SPECIAL RULES FOR THE CERTIFICATION OF BUSINESS CONTINUITY MANAGEMENT SYSTEMS
RSCO

Valid from 01-12-2020

Italia

CONTENTS

Description of the Revision	Updated references to EN ISO 22301:2019 and related standards.

	Department	Date	Name	Signature
Prepared by:	CTSQ	2020-08-07	Danilo Diomede	*Document unsigned, as approved by the TÜV Italia srl digital management system*
Checked by:	T&QM	2020-11-06	Stefano Parini	
Approved by:	MDBA	2020-11-06	Andrea Coscia	

1. Purpose and effective date of this document

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 Business Continuity Management Systems (BCMS).
These rules will come into effect on the date indicated in the heading.

2. Field of application

These rules apply to activities for the certification of business continuity management systems (BCMS) carried out under ACCREDIA certification and also without ACCREDIA certification.
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 BCMS:

- UNI EN ISO 22301:2019 “Security and resilience - Business continuity management systems - Requirements”, national edition of ISO 22301:2019
- UNI EN ISO 22301:2014 “Security and resilience - Business continuity management systems - Requirements”, national edition of ISO 22301:2012. This standard is in force until 30/10/2022.
- the UNI EN ISO 22313:2020 guideline 'Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301'
- The national standard UNI CEI EN ISO/IEC 17021-1:2015 “Conformity assessment - Requirements for bodies providing audit and certification of management systems”
- The national standard UNI CEI ISO/IEC TS 17021-6:2015 “Conformity assessment - Requirements for bodies providing audit and certification of management systems - Competence requirements for auditing and certification of business continuity 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
- Circular no. 01/2020 of 15/01/2020 (DC2020SPM001)
- Technical Regulations (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:

- UNI EN ISO 22300:2018 'Safety and resilience - Vocabulary'
- UNI EN ISO 9000:2015 "Quality management systems - Fundamentals and vocabulary";
- UNI CEI EN 45020:2007: "Standardization and related activities - General vocabulary".
- -ISO/IEC 17000:2004 “Conformity assessment- Vocabulary and general principles

The following acronyms are used in this regulation, in particular:

- BCMS (Business Continuity Management System)
- BCP (Business Continuity Plan)
- BIA (Business Impact Analysis)

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

These rules are available to interested parties at www.tuvsud.com/it.
Organisations may 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 BCMS, that cannot be excluded.
- It follows from the above that TÜV Italia, as the certification body for BCMS, has the task of assessing documentation and the implementation of all requirements in sections 4 to 10; 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 BCMS, such as: the policy, general and detailed objectives, results of business impact analysis and risk assessment, risk treatment strategies, responsibilities, training and communication programmes, procedures, BCP implementation tests, etc.
- As regards compliance with mandatory requirements (legal provisions, regulations, directives, etc.), the general principle is that maintaining and assessing compliance with these mandatory requirements is the responsibility of the organisation that manages the BCMS and issues the appropriate certificate to TÜV Italia (through the RL form provided by the audit team leader); TÜV Italia merely carries out random audits to obtain assurance that the BCMS is effective from this point of view and that – in the eventuality of nonconformity to requirements – the organisation will take appropriate corrective actions.
- The organisation may manage production and/or service processes that are under the control of a single BCMS 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 IAF MD1 and the current edition of ISO/IEC 17021, as well as in the Regulations issued by ACCREDIA).

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, business continuity strategies); in this case, TÜV Italia will assess whether the information it can access is sufficient for the purposes of assessing the BCMS; 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 BCMS; 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 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 BCMS 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

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) Verification of BCMS documentation (first page of stage 1)

BCMS documentation is always controlled, with limitations, if any, due to reasons of confidentiality indicated in section 6.2.

BCMS documentation means:

- the documents identified by the standard as 'documented information'
- (exclusively for audits to UNI EN ISO 22301:2014) the list of mandatory requirements applicable to the BCMS, supplemented by a written statement of compliance with these requirements issued by the organisation (on the RL form).

Documents specified in the standard and subject to document review include, in particular, documents relating to the BIA, risk assessment, business continuity policy and related objectives, and documented business continuity procedures.

It should also be noted that the scope of the BCMS, as well as its perimeter, shall be clearly stated in these documents. Any interfaces/interactions with services or activities not included in the scope shall be identified and included in the risk assessment (e.g. this could be the case for the logistics process related to the industrial production of goods).

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 if necessary) of the organisation.
The audit allows TÜV Italia to better understand:
- the size and characteristics of the organisation's BCMS;
- the extent of the organisation's suitability to undergo the certification procedure;
- the applicability of standards and legislative requirements relating to business continuity;
- 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 BCMS;
- the identification of any deficiencies in the adoption of the BCMS.

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. In the event of deficiencies in the implementation of the BCMS, the client shall be informed in the above-mentioned report, which lists the deficiencies to be remedied before stage 2.
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 BCMS shall be operative; in particular, the organisation shall have defined business continuity objectives that are measurable and - where applicable - quantified, it shall 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 shall comply with the requirements in sections 8 and 11 of these rules.

The audit is conducted on the basis of an audit plan designed to take into account the outcome of activities already carried out (stage 1 audit), with an emphasis on the most significant elements of the BCMS (BIA, business continuity risk assessment and consistency of results); definition of interruption scenarios and business continuity plans; preparation and implementation of strategies and processes for training, communication, alerting and response to disruptive events; review of the effectiveness of the BCMS and measurement of the effectiveness of processes for incident response, business continuity and business recovery, 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.
This plan shall be sent to the organisation at least one week before the audit.
The purpose of the certification audit is to ascertain that the BCMS is implemented in accordance with relevant documentation (policy and objectives, BIA, risk assessment, incident response, business continuity and recovery organisation and procedures, legal requirements, any other mandatory requirements, programmes, etc.) and in an effective manner, and therefore meets the requirements of the reference standard.
The audit team also assesses whether:
- the analysis of the impact on disruptive events on processes is adequate for the organisation's processes and their legal criticality;
- the organisation has established adequate procedures for the identification, review and assessment of business continuity risks, and that the adoption of strategies for business

continuity is consistent with and suitable for the policy, objectives and targets defined by the organisation;
- measurements of the effectiveness of performance indicators are consistent.

6.7 First issue of certification and renewals

The contents of section 6.7 of the RGSG will apply.

6.8 Surveillance audit

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

At the time of this audit, the organisation's BCMS shall 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 BCMS in achieving the objectives set out in the business continuity policy;
- the functioning of procedures for the periodic assessment of legal and regulatory conformity;
- the performance of Business Continuity Plan tests
- the actions taken for nonconforming situations identified in the previous audit;
- the handling of complaints made by parties concerned to TÜV Italia;
- any changes in the definition of business continuity scenarios underlying the Business Continuity Plans;
- 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 BCMS shall 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. 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.
- Reassessment of the impact on the business and the related level of risk.
- Assessment of interactions with other parts of the BCMS

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.

Furthermore, considering that IAF MLA mutual recognition agreements do not concern the ISO 22301 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.