



ISO 22301:2019 Certification â?? Complete Guide to Business Continuity Management.

Description

A business can have excellent employees, modern technology, strong customers and healthy revenuesâ??and still face serious operational disruption when an unexpected event occurs.

A cyberattack can interrupt critical systems.

A fire can make a facility unavailable.

A prolonged power or network failure can stop operations.

A critical supplier can suddenly become unavailable.

A natural disaster can affect infrastructure and employees.

A pandemic or public-health emergency can disrupt normal operating models.

And sometimes the disruption is much smaller:

- loss of a key employee
- failure of a critical application
- telecom outage
- cloud-service disruption
- equipment failure
- supplier failure
- data-centre issue
- building access problem

The important question is not whether an organization can **prevent every disruption**.

It is:

Can the organization prepare for disruption, respond effectively, continue critical activities and recover in a controlled manner?

This is where **ISO 22301:2019** becomes relevant.

ISO 22301 is the international requirements standard for a **Business Continuity Management System (BCMS)**. ISO states that it helps organizations prepare for, respond to and recover from disruptive incidents.

For organizations considering certification, ISO 22301 provides a structured management-system approach to business continuity rather than treating continuity planning as a collection of isolated emergency documents.

What is ISO 22301:2019?

ISO 22301:2019 is an international standard that specifies requirements for establishing, implementing, maintaining and continually improving a **Business Continuity Management System (BCMS)**. It helps organizations prepare for disruptive incidents, respond to them and recover while maintaining the continuity of important products and services at an acceptable predefined capacity. The standard is applicable to organizations of different sizes, sectors and operating models. ISO 22301:2019 is the current published edition, with Amendment 1:2024 adding climate-action considerations. ISO is also developing a future revision, currently identified as ISO/CD 22301, but that draft is not the current published standard.

What is ISO 22301 certification?

ISO 22301 certification is independent conformity assessment of an organization's **Business Continuity Management System** against the applicable requirements of **ISO 22301**.

It demonstrates that the organization has established a structured BCMS covering areas such as:

- Business continuity planning
- Risk and disruption preparedness
- Business impact analysis
- Continuity strategies
- Response arrangements
- Recovery
- Testing and exercising
- Performance evaluation
- Continual improvement

The certificate is issued by an **independent certification body**, not by ISO itself.

What Is ISO 22301?

ISO 22301:2019 is formally titled:

Security and resilience – Business continuity management systems – Requirements

It belongs to the ISO/TC 292 family covering **security and resilience**.

The standard provides requirements for a management system that enables an organization to establish an organized approach to business continuity.

ISO describes the purpose of business continuity management as helping organizations prepare for disruptive events and maintain the delivery of products and services during disruption.

The concept is broader than simply creating a disaster recovery plan.

Business continuity asks:

What must continue?

How quickly must it continue?

At what minimum acceptable capacity?

What resources are required?

What could disrupt it?

How will we respond?

How will we recover?

How will we test whether the arrangements actually work?

That is the foundation of a BCMS.

ISO 22301 Is More Than a Business Continuity Plan

This is one of the most important concepts to understand.

Many organizations have a document called:

Business Continuity Plan

But having a document does not automatically mean that an effective Business Continuity Management System exists.

A BCMS is a **management system**.

It involves:

Leadership

Context

Risk & Opportunity

Business Impact Analysis

Continuity Requirements

Strategy

Plans & Procedures

Response

Testing & Exercising

Performance Evaluation

Improvement

default watermark

This creates a continuous management cycle rather than a document that is opened only during an emergency.

Business Continuity vs Disaster Recovery

These terms are frequently used interchangeably, but they are not identical.

Business Continuity

Business continuity focuses on the organization's ability to continue important products and services at an acceptable predefined capacity during and following disruption.

It considers the broader organization.

For example:

- people
- facilities
- technology
- suppliers
- processes
- communications
- information
- customers
- critical activities

default watermark

Disaster Recovery

Disaster recovery is generally more focused on restoring technology, infrastructure, applications or data after a disruptive event.

For example:

Server failure → backup → restoration → system recovery

That can be an important component of continuity.

But business continuity asks a larger question:

How does the business continue delivering its critical products and services while the disruption is being managed?

Simple way to remember it:

Disaster Recovery = Recover systems

Business Continuity = Continue critical business services

They can work together, but they are not interchangeable concepts.

Why Business Continuity Needs a Management System

Imagine an organization has a 100-page business continuity plan.

Now ask:

- Who owns it?
- Who updates it?
- Who approves it?
- Who knows their role?
- When was it last tested?
- What assumptions were made?
- What happens if the primary site is unavailable?
- What happens if the critical supplier fails?
- What happens if key personnel are unavailable?
- What happens if the recovery technology doesn't work?
- What did the last exercise reveal?
- Were corrective actions completed?

These questions move the discussion from:

“Do we have a plan?”

to:

“Do we have a functioning continuity capability?”

That distinction is central to the management-system approach.

Who Needs ISO 22301?

One of the strengths of ISO 22301 is that it is not restricted to one industry.

ISO's published material states that ISO 22301 is applicable to organizations regardless of their size, industry or nature of business.

That means its potential application is broad.

1. IT & Technology Companies

Technology companies often depend on:

- cloud infrastructure
- data centres
- applications
- networks
- skilled technical personnel
- third-party platforms
- cybersecurity controls
- telecommunications

A disruption to any of these can affect service delivery.

ISO 22301 can provide a structured framework for identifying critical services and establishing continuity arrangements.

2. SaaS Companies

For SaaS organizations, availability and service continuity are often directly connected to customer expectations.

Consider a SaaS platform that becomes unavailable.

The organization may need to consider:

- application availability
- cloud infrastructure
- database recovery
- communication
- customer support
- incident response
- supplier dependencies
- recovery priorities
- alternative operating arrangements

ISO 22301 can therefore be relevant to SaaS companies seeking a systematic BCMS.

3. BFSI Organizations

Banking and financial services organizations operate in environments where service disruption can have significant operational and regulatory consequences.

Potential continuity considerations include:

- critical banking services
- payment systems
- customer access
- technology infrastructure
- third-party providers
- data availability
- communication
- workforce continuity

A structured BCMS can help establish defined continuity arrangements.

4. Healthcare Organizations

Healthcare organizations need continuity of important services even when normal operating conditions are disrupted.

Potential scenarios include:

- infrastructure failure
- power disruption
- IT outage
- supply disruption
- facility unavailability
- workforce disruption
- technology failure

The exact continuity requirements depend on the organization's services and regulatory environment.

5. Manufacturing Organizations

Manufacturers can face disruption from:

- machinery failure
- raw-material shortages
- utility interruption
- supplier failure
- logistics disruption
- facility damage

- workforce shortages
- IT or operational technology failures

Business continuity management can help organizations identify critical processes and dependencies before a major disruption occurs.

6. Logistics & Supply Chain Organizations

A logistics organization may depend on:

- transportation
- warehouses
- fleet
- fuel
- IT systems
- telecommunications
- suppliers
- ports
- roads
- personnel

default watermark

A disruption at one point in the chain can affect multiple downstream activities.

A BCMS helps organizations systematically consider these dependencies.

7. Data Centres & Cloud Infrastructure

For infrastructure providers, continuity is fundamental to service delivery.

Relevant considerations can include:

- power
- cooling
- network connectivity
- physical security
- redundancy
- personnel
- suppliers
- backup systems
- recovery arrangements

ISO 22301 can complement technical resilience and disaster-recovery arrangements by placing them within a broader management-system framework.

8. GCCs and Shared Service Centers

Global Capability Centers and shared service organizations often support business-critical functions across multiple geographies.

Examples include:

- finance
- HR
- IT
- procurement
- analytics
- customer support
- engineering
- cybersecurity

A continuity failure at a shared-service center can affect multiple business units or countries.

9. Government & Public-Sector Organizations

Public-sector organizations may have continuity responsibilities involving:

- citizen services
- public infrastructure
- emergency response
- administrative services
- information systems
- critical facilities

Business continuity can therefore form part of broader resilience planning.

10. Small and Medium-Sized Businesses

ISO 22301 isn't only for large enterprises.

A smaller organization can be highly dependent on:

- one facility
 - a few key employees
 - one supplier
 - one application
 - one customer
 - one production line
-

- one logistics provider

This can actually make continuity planning particularly important.

The scale of the BCMS should reflect the organization's **size, complexity, context and risk environment**.

Who Should Consider ISO 22301?

A useful question is not simply:

• "Are we a large company?" •

Instead ask:

Does your organization depend on critical services or processes?

Would a significant disruption affect customers?

Could a disruption stop revenue-generating activities?

Do you have critical suppliers?

Do customers expect continuity commitments?

Are there contractual or regulatory continuity requirements?

Would loss of a facility affect operations?

Would a technology outage significantly affect services?

Do you need to demonstrate structured business continuity capability?

If several answers are **yes**, a formal BCMS may be relevant.

What Does ISO 22301 Actually Help an Organization Do?

ISO identifies several benefits associated with business continuity management, including enhanced resilience, improved preparedness, stakeholder confidence and support for continuity of products and services during disruption.

Let’s look at the practical implications.

1. Improve Organizational Resilience

Resilience isn’t simply:

“Nothing bad will happen.”

It is the ability to:

Prepare Respond Continue Recover Improve

That changes the organization’s approach to disruption.

2. Identify Critical Business Activities

Organizations cannot necessarily protect everything at the same priority level.

A BCMS helps establish which activities are critical and what their continuity requirements are.

For example:

Business Activity	Criticality	Potential Impact
Customer support	High	Customer dissatisfaction
Payment processing	Critical	Revenue disruption
Production	Critical	Supply interruption
HR administration	Medium	Internal disruption
Marketing	Lower during emergency	Delayed campaigns

The actual classification must be determined by the organization based on its context and requirements.

3. Understand Dependencies

A business activity rarely operates independently.

Consider:

Customer Service

depends on

CRM

which depends on

Cloud Infrastructure

which depends on

Cloud Provider

which may depend on

Power + Network + Data Centre

A continuity assessment needs to understand these relationships.

4. Establish Recovery Priorities

Not everything can necessarily be restored simultaneously.

A BCMS helps an organization establish priorities around critical activities and resources.

This leads to questions such as:

- What must resume first?
 - What can wait?
 - What resources are essential?
 - What alternatives exist?
 - What recovery capability is required?
-

5. Improve Preparedness

Preparedness is more than documentation.

It includes:

- roles
 - responsibilities
 - communications
 - resources
 - procedures
 - training
 - exercises
 - testing
 - lessons learned
-

A plan that has never been tested provides less confidence than one that has been exercised and improved based on evidence.

6. Strengthen Stakeholder Confidence

Customers, regulators, partners and other stakeholders may want evidence that an organization has considered continuity risks.

ISO notes stakeholder confidence as one of the benefits associated with a structured business continuity approach.

For B2B organizations, continuity capability can also become part of supplier or customer due diligence.

ISO 22301 and Risk Management

Risk management is an important part of business continuity.

But there is a useful distinction.

Risk management asks:

What could happen, and how can we manage the risk?

Business continuity asks:

If disruption occurs, how do we continue critical activities?

The two approaches complement one another.

For example:

Risk

Cloud service outage.

â??

Potential impact

Customer-facing SaaS service unavailable.

â??

Continuity requirement

Maintain critical customer services at a predefined capacity.

â??

Strategy

Alternative infrastructure / redundancy / recovery capability.

â??

Response

Activate appropriate continuity arrangements.

â??

Recovery

Restore normal service.

â??

Improvement

Review performance and update arrangements.

That is the continuity lifecycle.

ISO 22301 and Business Impact Analysis

One of the concepts that frequently appears in business continuity implementation is:

Business Impact Analysis â?? BIA

A BIA helps an organization understand the consequences of disruption to activities and establish continuity priorities and requirements.

A BIA may examine:

- Business activities
 - Products and services
 - Customers
 - Dependencies
-

- Impacts
- Maximum tolerable disruption considerations
- Recovery priorities
- Required resources
- Time-related requirements

The exact methodology should be tailored to the organization’s context and applicable requirements.

Business Continuity Is Not Just IT

This is another major misconception.

A company may have an excellent disaster recovery solution and still have a weak overall continuity capability.

Consider a scenario:

IT systems recover in 4 hours.

But:

- The building is unavailable.
- Employees cannot access the site.
- A critical supplier is unavailable.
- Customer communications aren’t defined.
- Key personnel are unavailable.
- Alternative logistics aren’t arranged.

The servers may have recovered.

But the **business may still not be able to operate normally.**

That’s why ISO 22301 takes a broader management-system perspective.

ISO 22301 vs ISO 27001

Organizations sometimes confuse these standards.

They address different management-system objectives.

Area	ISO 22301	ISO/IEC 27001
Primary focus	Business continuity	Information security
Management system	BCMS	ISMS

Area	ISO 22301	ISO/IEC 27001
Main concern	Continuity during disruption	Confidentiality, integrity & availability of information
Business impact analysis	Important continuity activity	Not the central objective
Security risk	Relevant where applicable	Central
Recovery	Core continuity concern	Relevant to information-security resilience
Certification	Available	Available

They can also be implemented together.

For a technology company, for example:

ISO/IEC 27001 can address information-security management.

ISO 22301 can address business continuity management.

Together they can support broader organizational resilience.

ISO 22301 vs ISO 9001

These standards also have different primary purposes.

ISO 9001

Focuses on:

Quality Management

ISO 22301

Focuses on:

Business Continuity Management

An organization can have a high-quality process that becomes unavailable during a major disruption.

Therefore:

Quality & Continuity

But the two systems can be integrated.

For example:

ISO 9001 + ISO 22301

can connect quality objectives with continuity requirements.

ISO 22301 vs Disaster Recovery

ISO 22301	Disaster Recovery
Business continuity management system	Recovery capability/activity
Organization-wide perspective	Often technology/infrastructure focused
Critical products/services	IT systems/data/infrastructure
BIA	Technical recovery assessment
Continuity strategies	Recovery procedures
Response arrangements	System restoration
Exercises	DR testing
Continual improvement	Lessons learned and technical improvement

The exact boundary depends on the organization’s operating model.

The important point is:

Disaster recovery can be part of business continuity, but business continuity is broader than disaster recovery.

ISO 22301 and Organizational Resilience

The concept of resilience is becoming increasingly important for organizations dealing with:

- Cyber threats
- Supply-chain disruption
- Extreme weather
- Technology dependency
- Workforce dependency
- Infrastructure disruption
- Global operations
- Third-party services

ISO describes ISO 22301 within its broader **security and resilience** standards family.

This makes ISO 22301 particularly relevant for organizations that want to move from reactive disaster planning toward a structured resilience capability.

• Important 2026 Update: ISO 22301 Is Being Revised

This is important for anyone researching ISO 22301 today.

The currently published standard is:

ISO 22301:2019

It has:

Amendment 1:2024 • Climate action changes

However, ISO is currently developing:

ISO/CD 22301

The committee draft is intended to replace ISO 22301:2019, but it is **still under development**. ISO's current project page identifies it as a Committee Draft and states that it will replace the 2019 edition.

Therefore:

For current certification discussions, we should refer to:

ISO 22301:2019 + applicable Amendment 1:2024

and **not describe the 2026 committee draft as the current certification standard**.

This distinction will be important throughout our CK Associates content series.

ISO 22313 • The Guidance Standard

Organizations researching ISO 22301 should also know about:

ISO 22313:2020

It provides guidance and recommendations for applying the requirements of ISO 22301.

ISO currently lists ISO 22313:2020 as reviewed and confirmed in 2025, meaning that version remains current.

So, conceptually:

ISO 22301 Requirements

ISO 22313 Guidance

This is useful when designing implementation methodology.

ISO 22301 Certification What It Does Not Mean

Certification does **not** mean:

• The organization will never experience disruption.

• Every business process will continue under every scenario.

• Every disaster risk has been eliminated.

• Recovery will always happen within a particular timeframe.

• The organization is immune from cyberattacks, natural disasters or supplier failures.

Instead, certification relates to conformity of the organization's BCMS with the applicable requirements of the standard.

The organization's actual continuity capability depends on its scope, risks, strategies, resources, implementation and ongoing improvement.

What Does an ISO 22301 Consultant Actually Do?

A competent implementation consultant should not simply hand an organization a generic business continuity manual.

The work should begin with understanding the organization.

A typical implementation methodology may include:

1. Scope Definition

Determine what the BCMS covers.

2. Gap Assessment

Assess current continuity practices.

3. Context Assessment

Understand organizational and stakeholder requirements.

4. Risk & Impact Analysis

Identify threats, dependencies and potential impacts.

5. BIA

Determine critical activities and continuity requirements.

6. Strategy Development

Identify appropriate continuity strategies.

7. Documentation

Develop necessary policies, plans and procedures.

8. Implementation

Put arrangements into operation.

9. Training & Awareness

Ensure relevant personnel understand their roles.

10. Exercises & Testing

Validate continuity arrangements.

11. Internal Audit

Evaluate conformity and effectiveness.

12. Management Review

Ensure leadership evaluates the BCMS.

13. Corrective Action

Address identified weaknesses.

14. Certification Readiness

Prepare the organization for independent certification assessment.

These activities will be explored in detail in **Part 3**.

Hyderabad & India Perspective

For organizations operating in **Hyderabad, Telangana and across India**, business continuity can be particularly relevant to sectors with significant technology, supply-chain, infrastructure and customer-service dependencies.

Examples include:

- IT services
- SaaS
- GCCs
- BFSI
- Healthcare
- Manufacturing
- Pharmaceuticals
- Logistics
- Data centres
- E-commerce
- Telecommunications
- Professional services

Organizations in **HITEC City, Gachibowli, Financial District, Madhapur, Kondapur and other Hyderabad business clusters** may have continuity requirements spanning customers, cloud infrastructure, employees, suppliers and global operations.

For a multinational or GCC, the continuity question may extend across countries.

For a manufacturing organization, it may extend across production, suppliers and logistics.

For a SaaS company, it may extend across cloud infrastructure, applications, people and customer commitments.

Therefore, the BCMS should be designed around the organization's **actual operating model**, rather than using a generic template.

CK Associates Consultant's Insight

One of the most important questions in business continuity implementation is:

What happens if this process stops tomorrow?

Not:

Do you have a business continuity document?

Start with the business.

Ask:

What must continue?

Then:

How long can it be unavailable?

Then:

What happens if it stops?

Then:

What resources are required to continue it?

Then:

What dependencies could fail?

Then:

What strategy will we use?

Then:

How do we test it?

Then:

What did the test teach us?

That approach turns business continuity from a document exercise into a **management discipline**.

ISO 22301 at a Glance

Element	ISO 22301 Perspective
Standard	ISO 22301:2019

Element	ISO 22301 Perspective
Subject	Business Continuity Management
Management System	BCMS
Current amendment	Amendment 1:2024
Main objective	Manage continuity during disruption
Applicability	Organizations of different sizes and sectors
Key concepts	BIA, risk, continuity strategy, response, recovery
Testing	Exercises and validation are important
Improvement	Continual improvement
Certification	Available through independent certification bodies
Guidance	ISO 22313:2020
Future revision	ISO/CD 22301 under development

Current standard and amendment status: ISO.

Key Takeaways

- ISO 22301 is a Business Continuity Management System standard.
- It is broader than a disaster recovery plan.
- It can apply to organizations of different sizes, industries and operating models.
- Business continuity focuses on maintaining important products and services during disruption.
- Business Impact Analysis helps organizations understand critical activities, impacts and continuity requirements.
- Technology recovery is important, but business continuity extends beyond IT.
- ISO 22301 can be integrated with standards such as ISO 9001 and ISO/IEC 27001.
- ISO 22313:2020 provides guidance for applying ISO 22301.
- ISO 22301:2019 has a 2024 climate-action amendment.

ð??¹ A future ISO 22301 edition is under development, but the draft is not the current published certification standard.

What Weâ??ll Cover in Part 2

ISO 22301 Clauses Explained â?? From Context to Continual Improvement

In Part 2, we will go deeper into the actual structure of ISO 22301 and explain:

Clause 4

Context of the Organization

Clause 5

Leadership

Clause 6

Planning

Clause 7

Support

Clause 8

Operation

Including the important business continuity activities around:

- Business Impact Analysis
- Risk Assessment
- Business Continuity Strategies
- Business Continuity Plans
- Response
- Exercises and Testing
- Evaluation

Clause 9

Performance Evaluation

Clause 10

Improvement

We will also explain how these clauses translate into **real implementation evidence**.

CK ASSOCIATES | ISO KNOWLEDGE SERIES | BLOG PART 1 OF 3

ISO 22301:2019 Certification – Complete Guide to Business Continuity Management

Part 1: What Is ISO 22301, Who Needs It & Why It Matters
Build resilience. Ensure continuity. Be prepared for the unexpected.

Business Continuity Resilience Growth

- Prepare for Disruptions**
Be ready for unforeseen events.
- Maintain Critical Services**
Ensure continuity at acceptable levels.
- Protect People & Assets**
Safeguard employees, facilities and information.
- Strengthen Stakeholder Confidence**
Build trust with customers, partners and regulators.
- Improved Organizational Resilience**
Respond, recover and grow stronger.
- Identify Critical Activities**
Focus on what truly matters.
- Manage Risks and Dependencies**
Understand and reduce business impact.
- Applicable to Any Organization**
All sizes. All sectors. All geographies.

Resilient Businesses Build a Stronger Tomorrow

People Stay Safe | Services Continue | Customers Stay Confident | Operations Stay Strong | Businesses Grow

RISK AWARENESS | BUSINESS CONTINUITY PLANNING | OPERATIONAL RESILIENCE

Hyderabad, Telangana, India | www.ckassociates.biz | sirish.kaza@gmail.com | +91 98853 07909

20+ YEARS | 450+ CERTIFICATIONS | 8+ EXPERT CONSULTANTS | MULTI STANDARDS | PAN INDIA

What are the ISO 22301 clauses?

ISO 22301:2019 structures its Business Continuity Management System requirements through Clauses 4 to 10. Clause 4 addresses organizational context, Clause 5 leadership, Clause 6 planning, Clause 7 support, Clause 8 operation, Clause 9 performance evaluation, and Clause 10 improvement. Clause 8 contains the core operational business-continuity activities, including business impact analysis and risk assessment, continuity strategies and solutions, continuity plans and procedures, exercises, and evaluation of continuity capabilities. Together, these clauses create a management-system framework for preparing for disruption, responding to incidents, maintaining important products and services, and continually improving continuity capability. ISO's published material also emphasizes leadership, resources, competence,

awareness and communication as important elements of BCMS implementation.

What are Clauses 4-10 of ISO 22301?

Clause	Subject
Clause 4	Context of the Organization
Clause 5	Leadership
Clause 6	Planning
Clause 7	Support
Clause 8	Operation
Clause 9	Performance Evaluation
Clause 10	Improvement

A simple way to remember the structure is:

Understand -> Lead -> Plan -> Support -> Operate -> Evaluate -> Improve

1. Clause 4 -> Context of the Organization

Before an organization can build a BCMS, it needs to understand **what it is trying to protect and the environment in which it operates**.

Clause 4 establishes the organizational foundation for the BCMS.

It requires the organization to consider:

- Internal issues
- External issues
- Interested parties
- Relevant requirements
- The scope of the BCMS
- The management system itself

ISO's business-continuity material explains that understanding the organization's context helps determine the scope of the BCMS.

4.1 Understanding the Organization and Its Context

The organization needs to determine the internal and external issues relevant to its purpose and that affect its ability to achieve the intended results of the BCMS.

Examples can include:

Internal issues

- Organizational structure
- Workforce
- Critical processes
- Technology
- Facilities
- Organizational culture
- Existing management systems
- Financial resources
- Operational dependencies

External issues

- Regulatory environment
- Market conditions
- Supply-chain dependencies
- Climate-related conditions
- Technology changes
- Infrastructure
- Geopolitical conditions
- Customer expectations
- Economic conditions

• Climate change consideration

This clause has an important current update.

ISO 22301:2019 received **Amendment 1:2024 • Climate action changes**. The amendment applies to ISO 22301:2019.

The ISO/IAF communiqué explains that climate-change considerations were added to management-system standards so organizations consider whether climate change is a relevant issue affecting the intended results of their management systems.

For business continuity, this can be particularly relevant because climate-related events may affect:

- Facilities
- Utilities
- Transport
- Supply chains
- Workforce availability
- Data centres
- Infrastructure
- Customer operations

The organization needs to determine **whether climate change is a relevant issue for its BCMS context** rather than simply adding generic statements.

4.2 Understanding the Needs and Expectations of Interested Parties

A BCMS does not operate in isolation.

Organizations may have continuity-related requirements from:

- Customers
- Regulators
- Employees
- Suppliers
- Business partners
- Investors
- Insurers
- Government authorities
- Parent organizations
- Contracting parties

For example, a major customer may require a supplier to demonstrate business continuity capability.

A regulator may establish continuity expectations.

A contractual agreement may specify service availability or recovery requirements.

These requirements need to be understood and considered within the BCMS.

4.3 Determining the Scope of the BCMS

This is one of the most important decisions in implementation.

The organization needs to define:

What exactly does our BCMS cover?

Possible scope dimensions include:

- Products
 - Services
 - Business units
 - Locations
 - Processes
 - Technology
 - Employees
-

- Supporting functions
- Suppliers
- Geographic areas

Example

A company could define its BCMS around:

Provision of cloud-based software services to external customers, including application operations, customer support, infrastructure and supporting business processes.

Another organization could define its scope around:

Manufacturing and distribution operations at a specific facility.

The scope should reflect the organization's actual continuity objectives and operating environment.

4.4 Business Continuity Management System

The organization then establishes, implements, maintains and continually improves its BCMS in accordance with the requirements of the standard.

This is where the concept becomes important:

ISO 22301 is not simply a collection of plans.

It is a **management system**.

That means it needs:

Leadership + Planning + Resources + Operations + Evaluation + Improvement

2. Clause 5 Leadership

Business continuity cannot be delegated entirely to an emergency-response team.

Top management has an important role in establishing and supporting the BCMS.

ISO's business-continuity guidance specifically highlights leadership, resource provision and assignment of responsibilities as important elements of BCMS implementation.

5.1 Leadership and Commitment

Top management should demonstrate commitment to the BCMS.

This means ensuring that business continuity:

- Supports organizational direction
- Receives appropriate resources
- Has defined responsibilities
- Is integrated into relevant business processes
- Is communicated appropriately
- Is reviewed for effectiveness
- Supports continual improvement

The practical question:

Does management treat business continuity as a strategic management issue or merely an emergency document?

That distinction matters.

5.2 Business Continuity Policy

The organization needs an appropriate business continuity policy.

The policy establishes the organization's overall direction and commitment to business continuity.

It should be consistent with:

- Organizational purpose
- Business requirements
- BCMS objectives
- Applicable requirements

It should also provide a framework for establishing business continuity objectives.

5.3 Organizational Roles, Responsibilities and Authorities

People need to know:

- Who owns the BCMS?
 - Who owns critical processes?
-

- Who activates continuity arrangements?
- Who communicates during an incident?
- Who coordinates recovery?
- Who manages suppliers?
- Who reports to management?
- Who reviews the effectiveness of the BCMS?

A continuity plan that says **“Management will take action”** without defining who does what is unlikely to provide adequate operational clarity.

3. Clause 6 “Planning”

Clause 6 converts organizational understanding into structured planning.

It addresses areas such as:

- Risks and opportunities
 - Business continuity objectives
 - Planning to achieve objectives
 - Changes to the BCMS
-

6.1 Actions to Address Risks and Opportunities

The organization needs to determine risks and opportunities relevant to the BCMS.

This is not necessarily the same as the detailed **business continuity risk assessment** performed as part of Clause 8.

The management-system planning process considers risks and opportunities that could affect the ability of the BCMS to achieve its intended results.

Example

If the organization depends heavily on one facility, a relevant continuity concern could be:

Single-site dependency

Potential consequence:

Facility unavailable “critical operations interrupted”

The organization can then determine appropriate action.

6.2 Business Continuity Objectives

Objectives should be established at relevant functions and levels.

A good objective should be meaningful and measurable where appropriate.

Examples might include:

- Improve continuity exercise completion
- Reduce identified recovery gaps
- Increase awareness training completion
- Improve supplier continuity assurance
- Complete testing of critical continuity arrangements
- Close corrective actions within defined targets

The objective should connect to the organization's actual continuity needs.

6.3 Planning Changes to the BCMS

Business continuity systems themselves can change.

For example:

- New facility
- New cloud provider
- Acquisition
- New critical product
- Outsourcing
- New technology
- Organizational restructuring
- New regulatory requirement

When significant changes occur, the organization should consider their impact on the BCMS.

4. Clause 7 Support

A BCMS cannot operate without resources and competent people.

Clause 7 addresses the infrastructure supporting the management system.

Major areas include:

- Resources
 - Competence
-

- Awareness
- Communication
- Documented information

ISO's published material specifically highlights competence and awareness, including ensuring people have appropriate knowledge, skills and experience and understand their roles during incidents.

7.1 Resources

The organization needs to determine and provide resources required for establishing, implementing, maintaining and continually improving the BCMS.

Resources can include:

People

- BCMS manager
- Process owners
- Crisis-management team
- IT recovery team
- Communications team
- Facility representatives

Technology

- Backup infrastructure
- Communication systems
- Recovery platforms
- Notification systems

Facilities

- Alternate workplace
- Recovery site
- Emergency facilities

Financial resources

- Continuity investments
 - Recovery contracts
 - Testing
 - Training
-

7.2 Competence

People performing work that affects BCMS performance should have appropriate competence.

Competence may come from:

- Education
- Training
- Experience
- Exercises
- Practical involvement

For example, a person responsible for crisis communication needs to understand:

- Their role
 - Escalation process
 - Communication channels
 - Stakeholder requirements
 - Incident-response responsibilities
-

7.3 Awareness

Employees should understand relevant aspects of the BCMS.

They may need to know:

- The business continuity policy
- Their role
- Their responsibilities
- What to do during an incident
- How to report an incident
- How to access continuity procedures

This is why **employee awareness** matters.

A continuity plan hidden inside a document repository does not help employees who do not know it exists.

7.4 Communication

Communication is critical before, during and after disruption.

The organization should consider:

Internal communication

- Employees
- Management
- Crisis teams
- Process owners

External communication

- Customers
- Suppliers
- Regulators
- Emergency services
- Partners
- Media, where applicable

And importantly:

What happens if the normal communication channel is itself unavailable?

ISO's business continuity guidance specifically highlights communication within the BCMS and preparedness to communicate following an incident when normal channels may be disrupted.

7.5 Documented Information

A BCMS requires appropriate documented information.

This can include:

- Policies
- Scope
- Objectives
- Analysis results
- Strategies
- Plans
- Procedures
- Exercise records
- Audit records
- Management-review records
- Corrective-action records

But the principle is:

Document what the system requires and control it effectively.

The goal is not to create documentation for its own sake.

5. Clause 8 â?? Operation

This is the operational heart of ISO 22301.

Clause 8 moves the organization from:

â??We have planned for continuity.â?•

to:

â??We have established and operate continuity arrangements.â?•

The major operational components include:

1. Operational planning and control
2. Business impact analysis and risk assessment
3. Business continuity strategies and solutions
4. Business continuity plans and procedures
5. Exercise programme
6. Evaluation of business continuity documentation and capabilities

This is where the BCMS becomes highly practical.

8.1 Operational Planning and Control

The organization needs to plan, implement and control the processes necessary to meet BCMS requirements.

This includes:

- Establishing criteria
- Implementing controls
- Maintaining documented information
- Controlling planned changes
- Reviewing unintended changes
- Controlling relevant outsourced processes

The objective is to ensure that continuity activities are not informal or inconsistent.

8.2 Business Impact Analysis and Risk Assessment

This is one of the most important areas of ISO 22301 implementation.

Business Impact Analysis – BIA

The BIA helps determine:

- What activities are critical?
- What happens if they stop?
- How severe is the impact?
- How quickly must they resume?
- What resources do they require?
- What dependencies exist?

Example

Imagine a SaaS organization has these activities:

Activity	Potential Impact of Disruption
Customer-facing application	Very high
Customer support	High
Billing	High
Marketing	Medium
Internal training	Lower during a major disruption

The organization then needs to understand the continuity requirements for the critical activities.

Risk Assessment

The risk assessment considers threats that could cause disruption.

Examples:

- Fire
- Flood
- Cyberattack
- Power failure
- Network failure
- Cloud outage

- Supplier failure
- Workforce unavailability
- Equipment failure
- Extreme weather
- Facility loss

But the objective isn't simply to create a long list of disasters.

The organization should connect:

Threat → Vulnerability → Disruption → Impact → Continuity Requirement

BIA + Risk Assessment

These two activities should work together.

Risk Assessment asks:

What could disrupt us?

BIA asks:

What happens if our activities are disrupted?

Together they help establish:

Priority → Requirement → Strategy → Response

8.3 Business Continuity Strategies and Solutions

Once the organization understands:

- Critical activities
- Impacts
- Risks
- Dependencies
- Recovery requirements

it can determine appropriate continuity strategies and solutions.

Examples may include:

People

- Cross-training
- Alternate personnel
- Remote-working capability

Facilities

- Alternate location
- Work-from-home
- Recovery site

Technology

- Redundancy
- Backup systems
- Alternate infrastructure
- Recovery environments

Suppliers

- Alternate suppliers
- Secondary logistics providers
- Contractual continuity requirements

Information

- Backups
- Alternate access
- Recovery arrangements

Operations

- Manual workarounds
- Alternate processes
- Prioritized services

There is no universal strategy.

The appropriate solution depends on:

Risk + Impact + Requirements + Cost + Organizational Context

8.4 Business Continuity Plans and Procedures

Now the organization documents how it will respond.

Plans may address:

- Incident response
- Crisis management
- Communication
- Continuity arrangements
- Recovery
- Escalation
- Roles
- Responsibilities
- Resource requirements

A good plan should answer:

Who?

Who takes action?

What?

What needs to happen?

When?

When is the plan activated?

How?

How are activities performed?

Who communicates?

Who informs customers, employees, suppliers or authorities?

What happens next?

How does the organization transition toward recovery and normal operations?

8.5 Exercise Programme

This is where many organizations underestimate ISO 22301.

A plan is an assumption.

An exercise provides evidence.

Testing and exercising can reveal:

- Missing contact information
- Unclear responsibilities
- Communication failures
- Unrealistic recovery assumptions
- Supplier weaknesses
- Technology limitations
- Training gaps

Possible exercises include:

Tabletop Exercise

Teams discuss a scenario.

Simulation

Participants respond to a simulated disruption.

Technical Recovery Test

Technical teams test recovery arrangements.

Communication Test

Notification and escalation channels are tested.

Full Exercise

A broader scenario tests multiple parts of the continuity arrangement.

The exercise methodology should match the organization's risks and continuity requirements.

8.6 Evaluation of Business Continuity Documentation and Capabilities

After exercises and other evaluations, the organization should determine whether its continuity arrangements remain suitable and effective.

Ask:

- Did the exercise achieve its objectives?
-

- Did people understand their roles?
- Were communication channels effective?
- Did recovery assumptions work?
- Were dependencies correctly identified?
- Were there unexpected failures?
- What needs to change?

This creates an important loop:

Exercise → Findings → Corrective Action → Improvement

That is how the BCMS matures.

6. Clause 9 → Performance Evaluation

Once the BCMS is operating, the organization needs to evaluate whether it is effective.

Clause 9 covers areas such as:

- Monitoring
 - Measurement
 - Analysis
 - Evaluation
 - Internal audit
 - Management review
-

9.1 Monitoring, Measurement, Analysis and Evaluation

Organizations should determine what needs to be:

Monitored

Measured

Analysed

Evaluated

Possible indicators include:

- Exercise completion
 - Training completion
 - Corrective-action closure
-

- Recovery-test performance
- Supplier continuity performance
- Plan review completion
- Incident-response performance
- BIA review status

The exact KPIs should reflect the organization's BCMS objectives.

9.2 Internal Audit

An internal audit provides an opportunity to evaluate whether the BCMS:

- Meets applicable requirements
- Is effectively implemented
- Is maintained
- Is producing intended results

A good internal audit shouldn't merely ask:

“Do you have the document?”

It should ask:

“Show me the evidence that the process works.”

For example:

Business Continuity Exercise

Don't just ask:

“Do you have an exercise procedure?”

Ask:

“Show me the last exercise, findings and resulting actions.”

That is much stronger evidence.

9.3 Management Review

Top management should review the BCMS at planned intervals.

Management review provides visibility into:

- BCMS performance
- Changes in context
- Audit results
- Exercise results
- Nonconformities
- Corrective actions
- Resource requirements
- Opportunities for improvement

Management review is important because business continuity is ultimately a **management responsibility**.

7. Clause 10 â?? Improvement

The final clause is:

Improvement

A BCMS cannot remain static.

The organization needs mechanisms to address problems and continually improve its continuity capability.

10.1 Nonconformity and Corrective Action

When a nonconformity occurs, the organization should:

Identify â?? Correct â?? Analyse Cause â?? Take Action â?? Verify Effectiveness

For example:

Finding

Emergency contact list contained outdated phone numbers.

Immediate correction

Update contact information.

Root cause

No defined ownership for contact-list review.

Corrective action

Assign ownership and establish periodic review.

Effectiveness check

Verify during the next exercise.

That is stronger than simply changing the phone numbers.

10.2 Continual Improvement

Continual improvement should be driven by evidence.

Sources can include:

- Internal audits
- Exercises
- Incidents
- Management reviews
- Corrective actions
- KPI trends
- Changes in technology
- Changes in suppliers
- Organizational changes
- Regulatory changes
- Climate-related considerations

The organization should continuously ask:

How can our continuity capability become more effective?

The ISO 22301 Management-System Cycle

The clauses can be visualized as a complete cycle:

CLAUSE 4

Understand the Organization

â??

CLAUSE 5

Leadership & Commitment

â??

CLAUSE 6

Plan

â??

CLAUSE 7

Provide Resources & Support

â??

CLAUSE 8

Operate the BCMS

â??

CLAUSE 9

Measure & Evaluate

â??

CLAUSE 10

Improve

â??

Back to Clause 4

Because the organizationâ??s environment changes.

ISO 22301 Clause 8 â?? The Operational Core

For many organizations, Clause 8 is where implementation becomes most tangible.

Think of it as:

Context

??

Critical Activities

??

Impact

??

Risk

??

Continuity Requirements

??

Strategy

??

Plans

??

Exercises

??

Evaluation

??

Improvement

This is the heart of a functioning BCMS.

ISO 22301: BIA vs Risk Assessment vs Business Continuity Plan

These three concepts are often confused.

Element	Main Question
Risk Assessment	What could disrupt us?

Element	Main Question
BIA	What happens if critical activities are disrupted?
Continuity Strategy	What approach will allow us to continue?
BC Plan	What will we actually do during disruption?
Exercise	Does the plan work?
Improvement	What should we change?

This sequence is extremely useful when explaining ISO 22301 to management teams.

ISO 22301 and ISO 27001 Integration

For technology-dependent organizations, integrating BCMS and ISMS can be useful.

ISO/IEC 27001

Focus:

Information Security

ISO 22301

Focus:

Business Continuity

The systems can share:

- Risk-management approaches
- Internal audit
- Management review
- Corrective action
- Competence
- Awareness
- Document control
- Leadership processes

But their objectives remain distinct.

ISO 22301 and ISO 9001 Integration

The same principle applies to quality management.

ISO 9001

Can we consistently provide products/services meeting requirements?

ISO 22301

Can we maintain important products/services when disruption occurs?

For many organizations, these management systems can be integrated rather than managed as completely separate programs.

Current ISO 22301 Status â?? Important for 2026

There are **two different things** organizations need to distinguish.

Current published standard

ISO 22301:2019

with:

ISO 22301:2019/Amd 1:2024 â?? Climate action changes

ISO currently lists the 2019 standard as published and its lifecycle indicates that it is to be revised.

Future revision

ISO currently has:

ISO/CD 22301

as a Committee Draft under development. ISO states that the draft will replace ISO 22301:2019, but it remains under development and is **not yet the published replacement standard**.

Therefore, for current certification content:

We should refer to:

ISO 22301:2019 + Amendment 1:2024

and clearly distinguish that from the future revision.

This distinction will also be important in Part 3 when discussing implementation and certification.

What Should an Auditor Look For?

A certification auditor is not simply looking for a beautifully formatted BCMS manual.

The organization should be able to demonstrate **objective evidence**.

For example:

Requirement Area	Potential Evidence
Context	Context analysis
Scope	Approved BCMS scope
Leadership	Policy, roles, management evidence
Objectives	BCMS objectives and monitoring
BIA	Approved BIA results
Risk Assessment	Risk assessment records
Strategy	Approved continuity strategies
Plans	Current BC plans
Training	Training records
Exercises	Exercise reports
Evaluation	Test/exercise results
Internal Audit	Audit reports
Management Review	Meeting records
Corrective Action	CARs and effectiveness evidence
Improvement	Improvement records

The key principle:

Documents show what you planned. Evidence shows what you did.

Common ISO 22301 Implementation Mistakes

• Mistake 1: Treating BCMS as an IT project

Business continuity is broader than IT recovery.

• Mistake 2: Creating a generic BCP

A generic template may not reflect actual processes, dependencies or risks.

• Mistake 3: Skipping the BIA

Without understanding business impacts, continuity priorities can become arbitrary.

• Mistake 4: Creating plans without testing them

An untested plan contains assumptions.

• Mistake 5: Ignoring suppliers

Third-party dependencies can become critical points of failure.

• Mistake 6: Forgetting people

A technically recoverable system may still fail if nobody knows what to do.

• Mistake 7: Treating the BCMS as a one-time project

Business continuity requirements change as the organization changes.

CK Associates Consultant's Insight

When implementing ISO 22301, one of the most useful questions to ask is:

•Show me what happens if this critical activity stops.•

Then follow the chain.

What stops?

•

Who is affected?

•

What is the impact?

•

How quickly must it recover?

â??

What resources are required?

â??

What dependencies exist?

â??

What continuity strategy is available?

â??

Who activates the plan?

â??

How do we test it?

â??

What did the test teach us?

That conversation often reveals more about BCMS maturity than simply reviewing a stack of documents.

ISO 22301 Clause 4â??10 Quick Reference

Clause	Main Focus	Practical Question
4	Context	What are we protecting and what affects us?
5	Leadership	Who owns and supports continuity?
6	Planning	What objectives and actions are needed?
7	Support	Do we have competent people and resources?
8	Operation	How do we prepare, respond and recover?
9	Evaluation	How do we know the BCMS works?
10	Improvement	How do we correct and improve?

Key Takeaways

- â? Clause 4 establishes the organizational context and BCMS scope.
- â? Clause 5 establishes leadership, policy and responsibilities.

â? Clause 6 addresses risks, opportunities and BCMS objectives.

â? Clause 7 provides resources, competence, awareness, communication and documented information.

â? Clause 8 is the operational core, covering BIA, risk assessment, strategies, plans, exercises and evaluation.

â? Clause 9 evaluates BCMS performance through monitoring, internal audit and management review.

â? Clause 10 addresses nonconformity, corrective action and continual improvement.

â? A BIA is not the same as a risk assessment.

â? A business continuity plan is not the same as a BCMS.

â? Exercises provide evidence that continuity arrangements can actually be tested and improved.

â? ISO 22301:2019 has a published 2024 climate-action amendment.

â? A future ISO/CD 22301 revision is under development and should not be confused with the current published certification standard.



How do you implement ISO 22301:2019?

ISO 22301:2019 implementation involves establishing, implementing, maintaining and continually improving a Business Continuity Management System (BCMS). A practical implementation normally begins by defining the BCMS scope and understanding organizational context and interested parties. The organization then performs a gap analysis, identifies business continuity risks, conducts a Business Impact Analysis (BIA), establishes continuity strategies and develops appropriate plans and procedures. Training, awareness, communication and exercising are then used to demonstrate that the BCMS can operate in practice. Internal audits and management review provide formal performance evaluation before corrective actions and certification readiness activities. An independent certification body can then conduct the certification audit. ISO 22301:2019 currently has Amendment 1:2024 concerning climate action considerations; ISO also has a future ISO/CD 22301 under development, which is not the current published certification standard.

What are the steps for ISO 22301 certification?

The typical ISO 22301 implementation and certification journey is:

Scope Gap Analysis Context & Risk Assessment BIA Continuity Strategy BCMS Documentation Plans & Procedures Training Exercises Internal Audit Management Review Corrective Action Certification Audit Continual Improvement

The exact implementation sequence should be adapted to the organization's size, complexity, products/services, risks and continuity requirements.

Having understood **what ISO 22301 is** in Part 1 and the **requirements of Clauses 4-10** in Part 2, the next practical question is:

How does an organization actually implement ISO 22301 and become ready for certification?

This is where many organizations encounter difficulties.

Creating a Business Continuity Plan alone does not establish an effective BCMS.

ISO 22301 is a **management system**, which means the organization needs a structured mechanism for understanding disruption risks, determining priorities, establishing continuity capabilities, testing those capabilities, evaluating performance and continually improving the system.

ISO describes ISO 22301:2019 as a framework for organizations to plan, establish, implement, operate, monitor, review, maintain and continually improve a BCMS.

This guide explains a practical implementation pathway from the first gap analysis through certification readiness.

1. Start by Defining the BCMS Scope

The first major implementation decision is:

What exactly will the BCMS cover?

The scope should clearly identify the organizational activities, locations, products, services, processes and relevant interfaces covered by the BCMS.

For example:

Provision of cloud-based software development, hosting, technical support and managed IT services from the organization's Hyderabad operations and associated supporting infrastructure.

Another organization may define a scope around:

- manufacturing operations
- warehouse and logistics
- healthcare services
- financial services
- data-centre operations
- customer support
- shared services
- corporate functions

Why scope matters

An unclear scope can create problems later during:

- BIA
- risk assessment
- continuity planning
- exercise design
- internal audit
- certification audit

The scope should therefore reflect the organization’s actual continuity requirements rather than simply listing every department.

2. Conduct an ISO 22301 Gap Analysis

Before building the BCMS, determine:

Where are we today?

A gap analysis compares the organization’s existing business continuity arrangements against applicable ISO 22301 requirements.

A practical gap assessment may examine:

Area	Questions
Context	Have internal and external issues been identified?
Interested parties	Are relevant requirements understood?
Scope	Is the BCMS scope clearly defined?
Leadership	Is management actively supporting continuity?
Policy	Is there an appropriate BCMS policy?
Risk	Are continuity-related risks assessed?
BIA	Are critical activities and impacts identified?
Strategy	Are continuity strategies established?
Plans	Are response and recovery arrangements documented?

Area	Questions
Resources	Are people, technology and facilities available?
Exercises	Are plans tested?
Internal audit	Is the BCMS independently evaluated internally?
Management review	Does top management review BCMS performance?

The result should not simply be a list of missing documents.

A good gap analysis identifies:

Requirement Current Practice Evidence Gap Risk/Impact Action Required
Responsibility Target Date

3. Understand Organizational Context

The implementation team should establish the context in which continuity decisions will be made.

Consider factors such as:

Internal issues

- organizational structure
- critical personnel
- technology dependencies
- facilities
- infrastructure
- financial resources
- supplier dependencies
- operational processes
- existing management systems

External issues

- regulatory requirements
- customer requirements
- market conditions
- geographic risks
- supply-chain dependencies
- infrastructure availability
- environmental conditions
- climate-related considerations
- technology changes

The 2024 climate amendment applies to ISO 22301:2019, so organizations implementing or maintaining the standard should consider whether climate change is a relevant issue affecting the

BCMS's intended results.

4. Identify Interested Parties and Continuity Requirements

Business continuity is not determined only by internal management.

Organizations may have continuity-related requirements from:

- customers
- regulators
- government authorities
- shareholders
- employees
- suppliers
- business partners
- insurers
- lenders
- parent companies
- contractual customers

default watermark

For example, an enterprise customer may require:

- defined recovery expectations
- incident communication
- disaster recovery testing
- alternate-site capability
- supplier continuity
- documented recovery arrangements

These requirements should feed into the BCMS.

5. Conduct the Business Impact Analysis (BIA)

The **Business Impact Analysis** is one of the most important activities in ISO 22301 implementation.

The objective is to understand:

What happens if a particular activity or service is disrupted?

A BIA typically evaluates:

- critical products/services

- supporting activities
- dependencies
- impacts of disruption
- maximum tolerable period of disruption
- recovery priorities
- required resources
- recovery objectives
- internal and external dependencies

Example BIA

Consider an online payment platform.

Activity	Impact of disruption	Priority
Payment processing	Revenue/customer impact	Critical
Customer support	Service dissatisfaction	High
Internal reporting	Management information delayed	Medium
Administrative filing	Limited immediate impact	Lower

The organization can then determine which activities require the fastest recovery and which resources are essential.

6. Perform Business Continuity Risk Assessment

BIA and risk assessment are related, but they answer different questions.

Risk Assessment asks:

What could disrupt us, and how likely/severe could it be?

BIA asks:

What happens to our organization if an activity is disrupted, and how quickly must it be recovered?

Potential disruption scenarios can include:

- cyber incidents
- power failure

- telecommunications failure
- fire
- flood
- extreme weather
- critical supplier failure
- facility unavailability
- workforce disruption
- technology failure
- data loss
- transportation disruption
- utility interruption

The assessment should consider the organization's actual operating environment rather than relying on generic risk registers.

7. Establish Business Continuity Strategies

Once critical activities, impacts and risks are understood, the organization needs to determine:

How will we continue or recover?

Possible strategies can involve:

- alternate work locations
- remote working
- backup infrastructure
- redundant systems
- alternate suppliers
- additional inventory
- backup communication channels
- data backup
- alternate utilities
- cross-trained personnel
- succession arrangements
- reciprocal arrangements
- manual workarounds
- cloud-based recovery infrastructure

The appropriate strategy depends on the organization's:

- risk profile
- BIA results
- regulatory requirements
- technology architecture
- financial resources
- customer commitments

- operational complexity
-

8. Develop Business Continuity Plans and Procedures

The strategy needs to become operational.

A BCMS may therefore include documented arrangements for:

Incident response

What happens when a disruption occurs?

Crisis management

Who makes strategic decisions?

Emergency response

How are immediate safety and operational issues handled?

Business continuity

How are critical activities maintained?

IT disaster recovery

How are technology services restored?

Recovery

How does the organization return to normal or stabilized operations?

Communication

Who communicates with employees, customers, regulators and other interested parties?

9. Establish Roles and Responsibilities

A continuity plan is ineffective if everyone assumes somebody else will activate it.

Clearly define:

- BCMS manager/coordinator
- crisis management team
- incident response team
- IT recovery team
- facilities team
- HR responsibilities
- communications responsibility
- department continuity coordinators
- top-management authority
- escalation routes

The organization should also define:

Who can activate the plan?

Who declares a crisis?

Who communicates externally?

Who authorizes emergency expenditure?

Who coordinates recovery?

10. Training and Awareness

People are a central component of business continuity.

Employees should understand:

- the organization's continuity policy
- their responsibilities
- escalation procedures
- emergency contacts
- communication channels
- relevant continuity procedures
- incident reporting
- recovery responsibilities

Training should be appropriate to the person's role.

For example, an IT recovery team needs different training from a customer-service employee.

11. Test the BCMS Through Exercises

One of the most important differences between a documented plan and an operational BCMS is **testing**.

A plan may appear excellent on paper but fail during an actual disruption.

Organizations can use different exercise methods, such as:

Tabletop exercise

Teams discuss a simulated scenario.

Walkthrough

Participants review procedures step by step.

Simulation

A realistic scenario is used to test decision-making and response.

Technical recovery test

Technology recovery capabilities are tested.

Communication exercise

Emergency communication channels are tested.

Full-scale exercise

Multiple teams and capabilities participate in a coordinated scenario.

The exercise should produce evidence.

For example:

Scenario Participants Objective Actions Observations Gaps Corrective Actions Re-test

12. Evaluate Continuity Documentation and Capabilities

Testing should not become a “tick-box” exercise.

After an exercise, ask:

- Did people know their roles?
- Were contact details current?
- Could the required systems be accessed?
- Were escalation routes effective?
- Were recovery priorities understood?
- Did suppliers respond as expected?
- Were communication channels available?
- Were recovery targets realistic?
- Were there resource constraints?

This evaluation provides evidence for continual improvement.

13. Establish Internal Audit

Before certification, the organization should conduct an internal audit of the BCMS.

The internal audit should evaluate whether:

1. the BCMS conforms to applicable requirements;
2. documented processes are implemented;
3. operational arrangements are functioning;
4. evidence supports the claimed controls;
5. exercises and evaluations are being performed;
6. corrective actions are being addressed.

A strong internal audit should go beyond:

• Is the document available?

It should also ask:

• Can the organization demonstrate that the process works?

14. Conduct Management Review

Top management should review the BCMS to determine whether it remains suitable, adequate and effective.

Typical management review inputs can include:

- internal audit results
 - objectives
 - continuity exercise results
-

- incidents
- nonconformities
- corrective actions
- performance trends
- changes in internal/external issues
- interested-party requirements
- risks and opportunities
- resource requirements
- opportunities for improvement

The output should include decisions and actions where required.

15. Correct Nonconformities Before Certification

The internal audit may identify:

- missing evidence
- outdated procedures
- incomplete BIA
- insufficient exercise evidence
- unclear responsibilities
- ineffective corrective actions
- outdated contact lists
- supplier continuity gaps
- inconsistent documentation

These should be addressed systematically.

A practical corrective-action structure is:

Nonconformity	Root Cause	Correction	Corrective Action	Responsibility	Target Date	Verification of Effectiveness
---------------	------------	------------	-------------------	----------------	-------------	-------------------------------

16. Certification Audit

Once the BCMS has been implemented and the organization considers itself ready, it can engage an independent certification body.

The certification process commonly involves two stages.

Stage 1 – Readiness / Documentation Review

Stage 1 generally evaluates whether the organization has established a sufficiently developed management system and is prepared for the main certification assessment.

Typical areas include:

- BCMS scope
- organizational context
- policy
- objectives
- risk approach
- BIA methodology/results
- continuity strategies
- documented information
- preparedness for Stage 2
- organizational understanding of requirements

The certification body determines its audit activities according to applicable certification rules and the organization's circumstances.

17. Stage 2 – Certification Audit

Stage 2 focuses on the implementation and effectiveness of the BCMS.

Auditors may examine evidence such as:

- employee interviews
- BIA records
- risk assessments
- continuity plans
- exercise records
- training records
- incident records
- supplier arrangements
- internal audit reports
- management review records
- corrective-action records
- operational evidence

The key question is not merely:

“Do you have a document?”

It is:

• Can you demonstrate that the BCMS is implemented and functioning? •

18. Certification Decision

After the certification audit, the certification body evaluates the audit findings through its certification process.

Possible audit outcomes can involve:

- conformity
- opportunities for improvement
- nonconformities requiring corrective action

The exact handling and timelines depend on the certification body's applicable certification procedures.

Once certification is granted, the organization enters the applicable surveillance and recertification cycle.

19. ISO 22301 Certification Timeline

There is **no universal implementation timeline** for ISO 22301.

It depends on:

- organization size
- number of locations
- BCMS scope
- process complexity
- number of critical services
- existing continuity arrangements
- technology dependencies
- supplier complexity
- availability of management and process owners
- maturity of existing documentation
- exercise requirements
- speed of corrective actions

A practical project structure could look like:

Phase	Major Activities
Phase 1	Scope + Gap Analysis

Phase	Major Activities
Phase 2	Context + Interested Parties
Phase 3	BIA + Risk Assessment
Phase 4	Continuity Strategies
Phase 5	Plans + Procedures
Phase 6	Training + Awareness
Phase 7	Exercises + Evaluation
Phase 8	Internal Audit
Phase 9	Management Review
Phase 10	Corrective Actions
Phase 11	Certification Audit

The organization should establish its actual schedule based on its complexity rather than selecting an arbitrary number of weeks.

20. ISO 22301 Certification Cost in India

The total cost of ISO 22301 certification can contain several components.

Consulting / implementation cost

Depending on the project, this can include:

- gap analysis
- BIA facilitation
- risk assessment
- documentation
- implementation support
- training
- exercises
- internal audit
- management review support
- certification preparation

Certification body cost

The certification body's fee can depend on factors such as:

- organization size
- employee count
- scope
- number of locations
- complexity

- audit duration
- applicable certification rules

Additional costs

Organizations may also incur costs associated with:

- disaster recovery technology
- backup infrastructure
- alternate facilities
- emergency communication systems
- specialist training
- exercise implementation
- travel
- additional operational resources

Therefore, an organization should not interpret **ISO 22301 certification cost** as simply the price of the certificate.

The larger financial consideration is often the resources required to establish and maintain effective continuity capability.

21. Common ISO 22301 Implementation Mistakes

• Mistake 1: Treating ISO 22301 as a document project

A large collection of documents does not automatically demonstrate an effective BCMS.

• Mistake 2: Copying a generic BCP

A continuity plan should reflect the organization's actual processes, dependencies and recovery requirements.

• Mistake 3: Conducting BIA as a questionnaire exercise

The BIA should support real prioritization and continuity decisions.

• Mistake 4: Ignoring suppliers

A critical service may depend on an external supplier.

• Mistake 5: Not testing plans

Untested plans provide limited evidence of operational capability.

• Mistake 6: Ignoring people dependency

Critical processes may depend on specific individuals or specialized skills.

• Mistake 7: Combining cybersecurity and business continuity without understanding the difference

Cybersecurity is an important continuity consideration, but business continuity encompasses a wider range of disruptions.

• Mistake 8: Forgetting management involvement

BCMS effectiveness requires leadership, resources and organizational ownership.

• Mistake 9: Treating internal audit as a formality

Internal audit should identify genuine implementation weaknesses before the external audit.

• Mistake 10: Ignoring the current climate amendment

ISO 22301:2019 has Amendment 1:2024 concerning climate action considerations. Organizations should ensure this amendment is appropriately considered within their BCMS.

22. ISO 22301 + ISO 27001 Integration

For technology-driven organizations, integrating ISO 22301 with **ISO/IEC 27001** can be practical because the two management systems address related but distinct areas.

ISO 22301 focuses on:

Business continuity and organizational resilience

ISO/IEC 27001 focuses on:

Information security management

There can be common areas such as:

- organizational context
 - leadership
 - risk management
 - documented information
 - competence
-

- internal audit
- management review
- corrective action

This can support an **Integrated Management System (IMS)** approach where appropriate.

23. ISO 22301 + ISO 9001 Integration

Organizations already operating ISO 9001 may also integrate BCMS processes into their existing management-system framework.

Potential common areas include:

- context
- leadership
- objectives
- competence
- documented information
- internal audit
- management review
- corrective action
- continual improvement

default watermark

The integration should preserve the specific requirements and objectives of each standard.

24. Practical ISO 22301 Implementation Example

Consider a Hyderabad-based SaaS company providing a business-critical platform to customers across India.

Step 1 ??? Scope

The organization includes:

- SaaS platform
- cloud infrastructure management
- technical support
- customer operations
- critical corporate support functions

Step 2 ??? BIA

The company determines that:

Platform availability is critical.

Customer support is high priority.

Internal reporting is lower priority.

Step 3 â?? Risk Assessment

Potential disruptions include:

- cloud infrastructure outage
- cyber incident
- internet connectivity failure
- power disruption
- key-person dependency
- third-party service failure

Step 4 â?? Strategy

The organization establishes:

- redundant infrastructure
- backup systems
- alternate communication channels
- cross-trained personnel
- supplier escalation arrangements
- documented recovery procedures

Step 5 â?? Exercise

A simulated cloud-service disruption is conducted.

The organization discovers that:

One critical supplier escalation contact is outdated.

Step 6 â?? Corrective Action

The organization:

- updates supplier information
- assigns ownership
- introduces periodic verification
- tests the escalation route again

This is an important BCMS principle:

Exercise â?? Evidence â?? Gap â?? Corrective Action â?? Re-test â?? Improvement

That cycle demonstrates how business continuity becomes a management system rather than a static emergency document.

25. ISO 22301 Certification Readiness Checklist

Before inviting the certification body, organizations should be able to demonstrate evidence across the BCMS.

Governance

- BCMS scope established
- BCMS policy established
- roles and responsibilities defined
- management commitment demonstrated

Context

- internal issues identified
- external issues identified
- interested parties identified
- applicable requirements determined
- climate change relevance considered

Risk & BIA

- BIA methodology established
- BIA completed
- critical activities identified
- dependencies identified
- continuity risks assessed
- recovery priorities established

Strategy

- continuity strategies defined
- resources identified
- supplier dependencies considered
- technology dependencies considered

Plans

- continuity plans established
- incident response arrangements established

- communication arrangements established
- recovery procedures established
- responsibilities assigned

People

- competency requirements identified
- training completed
- awareness conducted
- emergency contacts verified

Testing

- exercise programme established
- exercises conducted
- exercise results documented
- gaps identified
- corrective actions completed

Performance Evaluation

- monitoring established
- internal audit completed
- management review completed

Improvement

- nonconformities addressed
- corrective actions implemented
- effectiveness verified
- continual improvement demonstrated

26. What Auditors May Look for During ISO 22301 Assessment

A useful way to prepare is to think in terms of **evidence chains**.

For example:

Requirement

Critical business activity needs continuity.

â??

Evidence

BIA identifies the activity as critical.

â??

Strategy

A documented continuity strategy exists.

â??

Plan

A responsible team has a documented procedure.

â??

Capability

People have been trained.

â??

Exercise

The procedure has been tested.

â??

Evaluation

Exercise results identify gaps.

â??

Improvement

Corrective actions were implemented and effectiveness evaluated.

This evidence chain is much stronger than simply presenting a folder of documents.

27. ISO 22301 Current Status: An Important 2026 Note

Organizations researching ISO 22301 may encounter information about a future revision.

As of 2026, ISO lists:

Current published standard

ISO 22301:2019

with:

ISO 22301:2019/Amd 1:2024 Climate action changes

ISO’s official page currently lists the 2019 standard as published and identifies Amendment 1:2024 as applying to it.

Future revision

ISO/CD 22301 is currently under development and is intended to replace ISO 22301:2019. It is a **Committee Draft**, not the current published certification standard.

Therefore, organizations should be careful with online articles claiming that a new ISO 22301 edition has already replaced the 2019 edition.

For implementation and certification discussions, the current published basis should be clearly distinguished from the future revision.

28. ISO 22313:2020 The Supporting Guidance Standard

Organizations implementing ISO 22301 may also refer to ISO 22313:2020.

ISO describes ISO 22313 as guidance and recommendations for applying ISO 22301’s BCMS requirements. It is applicable to organizations of different sizes and types.

ISO’s current information also shows that ISO 22313:2020 remains the published guidance edition while a future ISO/AWI 22313 project is under development.

This distinction is important:

Document	Role
ISO 22301:2019	BCMS requirements
ISO 22301:2019/Amd 1:2024	Climate action amendment
ISO 22313:2020	Guidance for applying ISO 22301
ISO/CD 22301	Future revision under development

Document	Role
ISO/AWI 22313	Future guidance revision under development

29. ISO 22301 Implementation: The Complete Roadmap

A simplified implementation roadmap looks like this:

- DEFINE
 - â??
- BCMS SCOPE
 - â??
- GAP ANALYSIS
 - â??
- CONTEXT & INTERESTED PARTIES
 - â??
- BUSINESS IMPACT ANALYSIS
 - â??
- RISK ASSESSMENT
 - â??
- CONTINUITY STRATEGIES
 - â??
- PLANS & PROCEDURES
 - â??
- TRAINING & AWARENESS
 - â??
- EXERCISES & TESTING
 - â??
- PERFORMANCE EVALUATION
 - â??
- INTERNAL AUDIT
 - â??
- MANAGEMENT REVIEW
 - â??
- CORRECTIVE ACTION
 - â??
- CERTIFICATION AUDIT
 - â??
- CONTINUAL IMPROVEMENT

This is the practical transformation:

Risk â?? Preparedness â?? Response â?? Recovery â?? Learning â?? Improvement

Consultantâ??s Insight â?? CK Associates

In practical ISO 22301 implementation, one of the most important questions is not:

Do you have a Business Continuity Plan?

The more useful question is:

Can your organization demonstrate that its critical services can continue or recover at the required capacity when a realistic disruption occurs?

That changes the implementation approach significantly.

A mature BCMS connects:

BIA + Risk Assessment + Strategy + Resources + Plans + People + Technology + Suppliers + Exercises + Management Review

rather than treating each component as an isolated document.

For organizations in **Hyderabad, Telangana and across India**, this is particularly relevant for sectors with strong technology, customer-service, manufacturing, healthcare, logistics, financial-service and shared-service dependencies.

The objective of ISO 22301 implementation should therefore be to establish an operational management system that supports organizational resilience—not simply to prepare documentation for an audit.

Why Trust This Guidance?

CK Associates provides ISO management-system consulting and implementation support with:

- **20+ years** of consulting experience
- **450+ certification projects**
- **8+ expert consultants**
- Experience across multiple ISO management-system standards
- Implementation support covering gap analysis, documentation, training, internal audit and certification readiness
- Hyderabad-based consulting with support across India

Founder & Lead ISO Consultant:
Sirish K

Frequently Asked Questions

1. How long does ISO 22301 implementation take?

There is no single mandatory implementation period. The timeline depends on organizational size, scope, complexity, existing BCMS maturity, number of locations, critical services, BIA requirements, exercises and availability of resources.

2. Is a Business Continuity Plan enough for ISO 22301 certification?

No. ISO 22301 is a Business Continuity Management System standard. A BCP is one component of a broader system involving context, leadership, planning, BIA, risk assessment, strategies, plans, exercises, performance evaluation and continual improvement.

3. Is BIA mandatory for ISO 22301?

Business Impact Analysis is a central part of the operational requirements of ISO 22301 and is used to determine the impact of disruption and continuity priorities. It should be integrated into the organization's BCMS methodology rather than treated as an isolated report.

4. Does ISO 22301 cover disaster recovery?

ISO 22301 addresses business continuity at the organizational level. Disaster recovery, particularly IT disaster recovery, can form an important component of the organization's continuity strategies and arrangements, but business continuity is broader than IT recovery alone.

5. Can ISO 22301 be integrated with ISO 27001?

Yes. Organizations can integrate relevant management-system elements where their scopes and processes support integration. ISO 22301 addresses business continuity, while ISO/IEC 27001 addresses information security management.

6. Can SMEs implement ISO 22301?

Yes. ISO states that ISO 22301 and its supporting guidance are applicable to organizations of different sizes and types. The extent and complexity of implementation should reflect the organization's operating environment and complexity.

7. Is ISO 22301:2019 still current?

ISO currently lists ISO 22301:2019 as the published standard and also lists Amendment 1:2024 concerning climate action changes. A new ISO/CD 22301 is under development, but it is not the current published certification standard.

8. What is ISO 22313?

ISO 22313:2020 provides guidance and recommendations for applying ISO 22301's BCMS requirements. It is a guidance standard rather than the certification requirements standard itself.

9. What happens after ISO 22301 certification?

Certification does not mean the BCMS project ends. The organization needs to maintain the management system, monitor performance, conduct applicable audits and reviews, exercise continuity arrangements and continually improve the BCMS.

10. Can CK Associates help with ISO 22301 implementation in Hyderabad?

CK Associates can support organizations through the major implementation activities, including **gap analysis, BCMS design, documentation, BIA, risk assessment, training, implementation support, internal audit and certification readiness.**

For organizations seeking ISO 22301 certification in Hyderabad or elsewhere in India, the appropriate project approach depends on the organization's scope and continuity requirements.

Key Takeaways

ISO 22301 implementation is not simply documentation.

It is a structured management-system journey:

1. Define the scope
 2. Understand the organization
 3. Conduct gap analysis
 4. Perform BIA
 5. Assess continuity risks
 6. Establish strategies
 7. Develop plans and procedures
 8. Train people
 9. Exercise the BCMS
 10. Audit the system
-

11. Conduct management review
12. Correct gaps
13. Complete certification audit
14. Continually improve

The strongest BCMS is one that can demonstrate its capability **before** a disruption happens.

Summary

ISO 22301:2019 is the international standard for Business Continuity Management Systems (BCMS). Its implementation involves defining the BCMS scope, understanding organizational context and interested parties, conducting Business Impact Analysis and continuity risk assessment, establishing continuity strategies, developing plans and procedures, training personnel, exercising the BCMS, performing internal audits and management review, addressing nonconformities and preparing for independent certification. ISO 22301:2019 currently has **Amendment 1:2024 on climate action changes**. A future ISO/CD 22301 revision is under development and should not be confused with the current published certification standard. ISO 22313:2020 provides guidance for applying ISO 22301.



[Let's Start Implementing](#)

Category

1. Blog

Date Created

20/09/2026

Author

ckassociates-biz

default watermark