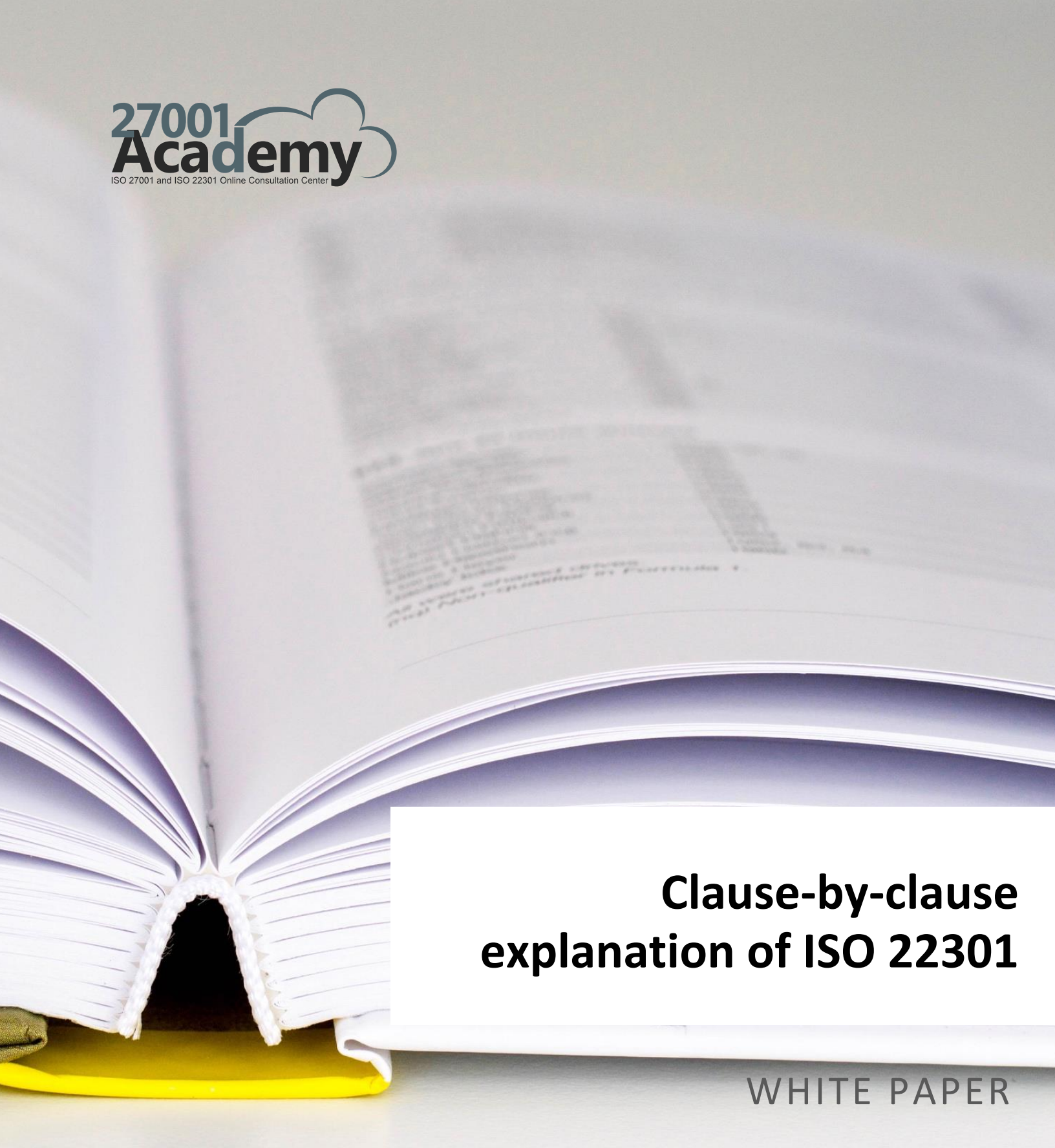
27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center



Clause-by-clause explanation of ISO 22301

WHITE PAPER

Advisera
Making certification simple.

Table of Contents

Executive summary

Surviving a business disruption is a matter of being well prepared. This white paper is designed to help top management and employees from organizations that decided to achieve the necessary readiness by establishing and maintaining an ISO 22301:2012-based Business Continuity Management System (BCMS).

In this document, you will find each clause of ISO 22301, from sections 4 to 10, explained to facilitate understanding of the standard. The clauses are presented in the same order and with the same clause numbers as in the ISO 22301:2012 standard. In addition, you'll find links to supplementary learning materials like articles and other white papers.

Please note: This white paper is not a replacement for ISO 22301 – to get the standard, visit the ISO website: http://www.iso.org

0. Introduction

Business continuity systems are often regarded by organizations as simple checklists and work instructions to be used only in improbable situations, far from the way they do their normal business. By sticking to these beliefs, organizations prevent themselves from properly building a BCMS (Business Continuity Management System) and achieving its full potential, either in operational and financial performance, or marketing reputation.

Fortunately, there are many frameworks in the market that can help organizations to handle this situation, among them being ISO 22301:2012.

Whether standing alone or integrated with another management system, such as ISO 9001 (Quality), ISO 27001 (information security), ISO 14001 (Environment), or OHSAS 18001 (Operational Health and Safety), the ISO 22301:2012 standard provides guidance and direction on how an organization, regardless of its size and industry, should manage, mitigate, and recover from disruptive incidents when they arise, which can bring many benefits not only for the organization itself, but also to clients, suppliers, and other interested parties.

But, for those unfamiliar with ISO standards or business continuity concepts, ISO 22301 may be confusing, so we developed this whitepaper to help you get inside this world.

Sections 1 to 3 will cover the concepts of processes, a process approach, and the PDCA cycle applicable to ISO management standards, as well as the most important definitions a beginner in business continuity should know.

The main content of this white paper will follow the same order and numbering of the sections required to certify a BCMS against ISO 22301:2012:

4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Besides all this explanatory information, you will find both throughout, and at the end of this white paper, references to other learning materials.

1. Process and process approach

1.1 Terms and definitions

Process: a group of repeatable and interrelated activities performed to transform a series of inputs into defined outputs.

Process approach: the management of a group of processes together as a system, where the interrelations between processes are identified and the outputs of a previous process are treated as the inputs of the following one. This approach helps to ensure that the results of each individual process will add business value and contribute to achieving the final desired results.

Inputs: a group of elements that are required to perform a process, for example: employees, raw material, equipment, information, etc. The input of a process may be the output of a previous one.

Outputs: the results of a process. They can be desired (e.g., product and/or service) or undesired (e.g., waste or pollution). The output of a process may be the final desired result, or the input of a subsequent process.

Business continuity: the ability to deliver previously agreed products and services even under extremely negative situations (e.g., during or after a natural disaster or massive process failure). It should be noted that the delivery may be either to internal or external parties (e.g., between processes or to the final customer).

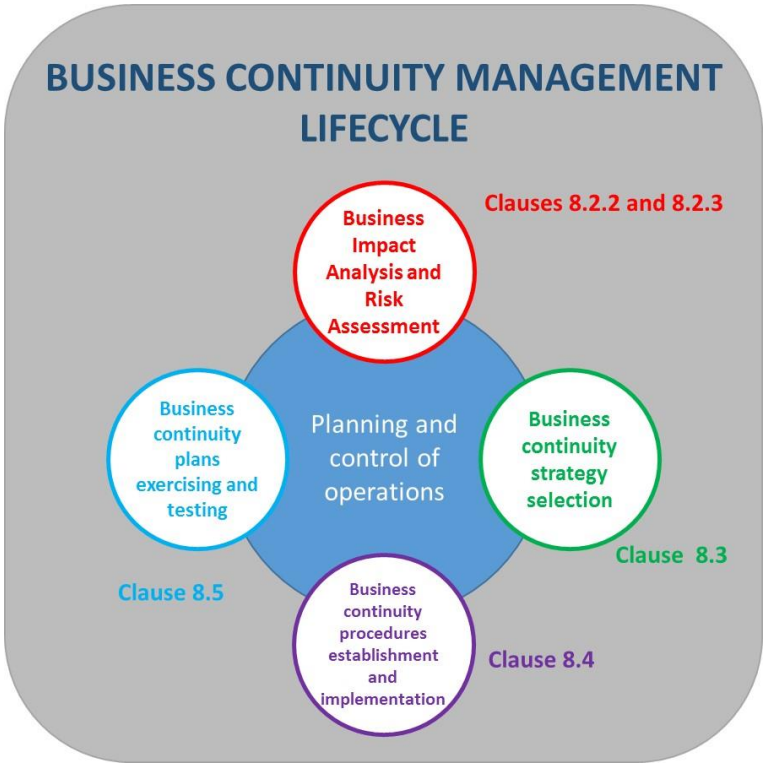
Business continuity management: a management process that covers the identification of situations that may have a high negative impact on business operations, and the implementation of capabilities to properly respond to them and protect the interest of the business and other relevant interested parties (e.g., customers, employees, etc.).

Business Impact Analysis (BIA): a process that helps to identify the effects that a disruption situation can have on business activities.

Business continuity plan: a set of procedures and instructions to guide an organization during and after a disruption event, to speed up immediate response, recovery, and resumption of minimum operational conditions, and restoration of normal operations.

2. Process approach impact

Compliance with the ISO 22301:2012 standard is mandatory for certification, but compliance alone doesn't guarantee the capacity of an organization to respond to and survive a disruptive incident. Using the process approach is useful to create a link between requirements, policies, objectives, performance, and actions. As we can see in the following diagram, a process approach is a good way to organize and manage business continuity activities to create value for an organization and other interested parties.



So, by adopting a process approach for business continuity, an organization can have a better view of how each step contributes to the main objectives of enduring and surpassing a disruptive incident, allowing it to quickly identify problematic points in performing the process.

3. The Plan-Do-Check-Act cycle

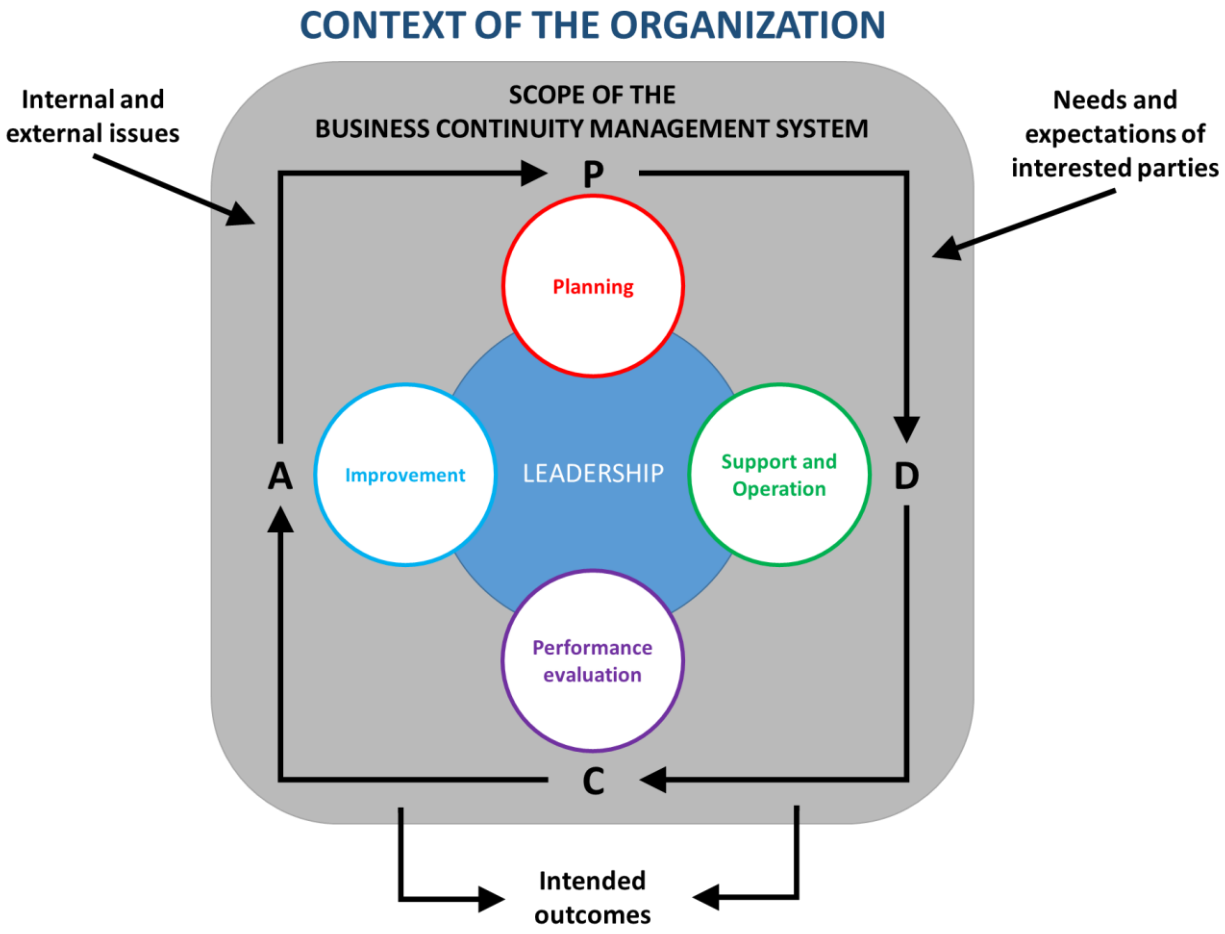
Because any business is a living thing, changing and evolving due to internal and external influences, it is necessary that the Business Continuity Management System (BCMS) also be capable of adjusting itself (e.g., its objectives and procedures) to follow business changes and remain relevant and useful. The ISO 22301:2012 standard ensures that this condition is achieved by adopting a "Plan-Do-Check-Act" cycle (PDCA) in its framework, which can be described as follows:

Plan: the establishment of policies, objectives, targets, controls, processes, and procedures related to business continuity, which support the delivery of results aligned with the organization's core business.

Do: the implementation and operation of the planned processes.

Check: the monitoring, measuring, evaluation, and review of results against the business continuity policy and objectives, so corrective and/or improvement actions can be determined and authorized.

Act: the performing of authorized actions to ensure that the BCMS delivers its results and is improved upon.



It should be noted that the PDCA cycle is a globally recognized management system methodology that is used across various business management systems, but its use is both compulsory and highly beneficial within ISO 22301:2012.

4. Context of the organization

4.1 Understanding the organization and its context

This clause requires the organization to determine all internal and external issues that may be relevant to its business purposes and to the achievement of the objectives of the BCMS itself. This includes all elements that affect, or may be affected by, potential disruptive incidents.

4.2 Understanding the needs and expectations of interested parties

The standard requires the organization to assess who the interest parties are in terms of its BCMS, what their needs and expectations may be, which legal and regulatory requirements are applicable, and consequently, if any of these should become compliance obligations. Legal and regulatory requirements must be documented, kept updated, and communicated to all interested parties.

Tip: For more information on this topic, see the article How to identify interested parties according to ISO 27001 and ISO 22301.

4.3 Determining the scope of the business continuity management system

The scope and boundaries of the BCMS must be examined and defined considering the internal and external issues, interested parties, their needs and expectations, as well as legal and regulatory compliance obligations.

Additional required considerations for the BCMS scope are: products, services, and organizational size, nature, and complexity. The scope and justified exclusions must be kept as “documented information.”

4.4 Business continuity management system

The standard indicates that a BCMS should be established and operated and, by using interacting processes, be controlled and continuously improved.

5. Leadership

5.1 Leadership and commitment

Top management and line managers with relevant roles in the organization must demonstrate genuine effort to engage people to support the BCMS.

For more information on this topic, please see the article Roles and responsibilities of top management in ISO 27001 and ISO 22301.

5.2 Management commitment

This clause provides many examples of top management commitment with enhanced levels of leadership, involvement, and cooperation in the operation of the BCMS, by ensuring aspects like:

- business continuity policy and objectives alignment with each other, and with the strategic policies and overall direction of the business
- business continuity activities integration with other business systems, where applicable
- provision for resources so the BCMS can be operated efficiently
- definition of business continuity responsibilities to people within the BCMS, and their correct support, training, and guidance to complete their tasks effectively
- relevant, proper, and timely communication with both internal and external interested parties
- support of the BCMS during all its lifecycle, considering a PCDA approach

5.3 Policy

Top management has the responsibility to establish a business continuity policy, which is aligned to the organization's purpose, provides a framework for setting business continuity objectives, including a commitment to attend applicable requirements and, with the BCMS, continual improvement and its results. The business continuity policy must be maintained as documented information, be

communicated within the organization, be available to all interested parties, and be periodically reviewed, or when significant changes occur in the organizational context.

For more information on this topic, please see the article The purpose of Business continuity policy according to ISO 22301.

5.4 Organizational roles, responsibilities and authorities

The standard states that it is the responsibility of top management to ensure that roles, responsibilities, and authorities are delegated and communicated effectively. The responsibility shall also be assigned to ensure that the BCMS meets the terms of the ISO 22301:2012 standard itself, and that the BCMS performance can be accurately reported to top management.

For more information on this topic, please see the article The challenging role of the ISO 22301 BCM Manager.

6. Planning

6.1 Actions to address risks and opportunities

Before the ISO 22301 standard, the most widely used reference for Business Continuity Management Systems was BS 25999-2. In fact, ISO 22301 was mostly based on BS 25999-2, and this clause 6.1 seeks to replace the "preventive action" stated in BS 25999-2. The organization must plan actions to handle risks and opportunities relevant to the context of the organization (section 4.1) and the needs and expectations of interested parties (section 4.2), as a way to ensure that the BCMS can achieve its intended outcomes and results, prevent or mitigate undesired consequences, and continuously improve.

For more information on this topic, please see the article ISO 22301 vs. BS 25999-2 – An Infographic.

6.2 Business continuity objectives and plans to achieve them

Business continuity objectives should be established and communicated at appropriate levels and intervals, having considered the alignment with the business continuity policy, minimum levels of delivery of products and services, and compliance obligations.

They must be thought of in terms of what needs to be done, when it needs to be done by, what resources are required to achieve them, who is responsible for the objectives, and how results are to be measured and evaluated, to ensure objectives are being achieved and can be updated when circumstances require.

Again, it is mandatory that documented information is kept outlining the business continuity objectives.

For more help with business continuity objectives and how to plan and achieve them, please see the article Setting the business continuity objectives in ISO 22301.

7. Support

7.1 Resources

No mystery here, the standard states that resources required by the BCMS to achieve stated objectives and show continual improvement must be made available by the organization.

7.2 Competence

The competence of people given responsibility for the BCMS who work under the organization's control must meet the terms of the ISO 22301:2012 standard, to ensure they are capable and confident. Competence can be demonstrated by experience, training, and/or education regarding the assumed tasks. When the competence is not enough, training must be identified and delivered, as well as measured to ensure the required level of competence was achieved. This is also another aspect of the standard that must be kept as documented information for the BCMS.

For more help with business continuity training, please see the article How to perform training & awareness for ISO 27001 and ISO 22301.

7.3 Awareness

Awareness is closely related to competence in the standard. People who work under the organization's control must be made aware of the business continuity policy and its contents, what their personal performance means to the BCMS and its objectives, what the implications of nonconformities may be to the BCMS, and which roles they must perform during disruptive incidents.

7.4 Communication

Processes for internal and external communication need to be established and recorded as documented information within the BCMS. The key elements that need to be decided, actioned, and recorded are what needs to be communicated, when it should be done, and who needs to receive the communication.

Internal and external communication processes should consider the involvement of all relevant interested parties, the availability of communication resources during disruptive events, and the operation and testing of those communication resources meant to be used only during disruptive incidents that impact the normal communication channels.

7.5 Documented information

7.5.1 General

"Documented information," which you will see mentioned several times during this white paper, now covers both the "documents" and "records" concepts seen in the previous revision of the ISO 22301 standard.

This change is designed to facilitate the management of documents and records required by the standard, as well as those viewed as critical to the BCMS and its operation. It should also be noted that the amount and coverage of documented information that an organization requires will differ, according to its size, operating sector, and complexity of processes and their interrelations.

7.5.2 Creating and updating

The standard requires that documented information created or updated in the scope of the BCMS must be properly identified and described, also considering its content presentation, and media used. All documented information must go under proper review and approval procedures to ensure it is fit for purpose.

7.5.3 Control of documented information

The standard states that documented information required by the BCMS, either from internal or external origin, must be available and fit for use where and when needed, and reasonably protected against damage or loss of integrity and identity.

For a proper control of documented information, the organization must consider for them the provision of processes regarding the distribution, retention, access, usage, retrieval, preservation and storage, control, and disposition.

It should also be noted that there must be controls in place to prevent the unintentional use of obsolete information.

To learn more about this topic, please see the article Mandatory documents required by ISO 22301.

8. Operation

8.1 Operational planning and control

To ensure that risks and opportunities are treated properly (clause 6.1), and that the standard's requirements are fulfilled, a BCMS must define clear criteria to plan, implement, and control its processes, as well as any relevant outsourced process, effectively implement those controls, and retain documented information deemed to be necessary to provide confidence the processes are being performed and achieving their results as planned.

Being focused on keeping the delivery of products and services, the BCMS also should consider in its planning and control the monitoring of planned changes, and impact analysis of unexpected changes, to be able to take actions to mitigate adverse effects if necessary.

8.2 Business impact analysis and risk assessment

8.2.1 General

The standard requires that adverse impacts to the organization's products, services, and operations must be systematically analyzed and treated, considering criteria to define potential disruption events, business, legal and other requirements the organization must fulfill, the main risks to be treated, and strategies to be followed.

Because the resulting information reveals the organization's potential vulnerabilities and drives the main decisions about resources allocation, the organization must also define controls to prevent its unauthorized disclosure and to ensure it is kept updated.

8.2.2 Business impact analysis

The standard recognizes that organizations' resources are not infinite, and that they play an even more critical role during disruptive events, so it requires their BCMS to have means, kept as documented information, to systematically identify continuity and recovery priorities and define objectives and goals to be achieved, in terms of minimal acceptable performance and time to achieve those.

These priorities, objectives, and goals should be identified considering how activities, resources, and dependencies that support the delivery of the organization's products and services are impacted by potential disruptive events.

To learn more about this topic, please see the article How to implement business impact analysis (BIA) according to ISO 22301.

8.2.3 Risk assessment

To help support a business impact analysis, an organization's BCMS must have in place, as documented information, a risk assessment process to identify, analyze, evaluate, and treat risks that may lead to disruptive situations. The risk assessment and treatment criteria must consider business continuity objectives and the organization's risk appetite.

To learn more about this topic, please see the article Risk assessment vs. business impact analysis.

8.3 Business continuity strategy

8.3.1 Determination and selection

The overall way an organization outlines its business continuity strategy must consider the business continuity analysis results and cover the protection, stabilization, continuity, resume and recovery of priority activities, and the mitigation, response, and management of impacts resulting from a disruptive event. During the business continuity strategy definition and selection activities, interdependencies and support resources must also be considered.

To learn more about this topic, please see the article Can business continuity strategy save your money?

8.3.2 Establishing resources requirements

To support business continuity strategies, the organization must define needed resources, like people, information and data, buildings and facilities, equipment and consumable resources, transportation, suppliers and partners.

8.3.3 Protection and mitigation

Considering its risk appetite, the organization must consider protective and mitigation controls to minimize disruption probabilities, disruption duration, and the impact of disruptions over products and services.

8.4 Establish and implement business continuity procedures

8.4.1 General

To ensure activities' continuity and incident management in line with the recovery objectives identified during the business impact analysis, an organization must establish, implement, maintain, and document business continuity procedures.

The procedures must cover external and internal communication and specific measures to be taken during a disruption, with focus on the disruption impacts. They also must be flexible enough to handle unforeseen threats and changes in internal and external issues.

To learn more about this topic, please see the article Activation procedures for business continuity plan.

8.4.2 Incident response structure

To effectively respond to a disruption, ISO 22301:2012 requires an organization to have in place procedures and people, with proper authority and competence, to manage incidents, considering the incident identification, impact nature and extension evaluation, and activation of proper continuity response, including communications with relevant interested parties.

Processes and procedures must be documented, and resources to support them must be available.

To learn more about this topic, please see the article Incidents in ISO 22301 vs. ISO 27001 vs. ISO 20000 vs. ISO 28003.

8.4.3 Warning and communication

Besides procedures to handle incidents (clause 8.4.2), an organization's BCMS must have in place procedures to detect real and potential incidents, and manage communication with interested parties, internal and external, including risk warning systems.

The procedures must be defined in such a way that they can provide timely alerts to interested parties impacted by a disruptive event, real or imminent, ensure communication availability during disruptive

events, and facilitate communication with emergency teams. All people related to these procedures must be regularly exercised on

Information relative to incidents, actions, and decisions must be stored.

8.4.4 Business continuity plan

In this clause, the standard states that the organization must plan to take actions to respond to disruptive incidents, ensure operations continuity and recovery within defined objectives and goals, and fulfill additional requirements from those who will use it.

The business continuity plan is a key element to ensure business continuity, and a number of elements should be covered, like roles, responsibilities, and authorities to be performed during and after an incident, a process to activate the incident and response structure, activities to manage immediate impacts, the communication flow with interested parties, and the continuity and recovery activities.

To learn more about this topic, please see the article Business continuity plan: How to structure it according to ISO 22301.

8.4.5 Recovery

Surviving a disruptive event is only half the story. ISO 22301:2012 also requires a BCMS to have, as documented procedures, the activities needed to restore and return business activities from temporary conditions, defined as achieving the minimum performance levels agreed upon for a situation of "business as usual," operating under normal conditions.

8.5 Exercising and testing

Business continuity procedures must be systematically and periodically exercised and tested to ensure they are fit for purpose, updated, and compatible with continuity objectives.

All planned exercises and tests must be aligned with the BCMS scope and objectives, considering possible scenarios, the information that must be recorded to provide data for exercising and testing critical review, so the accuracy of the planned actions and the interactions between interested parties can be evaluated, as well as the plans' capability to achieve their defined objectives, increasing confidence on planning effectiveness or collaborating for continual improvement by correction of vulnerabilities or implementation of improvements.

To learn more about this topic, please see the article How to perform business continuity exercising and testing according to ISO 22301.

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

The organization not only has to establish and evaluate performance metrics regarding the effectiveness and efficiency of the processes, procedures, and functions that protect its most critical activities, but should also consider metrics for the BCMS performance, regarding compliance with the standard, preventive actions in response to adverse trends, and the degree to which the business continuity policy, objectives, and goals are being achieved.

The methods established should have considerations about what needs to be monitored and measured, how to ensure the accuracy of results, and periods to perform the monitoring, measurement, analysis, and evaluation of BCMS data and results. It should also be noted that performance results should be properly retained as evidence of compliance and as a source to facilitate subsequent corrective actions.

9.1.2 Evaluation of business continuity procedures

The standard recognizes the importance of planned periodic evaluations of business continuity procedures, through exercises, tests, and post-incident reviews, to ensure they are continuously effective, up to date, and fit for purpose to handle the level of risk faced by all key products and services identified. The procedures should also be reviewed regarding compliance with legal and regulatory requirements, as well as their alignment with the business continuity policy and objectives, not only at planned intervals, but after significant changes, so timely adjustments can be made.

9.2 Internal audit

Internal audits should be performed at planned intervals, considering the processes' relevance, and results of previous audits, to ensure compliance with the standard's requirements and the requirements defined by the organization itself.

Auditors should be independent and have no conflict of interest over the audit subject, report the audit results to the standard reminds us, and it should be noted that non-conformities should be submitted to the responsible managers, who must ensure that any corrective measures needed are implemented in a timely manner. The auditor must also verify the effectiveness of corrective actions taken.

To learn more about this topic, please see the article How to make an Internal Audit checklist for ISO 27001 / ISO 22301.

9.3 Management review

The management review exists so the BCMS can be kept continuously suitable, adequate, and effective to support the business continuity.

It must be performed at planned intervals, in a strategic and top management level, covering the required aspects all at once or by parts, in a way that is most suitable to business needs.

The status of actions defined in previous reviews, significant internal and external factors that may impact the BCMS, business continuity performance, and opportunities for improvement should be reviewed by top management, so relevant adjustments and improvement opportunities can be implemented.

The management review is the most relevant function to the continuity of a BCMS, because of the top management's direct involvement, and all details and data from the management review must be documented and recorded to ensure that the BCMS can follow the specific requirements and general strategic direction for the organization detailed there.

Tip: For more details on this topic, please see the article Why is management review important for ISO 27001 and ISO 22301?.

10. Improvement

10.1 Nonconformity and corrective action

Outputs from management reviews, internal audits, and compliance and performance evaluation should all be used to form the basis for nonconformities and corrective actions. Once identified, a nonconformity or corrective action should trigger, if considered relevant, proper and systematic responses to mitigate its consequences and eliminate root causes, by updating processes and procedures, to avoid recurrence.

The effectiveness of actions taken must be evaluated, and documented along with the originally reported information about the nonconformity / corrective action and the results achieved.

For more detail on this subject, please take a look at the article Practical use of corrective actions for ISO 27001 and ISO 22301.

10.2 Continual improvement

Continual improvement is a key aspect of the BCMS, to achieve and maintain the suitability, adequacy, and effectiveness of the business continuity effort as it relates to the organization's objectives.

For more detail on this subject, please take a look at the article The blessing of continuous improvement in ISO 22301.

Conclusion

ISO 22301:2012 provides organizations with guidance to manage, mitigate, and recover from disruptive incidents with the ultimate goal of business survival, but delivering all of the clauses of the standard and truly understanding them can benefit your organization in many ways. Accreditation and compliance can bring reputational, motivational, and financial benefits to your organization, bringing customers who have greater confidence that you can deliver products and services at agreed performance levels, along with improvements in your supply chain. All of these elements are closely related to your organization's ability to deliver satisfaction to your customers, and fulfill the expectations and wishes of your stakeholders, while protecting the organization's capacity for doing business in the long run. Bearing all this in mind, can your organization afford not to have ISO 22301:2012?

Sample of documentation templates or toolkits

You can download a free preview of our ISO 22301/BS 25999 Documentation Toolkit, which will allow you to view samples of the toolkit available to help you to implement ISO 22301:2012 without the assistance and cost of external consultancy.

References

27001Academy

International Organization for Standardization

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

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

Email: support@advisera.com
Phone: +1 (646) 759 9933
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Fax: +385 1 556 0711

EXPLORE **ADVISERA**

27001 Academy · 9001 Academy · 14001 Academy · 18001 Academy · 20000 Academy

Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple.