*To all accredited and applicant Certification Bodies operating QMS, ISMS and ITSM certification.*

*To all interested Bodies*

*Our ref.:* DC2017SSV324 *Milan,* 06/11/2017

*Object:* **Technical circular N° 22/2017 - ACCREDIA Department of Certification and Inspection**
**New informative communication regarding accreditation for the certification scheme ISO 22301:2012 - Business Continuity Management Systems (BCMS) revision 1**

This informative circular replaces the previous ACCREDIA circular N° 01/2015 ref. DC2015SSV023 of 26/01/2015.

**Introduction**

In the current market conditions where organizations base their success and ability to satisfy clients' needs, precisely and fully both nationally and internationally, corporate processes are driven hard towards the reduction of costs. In some sectors, such as information and communication technology or in complex production chains,(automotive, aerospace, defense, railways) or in sectors of services such as hospitals, banking, insurance), the capacity to provide products and services – also when adverse circumstances compromise operations, is becoming a decisive factor. Processes need to be thought out in terms of risk management and taking into consideration the elements which may limit capacities to reach specific objectives, often concerning critical activities.
Management system certification for operative continuity does not substitute certification for specific risk areas (environment, health and safety) given that the approach to the management of emergencies is limited to the major ones and it always regards business and institutional aims which are not specific for the environment, health and safety. This does not mean that an organization developing a Business Continuity Management System should not also include the management of any possible crises.

**Normative context**
ISO 22301:2012 is the standard for Business Continuity Management Systems aimed at companies in all sectors. It sets out the necessary processes for an operative management system and is based on the PDCA model and on the recent "Annex SL", defined at ISO level as the new reference model for management systems for which a common structure and text have been defined for all management system areas in order to promote integration in the broadest possible management system system for companies.
ISO 22301:2012 can be integrated with other management system standards, e.g. ISO 9001 - quality - ISO/IEC 20000 – IT services management, and ISO/IEC 27001 – information security.
The aim of ISO 22301:2012 is to provide a guide for defining a BCMS which can meet the needs of the interested parties. It is a recognized reference used by the Public Authorities for their policy documents such as the Code of Digital Administration.

The standard ISO 22301:2012 was designed for use for BCMS certification.

CBs have the option of deciding whether or not to apply for accreditation. If requested, ACCREDIA can confirm the possession of valid accreditation of CABs to other ABs or competent authorities only if the accreditation scope explicitly contains reference to ISO 22301:2012.

## 1) Accreditaton standards and rules

| | |
|---|---|
| Accreditation standard | UNI CEI EN ISO/IEC 17021-1:2015 |
| Competence requirements of the CB’s audit team | The requirements of § 7 of UNI CEI EN ISO/IEC 17021-1:2015 are applicable with the following specifications, consistent with ISO/IEC TS 17021-6.<br>CBs shall show that the staff involved in the management, evaluation and review of the application possess specific competences.<br>a) Necessary competences for the management of the application and the review<br>• Knowledge of BCM terminology (see UNI EN ISO 22300:2014);<br>• Basic knowledge of Risk Management terminology;<br>• Comprehension of the basic requirements of operative continuity;<br>• Knowledge of the basic logic and requirements of the MS;<br>• Knowledge of the laws and standards applicable to MSs for operative continuity in the sectors in which the CB operates.<br>b) Necessary competences for deciding the issue of certification<br>• Knowledge of the terminology of UNI EN ISO 22300:2014;<br>• Knowledge of risk management terminology;<br>• Knowledge of the basic requirements for conducting a risk management;<br>• Knowledge of the meaning and use of Business Impact Analysis;<br>• Knowledge of the requirements of § 9 of UNI CEI EN ISO/IEC 17021-1:2015;<br>• Specific knowledge of UNI EN ISO 22301:2014;<br>• Knowledge of the business continuity schemes or the schemes it can be applied to (e.g. ISO 9001, ISO/IEC 27001 or ISO/IEC 20000);<br>• Knowledge of the main characteristics of the reference sector of the organization (products, services, main processes, applicable legislation including public service requirements);<br>• Knowledge of ISO 31000.<br>c) Competence of the audit team<br>The audit team shall consist of professionals, and, when necessary, technical and legal experts, able to understand fully the applicable requirements of UNI EN ISO 22301:2014 as well as points a) and b) above.<br>If team members are qualified for other MSs they must successfully complete a course of 24 hours, with exam, regarding knowledge of ISO 22301: If there are auditors qualified for information security system management (ISO/IEC 27001), the course can be 8 hours with final exam.<br>If they are not qualified they must successfully complete a course of 40 hours in BCMS auditing.<br>Lead Auditors operating in the BCMS scheme must have at least 10 years’ experience of which 5 as Lead Auditor.<br>Sectors applicable to ISO 22301.<br>A. Industry and related distribution (e.g. pharmaceutical, food)<br>B. Critical infrastructures (energy distribution, communications, transport etc)<br>C. Energy production (refineries, power plants etc.) |

| | |
|---|---|
| | D. Public Authorities (if not already included)<br>E. Health (e.g.: structures with reanimation units, ORs, intensive care, respiratory support)<br>F. Services<br>G. Financial and courier services (banks, insurance, money transfer)<br>H. IT services (invoices, Internet Service Provider etc.) |
| Audit times and criteria | The QMS table of the document IAF MD 5 is applicable.<br>The calculation of audit days as specified in IAF MD 5 shall not take into consideration specifically all the human resources of the organization, but it shall take into consideration those involved in the processes covered by the certification independently of the form of contract in question, and also the external resources involved in the processes involved.<br>In cases of multi-site organizations with sampling, as defined in the document IAF MD 1 and also multi-site organizations without sampling (see the document IAF MD 19) the requirements for size and sampling shall be applied according to the documents referred to.<br>The document IAF MD 11 is also applicable for integrated MS audits.<br>CBs shall have a documented procedure for calculating the duration of audits to obtain repeatable results if applied to different operators of the same organizations and which also permits the verification of calculations carried out on the basis of formulated hypotheses.<br>Both Stages 1 and 2 shall be conducted on-site at the organizations location/s.<br>All audits shall include the auditing of training for operative continuity and the evaluation of the effectiveness of the performance of the relative simulations. At every audit, if technically possible, it is suggested to include in the 3-year certification period, the performance of tests of all the continuity plans defined by the organization during the audits; to give evidence of tests in paper form in order to verify the knowledge of the personnel .in question and the feasibility, within the defined possibilities.<br>The lead auditor shall ensure that the risk analysis carried out by the organization and, in particular, the business impact analysis, take into account the risk management criteria in a way that makes sense to the interested parties and in particular that a risk allowance level was established for the operative continuity management processes regarding the policy aims set out ini the planning. Depending on the interested parties, the risk calculation can be based on different criteria: for ownership they can pertain to economics and to reputation, for collective activities they can be more operative.<br>The lead auditor shall include in the audit report sufficient information to guarantee that the risk analysis and the BIA make sense to the interested parties and that the organization’s actions to respond to risks are in line with these evaluations. This means that the BC system shall regard all the needs of the various interested parties.<br>Certifications cannot be granted to processes which do not present real criticalities concerning a service or final product (as they are placed on the market), in other words, that do not show criticalities for operative continuity against the requirements of the various interested parties.<br>The scope of certification, including the processes, shall refer clearly to the operative units and sites in question. For example, a company which undertakes the service of keeping non-material documents such as those |

| | |
|---|---|
| | operating in the field of the process of electronic invoicing required by the Public Authorities, shall be certified clearly for this service and not for non-critical processes so as to avoid that the certification is not properly used, undermining the credibility of accreditation.<br>Only processes and units which have been effectively audited may be certified and included in conformity certificates issued by the CB.<br>The CB can evaluate whether or not to include in the certificate specific plants or sites, as long as this does not conflict with the principle of transparency of the scope of certification. Normally the scope of certification of a management system of operative continuity shall be aimed at the maintenance of operative continuity of one or more business or institutional areas which are typical of the organization's mission rather than the survival of specific systems: for example, for an industrial group the scope can be to maintain the flow of goods or services delivered to the market, while for a Public Authority it could be of continued benefit in the public interest.<br><br>CBs may issue certifications of conformity to complex BUs where the following conditions exist:<br>1) The policy of the BU is supported or dictated by the Board of the organization;<br>2) The BCMS covers the processes which characterize the BU's mission;<br>3) The management review and the policy regarding the BCMS are shared with the organization's Board.<br><br>The completeness and accuracy of a scope of certification must be confirmed at every audit.<br><br>Every audit (initial, surveillance and renewal) shall include the update of the general risk analysis and that of the BIA and of the management of the training program and the relative practical activities with reference to the interactive scenarios identified by the analysis of impact on business.<br>These evaluations shall also consider the performances, reliability and exposure to risk of suppliers.<br>A specific evaluation shall be carried out for outsourced services which shall be included in the ambit of the BCMS.<br><br>The legal requirements regarding the management for operative continuity are many, and often tied to a "critical infrastructure" and to the principles of national and European Union security.<br>The audit teams shall ensure that the operative continuity MS guarantees to the organization that it has knowledge, manages external origin documents and respects the applicable rules, and that it understands the obligations and the opportunities available for the organization.<br>The audit teams shall also verify that the choices of the organization with regard to operative continuity shall be in line with the applicable laws. |
| Object of the audit | To verify the conformity of the business continuity MS with the requirements of UNI EN ISO 22301:2014.<br>There can be no exclusions from the requirements. |
| Certificate | It shall refer to ISO 22301:2012 or to UNI EN ISO 22301:2014 and subsequent revisions<br><br>State the IAF sector analogous to the ISO 9001 certificates. |

## 2) Accreditation process

There can be various cases with regard to ACCREDIA accreditations already held by CBs presenting an application for accreditation or extension.

The requirements of RG-01 and RG-01-01 remain unchanged for granting accreditation and extension. CBs accredited to ISO/IEC 17021-1 do not need to have issued certificates in this scheme in order to be able to make an application for the extension of accreditation.

BCMS accreditation is issued for sectors:

These are the sectors applicable to ISO 22301:

A. Industry and distribution (e.g. food, pharmaceutical)
B. Critical infrastructures (e.g. energy distribution, communications, transport)
C. Energy production (e.g. refineries, power plants)
D. Public Administration (if not already included in the previous sectors)
E. Health (e.g. health structures with reanimation centers, operating rooms, intensive therapy, respiratory support)
F. Services
G. Financial and courier services (e.g. banks, insurers, couriers, moner transfer)
H. IT services (e.g. electronic invoice files, Internet Service Providers)

See the attached table for the relationship between the IAF and the ISO 22301 sectors.

The CB shall indicate in the certificate the pertinent sectors of the certified organization.

ACCREDIA shall undertake a witness assessment

- at, at least one, organization accredited for this certification scheme
- for sectors B, C, E and H a witness assessment is always necessary before granting extension to the sector
- for sectors A, D, F and G a document review is sufficient before granting extension to the sector

it is possible that one witness is enough for granting in a number of sectors if relevant for the organization and if they have been the object of a valid assessment.

| | |
|---|---|
| A CB which is already accredited for ISO 17021:2011, for ISO 27001 or for ISO 20000 | Document examination of half a day<br>On-site audit of half a day. If necessary closure/integration of document review: 1 day. Witness assessment in accordance with the above rules |
| A CB which is already accredited for ISO 17021:2011 but not for ISO 27001 or ISO 20000 | Document examination of half a day<br>Audit at the main office of 2 days.<br>Witness in accordance with the above rules |
| CB not yet accredited ISO 17021:2011, but accredited for other accreditation schemes | Document examination of 1 day<br>Audit at the CB's head office of 2 days<br>Witness audit in accordance with the above rules |
| CB not accredited in any Scheme | Document examination of 1 day<br>Audit at the CB's head office of 4 days<br>Witness audit in accordance with the above rules |

Documents to be presented to ACCREDIA for examination:

a) Checklist, guideline or instructions made available to the audit team by the CB with specific indications regarding the laws related to the requested sectors
b) CVs of the auditors and decision-makers.
c) Module of the audit report
d) Attestation/certificate issued by the CB
e) List of certificates already issued and of upcoming audit activities (if a witness audit is necessary).
f) Contractual procedures/regulations applicable to the audit as well as internal procedures for the management of the certification
g) For CBs without ISO/IEC 17021 accreditation, as well as the above documents, it is necessary to send all the documents required for the application of accreditation.

**3) Maintenance of accreditation**

For the maintenance of accreditation, during the whole accreditation cycle, except in particular situations (e.g.: handling complaints and remarks, modifications in the certification scheme, changes to the CB,s structure…), the following assessments shall be conducted:

- If the CB has granted less than 50 certificates in the scheme, at least 2 witness assessments and 1 office assessment shall be carried out in the accreditation cycle
- If the CB has granted from 51 to 200 certificates in the scheme, at least 2 witness assessments and 1 office assessment shall be carried out in the accreditation cycle
- If the CB has granted more than 201 certificates in the scheme, at least 3 witness assessments and 1 office assessments shall be carried out in the accreditation cycle

We remain available for any clarification.

With kind regards,

Director of the Department
Emanuele Riva

Correlation table between IAF and BCMS sectors

| IAF | Description of IAF sector | BCMS sector |
|---|---|---|
| 1 | Agriculture, fishing | A Industry and distribution |
| 2 | Mining and quarrying | A Industry and distribution |
| 3 | Food products, beverages and tobacco | A Industry and distribution |
| 4 | Textiles and textile products | A Industry and distribution |
| 5 | Leather and leather products | A Industry and distribution |
| 6 | Wood and wood products | A Industry and distribution |
| 7 | Pulp, paper and paper products | A Industry and distribution |
| 8 | Publishing companies | A Industry and distribution |
| 9 | Printing and related companies | A Industry and distribution |
| 10 | Manufacture of coke and refined petroleum products | A Industry and distribution |
| 11 | Nuclear fuel | B Critical infrastructures |
| 12 | Chemicals, chemical products and fibers | A Industry and distribution |
| 13 | Pharmaceuticals | A Industry and distribution |
| 14 | Rubber and plastic products | A Industry and distribution |
| 15 | Non-metallic mineral products | A Industry and distribution |
| 16 | Concrete, cement, lime, plaster etc | A Industry and distribution |
| 17 | Metals and alloys and fabricated metal products | A Industry and distribution |
| 17a | Metallurgy | A Industry and distribution |
| 17b | Manufacture of metal products excluding machines and plants | A Industry and distribution |
| 18 | Machinery, equipment and mechanical systems | A Industry and distribution |
| 19 | Electrical and optical equipment | A Industry and distribution |
| 19a | Medical devices | A Industry and distribution |
| 19b | Sterilization of medical devices | A Industry and distribution |
| 20 | Shipbuilding and repairing | A Industry and distribution |
| 21 | Aerospace and space vehicles | A Industry and distribution |
| 22a | Production of cycles, motorbikes, vehicles, trailers, parts and accessories | A Industry and distribution |
| 22b | Production of railway material and accessories | A Industry and distribution |
| 23a | Production of jewellery | A Industry and distribution |
| 23b | Production of musical instruments | A Industry and distribution |
| 23c | Production of sporting goods | A Industry and distribution |
| 23d | Production of games and toys | A Industry and distribution |
| 23e | Furniture production and furnishing | A Industry and distribution |
| 23f | Prefabricated products for insulation and their application | A Industry and distribution |
| 24 | Recycling | A Industry and distribution |
| 25 | Electricity production and supply | C Energy producton |
| 26 | Gas production and supply | B Critical infrastructures |
| 27 | Water production and supply | B Critical infrastructures |
| 28 | Construction, installation of plants and services | A Industry and distribution |
| 28a | Construction and maintenance organizations | A Industry and distribution |
| 28b | Organizations performing the design, production and maintenance of plants | A Industry and distribution |
| 29a | Wholesale and retail trade and intermediation | F Services |
| 29b | Repair of motor vehicles, motorcycles | F Services |
| 29c | Repair of personal and household goods | F Services |

| IAF | Description of IAF sector | BCMS sector |
|---|---|---|
| 30 | Hotels, restaurants and bars | F Services |
| 31 | Transport, storage and communication | G financial and courier services |
| 32 | Financial intermediation; real estate; renting | G financial and courier services |
| 31a | Logistics: transport, storage and courier services | G financial and courier services |
| 31b | Post and Telecommunication | G financial and courier services |
| 32a | Financial intermediation and auxiliary activities to intermediation | G financial and courier services |
| 32b | Insurance and pension funds, excluding obligatory social insurance; auxiliary insurance, pension funds, property, renting, professional and business activities | G financial and courier services |
| 33 | IT | H IT services |
| 34a | Research and development | F Services |
| 34b | Architecture and engineering services | F Services |
| 35 | Professonal business services | F Services |
| 36 | Public administration authorities | D Pubblic administration authorities |
| 37 | Education | F Services |
| 38 | Health and social  services | E Health |
| 38a | Hospital services | E Health |
| 38b | Other health services: medical studies and dentistry | E Health |
| 38c | Other health services: clinical analysis labs, Hygiene and prevention labs, Diagnostic imaging labs | E Health |
| 38d | Professional, independent, paramedical activities and ambulance, blood banks and other health services | E Health |
| 38e | Veterinary services | F Services |
| 38f | Health and social work | F Services |
| 39 | Public services | F Services |
| 39a | Disposal of solid waste, sewage and similar | 6 Critical infrastructures |
| 39b | Other social services | F Services |