ISO 22301:2019

BUSINESS CONTINUITY STANDARD IMPLEMENTATION GUIDE

nqa.

> ISO 22301:2019

IMPLEMENTATION GUIDE

Contents

INTRODUCTION TO THE STANDARD

ISO 22301:2019 is the latest version of the international standard for Business Continuity Management Systems. This standard provides a best practice framework to support organizations to effectively manage the impact of a disruption to its normal operation.

The purpose of the standard is not necessarily to achieve total mitigation of impact from disruption. It is to support an organization to understand the amount and type of impact it is willing to accept following a disruption. Following which the organization develops a business continuity system sized correctly for the organizational need.

Many organizations will at some point experience a business disruption. The cause and nature of disruptive events is ever-changing. Organizations need to be able to think dynamically about this changing threat landscape and put in place appropriate plans to mitigate impacts.

The ISO 22300 Family

Origin of the ISO 22301 standard heralds back to the ISO technical committee ISO/TC 23, which focussed on addressing concerns related to societal security. The standard is now managed by ISO/TC 292 - Security and Resilience. The first iteration of the ISO 22301 standard was published in 2012. The second edition was published in October 2019 and is the focus of this implementation guide.

There are currently 11 standards in the ISO 22300 series. The other standards in the series provide more detailed guidance and requirements for specific issues related to business continuity. This ranges from emergency response management through to mass evacuations.

Regular Reviews and Updates

ISO standards are subject to review approximately every five years to assess whether an update is required.

The most recent update to the ISO 22301 standard in 2019 brought about a number of changes. Whilst previous edition (2012) was one of the forerunner standards in adopting an Annex SL type format, the new edition firmly aligns the standard with Annex SL.

The 2019 version of the standard is reflective of the broader movement of ISO standards towards the application of risk based thinking, understanding organizational context and satisfying the needs of interested parties. The 2019 version contains less prescriptive requirements and is more flexible in its approach to documented information. The 2019 version additionally includes the new requirement to effectively plan changes to the Business Continuity Management System (BCMS).

Within the series, the most important standards for an organization seeking to implement an effective Business Continuity Management System are:

- **ISO 22300:2018 - Security and resilience**
  - Vocabulary
- **ISO 22301:2019 - Security and resilience**
  - Business Continuity Management Systems
  - Requirements
- **ISO 22313:2020 - Security and resilience**
  - Business Continuity Management Systems
  - Guidance. Provides helpful direction in support of the practical implementation and operation of a business continuity system

BENEFITS OF IMPLEMENTATION

It has been demonstrated in recent times that a company's ability to manage disruptive events is becoming central to its survival. The variety of threats which can cause business disruption is ever-increasing. From cyber-attacks and global pandemics to natural disasters; an organization needs a toolset to manage itself through uncertain times.

In the past, business continuity planning tended to be reserved for critical national infrastructure and major corporations. Today, business continuity is an issue that affects practically all organizations to some degree. A correctly implemented Business Continuity Management System should be scaled to the size and complexity of the organization – making it suitable for SME and large corporation alike.

The core purpose of a Business Continuity Management System is to enable the mitigation of a disruption. Depending on the organization the benefits this will work in support of its goals; whether that is to save lives in a hospital or to reduce financial impact to a manufacturing company.

VISIBLE RESILIENCE

An effective BCMS provides evidence to current and potential customers of organizational preparedness for disruption. This is particularly important in sectors where disruption can have significant impacts on people's lives as well as financial impacts; including government, healthcare, financial, defence, social services.

COMPETITIVE ADVANTAGE

Being able to continue to operate during or shortly after a disruption gives a company a competitive advantage. In the short term it may be able to win business from competitors which are unable to operate or are doing so in a diminished capacity. In the longer term, a company can generate reputational benefits that will attract customers as well as benefit from stronger financial capabilities.

In addition, a Business Continuity Management System supports an organization to bid or tender more effectively.

PROTECT ORGANIZATIONAL VALUE

A BCMS helps to mitigate the negative impact of a disruptive event. Practically speaking, this can save the organization significant amounts of money, time and reputational impact.

PEACE OF MIND

The future is uncertain. An effectively implemented BCMS gives an organization confidence to move forward knowing it can manage a disruption. This peace of mind spans the organization from personnel operations teams to board membership.

ENHANCE CYBER SECURITY AND IT FAILURE RESILIENCE

Cyber security and IT disaster planning is high on the agenda of many organizations. A business continuity plan supports a company to manage the impact of the IT disruption. This can be by malicious action or from infrastructure failure. Crypto viruses, DDoS attacks and data centre failures can create deep and long lasting disruption to all functions of an organization.

Cyber security certifications such as ISO 27001 and Cyber Essentials do not fully address continuity challenges in the event of a disruption. The ISO 27001 attempts to address continuity within the IT function itself but this does not extend to the rest of the organization. ISO 22301 provides a framework for addressing the wider organizational impact of IT failure. As a result, a Business Continuity Management System (ISO 22301) is well suited to be integrated with an ISO 27001 information security management system.

High Level View

A Business Continuity Management System operates on similar principles to other management systems. The system is built on the Plan-Do-Check-Act model.

- **Determine the organizational needs and understand the rationale for business continuity plans:**
  - What is important to continue in the event of a disruption
  - Why is that important and to whom?
  - What level of disruption is the organization and its stakeholders prepared to accept?
- **Putting in place a framework for achieving the mitigation of the disruption. This can include:**
  - Processes
  - Capabilities
  - Response structures
- **Check the performance and effectiveness of the system through monitoring. Practically speaking this will involve testing BC plans through various means.**
- **Improve the system based on measures established, revisit the rationale for the business continuity plans and their alignment to what has been implemented.**

One of the practical challenges with BCMS is that it comes into action infrequently. Whilst quality management systems are implemented into the company's day to day operation, business continuity systems are only fully brought into action when a disruption occurs. This means there needs to be a greater emphasis on:

- Business continuity plan (BCP) testing or drills
- Retaining and refreshing organizational capabilities to support business continuity
- Periodic reviews of the system, its processes and rationale to ensure it remains aligned to a changing organization.

KEY PRINCIPLES OF BUSINESS CONTINUITY

Business continuity is grounded in a number of key principles which need to be consistently applied to a business continuity system for it to be effective.

Responsibility

An organization's senior management and board of directors are responsible for business continuity, this responsibility must be understood and accepted. Business continuity management should be an integral component of overall risk management.

In the event of a disruption, the absence of clearly defined responsibilities, authorities and roles can cause a business continuity plan to become ineffective.

Clear Objectives

An organization should have in place clear business continuity objectives that reflect the nature of their activities and their impact on stakeholders. This supports the prioritisation and resource allocation to the business continuity process. These objectives should clearly define the expected continuity levels and continuity times.

Impact and Risk Evaluation

The business continuity standard is different from others in that it focusses on the "what if". The ability to identify and plan for potential business impacts and risks is key to an effective business continuity system.

Communication

Organizations should include within their business continuity plans how and when they will communicate within their organizations, with customers and interested parties (such as regulators or suppliers).

Testing

The Business Continuity Management System should be periodically tested in order to evaluate its effectiveness and make changes as required.

PDCA CYCLE

ISO 22031 is based on the Plan-Do-Check-Act (PDCA) cycle, also known as the Deming wheel or the Shewhart cycle. The PDCA cycle can be applied not only to the management system as a whole but to each individual element to provide an ongoing focus on continuing improvement. In brief:

Plan:

Understand external context and needs of interested parties. Identify risk and opportunity. Establish objectives and resources required.

Do:

Implement what has been planned. From a new Business Continuity Management System down to small process changes.

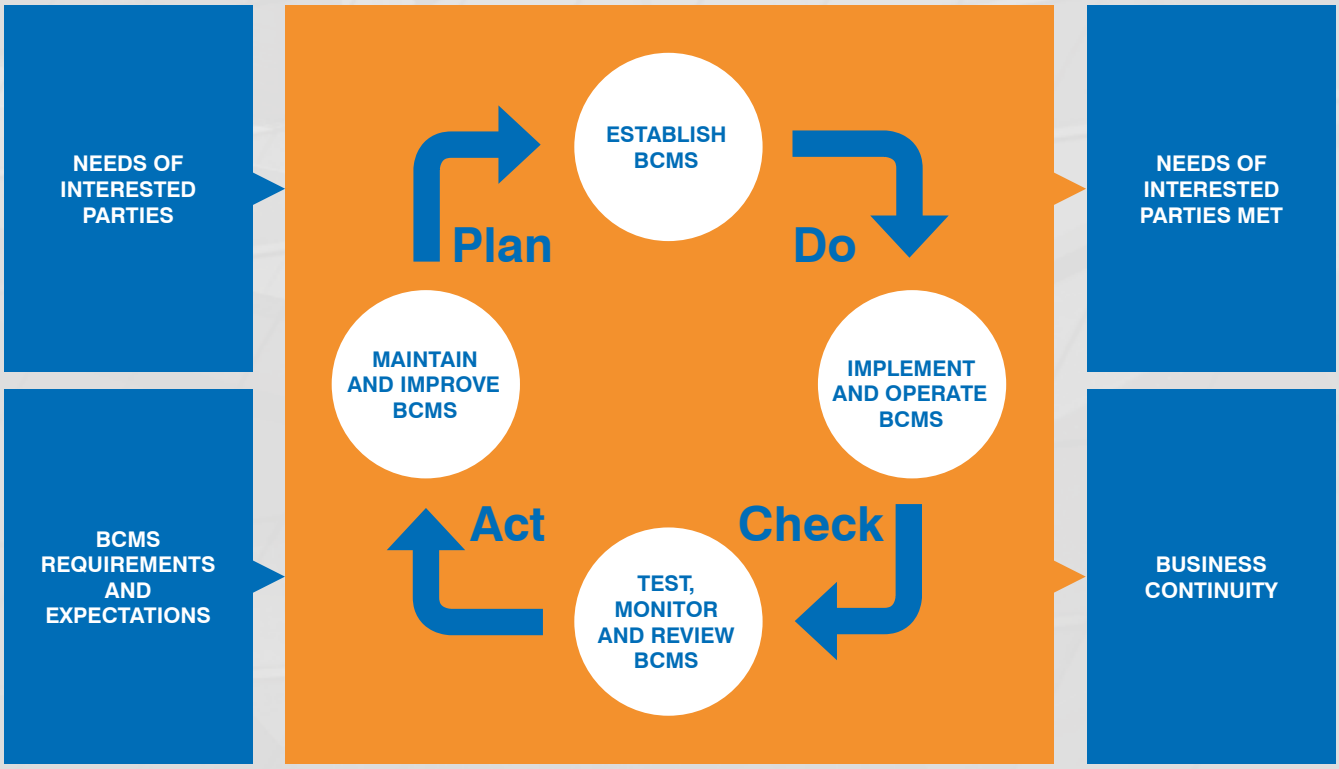
Check:

Monitor and measure the effectiveness of the business continuity. Test business continuity plans and monitor outcomes.

Act:

Take action where necessary based on monitoring, measuring and other drivers for action.

PDCA Model ISO 22301



Plan-Do-Check-Act is an example of a closed-loop system. This ensures the learning from the 'do' and 'check' stages are used to inform the 'act' and subsequent 'plan' stages. In theory this is cyclical, however it's more of an upward spiral as the learning moves you on each time you go through the process.

RISK BASED THINKING/AUDITS

Audits are a systematic, evidence-based, process approach to evaluation of your Business Continuity Management System. They are undertaken internally and externally to verify the effectiveness of the BCMS. Audits are a brilliant example of how risk-based thinking is adopted within Business Continuity Management.

1st Party Audits – Internal Audits

Internal audits are a great opportunity for learning within your organization. They provide time to focus on a particular process or department in order to truly assess its performance. The purpose of an internal audit is to ensure adherence to policies, procedures and processes as determined by you, the organization, and to confirm compliance with the requirements of ISO 22301.

Audit Planning

Devising an audit schedule can sound like a complicated exercise. Depending on the scale and complexity of your operations, you may schedule internal audits anywhere from every month to once a year. There's more detail on this in section 9 – performance evaluation.

Risk-Based Thinking

The best way to consider frequency of audits is to look at the risks involved in the process or business area to be audited. Any process which is high risk, either because it has a high potential to go wrong or because the consequences would be severe if it did go wrong, should be audited more frequently than a low risk process.

How you assess risk is entirely up to you. ISO 22301 doesn't dictate any particular method of risk assessment or risk management.

2nd Party – External Audits

Second party audits are usually carried out by customers or by others on their behalf, or you may carry them out on your external providers. 2nd party audits can also be carried out by regulators or any other external party that has a formal interest in an organization.

You may have little control over the timing and frequency of these audits, however establishing your own BCMS will ensure you are well prepared for their arrival.

3rd Party – Certification Audits

Third party audits are carried out by external bodies, usually UKAS accredited certification bodies such as NQA.

The certification body will assess conformance to the ISO 22301:2019 standard. This involves a representative of the certification body visiting the organization and assessing the relevant system and its processes. Maintaining certification also involves periodic reassessments.

Certification demonstrates to customers that you have a commitment to quality.

CERTIFICATION ASSURES:

- regular assessment to continually monitor and improve processes
- credibility that the system can achieve its intended outcomes
- reduced risk and uncertainty and increase market opportunities
- consistency in the outputs designed to meet stakeholder expectations.

PROCESS BASED THINKING/AUDITS

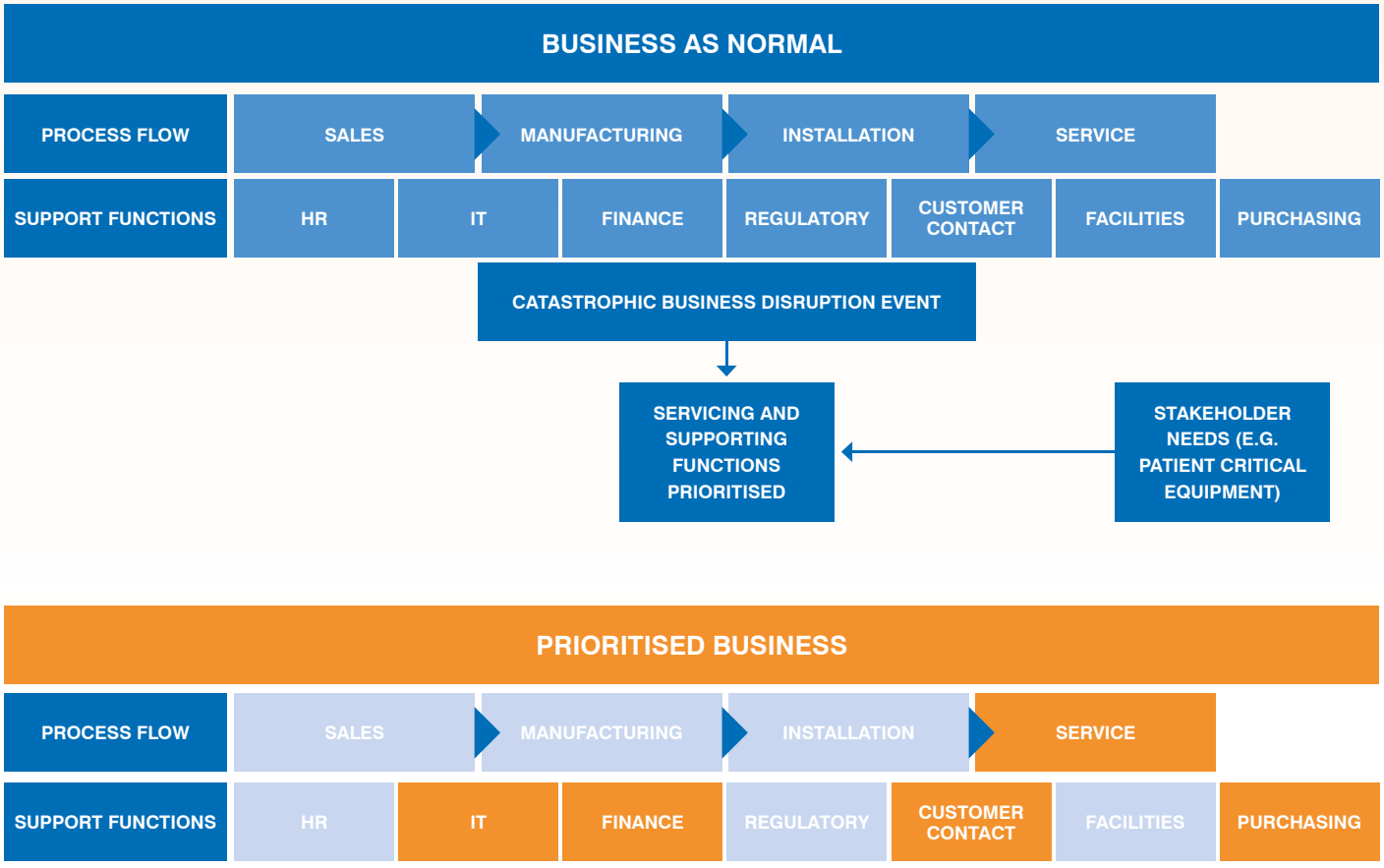
A process is the transformation of inputs to outputs, which takes place as a series of steps or activities which result in the planned objective(s). Often the output of one process becomes an input to another subsequent process. Very few processes operate in isolation from any other.

Process based thinking is critical to business continuity planning. In order to achieve business continuity objectives, an organization has to create business continuity plans which will be process based. Spanning multiple processes and organizational functions.

In practice this means that a business continuity system should consider the end to end process through the organization and incorporate relevant support functions to achieve its objectives.

A business continuity system that is applicable to just one department is not likely to achieve valid continuity objectives.

The diagram below illustrates how an organization could consider prioritising its business continuity objectives through its business continuity strategy. In the example below, an organization providing critical healthcare equipment prioritises its servicing activity and key support functions after a major disruptive event.

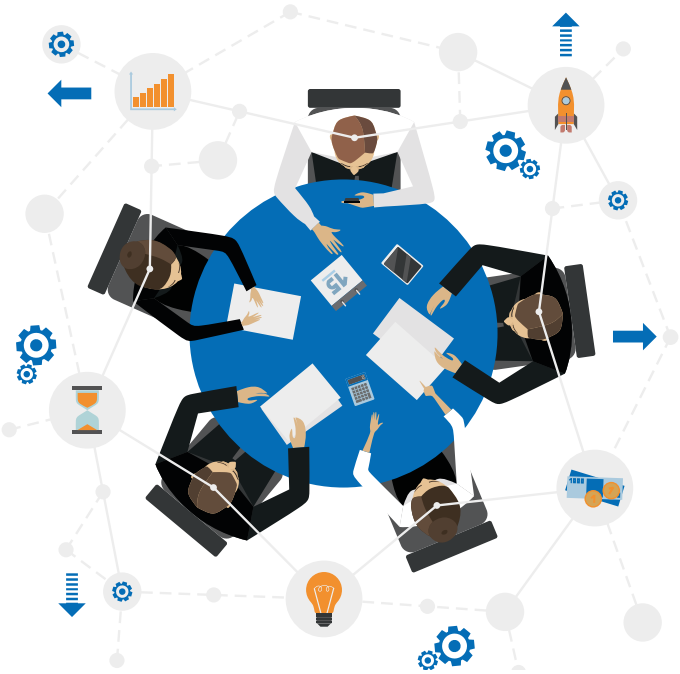


ANNEX SL

One of the major changes introduced into the 2019 revision of ISO 22301 was the adoption of Annex SL for the clause structure of the revised standard. Annex SL (previously known as ISO Guide 83) was used within ISO by standards writers to provide a common core structure for management system standards.

ISO 22301 (Business Continuity Management Systems) adopted this structure during its 2019 revision. ISO 27001 (Information Security Management System Standard) also adopted this structure during its 2013 revision as well as ISO 14001 (Environmental Management System Standard) which adopted this structure during its 2015 revision. The newly published ISO 45001 (Health and Safety Management System Standard) also follows this same common structure.

Prior to the adoption of Annex SL there were many differences between the clause structures, requirements and terms and definitions used across the various management system standards. This made it difficult for organizations to integrate the implementation and management of multiple standards; Environment, Quality, Health and Safety and Information Security being among the most common.



High Level Structure

Annex SL consists of 10 core clauses:

1. Scope
2. Normative References
3. Terms and Definitions
4. Context of the Organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance Evaluation
10. Improvement

Of these clauses, the common terms and core definitions cannot be changed. Requirements may not be removed or altered, however discipline-specific requirements and recommendations may be added.

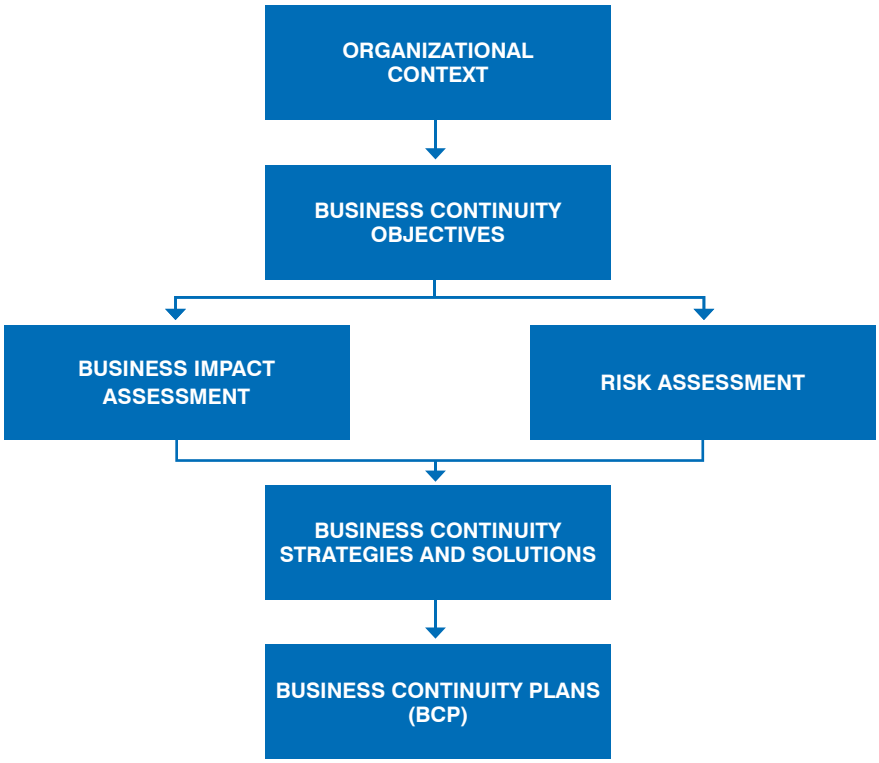
All management systems require a consideration of the context of the organization (more on this in section 4); a set of objectives relevant to the discipline, in this case quality, and aligned with the strategic direction of the organization; a documented policy to support the management system and its aims; internal audits and management review. Where multiple management systems are in place, many of these elements can be combined to address more than one standard.

THE 10 CLAUSES OF ISO 22301:2019

ISO 22301 is made up of 10 sections, known as clauses.

As with most other ISO management system standards, the requirements of ISO 22301 that need to be satisfied are specified in Clauses 4.0 – 10.0. Similar to ISO 27001, the organization must comply with all of the requirements in Clauses 4.0 – 10.0; they cannot declare one or more clauses as being not applicable to them.

The diagram to the right provides an illustrative flow of the concepts in the standard:



CLAUSE 1: SCOPE

The Scope Section of ISO 22301 Sets Out:

- the purpose of the standard
- the types of organizations it is designed to apply to
- the sections of the standard (called Clauses) that contain requirements that an organization needs to comply with in order for the organization to be certified as "conforming" to it (i.e. being compliant).

ISO 22301 is designed to be applicable to any type of organization. Regardless of size, complexity, industry sector, purpose or maturity, any organization can implement and maintain a BCMS that complies with ISO 22301.

CLAUSE 2: NORMATIVE REFERENCES

In ISO standards, the normative references section lists any other standards that contain additional information that is relevant to determining whether or not an organization complies with the standard in question. In ISO 22301 only one document is listed – ISO 22300, Security and Resilience – Vocabulary.

Some of the terms used or requirements detailed in ISO 22301 are explained further in ISO 22300. Reference to ISO 22300 is very useful in helping you to understand a requirement better or identify the best way to comply with it.

TIP – External auditors will expect you to have taken the information contained in ISO 22300 into account in the development and implementation of your BCMS.

CLAUSE 3: TERMS AND DEFINITIONS

There are 31 terms and definitions given in ISO 22301 and reference is made to the most current version of ISO 22300 Security and Resilience –Vocabulary. The current version of this document contains 277 definitions of terms that are used in ISO 22301.

In addition to the terms explained in the "Key Principles and Terminology" section above, the most important terms used in ISO 22301 are:

'Business Continuity'

– capability of an organization to continue the delivery of product or services at acceptable predefined levels following a disruption.

'Business Continuity Management'

– holistic management process that identifies potential threats to an organization and the impact those threats, if realised, can cause on business operations, and provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of key interested parties, reputation, brand and value-creating activities.

'Business Continuity Plan'

– documented procedures that guide an organization to respond, recover, resume and restore itself to a pre-defined level of operation following a disruption.

'Business Impact Analysis'

– process of analysing activities and the effect that a business disruption can have upon them.

'Crisis Management Team'

– group of individual functionality responsible for directing the development and execution of the response and operational continuity plan, declaring and operational disruption or emergency crisis situation, and providing direction during the recovery process, both pre- and post-disruptive incident.

'Disruption'

– event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), that cause an unplanned, negative deviation from the expected delivery of products or services according to an organizations objectives.

'Invocation'

– act of declaring that an organizations business continuity arrangements need to be put into effect in order to continue delivery of key products or services.

'Maximum Tolerable Period of Disruption (MTPD)'

– time it would take for adverse impacts, which can arise as a result of not providing a product/service or performing an activity, to become unacceptable.

'Minimum Business Continuity Objective (MBCO)'

– minimum level of services and/or products that is acceptable to an organization to achieve its business objectives during a disruption.

'Recovery Point Objective (RPO)'

– point to which information used by an activity is restored to enable the activity to operate on resumption.

'Recovery Time Objective (RTO)'

– period of time following and incident within which a product or service or an activity is resumed or resources are recovered.

When you write your Business Continuity Management System documentation, you don't have to use these exact terms. However, it does help to clarify the meaning and intention if you can define the terms you have used. Providing a glossary within your system documentation may be useful.

CLAUSE 4: CONTEXT OF THE ORGANIZATION

The purpose of a BCMS is to enable an organization to effectively respond to a disruptive incident and to continue delivery of key products and services at a pre-defined level, until the resumption of normal operations.

Internal Context

The following are examples of the areas that should be considered when assessing the internal issues that may have a bearing on the BCMS:

- **Maturity:** are you an agile start-up with a blank canvas to work on, or a 30+ year old institution with well-established processes and contingency plans?
- **Organization culture:** is your organization relaxed about how, when and where people work, or extremely regimented?
- **Dependencies:** what are the internal dependencies that you require to respond effectively to the disruptive incident (IT Services, power, equipment)?
- **Management:** are there clear communication channels and processes from the organization's key decision makers through to the rest of the organization?
- **Resource size:** are you working with a limited amount resources, personnel and equipment?
- **Resource maturity:** are the available resources (employees/ contractors) knowledgeable, fully trained, dependable and consistent, or are personnel inexperienced and constantly changing?
- **Consistency:** do you have uniform processes in place across the organization, or a multitude of different operating practices with little consistency?
- **Equipment:** do you require specialist equipment.

External Context

The following are examples of the areas that can be considered when assessing the external issues that may have a bearing on the BCMS:

- **Landlord:** do you need approval to upgrade physical security?
- **Suppliers:** are your suppliers able to provide you with suppliers on time?
- **Regulators / enforcement bodies:** are there any regulatory or statutory requirements that you need to consider when developing your BCMS? Do you need to inform them that you've invoked your BCP?
- **Economic/political:** do currency fluctuations impact your organization?
- **Dependencies:** what are the external dependencies that you require to respond effectively to the disruptive incident (IT Services, supplies, power, equipment)?
- **Environmental considerations:** are there any environmental issues that may impact on your BCMS?
- **Customers:** what impact will the invocation of your BCMS have on your customers? Do you need to inform them that you've invoked your BCP?
- **Shareholders:** are they very concerned about your organizations ability to respond to a disruptive incident?

Interested Parties

An interested party is anyone who can be affected by the invocation of your BCP. Your interested parties will become clear through the process of carrying out a thorough analysis of internal and external issues. They are likely to include shareholders, landlords, regulators, customers, employees, suppliers and may extend to the general public and the environment, depending on the nature of your business. You don't have to try to understand or satisfy their every need, but you do have to determine which of their needs and expectations are relevant to your BCMS.

Legal and Regulatory

Identify and keep up to date with any legal and regulatory requirements related to the continuity of your products and services, activities and resources when implementing and maintaining your BCMS.

- **Document:** document your legal, regulatory and other compliance requirement and your approach to meeting those requirements.

Scope of the Management System

To comply with ISO 22301, you must document the scope of your BCMS. Documented scopes typically describe:

- the boundaries of the physical site or sites included (or not included)
- the internal and external employee groups included (or not included)
- the internal and external processes, activities, products or services included (or not included)
- key interfaces at the boundaries of the scope.

If you want to prioritise resources by building a BCMS that doesn't cover all of your organization or its activities, selecting a scope that is limited to managing key stakeholder interests is a pragmatic approach. This can be done by including only specific sites, assets, processes, products and business units or departments.

TIP – Document or maintain a file of all of the information collated in your analysis of your organization's context and interested parties such as:

- Discussions with a senior representative of the organization, e.g. an MD, CEO or CTO
- Minutes of meetings or business plans
- A specific document that identifies internal/external issues and interested parties and their needs and expectations e.g. a SWOT analysis, PESTLE study, or high-level business risk assessment.

CLAUSE 5: LEADERSHIP

Leadership Commitment

Leadership in this context means active involvement in setting the direction of the BCMS, promoting its implementation; highlighting its importance and ensuring appropriate resources are made available.

- ensuring that the business continuity policy and business continuity objectives are established and aligned with the strategic direction of the organization
- ensuring the integration of the BCMS requirements into the organizations business practices
- ensuring that the BCMS is adequately resourced
- communicating the importance of business continuity and conforming to the requirements of the BCMS
- ensuring the BCMS achieves its intended outcomes
- directing and supporting persons to contribute to the effectiveness of the BCMS
- promoting continual improvement
- supporting other managerial roles to demonstrate their leadership and commitment.

ISO 22301 places great importance on active engagement by top management in the BCMS, based on the assumption that the engagement of top management is crucial in ensuring the effective implementation, maintenance and continual improvement of an effective BCMS by the wider employee group.

Business Continuity Policy

A vital responsibility of the leadership is to establish and document a Business Continuity Policy that is aligned to the strategic direction of the organization. BCMS requirements should be integrated in business processes and adequately resourced.

The policy shall:

- be appropriate for the purpose of the organization
- provide a framework for setting business continuity objectives
- includes a commitment to satisfy applicable requirements
- includes a commitment to continual improve the BCMS
- be communicated with the organization
- be available to interested parties as appropriate.

The Business Continuity Policy may refer to, or include sub-policies that cover, key processes and activities that are important to the continued provision of key products and services in the event of a disruptive incident and recovery to normal operations. To demonstrate the importance of the Business Continuity Policy it should be authorised by Senior Management.

TIP - To ensure your Business Continuity Policy is well communicated and available to interested parties, it is a good idea to:

- include it in induction packs and presentations for new employees and contractors
- post the key statement on internal noticeboards, intranets and your organization's website
- make compliance with it and/or support for it a contractual requirement for employees, contractors and critical suppliers.

Roles and Responsibilities

Roles and responsibilities for Business Continuity shall be established, assigned and communicated within the organization.

Responsibility shall be assigned for:

- ensuring that the BCMS conforms to the requirement of the standard
- reporting on the performance of the BCMS to top management.

For business continuity to form part of day to day activities, the business continuity responsibilities and accountabilities of all personnel are to be defined, understood and communicated.

Evidencing Leadership to an Auditor

Top management are the group of individuals who set the strategic direction of an organization and approve the allocations of resources to the organization or business area within the scope of your BCMS. Depending on the size and how your organization is structured, these individuals may or not be the day-to-day management team.

An auditor will typically test leadership commitment by interviewing one or more members of your top management and assessing their level of involvement and participation in the:

- evaluation of risks and opportunities
- establishment and communication of policies
- setting and communication of objectives
- review and communication of system performance
- allocation of appropriate resources, accountabilities and responsibilities.

TIP – Before your external audit, identify who from your top management will meet with the external auditor and prepare them for the interview with a dry run-through of the likely questions they will be asked.

CLAUSE 6: PLANNING

When planning its BCMS an organization needs to take into consideration the risks and opportunities identified when determining the context of the organization and scope of the BCMS. The organization needs to determine which risks and opportunities need to be addressed in order to:

- **provide assurance that the BCMS can achieve its intended outcomes**
- **prevent or reduce undesired effects**
- **achieve continual improvement**

Addressing Risk and Opportunities

An organization shall establish a methodology for assessing risks and opportunities that impact on the ability of the BCMS to achieve its intending outcomes and determine the action required address the risk and opportunities.

An organization shall:

- identify actions to address risks and opportunities
- implement the actions identify
- evaluate the effectiveness of these actions.

Business Continuity Objectives (and Planning to Achieve Them)

Business continuity objects need to be established at relevant functions and levels within an organization; objectives can be at an organizational or departmental level.

Objectives must be:

- consistent with the Business Continuity Policy
- be measurable
- take account of applicable requirement
- communicated
- monitored and updated as appropriate.

Objectives are to be communicated to relevant persons within the organization; be monitored and updated as required.

Achieving Objectives

An organization should establish a plan for achieving its objectives; the plan should take into consideration:

- what needs to be done
- the resources required
- who is responsible
- the date of completion; and
- how to evaluate the results.

Changes to the BCMS

It is likely that over time an organizations process, activities, products and services will change. As a result you will need to make changes to your BCMS, changes are to be conducted in a planned manner and should take into consideration:

- the purpose of the change and its potential consequences
- the integrity of the BCMS
- availability of resources
- re-allocation of responsibilities and authorities.


IDEA
SUCCESS
INCOME
Product
IDEA
MONEY
Business
SUCCESS
IDEA
MONEY

CLAUSE 7: SUPPORT

Clause 7 concerns itself with resources. This applies to people, infrastructure and environment as much as physical resources, materials, tools etc. There is also a renewed focus on knowledge as a significant resource within your organization. When planning your business continuity objectives, a major consideration will be the current capacity and capability of your resources as well as those you may need to source from external suppliers / partners.

Resources

To implement and maintain and effective BCMS an organization needs to identify and provide the supporting resources required to operate, maintain and continually improve it.

Resources need to be:

- **capable** – if the resource is equipment or infrastructure; and
- **competent** – if they are people; and
- **sufficient** – if they are supplies.

Competence

The implementation of an effective Business Continuity Management System relies heavily on the knowledge and skills of your employees, suppliers and contractors. To be certain of an appropriate knowledge and skills base you need to:

- define the knowledge and skills that are required
- determine who needs to have the knowledge and skills
- verify that the right people have the right knowledge and skills.

Your auditor will expect you to have documents detailing your knowledge and skills requirements. Where you believe the requirements are satisfied this will need to be supported with records such as training certificates, course attendance records or internal competency assessments.

TIP – Most organizations that already use tools such as training/skills matrices, appraisals or supplier assessments can satisfy the requirement for competence records by expanding the areas covered to include Business Continuity.

Awareness

In addition to ensuring specific competence of key personnel in relation to business continuity, the wider group of employees, suppliers and contractors will need to be aware of the basic elements of your BCMS. This is central to establishing a supportive culture within the organization.

All staff, suppliers and contractors should be aware of the following:

- That you have a BCMS and why you have one
- That you have a Business Continuity Policy and which particular elements of it are relevant to them
- How they can contribute to your organization responding to an adverse situation and maintaining continuity of products or services at a pre-defined level
- Which policies, procedures are relevant to them and what the consequences are of not complying with them.

TIP – The communication of this information can normally be done through existing processes and documents such as staff inductions, employment contracts, toolbox talks, supplier agreements, employee briefings or updates.

Communication

To enable the processes in your BCMS to work effectively you will need to ensure you have communication activities that are well planned and managed.

An organization shall establish:

- what needs to be communicated
- when it needs to be communicated
- to whom it needs be communicated
- what are the processes for communication
- who is responsible for communication.

TIP – If your communication requirements are well defined in your processes, policies and procedures then you do not need to do any more to satisfy this requirement. If they aren't then you should consider documenting your key communication activities in the form of a table or procedure that includes the headings detailed above. Remember, the content of these documents also needs to be communicated!

Documented Information

To be of use, the documented information you use to implement, maintain and improve your BCMS needs to:

- be accurate
- be clear, unambiguous and understandable to the individuals who use it regularly or occasionally
- support your compliance with legal requirements and manage the internal/external risk and issues that impact on the ability of your BCMS to achieve its intend outcomes.

In order for your documented information to satisfy these requirements you will need to have processes in place to ensure that:

- documented information is reviewed by appropriate individuals before it is released into general circulation
- documented information is available where and when required and suitable for use
- access to documented information is controlled so that it cannot be changed accidentally, corrupted, deleted or accessed by individuals to whom it is not appropriate
- information is disposed of securely or returned to its owner when there this a requirement to do this
- you can track changes to information to guarantee that the process is in control.

The source of your documented information may be either internal or external, so your control processes need to manage documented information from both sources.

TIP – Organizations that have good document control typically have one or more of the following in place:

- A single person or small team responsible for ensuring that new/modified documents are reviewed before they are issued, are stored in the right location, are withdrawn from circulation when superseded and that a register of changes is maintained
- An electronic document management system that contains automatic workflows and controls
- Robust electronic data back-up and hard-copy file archiving/ storage processes
- Strong employee awareness of document control, record keeping and information access/retention requirements.

CLAUSE 8: OPERATION

Having completed all the planning and risk assessment activities required by the standard, we now progress to the implementation and operation stage. This is where processes and actions identified to address the risks and opportunities are implemented and controlled.

To implement effective processes the following practices are crucial:

1. Processes are created by adapting or formalising an organization's "business as usual" activities.
2. Systematic identification of the business continuity risks relevant to each product and service.
3. Clear definition and communication of the set of activities required to manage the associated business continuity risks.
4. Clear assignment of the responsibilities for carrying out related activities.
5. Adequate allocation of resources to ensure that related activities can take place as and when required.
6. Routine assessment of the consistency with which each process is followed and its effectiveness in managing business continuity risks.

TIP – For each process, designate an individual as accountable for ensuring that steps 2-6 happen. This individual is often referred to as the Process Owner.

Business Impact Analysis and Risk Assessment

An organization is required to implement and maintain a process for analysing the business impact and assessing the risk of disruption to its key activities. The results of business impacts analysis and risk assessments will enable an organization to determine the appropriate strategy and solution required to respond to a disruptive incident.

Business Impact Analysis

The purpose of conducting a business impact analysis is to enable an organization to identify its business continuity requirements and priorities. The process for undertaking a business impact analysis shall:

- define the impact types and criteria relevant to the organization's context
- identify and prioritise key activities and the products and services required to achieve them
- assess the impacts over time from the disruption to the activities
- identify the point in time when the non-resumption of these activities would have a detrimental impact on the organization (MTPD)
- identify the time when resumption of these activities are to resume at an acceptable level (RTO)
- identify the resources needed to support the prioritised activities
- determine the internal and external dependencies required to support the priorities activities.

Risk Assessment

The risk assessment process will enable an organization to determine the likelihood of an incident occurring. It then helps to identify actions required to reduce the likelihood and impact to the organizations prioritised activities in the event of a disruptive incident. Risk assessments are to be conducted at planned intervals or when significant changes to the organization or the context in which it operates occur.

The risk assessment process shall:

- identify the risks to the organization's prioritised activities and their required resources
- analyse and evaluate the identified risk
- determine the risks which require treatment.

Business Continuity Strategy and Solutions

The results of the business impact analysis and risk assessment are to be used to determine the correct business continuity strategy and identify the resources required to respond to and manage the business continuity incident until return to normal operations.

Selection of Strategies and Solutions:

The selection of an organization's business continuity strategy and solutions shall be based on:

- the ability to meet the requirements to continue and recover prioritised activities at a predetermined capacity and to an agreed timeframe
- reduce the likelihood and period of disruption
- the resources required
- the organization's risk appetite
- costs and benefits.

Resource Requirements

When determining the resource required for the implementation of its business continuity solution, an organization shall consider the internal and external resource required.

As minimum resources should include:

- people
- information and data
- infrastructure and supporting utilities
- equipment and consumables
- IT and communication systems
- transport and logistics
- finance
- partners and suppliers.

Business Continuity Plans and Procedures

Based on the output of the selected business continuity strategies and solutions, an organization is required to establish a response structure and implement plans and procedures to manage the organization during a disruptive incident requiring activation of its business continuity solutions.

The procedures shall:

- identify the immediate steps taken during a disruption
- be able to adapt to changes in internal and external conditions as a result of disruption
- focus on the impact of incidents that could lead to disruption.
- minimise the impact of disruption
- assign roles and responsibilities for tasks within them.

Response Structure

The response structure is to consist of one or more teams (Crisis management team(s)) responsible for responding to and managing disruptions. The roles and responsibilities for each team is to be clearly defined, teams are to be competent to assess the impact of the disruption and implement the appropriate business continuity response. The response structure is to include procedures for communicating with internal and external interested parties, authorities and the media.

Business Continuity Plans

Documented business continuity plans and procedures providing guidance and information to enable teams to respond to a disruptive incident and recovery to normal operations shall be developed and maintained. Plans are to be made readily available where and when required.

Collectively business continuity plans shall contain:

- details of the actions each team will take in order to continue or recover prioritised activities, monitor the impact of the disruption and the organizations response
- reference to the pre-defined thresholds and processes for activating the response
- procedures to enable delivery of products and services at an agreed capacity
- details to manage the immediate consequences of a disruption taking into consideration welfare of individuals, the prevention of further disruption to prioritised activities and the impact on the environment.

Each plan shall:

- give the purpose, scope and objectives
- the roles and responsibilities of the team who will implement the plan
- identify actions to implement the solutions
- contain information required to activate, operate, coordinate and communicate the team's actions
- identify the internal and external dependencies required
- identify the resources required
- include reporting requirements
- a process for standing down.

Recovery

An organization shall have documented processes to return to normal operations after a business continuity incident.

Exercise Programme

To ensure that its business continuity strategies, solutions and plans remain valid an organization is required to establish an exercise programme to test the effectiveness of its business continuity arrangements. An organization need not test the entirety of its business continuity arrangements during each exercise.

The tests are to:

- be consistent with its business continuity objectives
- be based on appropriate scenarios with clearly defined aims and objectives
- develop teamwork and competence of business continuity teams and those with roles to perform during a disruption
- validate its business continuity strategies, solutions and plans
- produce post-exercise reports that contain outcomes, recommendations and actions for improvement
- to be performed at planed intervals or when there are significant changes within the organization or the context within which it operates.

Evaluation of Business Continuity Documentation and Capabilities

An organization shall evaluate the adequacy and effectiveness of its business impact analysis, risk assessment, strategies, solutions, plans and procedures at planned intervals, after an incident or invocation and when significant changes occur.

CLAUSE 9: PERFORMANCE EVALUATION

Monitoring, Measurement, Analysis and Evaluation

An organization needs to evaluate the performance and effectiveness of its BCMS to ensure it can achieve its intended outcomes. It needs to determine what needs to be monitored and measured, the methods of monitoring and measuring and how the results will be evaluated. The occasions when monitoring and measuring activity is to be conducted is to be planned, personnel undertaking monitoring and measuring activity are to be identified and selected taking into consideration competence and impartiality. Appropriate evidence of monitoring and measuring activity and results of monitoring and measuring activity is to be retained.

Internal Audit

The purpose of internal audits is to confirm that the BCMS has been effectively implemented and to identify any weakness and opportunities for improvement.

Internal audits should check:

- whether the BCMS meets the needs of the organization
- conforms to the requirement of ISO 22301:2019
- how consistently processes and procedures are being applied
- whether processes and procedures achieve the intended results.

Audit Programme Audits

An organization shall conduct internal audits at planned intervals. The audit programme shall:

- take into consideration the importance of the processes concerned and the results of previous audits
- define the criteria and scope for each audit
- select auditors and conduct audits to ensure objectivity and impartiality of the audit process
- ensure audit results are reported to the relevant managers
- retain documented evidence of the implementation of the audit programme and audit results
- ensure that any necessary corrective actions are taken without delay to address the nonconformities and their causes.

Management Review

Top management shall review the organization's BCMS at planned intervals to assess its continued adequacy, suitability and effectiveness in meeting the needs of the organization.

The inputs and outputs of management review meetings are to meet the requirements of clause 9.3 of the standard. Output shall include decisions related to continual improvement opportunities and any changes required to improve the efficiency and effectiveness of the BCMS.

An organization shall retain documented information as evidence of the results of management reviews and communicate the results to relevant interested parties.

CLAUSE 10: IMPROVEMENT

The main purpose for implementing a BCMS is to ensure an organization can respond to a disruptive incident in a timely manner, and to continue delivery of its key products and services at a pre-defined level until return to normal operations can be affected.

Nonconformity and Corrective Action

Organizations are to determine opportunities for improvement and implement actions to achieve the intended outcomes of its BCMS. Organizations are to react to nonconformities and take action to control and correct the nonconformities and deal with the consequences.

Root Cause Analysis

Organizations are to investigate nonconformities to:

- establish if the nonconformity exists elsewhere
- identify the root cause of the nonconformity
- identify any corrective action required to prevent a re-occurrence of the nonconformity
- identify any changes to the BCMS required.

Any corrective actions identified to address nonconformities are to be implemented without undue delay. The corrective action implemented is to be reviewed to determine its effectiveness.

GET THE MOST FROM YOUR MANAGEMENT SYSTEMS

Top Tips for the Successful Implementation of a BCMS

1. Start with “Why?”. Make sure the reasons for implementing an BCMS are clear and aligned with your strategic direction, otherwise you risk not getting the critical buy-in from top management.

2. Next consider “What for?”. Implementing and maintaining a BCMS requires significant commitment, so make sure your scope is broad enough to cover the critical information that needs protecting, but is not so broad that you do not have sufficient resources to implement and maintain it.

3. Get all of your key stakeholders involved at the appropriate times. Top management for context, requirements, policy and objectives setting; managers and employees with valuable knowledge for risk assessments, process design and procedure writing.

4. Communicate extensively throughout the process to all of your stakeholders. Let them know what you are doing, why you’re are doing it, how you plan to do it and what their involvement will be. Provide regular progress updates.

5. Get external help where you need it. Do not fail for lack of in-house technical skills or knowledge. Management of information security risks often requires specialist knowledge. However, be sure to check the credentials of a third party before engaging them.

6. Keep your processes and supporting documentation simple. It can develop to become more extensive over time if needed.

7. Design and implement rules you can follow in practice. Don’t make the mistake of documenting an over-elaborate rule that no-one can follow. It is better to accept a risk and to continue to look for ways to manage it.

8. Remember your suppliers. Some suppliers will help you enhance your BCMS, some will increase your risk. You need to ensure any high-risk suppliers have controls in place that are at least as good as yours. If they don’t then look for alternatives.

9. Train, train and train again. Business Continuity is likely to be a new concept for many or most of your employees. People may need to change habits ingrained over many years. A single awareness briefing is unlikely to be sufficient.

10. Remember to allocate sufficient resources to routinely test your controls. The threats your organization faces will constantly change and you need to test whether you are able to respond to those threats.

NEXT STEPS ONCE IMPLEMENTED

1 AWARENESS TRAINING

- Your organization should raise awareness about various standards covered under BCMS
- You should hold separate training meetings for top management, middle management and junior level management, which will help to create a motivating environment, ready for implementation.

2 POLICY AND OBJECTIVES

- Your organization should develop an Integrated Quality Policy/Environment Policy/Health & Safety Policy/Information Security Policy and relevant objectives to help meet the requirements
- By working with top level management your company should hold workshops with all levels of management staff to outline the integrated objectives.

3 INTERNAL GAP ANALYSIS

- Your organization should identify and compare the level of compliance of existing systems against requirements of the standards under your new BCMS
- Relevant staff should all understand the operations of the organization and develop a process map for the activities within the business.

4 DOCUMENTATION / PROCESS DESIGN

- The organization should create documentation of the processes as per requirements of relevant standard(s)
- You should write and implement a manual, functional procedures booklet, work instructions, system procedures and provide associated terms.

5 DOCUMENTATION / PROCESS IMPLEMENTATION

- Processes / Documents developed in step 4, should be implemented across the organization covering all the departments and activities
- The organization should hold a workshop on the implementation as per applicable for the ISO standard requirements.

6 INTERNAL AUDIT

- A robust internal audit system for the organization is essential. Internal Auditor Training is recommended and NQA can provide Internal Auditor Training for the standard(s) that you are implementing
- It is important to implement corrective actions for improvements, in each of the audited documents, in order to bridge gaps and ensure the effectiveness of the BCMS.

7 ORGANISE A MANAGEMENT 'SYSTEM' REVIEW MEETING

- Top level management must review various official business aspects of the organization, which are relevant to the standards being implemented
- Review the policy, objectives, results of internal audit, results of process performance, results of complaints/feedback/legal compliance, results of risk assessment/incidents and develop an action plan following the meeting - which must be minuted.

8 THOROUGH GAP ANALYSIS OF IMPLEMENTED SYSTEMS

- A formal pre-certification gap analysis should be conducted to assess effectiveness and compliance of system implementation in the organization
- This final gap analysis will prepare your organization for the final certification audit.

9 CORRECTIVE ACTIONS

- The organization should be ready for the final certification audit, providing that the gap analysis audit conducted in the last step and all the non-conformities (NC) have been assigned corrective actions
- Check that all the significant NCs are closed and the organization is ready for the final certification audit.

10 FINAL CERTIFICATION AUDIT

- Once completed, your organization is hopefully recommended for registration to the required standard
- CONGRATULATIONS!

nqa.app

Associate Partner Programme

NQA ASSOCIATE PARTNER PROGRAMME

If you are looking for a consultant to assist you with a new or existing management system, NQA can help!

Our APP has consultants from all over the country enlisted on it. The register is designed to help you find experienced consultants who can help.

> "We have been using JMT Quality Consultants as our ISO external auditor for the past couple of years and I wish that we had done so much earlier! We have found them to be very professional, providing not only a comprehensive audit report but additional ideas for improvement and contacts for our company that we could additionally benefit from."
>
> **SAFETYBOSS**

> "The professionalism and work-ethic Clark from CBO Associates showed during our ISO 9001 process was excellent. Clark is a professional in his delivery, a knowledgeable person that offers a high level of service which makes him an ideal QHSE Consultant. His ideas and delivery are both creative and effective."
>
> **CLARK-IT, ABERDEENSHIRE**

> "Since being certified to ISO 9001 and ISO 14001 we have relied on Martin Giddens from Morton Hodson for support with our annual process auditing. Martin understands our business and always advises us of which changes to guidance and regulations apply and what we need to do to implement them. Martin's expertise ensure that staying compliant is simple."
>
> **LONSDALE DIRECT SOLUTIONS**

To find a consultant to support you through your certification journey contact us on:

0800 052 2424 (option 2) or email sales@nqa.com

TRUSTED GLOBALLY OVER 30 YEARS SINCE 1988

UKAS MANAGEMENT SYSTEMS 0015

NOTES

Authored by: Tony Bevan, NQA UK Auditor