ISO 22301 (BUSINESS CONTINUITY) CHECKLIST

1 CLAUSE 4 Know your organization

Before you can begin to design your business continuity plans you need to be able to define your organization. An organization is not just defined by what its output is, but also by what shapes and influences it.

There may be stakeholders and regulations that have a say in what matters to your organization. They might influence your planning.

- List the internal and external issues that drive the need for business continuity planning:
- List your stakeholders and their requirements:
- List relevant laws and regulations and have a process for this:

2 CLAUSE 4 Limit your BCMS to what really matters

By knowing your organization and armed with your mission or business goals, you can set a boundary to your Business Continuity Management System (BCMS).

You probably don't need a plan for the entire organization; constrain the scope to the things that matter.

- List what parts of the organization that should be in the scope:
- List the outputs (Products and Services) that should be in the scope:
- Document and explain the exclusions:

3 CLAUSE 5 Make sure your top management is committed to business continuity

Just as senior leaders direct and resource an organization so it fulfills its purpose, they must do the same for business continuity management.

It starts with a policy that is a statement of intent, which in turn drives the need, the activities and the resources.

- Write a Business Continuity Policy:
- Disseminate the policy to everyone affected by it (both internal and external):
- Define roles and responsibilities for business continuity:
- Make sure someone from your senior leadership is responsible for the BCMS and document what their responsibilities are:

4 CLAUSE 6 Have some objectives

Once you have a business continuity policy, you can start planning.

Business continuity is not without its risks and its opportunities for your organization. If you know what they are you can set some objectives.

Figure out what the risks and opportunities are at the organizational level:

Decide what you need to do to address them and implement those actions into your operational processes:

Set some business continuity objectives and what you need to achieve them and who is responsible:

Decide how you're going to monitor and measure performance towards the objectives:

Make sure you've got change control processes for the BCMS in place:

5 CLAUSE 7 Are your resources capable, competent and sufficient?

People are an important resource in a business continuity plan and you will need equipment and supplies: Who, What, Why, When, How and Where.

Decide what resources are required (personnel, technology and infrastructure). In the case of personnel determine the knowledge and skills required:

Confirm that they're present in your organization:

Have a communications plan for the wider organization and external interested parties:

Document everything required by the standard (there's a list at the end of this checklist) and anything else you think necessary. Control the changes to your documents:

ISO 22301:2019 MANDATORY DOCUMENTS

CLAUSE	DOCUMENT	CLAUSE	DOCUMENT
4.2.2	Applicable legal requirements, regulations or laws, and any other identified requirements	8.4.2.4	Documented procedures for each response team
4.3.1	The scope of the BCMS	8.4.3.1	Warning and communication procedures
4.3.2	Exclusions from the scope of the BCMS	8.4.4.1	Business continuity plans
5.2.2	The Business Continuity Policy	8.4.5	Recovery and restoration processes
6.2.1	Business Continuity objectives	8.5	Post-exercise reports
7.2	Evidence of personnel competence	9.1	Results of monitoring, measurement, analysis and evaluation of the performance of the BCMS
7.5.1	Documentation required by the standard (this list) and anything else considered necessary for the effectiveness of the BCMS	9.2.2	Evidence of the implementation of the audit programme and the audit results
8.1	Information necessary to have confidence that the operational planning and control processes are being carried out as planned	9.3.3.2	Results of the management reviews
8.4.1	Business continuity plans and procedures	10.1.3	The nature of non-conformities and what was done about them, and the results of the corrective action

6 CLAUSE 8 Conduct a Business Impact Analysis

When bad things happen, it can be immediately or over a period. The consequences can continue for some time after.

You need to know what's important to the organization, what are the consequences of their disruption over time, and how long you can tolerate it. You work this out with a Business Impact Analysis (BIA).

Define some impacts and their criteria for performing the BIA. This will ensure the assessments are consistent and repeatable:

List the key activities that comprise your products and services:

Identify the internal and external resources required to deliver these products and activities (Personnel, Equipment, Technology (IT)), Supplies, Infrastructure):

Use the criteria to work out the business impact over time to the key activities:

Decide how long it will be before the business impacts become unacceptable (MTPD):

Set timeframes for recovering the activities to minimum acceptable levels (MBCO):

Once the impacts have been determined, you need to decide which activities should have priority for recovery, then:

Define some impacts and their criteria for performing the BIA. This will ensure the assessments are consistent and repeatable:

List the key activities that comprise your products and services:

7 CLAUSE 8 Conduct a Risk Assessment

Now you know what your key activities are you need to consider the risks to them. This will help you determine how likely it is they will be disrupted and therefore the impact to the business.

Prioritise the risks for treatment, which drives the business continuity strategies and then the plans. ISO 31000 is a good risk assessment resource.

8 CLAUSE 8 Build business continuity strategies and solutions

Your strategies should address your risks and requirements from the BIA.

Because this a risk-based approach there will be a cost-benefit consideration. And they need to be realistic, by taking into account the availability of whatever resources you think are needed to achieve success.

9 CLAUSE 8 Define procedures and plans to achieve the strategies

This is where you define your response to incidents. It's about the mobilization of the resources identified in your strategies in a timely and controlled manner.

Procedures:

- **Need to be both specific to address immediate steps but also sufficiently flexible to cope with the inevitable ambiguity in an incident:**
- **Establish a crisis management team(s):**
- **Have roles and responsibilities defined:**
- **Define a response structure for the responsible team:**
- **Must manage internal and external communications:**

Plans:

- **Provide guidance to teams on how to respond, including the order of activities:**
- **Specify criteria for invoking activities:**
- **Protect the welfare of individuals:**
- **What actions need to be taken:**

Recovery to normal operations

Develop a plan and processes to ensure a smooth transition from disaster recovery phase to normal operations.

10 CLAUSE 8 Test, test and test again

It's well known that very few plans survive their first use. It's far better to test plans before they're really needed. An exercise programme is the best way to ensure the plans work and to prevent knowledge fade. Evaluating the organization's capabilities is an essential part of the continual improvement cycle required by the standard.

11 CLAUSE 9 Continuously monitor your business continuity performance

Given everything defined in the preceding clauses, this is where you measure how well your BCMS is performing. You need to know what you should measure, by whom, how and by when. The standard tells you: - you need an ongoing internal audit programme and regular management reviews.

12 CLAUSE 10 Continuously improving

Sometimes things go wrong (non-conformities) so you must have a process for:

- **Controlling them:**
- **Fixing them:**
- **Working out why they went wrong:**
- **Taking steps to prevent it happening again:**