



# ISO 22301:2019 Checklist

22 Sep 2022 / Margareta Encarnacion

Complete

Score	216 / 228 (94.74%)	Flagged items	12	Actions	1
Site conducted					Unanswered
Conducted on					22 Sep 2022 15:17 PST
Prepared by					Margareta Encarnacion
Location					Hawaii, USA (19.8967662, -155.5827818)

<b>Flagged items &amp; Actions</b>	12 flagged, 1 action
Flagged items	12 flagged, 1 action
4. Context of the organization / 4.2 Understanding the needs and expectations of interested parties / 4.2.2 Legal and regulatory requirements	
<b>c) document this information and keep it up to date.</b>	Non-Compliant
Documentation from before has been lacking.	
<b>To do</b>   Priority: High   Due: 29 Sep 2022 15:18 PST   Created by: SafetyCulture Staff	
Improve documentation practices and ensure this checklist is documented also	
4. Context of the organization / 4.3 Determining the scope of the business continuity management system / 4.3.1 General	
<b>The scope shall be available as documented information.</b>	Non-Compliant
Not documented well.	
6. Planning / 6.2 Business continuity objectives and planning to achieve them / 6.2.1 Establishing business continuity objectives	
<b>The organization shall retain documented information on the business continuity objectives.</b>	Non-Compliant
7. Support / 7.5 Documented information / 7.5.1 General	
<b>a) documented information required by this document;</b>	Non-Compliant
7. Support / 7.5 Documented information / 7.5.1 General	
<b>b) documented information determined by the organization as being necessary for the effectiveness of the BCMS.</b>	Non-Compliant
7. Support / 7.5 Documented information / 7.5.2 Creating and updating	
<b>a) identification and description (e.g., a title, date, author, or reference number);</b>	Non-Compliant
8. Operation / 8.1 Operational planning and control	
<b>c) keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.</b>	Non-Compliant
8. Operation / 8.4 Business continuity plans and procedures / 8.4.2 Response structure	
<b>b) documented procedures to guide their actions (see 8.4.4), including those for the activation, operation, coordination and communication of the response.</b>	Non-Compliant
8. Operation / 8.4 Business continuity plans and procedures / 8.4.3 Warning and communication	
<b>b) receiving, documenting and responding to communications from interested parties, including any national or regional risk advisory system or equivalent;</b>	Non-Compliant
8. Operation / 8.4 Business continuity plans and procedures / 8.4.3 Warning and communication	
<b>f) recording the details of the disruption, the actions taken</b>	Non-Compliant

and the decisions made.



8. Operation / 8.6 Evaluation of business continuity documentation and capabilities

**e) update documentation and procedures in a timely manner.**



9. Performance evaluation / 9.1 Monitoring, measurement, analysis and evaluation

**The organization shall retain appropriate documented information as evidence of the results.**



Other actions

0 actions

<b>4. Context of the organization</b>	2 flagged, 1 action, 13 / 15 (86.67%)
4.1 Understanding the organization and its context	1 / 1 (100%)
<b>The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its BCMS.</b>	<b>Compliant</b>
NOTE: These issues will be influenced by the organization's overall objectives, its products and services and the amount and type of risk that it may or may not take.	
4.2 Understanding the needs and expectations of interested parties	1 flagged, 1 action, 4 / 5 (80%)
4.2.1 General	2 / 2 (100%)
When establishing its BCMS, the organization shall determine:	
<b>a) the interested parties that are relevant to the BCMS;</b>	<b>Compliant</b>
<b>b) the relevant requirements of these interested parties.</b>	<b>Compliant</b>
4.2.2 Legal and regulatory requirements	1 flagged, 1 action, 2 / 3 (66.67%)
The organization shall:	
<b>a) implement and maintain a process to identify, have access to, and assess the applicable legal and regulatory requirements related to the continuity of its products and services, activities and resources;</b>	<b>Compliant</b>
<b>b) ensure that these applicable legal, regulatory and other requirements are taken into account in implementing and maintaining its BCMS;</b>	<b>Compliant</b>
<b>c) document this information and keep it up to date.</b>	<b>Non-Compliant</b>
Documentation from before has been lacking.	
<b>To do</b>   Priority: High   Due: 29 Sep 2022 15:18 PST   Created by: SafetyCulture Staff	
Improve documentation practices and ensure this checklist is documented also	
4.3 Determining the scope of the business continuity management system	1 flagged, 7 / 8 (87.5%)
4.3.1 General	1 flagged, 4 / 5 (80%)
<b>The organization shall determine the boundaries and applicability of the BCMS to establish its scope.</b>	<b>Compliant</b>

When determining this scope, the organization shall consider:

<b>a) the external and internal issues referred to in 4.1;</b>	Compliant
<b>b) the requirements referred to in 4.2;</b>	Compliant
<b>c) its mission, goals, and internal and external obligations.</b>	Compliant
<b>The scope shall be available as documented information.</b>	Non-Compliant
Not documented well.	

4.3.2 Scope of the business continuity management system 3 / 3 (100%)

The organization shall:

<b>a) establish the parts of the organization to be included in the BCMS, taking into account its location(s), size, nature and complexity;</b>	Compliant
<b>b) identify products and services to be included in the BCMS.</b>	Compliant
<b>When defining the scope, the organization shall document and explain exclusions. They shall not affect the organization's ability and responsibility to provide business continuity, as determined by the business impact analysis or risk assessment and applicable legal or regulatory requirements.</b>	Compliant

4.4 Business continuity management system 1 / 1 (100%)

<b>The organization shall establish, implement, maintain and continually improve a BCMS, including the processes needed and their interactions, in accordance with the requirements of this document.</b>	Compliant
---	-----------

<b>5. Leadership</b>	17 / 17 (100%)
5.1 Leadership and commitment	8 / 8 (100%)

Top management shall demonstrate leadership and commitment with respect to the BCMS by:

<b>a) ensuring that the business continuity policy and business continuity objectives are established and are compatible with the strategic direction of the organization;</b>	Compliant
<b>b) ensuring the integration of the BCMS requirements into the organization's business processes;</b>	Compliant
<b>c) ensuring that the resources needed for the BCMS are available;</b>	Compliant
<b>d) communicating the importance of effective business continuity and of conforming to the BCMS requirements;</b>	Compliant
<b>e) ensuring that the BCMS achieves its intended outcome(s);</b>	Compliant
<b>f) directing and supporting persons to contribute to the effectiveness of the BCMS;</b>	Compliant
<b>g) promoting continual improvement;</b>	Compliant
<b>h) supporting other relevant managerial roles to demonstrate their leadership and commitment as it applies to their areas of responsibility.</b>	Compliant

NOTE: Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Policy	6 / 6 (100%)
5.2.1 Establishing the business continuity policy	4 / 4 (100%)

Top management shall establish a business continuity policy that:

<b>a) is appropriate to the purpose of the organization;</b>	Compliant
<b>b) provides a framework for setting business continuity objectives;</b>	Compliant
<b>c) includes a commitment to satisfy applicable requirements;</b>	Compliant
<b>d) includes a commitment to continual improvement of the BCMS.</b>	Compliant

5.2.2 Communicating the business continuity policy

2 / 2 (100%)

The business continuity policy shall:

**a) be available as documented information;**

N/A

Due to improper documentation practices before, some information is not available.

**b) be communicated within the organization;**

Compliant

**c) be available to interested parties, as appropriate.**

Compliant

5.3 Roles, responsibilities and authorities

3 / 3 (100%)

**Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.**

Compliant

Top management shall assign the responsibility and authority for:

**a) ensuring that the BCMS conforms to the requirements of this document;**

Compliant

**b) reporting on the performance of the BCMS to top management.**

Compliant

<b>6. Planning</b>	1 flagged, 23 / 24 (95.83%)
6.1 Actions to address risks and opportunities	6 / 6 (100%)
6.1.1 Determining risks and opportunities	3 / 3 (100%)

When planning for the BCMS, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

<b>a) give assurance that the BCMS can achieve its intended outcome(s);</b>	Compliant
<b>b) prevent, or reduce, undesired effects;</b>	Compliant
<b>c) achieve continual improvement.</b>	Compliant
6.1.2 Addressing risks and opportunities	3 / 3 (100%)

The organization shall plan:

<b>a) actions to address these risks and opportunities;</b>	Compliant
b) how to:	
<b>1) integrate and implement the actions into its BCMS processes (see 8.1);</b>	Compliant
<b>2) evaluate the effectiveness of these actions (see 9.1).</b>	Compliant

NOTE: Risks and opportunities relate to the effectiveness of the management system. Risks related to disruption of the business are addressed in 8.2.

6.2 Business continuity objectives and planning to achieve them	1 flagged, 12 / 13 (92.31%)
6.2.1 Establishing business continuity objectives	1 flagged, 7 / 8 (87.5%)
<b>The organization shall establish business continuity objectives at relevant functions and levels.</b>	Compliant

The business continuity objectives shall:

<b>a) be consistent with the business continuity policy;</b>	Compliant
<b>b) be measurable (if practicable);</b>	Compliant

<b>c) take into account applicable requirements (see 4.1 and 4.2);</b>	Compliant
<b>d) be monitored;</b>	Compliant
<b>e) be communicated;</b>	Compliant
<b>f) be updated as appropriate.</b>	Compliant
<b>The organization shall retain documented information on the business continuity objectives.</b>	Non-Compliant

6.2.2 Determining business continuity objectives

5 / 5 (100%)

When planning how to achieve its business continuity objectives, the organization shall determine:

<b>a) what will be done;</b>	Compliant
<b>b) what resources will be required;</b>	Compliant
<b>c) who will be responsible;</b>	Compliant
<b>d) when it will be completed;</b>	Compliant
<b>e) how the results will be evaluated.</b>	Compliant

6.3 Planning changes to the business continuity management system

5 / 5 (100%)

**When the organization determines the need for changes to the BCMS, including those identified in Clause 10, the changes shall be carried out in a planned manner.**

Compliant

The organization shall consider:

<b>a) the purpose of the changes and their potential consequences;</b>	Compliant
<b>b) the integrity of the BCMS;</b>	Compliant
<b>c) the availability of resources;</b>	Compliant
<b>d) the allocation or reallocation of responsibilities and authorities.</b>	Compliant

<b>7. Support</b>	3 flagged, 22 / 25 (88%)
-------------------	--------------------------

7.1 Resources	1 / 1 (100%)
---------------	--------------

**The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the BCMS.**

Compliant

7.2 Competence	3 / 3 (100%)
----------------	--------------

The organization shall:

**a) determine the necessary competence of person(s) doing work under its control that affects its business continuity performance;**

Compliant

**b) ensure that these persons are competent on the basis of appropriate education, training, or experience;**

Compliant

**c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;**

Compliant

**d) retain appropriate documented information as evidence of competence.**

N/A

NOTE: Applicable actions can include, for example, the provision of training to, the mentoring of, or the re-assignment of currently employed persons; or the hiring or contracting of competent persons.

7.3 Awareness	4 / 4 (100%)
---------------	--------------

Persons doing work under the organization's control shall be aware of:

**a) the business continuity policy;**

Compliant

**b) their contribution to the effectiveness of the BCMS, including the benefits of improved business continuity performance;**

Compliant

**c) the implications of not conforming with the BCMS requirements;**

Compliant

**d) their own role and responsibilities before, during and after disruptions.**

Compliant

7.4 Communication	5 / 5 (100%)
-------------------	--------------

The organization shall determine the internal and external communications relevant to the BCMS,

including:

<b>a) on what it will communicate;</b>	Compliant
<b>b) when to communicate;</b>	Compliant
<b>c) with whom to communicate;</b>	Compliant
<b>d) how to communicate;</b>	Compliant
<b>e) who will communicate.</b>	Compliant
7.5 Documented information	3 flagged, 9 / 12 (75%)
7.5.1 General	2 flagged, 0 / 2 (0%)

The organization's BCMS shall include:

<b>a) documented information required by this document;</b>	Non-Compliant
<b>b) documented information determined by the organization as being necessary for the effectiveness of the BCMS.</b>	Non-Compliant

NOTE: The extent of documented information for a BCMS can differ from one organization to another due to:

- the size of organization and its type of activities, processes, products and services, and resources;
- the complexity of processes and their interactions;
- the competence of persons.

7.5.2 Creating and updating	1 flagged, 2 / 3 (66.67%)
-----------------------------	---------------------------

When creating and updating documented information the organization shall ensure appropriate:

<b>a) identification and description (e.g., a title, date, author, or reference number);</b>	Non-Compliant
<b>b) format (e.g., language, software version, graphics) and media (e.g., paper, electronic);</b>	Compliant
<b>c) review and approval for suitability and adequacy.</b>	Compliant
7.5.3 Control of documented information	7 / 7 (100%)

7.5.3.1 Documented information required by the BCMS and by this document shall be controlled to ensure:

<b>a) it is available and suitable for use, where and when it is needed;</b>	Compliant
<b>b) it is adequately protected (e.g., from loss of confidentiality, improper use, or loss of integrity).</b>	Compliant

7.5.3.2 For the control of documented information, the organization shall address the following activities, as applicable:

<b>a) distribution, access, retrieval and use;</b>	Compliant
<b>b) storage and preservation, including preservation of legibility;</b>	Compliant
<b>c) control of changes (e.g., version control);</b>	Compliant
<b>d) retention and disposition.</b>	Compliant
<b>Documented information of external origin determined by the organization to be necessary for the planning and operation of the BCMS shall be identified, as appropriate, and controlled.</b>	Compliant

NOTE: Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

## 8. Operation

5 flagged, 92 / 97 (94.85%)

### 8.1 Operational planning and control

1 flagged, 4 / 5 (80%)

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, by:

**a) establishing criteria for the processes;**

Compliant

**b) implementing control of the processes in accordance with the criteria;**

Compliant

**c) keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.**

Non-Compliant

**The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.**

Compliant

**The organization shall ensure that outsourced processes and the supply chain are controlled.**

Compliant

### 8.2 Business impact analysis and risk assessment

14 / 14 (100%)

#### 8.2.1 General

2 / 2 (100%)

The organization shall:

**a) implement and maintain systematic processes for analysing the business impact and assessing the risks of disruption;**

Compliant

**b) review the business impact analysis and risk assessment at planned intervals and when there are significant changes within the organization or the context in which it operates.**

Compliant

NOTE : The organization determines the order in which the business impact analysis and risk assessment are conducted.

#### 8.2.2 Business impact analysis

8 / 8 (100%)

The organization shall use the process for analysing business impacts to determine business continuity priorities and requirements. The process shall:

**a) define the impact types and criteria relevant to the organization's context;**

Compliant

**b) identify the activities that support the provision of**

Compliant

<b>products and services;</b>	
<b>c) use the impact types and criteria for assessing the impacts over time resulting from the disruption of these activities;</b>	Compliant
<b>d) identify the time frame within which the impacts of not resuming activities would become unacceptable to the organization;</b>	Compliant

NOTE 1: This time frame can be referred to as the "maximum tolerable period of disruption (MTPD)".

<b>e) set prioritized time frames within the time identified in d) for resuming disrupted activities at a specified minimum acceptable capacity;</b>	Compliant
--	-----------

NOTE 2: This time frame can be referred to as the "recovery time objective (RTO)".

<b>f) use this analysis to identify prioritized activities;</b>	Compliant
<b>g) determine which resources are needed to support prioritized activities;</b>	Compliant
<b>h) determine the dependencies, including partners and suppliers, and interdependencies of prioritized activities.</b>	Compliant

8.2.3 Risk assessment 4 / 4 (100%)

<b>The organization shall implement and maintain a risk assessment process.</b>	Compliant
---	-----------

NOTE : The process for risk assessment is addressed in ISO 31000.

The organization shall:

<b>a) identify the risks of disruption to the organization's prioritized activities and to their required resources;</b>	Compliant
<b>b) analyze and evaluate the identified risks;</b>	Compliant
<b>c) determine which risks require treatment.</b>	Compliant

NOTE : Risks in this subclause relate to the disruption of business activities. Risks and opportunities related to the effectiveness of the management system are addressed in 6.1.

8.3 Business continuity strategies and solutions 19 / 19 (100%)

8.3.1 General	1 / 1 (100%)
---------------	--------------

**Based on the outputs from the business impact analysis and risk assessment, the organization shall identify and select business continuity strategies that consider options for before, during and after disruption. The business continuity strategies shall be comprised of one or more solutions.**

Compliant
-----------

8.3.2 Identification of strategies and solutions	6 / 6 (100%)
--	--------------

Identification shall be based on the extent to which strategies and solutions:

<b>a) meet the requirements to continue and recover prioritized activities within the identified time frames and agreed capacity;</b>	Compliant
<b>b) protect the organization's prioritized activities;</b>	Compliant
<b>c) reduce the likelihood of disruption;</b>	Compliant
<b>d) shorten the period of disruption;</b>	Compliant
<b>e) limit the impact of disruption on the organization's products and services;</b>	Compliant
<b>f) provide for the availability of adequate resources.</b>	Compliant

8.3.3 Selection of strategies and solutions	3 / 3 (100%)
---	--------------

Selection shall be based on the extent to which strategies and solutions:

<b>a) meet the requirements to continue and recover prioritized activities within the identified time frames and agreed capacity;</b>	Compliant
<b>b) consider the amount and type of risk the organization may or may not take;</b>	Compliant
<b>c) consider associated costs and benefits.</b>	Compliant

8.3.4 Resource requirements	8 / 8 (100%)
-----------------------------	--------------

The organization shall determine the resource requirements to implement the selected business continuity solutions. The types of resources considered shall include, but not be limited to:

<b>a) people;</b>	Compliant
<b>b) information and data;</b>	Compliant

<b>c) physical infrastructure such as buildings, workplaces or other facilities and associated utilities;</b>	Compliant
<b>d) equipment and consumables;</b>	Compliant
<b>e) information and communication technology (ICT) systems;</b>	Compliant
<b>f) transportation and logistics;</b>	Compliant
<b>g) finance;</b>	Compliant
<b>h) partners and suppliers.</b>	Compliant
8.3.5 Implementation of solutions	1 / 1 (100%)
<b>The organization shall implement and maintain selected business continuity solutions so they can be activated when needed.</b>	Compliant
8.4 Business continuity plans and procedures	3 flagged, 41 / 44 (93.18%)
8.4.1 General	7 / 7 (100%)
<b>The organization shall implement and maintain a response structure that will enable timely warning and communication to relevant interested parties. It shall provide plans and procedures to manage the organization during a disruption. The plans and procedures shall be used when required to activate business continuity solutions.</b>	Compliant
NOTE : There are different types of procedures that comprise business continuity plans.	
<b>The organization shall identify and document business continuity plans and procedures based on the output of the selected strategies and solutions.</b>	Compliant
The procedures shall:	
<b>a) be specific regarding the immediate steps that are to be taken during a disruption;</b>	Compliant
<b>b) be flexible to respond to the changing internal and external conditions of a disruption;</b>	Compliant
<b>c) focus on the impact of incidents that potentially lead to disruption;</b>	Compliant
<b>d) be effective in minimizing the impact through the implementation of appropriate solutions;</b>	Compliant

<b>e) assign roles and responsibilities for tasks within them.</b>	Compliant
8.4.2 Response structure	1 flagged, 11 / 12 (91.67%)
<b>8.4.2.1 The organization shall implement and maintain a structure, identifying one or more teams responsible for responding to disruptions.</b>	Compliant
<b>8.4.2.2 The roles and responsibilities of each team and the relationships between the teams shall be clearly stated.</b>	Compliant
8.4.2.3 Collectively, the teams shall be competent to:	
<b>a) assess the nature and extent of a disruption and its potential impact;</b>	Compliant
<b>b) assess the impact against pre-defined thresholds that justify initiation of a formal response;</b>	Compliant
<b>c) activate an appropriate business continuity response;</b>	Compliant
<b>d) plan actions that need to be undertaken;</b>	Compliant
<b>e) establish priorities (using life safety as the first priority);</b>	Compliant
<b>f) monitor the effects of the disruption and the organization's response;</b>	Compliant
<b>g) activate the business continuity solutions;</b>	Compliant
<b>h) communicate with relevant interested parties, authorities and the media.</b>	Compliant
8.4.2.4 For each team there shall be:	
<b>a) identified personnel and their alternates with the necessary responsibility, authority and competence to perform their designated role;</b>	Compliant
<b>b) documented procedures to guide their actions (see 8.4.4), including those for the activation, operation, coordination and communication of the response.</b>	Non-Compliant
8.4.3 Warning and communication	2 flagged, 7 / 9 (77.78%)
8.4.3.1 The organization shall document and maintain procedures for:	
<b>a) communicating internally and externally to relevant interested parties, including what, when, with whom and</b>	Compliant

**how to communicate;**



NOTE: The organization can document and maintain procedures for how, and under what circumstances, the organization communicates with employees and their emergency contacts.

<b>b) receiving, documenting and responding to communications from interested parties, including any national or regional risk advisory system or equivalent;</b>	Non-Compliant
<b>c) ensuring the availability of the means of communication during a disruption;</b>	Compliant
<b>d) facilitating structured communication with emergency responders;</b>	Compliant
<b>e) providing details of the organization's media response following an incident, including a communications strategy;</b>	Compliant
<b>f) recording the details of the disruption, the actions taken and the decisions made.</b>	Non-Compliant

8.4.3.2 Where applicable, the following shall also be considered and implemented:

<b>a) alerting interested parties potentially impacted by an actual or impending disruption;</b>	Compliant
<b>b) ensuring appropriate coordination and communication between multiple responding organizations.</b>	Compliant
<b>The warning and communication procedures shall be exercised as part of the organization's exercise programme described in 8.5.</b>	Compliant

8.4.4 Business continuity plans

16 / 16 (100%)

**8.4.4.1 The organization shall document and maintain business continuity plans and procedures. The business continuity plans shall provide guidance and information to assist teams to respond to a disruption and to assist the organization with response and recovery.**

N/A

8.4.4.2 Collectively, the business continuity plans shall contain:

a) details of the actions that the teams will take in order to:

<b>1) continue or recover prioritized activities within predetermined time frames;</b>	Compliant
<b>2) monitor the impact of the disruption and the</b>	Compliant

<b>organization's response to it;</b>	
<b>b) reference to the pre-defined threshold(s) and process for activating the response;</b>	Compliant
<b>c) procedures to enable the delivery of products and services at agreed capacity;</b>	Compliant
d) details to manage the immediate consequences of a disruption giving due regard to:	
<b>1) the welfare of individuals;</b>	Compliant
<b>2) the prevention of further loss or unavailability of prioritized activities;</b>	Compliant
<b>3) the impact on the environment.</b>	Compliant
8.4.4.3 Each plan shall include:	
<b>a) the purpose, scope and objectives;</b>	Compliant
<b>b) the roles and responsibilities of the team that will implement the plan;</b>	Compliant
<b>c) actions to implement the solutions;</b>	Compliant
<b>d) supporting information needed to activate (including activation criteria), operate, coordinate and communicate the team's actions;</b>	Compliant
<b>e) internal and external interdependencies;</b>	Compliant
<b>f) the resource requirements;</b>	Compliant
<b>g) the reporting requirements;</b>	Compliant
<b>h) a process for standing down.</b>	Compliant
<b>Each plan shall be usable and available at the time and place at which it is required.</b>	Compliant
8.5 Exercise programme	9 / 9 (100%)
<b>The organization shall implement and maintain a programme of exercising and testing to validate over time the effectiveness of its business continuity strategies and solutions.</b>	Compliant

The organization shall conduct exercises and tests that:

<b>a) are consistent with its business continuity objectives;</b>	Compliant
<b>b) are based on appropriate scenarios that are well planned with clearly defined aims and objectives;</b>	Compliant
<b>c) develop teamwork, competence, confidence and knowledge for those who have roles to perform in relation to disruptions;</b>	Compliant
<b>d) taken together over time, validate its business continuity strategies and solutions;</b>	Compliant
<b>e) produce formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements;</b>	Compliant
<b>f) are reviewed within the context of promoting continual improvement;</b>	Compliant
<b>g) are performed at planned intervals and when there are significant changes within the organization or the context in which it operates.</b>	Compliant
<b>The organization shall act on the results of its exercising and testing to implement changes and improvements.</b>	Compliant

8.6 Evaluation of business continuity documentation and capabilities

1 flagged, 5 / 6 (83.33%)

The organization shall:

<b>a) evaluate the suitability, adequacy and effectiveness of its business impact analysis, risk assessment, strategies, solutions, plans and procedures;</b>	Compliant
<b>b) undertake evaluations through reviews, analysis, exercises, tests, post-incident reports and performance evaluations;</b>	Compliant
<b>c) conduct evaluations of the business continuity capabilities of relevant partners and suppliers;</b>	Compliant
<b>d) evaluate compliance with applicable legal and regulatory requirements, industry best practices, and conformity with its own business continuity policy and objectives;</b>	Compliant
<b>e) update documentation and procedures in a timely manner.</b>	Non-Compliant
<b>These evaluations shall be conducted at planned intervals, after an incident or activation, and when significant changes</b>	Compliant

occur.

---



<b>9. Performance evaluation</b>	1 flagged, 35 / 36 (97.22%)
9.1 Monitoring, measurement, analysis and evaluation	1 flagged, 5 / 6 (83.33%)

The organization shall determine:

<b>a) what needs to be monitored and measured;</b>	Compliant
<b>b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;</b>	Compliant
<b>c) when and by whom the monitoring and measuring shall be performed;</b>	Compliant
<b>d) when and by whom the results from monitoring and measurement shall be analyzed and evaluated.</b>	Compliant
<b>The organization shall retain appropriate documented information as evidence of the results.</b>	Non-Compliant
<b>The organization shall evaluate the BCMS performance and the effectiveness of the BCMS.</b>	Compliant

9.2 Internal audit	10 / 10 (100%)
9.2.1 General	3 / 3 (100%)

The organization shall conduct internal audits at planned intervals to provide information on whether the BCMS:

a) conforms to:

<b>1) the organization's own requirements for its BCMS;</b>	Compliant
<b>2) the requirements of this document;</b>	Compliant
<b>b) is effectively implemented and maintained.</b>	Compliant

9.2.2 Audit programme(s)	7 / 7 (100%)
--------------------------	--------------

The organization shall:

<b>a) plan, establish, implement and maintain an audit programme(s) including the frequency, methods, responsibilities, planning requirements and reporting, which shall take into consideration the importance of the processes concerned and the results of previous audits;</b>	Compliant
--	-----------

<b>b) define the audit criteria and scope for each audit;</b>	Compliant
<b>c) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;</b>	Compliant
<b>d) ensure that the results of the audits are reported to relevant managers;</b>	Compliant
<b>e) retain documented information as evidence of the implementation of the audit programme(s) and the audit results;</b>	Compliant
<b>f) ensure that any necessary corrective actions are taken without undue delay to eliminate detected nonconformities and their causes;</b>	Compliant
<b>g) ensure that follow-up audit actions include the verification of the actions taken and the reporting of verification results.</b>	Compliant
9.3 Management review	20 / 20 (100%)
9.3.1 General	1 / 1 (100%)
<b>Top management shall review the organization's BCMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.</b>	Compliant
9.3.2 Management review input	13 / 13 (100%)
The management review shall include consideration of:	
<b>a) the status of actions from previous management reviews;</b>	Compliant
<b>b) changes in external and internal issues that are relevant to the BCMS;</b>	Compliant
c) information on the BCMS performance, including trends in:	
<b>1) nonconformities and corrective actions;</b>	Compliant
<b>2) monitoring and measurement evaluation results;</b>	Compliant
<b>3) audit results;</b>	Compliant
<b>d) feedback from interested parties;</b>	Compliant
<b>e) the need for changes to the BCMS, including the policy and objectives;</b>	Compliant

<b>f) procedures and resources that could be used in the organization to improve the BCMS' performance and effectiveness;</b>	Compliant
<b>g) information from the business impact analysis and risk assessment;</b>	Compliant
<b>h) output from the evaluation of business continuity documentation and capabilities (see 8.6);</b>	Compliant
<b>i) risks or issues not adequately addressed in any previous risk assessment;</b>	Compliant
<b>j) lessons learned and actions arising from near-misses and disruptions;</b>	Compliant
<b>k) opportunities for continual improvement.</b>	Compliant
9.3.3 Management review outputs	6 / 6 (100%)

9.3.3.1 The outputs of the management review shall include decisions related to continual improvement opportunities and any need for changes to the BCMS to improve its efficiency and effectiveness, including the following:

<b>a) variations to the scope of the BCMS;</b>	Compliant
<b>b) update of the business impact analysis, risk assessment, business continuity strategies and solutions, and business continuity plans;</b>	Compliant
<b>c) modification of procedures and controls to respond to internal or external issues that may impact the BCMS;</b>	Compliant
<b>d) how the effectiveness of controls will be measured.</b>	Compliant

9.3.3.2 The organization shall retain documented information as evidence of the results of management reviews. It shall:

<b>a) communicate the results of the management review to relevant interested parties;</b>	Compliant
<b>b) take appropriate action relating to those results.</b>	Compliant

<b>10. Improvement</b>	14 / 14 (100%)
10.1 Nonconformity and corrective action	12 / 12 (100%)
<b>10.1.1 The organization shall determine opportunities for improvement and implement necessary actions to achieve the intended outcomes of its BCMS.</b>	Compliant
10.1.2 When a nonconformity occurs, the organization shall:	
a) react to the nonconformity, and, as applicable:	
<b>1) take action to control and correct it;</b>	Compliant
<b>2) deal with the consequences;</b>	Compliant
b) evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere, by:	
<b>1) reviewing the nonconformity;</b>	Compliant
<b>2) determining the causes of the nonconformity;</b>	Compliant
<b>3) determining if similar nonconformities exist, or can potentially occur;</b>	Compliant
<b>c) implement any action needed;</b>	Compliant
<b>d) review the effectiveness of any corrective action taken;</b>	Compliant
<b>e) make changes to the BCMS, if necessary.</b>	Compliant
<b>Corrective actions shall be appropriate to the effects of the nonconformities encountered.</b>	Compliant
10.1.3 The organization shall retain documented information as evidence of:	
<b>a) the nature of the nonconformities and any subsequent actions taken;</b>	Compliant
<b>b) the results of any corrective action.</b>	Compliant
10.2 Continual improvement	2 / 2 (100%)
<b>The organization shall continually improve the suitability, adequacy and effectiveness of the BCMS, based on qualitative and quantitative measures.</b>	Compliant

**The organization shall consider the results of analysis and evaluation, and the outputs from management review, to determine if there are needs or opportunities, relating to the business, or to the BCMS, that shall be addressed as part of continual improvement.**

---



NOTE : The organization can use the processes of the BCMS, such as leadership, planning and performance evaluation, to achieve improvement.

---

**Completion**

**Comments/Recommendations**

---

**Name and Signature**

*Margaretta E.*

Margaretta Encarnacion  
22 Sep 2022 15:22 PST

---