDIA 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 standards and regulations are applicable to SMS:

- ISO/IEC 20000-1:2018 'Information Technology - Service Management - Part 1: Service management system requirement', identified hereafter as 'the Standard';
- ISO/IEC 20000-2:2019 'Information Technology - Service Management - Part 2: Guidance on the application of Service management systems”
- ISO/IEC 20000-3:2019 'Information Technology - Service Management - Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1”
- UNI CEI EN ISO/IEC 17021-1:2015 ”Conformity assessment - Requirements for bodies providing audit and certification of management systems”
- ISO/IEC 20000-6:2017 'Information Technology - Service Management - Part 6: Requirements for bodies providing audit and certification of service management systems”

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 Regulations and Circulars, if any

In order to have a specific feedback on activities carried out under ACCREDIA accreditation, it is possible to directly consult the website www.accredia.it or the website www.tuvsud.com/it, to view accreditation certificates with their attachments, related to sectors covered by the accreditation.

3. Terms and definitions

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

- ISO/IEC 20000-1:2018 “Information Technology – Service Management – Part 1: Service management system requirement” ;
- ISO/IEC TR 20000-10:2018 “Information Technology – Service Management – Part 10: Concepts 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 and industry terms are used in the text of these Special Rules:

- Service provider: Organisation or part of an organisation that manages and delivers one or more services to the customer. In the present edition of the Standard the definition has been retained, although it is entirely equivalent to "Organisation".
- the SLA (service level agreement): Documented agreement between the organisation/service provider and the customer, identifying the services and their agreed performance.
- Technical Area: Processes and services in the scope of the SMS

For the definition of:

- Deficiency (CA)

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

see the RGSG.

4. Responsibilities

The contents of section 4 of the RGSG will apply.

5. Control of the rules

The contents of section 5 of the RGSG will apply.

These special rules are available to interested parties at www.tuvsud.com/it, in the “Client Area” Section. Organisations may request a copy in printed or digital format.

6. Certification procedure

6.1 General information

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

- The term "Technical Area" refers to the SMS, including "service management" processes and services within its scope.
- The scope of certification shall be defined based on the document ISO/IEC TR 20000-3, which sets out the criteria, with particular reference to the supply chain and governance of services provided by third parties.
- The scope of certification shall specifically refer to the services provided or to the services catalogue. Similarly, TÜV Italia will indicate these references in its audit reports, so that the scope certification is always clear.
- In the case of contracts with critical suppliers, TÜV Italia will verify their control and monitoring methods through the examination of Quality Plans or other records. Only in exceptional cases - and in any case by prior agreement with the organisation - may it arrange for supplier audits to be conducted.
- Where the organisation/service provider adopts policies for the outsourcing of services included in the scope, TÜV Italia will consider only the organisation itself as responsible for compliance purposes, and not the outsourcer; the latter may be allocated responsibility for diligence in applying the policies contractually imposed by the organisation.
- In the case of a combined ISO 20000 / ISO 27001 audit, the process to manage *information security* of the SMS shall be audited to verify that:
  - The *information security* policy is appropriate to the SMS and the services;
  - *Information security* risks have been identified and controls are in place to support the SMS and services.

  The audit may benefit from evidence from the ISO 27001 management system, if the scope is the same as the SMS. Otherwise, evidence shall be produced in the context of the SMS.
- In the case of multi-site organisations, the audit programme will be determined based on sampling needs arising from the requirements of IAF MD 1:2018. The sampling method may be used if all sites:
  - Operate under the same, centrally managed SMS;
  - The sites are included in the internal audit programme
  - The sites are included in the management review programme.

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 and document 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 shall reach - where possible - an agreement on procedures to access all information which is essential for assessing the SMS; if an agreement cannot be reached, the certification procedure cannot be started. This agreement may consist of the organisation authorising the audit team to have access to confidential or sensitive information only for the time of the audit and in accordance with agreed procedures, or of sensitive information being examined by an intermediary with a competence recognised by TÜV Italia and independent of the audited organisation.
The audit objectives shall include verifying that interactions with subjects outside the scope of the management system are identified and under control. TÜV Italia shall also ascertain that the Organisation is aware of and able to manage the risks for the SMS and the services deriving from such interactions.
In terms of the accuracy of sampling processes and operational sites, the audit programme will take into account differences between:

- sites
- services
- clients
- any other parties
- languages
- possible shifts
- local versions of the management system
- regulatory requirements

A representative sample (see IAF MD 1) will be chosen based on the scope of the Management System, also taking into account the random element.
The audit programme shall cover the entire scope of the Management System over the three-year period.
The audit team shall have access to evidence of the identification of other parties involved in the provision of services how they are controlled based on the requirements of the Standard.
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 SMS have been met, and moreover, all documented information is identifiable in relation to the SMS, available, conforming to the above requirements, and the interfaces with other management systems have also been identified. The integrity of the SMS audit shall not be adversely affected by the combined audit.

6.3 Start of the certification procedure

The contents of section 6.3 of the RGSG will apply.

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:

Documentation review shall ascertain the presence of a management system containing the mandatory documents referred to in requirement 7.5.4 of ISO/IEC 20000-1:

a) the scope of the SMS
b) the policy and objectives for service management
c) the service management plan
d) change management" and "information security" policies, and service continuity plan(s)"
e) processes governed in the SMS
f) the requirements of the service(s)
g) the “services catalogue(s)”
h) the SLA (service level agreement)
i) Contracts with suppliers ("external supplier")
j) Agreements with internal suppliers or clients acting as suppliers

k) Procedures required by the Standard
l) Records needed to demonstrate conformity to the requirements of the Standard and the SMS

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:

TÜV Italia will sample all "technical areas" included in the scope.
It should be noted that the Audit Team will not enter into the technological merits of the services provided (e.g.: verification of computer codes), but instead will verify management and operational approaches, with essential reference to compliance with client contracts, in terms of requirements expressed by the client and their transformation into SLAs.

6.7 First issue of certification and renewals

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

TÜV Italia may list the services provided for respective clients as an attachment to the certificate, subject to the prior written consent of the parties concerned, also with regard to the method of publication of such attachments.

6.8 Surveillance audit

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

During surveillance audits, all technical areas shall be audited again, at least once. If changes to technical areas considered significant occur during the certificate validity period, TÜV Italia may verify them during the surveillance audit, or in special audits (as per section 6.10), reassessing the duration of the audit accordingly.

6.9 Renewal audit

The contents of section 6.9 of the RGSG will apply.

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. Management of claims and reports by client organisations and by interested parties

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

- Any notices to the authorities, if required by regulations.
- Assessment of effects on possible underpinning contracts and choice of mitigation methods
- Ensuring satisfactory interactions with other elements of the SMS

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.

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.

Furthermore, considering that IAF MLA mutual recognition agreements do not concern the ISO/IEC 20000-1 scheme, in order to assess the technical feasibility and before proceeding with the certification process, it will be necessary to verify the existence of bilateral agreements between Accredia and the accreditation body under which the applicant organisation has been certified.

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.