



Checklist of ISO 22301:2019 mandatory documentation

Table of Contents

1. Which documents and records are required?	3
2. Commonly used non-mandatory documents	4
3. How to structure documents and records	5
4. Sample documentation templates	11

1. Which documents and records are required?

The list below shows the minimum set of documents and records required by ISO 22301:2019 (the standard refers to documents and records as “documented information”):

Documents and records	ISO 22301 clause number
List of legal, regulatory and other requirements	4.2.2
Scope of the BCMS (Business Continuity Management System) and explanation of exclusions	4.3
Business continuity policy	5.2
Business continuity objectives	6.2
Competences of personnel	7.2
Business continuity plans and procedures	8.4
Documented communication with interested parties	8.4.3.1
Records of important information about the incident, actions taken and decisions made	8.4.3.1
Data and results of monitoring and measurement	9.1.1
Internal audit program	9.2
Results of internal audit	9.2
Results of management review	9.3
Nature of nonconformities and actions taken	10.1
Results of corrective actions	10.1

This is by no means a definitive list of documents and records that can be used during the ISO 22301 implementation – the standard allows any other documents to be added to improve the level of resilience.

2. Commonly used non-mandatory documents

Other documents that are very often used are the following:

Documents	ISO 22301 clause number
Procedure for identification of applicable legal and regulatory requirements	4.2.2
Implementation plan for achieving the business continuity objectives	6.2
Training and awareness plan	7.2 e 7.3
Procedure for control of documented information	7.5
Contracts and service level agreements (SLAs) with suppliers and outsourcing partners	8.1
Process for business impact analysis and risk assessment	8.2.1
Results of business impact analysis	8.2.2
Results of risk assessment	8.2.3
Strategies and solutions for business continuity	8.3.3
Incident scenarios	8.5
Exercise and testing plans	8.5
Post-exercise reports	8.5
Results of post-incident review	8.6
Methods for monitoring, measurement, analysis and evaluation	9.1.1
Procedure for internal audit	9.2
Procedure for corrective action	10.1

3. How to structure documents and records

Procedure for identification of applicable legal and regulatory requirements & List of legal, regulatory and other requirements (4.2.2)

This is usually a rather short procedure that defines who is responsible for compliance: who has to identify all the interested parties; who has to follow all the laws and regulations, and other requirements of interested parties; who will be responsible for complying with the requirements; how these requirements will be communicated; etc.

This procedure, and the resulting list, should be defined at the very beginning of the project, because it will provide inputs for the whole BCMS.

Read more here: [How to identify interested parties according to ISO 27001 and ISO 22301.](#)

Scope of the BCMS and explanation of exclusions (4.3)

This document is also very short, and should be written at the beginning of the business continuity project. It should define clearly to which parts of your organization the BCMS will be applied, based on identified requirements and the organization's aspirations. It should also explain the reason why some parts of your organization were excluded from the scope.

Very often, this document is merged into the Business continuity policy.

Business continuity policy and business continuity objectives (5.2, 6.2)

This is the central document in which the top management should state what they want to achieve with the BCMS, and how they will control it. Very often, the top management will approve only this top-level document, while the other BCMS documents are approved by lower-level managers.

This document is rather short, and smaller and medium-sized organizations usually merge the scope into it, as well as the BCMS objectives; larger organizations would normally have scope and objectives as separate documents.

The BCMS objectives shouldn't be mixed with Recovery Time Objectives (RTOs) – BCMS objectives are set for the whole BCMS, not for the activities.

Read more here: [The purpose of Business continuity policy according to ISO 22301.](#)

Training and awareness plan; competences of personnel (7.2, 7.3)

These plans are usually developed annually, and are normally developed by the person responsible for business continuity together with the human resources department (if you have one). Records of competences are usually maintained by the human resources department – if you don't have such a department, anyone who normally maintains the employees' records should be doing this job. Basically, a folder with all the documents inserted in it will do.

Read more here: [How to perform training & awareness for ISO 27001 and ISO 22301.](#)

Procedure for control of documented information (7.5)

This is normally a stand-alone procedure, 2 or 3 pages long. If you already implemented some other standard like ISO 9001, ISO 14001, ISO 22301, or similar, you can use the same procedure for all these management systems. Sometimes it is best to write this procedure as the first document in a project.

Read more here: [Document management in ISO 27001 & BS 25999-2.](#)

Contracts and service level agreements (8.1)

It is crucial that your suppliers and outsourcing partners react in an expected fashion when a disruptive incident occurs – this is why it would be best to produce a template with the minimum business continuity requirements that you should insert in each of the contracts you sign with them.

Process for business impact analysis & results (8.2.1, 8.2.2)

Before you start doing your business impact analysis (BIA), you need to define rules on how it is done – this is usually done with business impact analysis methodology. Such methodology should be written on 4 to 5 pages – short enough to be easily readable, but not so short that it is vague.

The collection of data for such analysis is done through BIA questionnaires, which can be in a simple Excel format, or you may use a BCM tool.

The results of the BIA process are documented either in the Business impact analysis report (for larger companies), or you can summarize the results in the Business continuity strategy (this is the shorter version – more applicable for smaller and medium-sized organizations).

Read more here: [How to implement business impact analysis \(BIA\) according to ISO 22301.](#)

Process for risk assessment & results (8.2.1, 8.2.3)

As well as Business impact analysis, the risk assessment also needs to be defined in a methodology before you start performing it. Because ISO 22301 doesn't really specify the requirements for risk assessment, you can use the methodology from ISO 27001 and ISO 27005, as these standards give probably the best methodology for business continuity risk assessment. The results of risk assessment should be documented in the Risk assessment report.

Learn more here: [Can ISO 27001 risk assessment be used for ISO 22301?](#)

Strategies and solutions for business continuity (8.3.3)

Strategies and solutions are the key link between business impact analysis, risk assessment, and the business continuity procedures – their purpose is to make all the agreements, purchases, and other arrangements in order to ensure that all the resources are available in case of a disruption. These are crucial because, without them, the business continuity plans won't be feasible. Business continuity strategies and solutions are usually top-level documents; you can add detailed strategies for each activity as appendices.

Read more here: [Can business continuity strategy save your money?](#)

Implementation plan for achieving the business continuity objectives (6.2)

Once business continuity objectives are set, you need to ensure, in the form of implementation plans, that all the activities and resources needed to implement the whole BCMS are defined, including the people responsible, their deadlines, and how to evaluate achieved results.

Business continuity plans, procedures & records about a disruptive incident (8.4)

Generally speaking, business continuity plans and procedures include:

- Incident response plans, for first response;
- Business recovery plans, focusing on recovering the business side of the organization;
- Disaster recovery plans, focusing on how to recover the information and communication technology infrastructure;
- Communication plans, defining what, when, with whom, and how to communicate with internal and external interested parties, and how to record information about the incident, actions taken, and decisions made. Also, templates may be developed for communicating with media, which will help you issue press releases quickly, if needed;
- Restoration plans, focusing on returning the business from temporary measures to normal operational status;
- Supporting documents such as equipment manuals, building blueprints, etc.

You can organize all such documents within a single Business continuity plan, which can have appendices for each mentioned element.

Regarding incident response plans, these need to address all the major risks your organization is facing and how to respond initially if such incidents happen; they also need to define the method of recording the facts about a disruptive incident – it can be something as easy as handwritten notes next to each step in the plan as it is executed.

See details in these articles: [Business continuity plan: How to structure it according to ISO 22301](#), [Activation procedures for business continuity plan](#), and [Disaster recovery vs. Business continuity](#).

Documented communication with interested parties (8.4.3.1)

Clause 8.4.3.1 refers to procedures for receiving, documenting, and responding to interested parties, i.e., the responses to what was communicated according to the communication plans. An important point here is the information exchanged between the organization and any national or regional risk advisory system, or its equivalent (e.g., Tsunami Warning Centers). As for communication plans, for smaller and mid-sized companies, such procedures will be part of the Incident response plan, while in larger companies they will be separate documents.

Incident scenarios (8.5)

These are short descriptions (or stories) of how a certain incident can develop and how it would impact the activities of your company.

They should be developed based on the results of the risk assessment (they should reflect major risks), and can be added either to the Exercise and testing plan, or to the Business continuity strategy.

Exercise and testing plans & Post-exercise reports (8.5)

Exercises and testing are crucial for the improvement of the business continuity procedures – normally, you should perform exercises and tests at least once a year, and they should become more and more challenging each subsequent year.

Each plan should define the objectives that are to be fulfilled, and the scenarios; the report has to state up to which point those objectives have been achieved.

Results of post-incident review (8.6)

The best method would be to create a form with all the necessary data that needs to be taken into account after a disruptive incident has occurred. When such form is filled in and appropriate conclusions are made (whether the business continuity plans performed well or not), it can provide good insights on how to keep and improve the BCMS.

Methods for monitoring, measurement, analysis and evaluation (9.1.1)

The easiest way to describe how the system is to be measured is through each policy and procedure – normally, this description can be written at the end of each document, and such description defines the kinds of KPIs (key performance indicators) that need to be measured for each document.

Data and results of monitoring and measurement (9.1.1)

These are all the reports, KPIs, unofficial results sent through email, decisions, etc. – all of these should be kept for a specified time period.

Internal audit procedure, internal audit program and results of internal audit (9.2)

The internal audit procedure is normally a stand-alone procedure that can be 2 to 3 pages long, and has to be written before the internal audit begins. As with the Procedure for document control, one procedure for internal audit can be used for any management system.

An internal audit program could be a simple one-page document describing when each audit will take place, and who will perform it.

The results of the internal audit are documented through the Internal audit report – such report should cover all the nonconformities, as well as observations.

Read more here: [How to make an Internal Audit checklist for ISO 27001 / ISO 22301](#).

For more information, see also this free online training: [ISO 27001:2013 Internal Auditor Course](#).

Results of the management review (9.3)

These records are normally in the form of meeting minutes – they have to include all the materials that were included at the management meeting, as well as all the decisions that were made. The minutes can be in paper or digital form.

Read more here: [Why is management review important for ISO 27001 and ISO 22301?](#)

Nonconformities and corrective actions (10.1)

Usually, this is covered through the Procedure for corrective actions – if you already have ISO 27001, ISO 9001, or another management standard, then you can use the existing procedure for this purpose.

Usually, such procedure is not more than 2 or 3 pages long. This procedure can be written at the end of the implementation project, although it is better to write it earlier so that employees can get used to it.

Results of corrective actions are traditionally included in corrective action forms (CARs). However, it is much better to include such records in some application that is already used in the organization for the Help Desk – because corrective actions are nothing but to-do lists with clearly defined responsibilities, tasks, and deadlines.

Read more here: [Practical use of corrective actions for ISO 27001 and ISO 22301](#).

For more information, please take a look at this useful handbook: [Managing ISO Documentation: A Plain English Guide](#).

4. Sample documentation templates

Here you can download a [free preview of the ISO 22301 Documentation Toolkit](#) – in this free preview, you will be able to see the table of contents of each of the mentioned plans, policies, and procedures, as well as a few sections from each document.



Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020

EXPLORE **ADVISERA**

