

## **MANDATORY DOCUMENTS REQUIRED BY 2019 REVISION OF ISO 22301**

What should your business continuity documentation contain? This is probably what you're asking yourself if you are implementing ISO 22301, preparing for the internal audit, or preparing for the certification audit.

### **ISO 22301 MANDATORY DOCUMENTS**

To help you out, here's the list of mandatory documentation for the Business Continuity Management System – BCMS:

- List of legal, regulatory and other requirements (clause 4.2.2) – lists everything you need to comply with.
- Scope of the BCMS and explanation of exclusions (clause 4.3) – defines where your BCMS will be implemented.
- Business continuity policy (clause 5.2) – defines main responsibilities, and the intent of the management.
- Business continuity objectives (clause 6.2) – defines measurable objectives that are to be achieved with business continuity.
- Competencies of personnel (clause 7.2) – defines knowledge and skills needed.
- Business continuity plans and procedures (clause 8.4) – includes plans and procedures for response, communication, recovery (including disaster recovery plans), restore and return activities.
- Documented communication with interested parties (clause 8.4.3.1) – these could be emails, but also official communication from sources such as government agencies and others.
- Records of important information about the disruption, actions taken and decisions made (clause 8.4.3.1) – normally these records are done through minutes or by filling out checklists of performed activities.
- Data and results of monitoring and measurement (clause 9.1.1) – this is the evaluation on whether your BCMS met the objectives.
- Internal audit program (clause 9.2)
- Results of internal audit (clause 9.2) – normally, this is the Internal audit report.
- Results of management review (clause 9.3) – usually, this is in the form of minutes or perhaps documented decisions.
- Nature of nonconformities and actions taken (clause 10.1) – this is a description of nonconformities, and their cause.
- Results of corrective actions (clause 10.1) – this is a description of what has been done to eliminate the cause of a nonconformity.

## **COMMONLY USED NON-MANDATORY BCMS DOCUMENTS AND RECORDS**

The list of documents usually doesn't end with the above list. In most cases (unless you are a small company) you would use also these documents, even though they are not strictly required by the standard:

- Procedure for identification of applicable legal and regulatory requirements (clause 4.2.2)
- Implementation plan for achieving the business continuity objectives (clause 6.2)
- Training and awareness plan (clauses 7.2 and 7.3)
- Procedure for control of documented information (clause 7.5)
- Contracts and service level agreements (SLAs) with suppliers and outsourcing partners (clause 8.1)
- Process for business impact analysis and risk assessment (clause 8.2.1)
- Results of business impact analysis (clause 8.2.2)
- Results of risk assessment (clause 8.2.3)
- Business continuity strategy (clause 8.3)
- Strategies and solutions for business continuity (clause 8.3.3)
- Incident scenarios (clause 8.5)
- Exercise and testing plans (clause 8.5)
- Post-exercise reports (clause 8.5)
- Results of post-incident review (clause 8.6)
- Methods for monitoring, measurement, analysis and evaluation (clause 9.1.1)
- Procedure for internal audit (clause 9.2)
- Procedure for corrective action (clause 10.1)

Note that some requirements can be documented through several other documents. One example of this is determining the context of the organization (clause 4.1) which, although it is not mandatory, can be documented through List of legal, regulatory and other requirements, Business continuity policy, etc.

On the other hand, you can merge some of these documents into a single document (especially if you are a smaller company). For example, you can report the results of business impact analysis and of risk assessment through the Business continuity strategy.