PACIFIC CERTIFICATIONS

ISO 22301:2019

BUSINESS CONTINUITY MANAGEMENT SYSTEM

IMPLEMENTATION GUIDE

Plan	Do	Check	Act
Understand context, continuity requirements, risks and business impacts	Implement continuity strategies, response procedures and recovery controls	Exercise, test, monitor, review, audit and evaluate BCMS performance	Correct gaps, improve capability and update continuity arrangements

A practical clause-wise implementation guide for organizations preparing for ISO 22301:2019 certification, internal implementation, readiness assessment, or business continuity improvement.

Use of this guide: This guide is a practical implementation document. It does not replace the official ISO 22301:2019 standard. Organizations should use the official standard for exact requirements and use this guide as an implementation support resource.

HOW TO USE THIS GUIDE

This guide is designed for management teams, BCMS coordinators, process owners, internal auditors and implementation teams. It follows the structure of ISO 22301:2019 and translates the requirements into practical actions, examples of documented information, and readiness checks.

Start by confirming scope and interested parties, then complete business impact analysis and risk assessment. Use the later sections to build continuity strategies, plans, exercises, internal audits and management review evidence.

No.	Section
1	Understanding ISO 22301:2019
2	BCMS fundamentals
3	Benefits of implementation
4	PDCA model for BCMS
5	Implementation roadmap
6	Clause 4 - Context of the organization
7	Clause 5 - Leadership
8	Clause 6 - Planning
9	Clause 7 - Support
10	Clause 8 - Operation: BIA and risk assessment
11	Clause 8 - Strategies, plans and response
12	Exercise and testing
13	Clause 9 - Performance evaluation
14	Clause 10 - Improvement
15	Documented information toolkit
16	Certification readiness checklist
17	90-day implementation planner
18	Frequently asked questions

1. UNDERSTANDING ISO 22301:2019

ISO 22301:2019 sets out requirements for a Business Continuity Management System (BCMS). The purpose of a BCMS is to help an organization continue priority activities at acceptable levels during disruption and recover in a structured manner.

The standard follows a management system approach. It connects business continuity with leadership, planning, support, operation, performance evaluation and continual improvement. This is different from a one-time disaster recovery document because it requires governance, evidence and regular review.

BCMS element	Practical meaning
Priority activities	Activities that must be restored quickly to protect critical products, services and obligations.
Business impact analysis	A method used to understand disruption consequences, recovery priorities and resource needs.
Risk assessment	Identification and evaluation of disruption scenarios that could affect continuity.
Continuity strategy	Chosen approach to maintain or restore activities, such as alternate site, backup systems or dual suppliers.
Business continuity plan	Documented response and recovery arrangements used during an incident.
Exercise and test	A planned activity to confirm whether arrangements work as intended.

Implementation note: ISO 22301 can be applied by small, medium and large organizations. The system should be scaled to the organization’s activities, risks, complexity, resources and customer requirements.

2. BUSINESS CONTINUITY MANAGEMENT SYSTEM FUNDAMENTALS

An effective BCMS helps an organization make practical decisions before disruption occurs. It defines what must continue, how quickly activities must recover, who will lead response, what resources are needed and how information will be communicated.

Topic	Implementation focus	Typical evidence
Scope	Define sites, services, departments and boundaries included in the BCMS.	BCMS scope statement, organization chart, process map
Interested parties	Identify customers, regulators, employees, suppliers, insurers and community expectations.	Interested party register, legal and contractual requirements
BIA	Determine impact over time and recovery priorities.	BIA templates, RTO/MTPD records, dependency mapping
Risk assessment	Identify threats and vulnerabilities affecting continuity.	Risk register, risk criteria, treatment plan
Plans	Define incident response, communication and recovery steps.	BCP, crisis plan, call tree, recovery procedures
Exercises	Validate capability through drills, tabletop exercises and tests.	Exercise plan, attendance, findings, action log

3. BENEFITS OF IMPLEMENTATION

ISO 22301 implementation gives structure to resilience. It helps organizations move from informal crisis response to planned, tested and auditable continuity capability.

Benefit area	Expected result
Operational resilience	Priority activities are identified and recovery arrangements are defined.
Customer confidence	Customers gain confidence that products and services can continue after disruption.
Legal and contractual assurance	Continuity obligations are identified and managed.
Risk control	Disruption scenarios are assessed and treatments are assigned.
Incident response	Escalation, roles and communications are clearer during a crisis.
Supply chain continuity	Dependencies and supplier risks are identified and addressed.
Management control	Exercises, audits and management reviews provide performance evidence.

Typical business outcomes

- Reduced interruption time for critical activities
- Improved preparedness for cyber, facility, supplier, utility and people-related disruptions
- Clear responsibilities during emergency response and recovery
- Better evidence for clients, tenders, insurers and regulators
- Improved integration with risk management and operational planning

4. PDCA MODEL FOR BUSINESS CONTINUITY MANAGEMENT

ISO 22301 uses the Plan-Do-Check-Act logic. The BCMS should be planned, implemented, monitored and improved through a controlled cycle.

PDCA stage	ISO 22301 clauses	What the organization should do
Plan	Clauses 4, 5, 6	Define context, scope, interested parties, BCMS policy, objectives, risks and continuity requirements.
Do	Clauses 7, 8	Provide support, conduct BIA and risk assessment, develop strategies and implement business continuity procedures.
Check	Clause 9	Monitor performance, exercise and test arrangements, conduct internal audit and management review.
Act	Clause 10	Correct nonconformities, capture lessons learned and improve the BCMS.

PDCA application: The PDCA cycle should apply not only to the entire BCMS but also to individual plans, departments, suppliers and recovery arrangements. Exercise findings should feed directly into improvement actions.

5. IMPLEMENTATION ROADMAP

Step	Activity	Output
Step 1	Confirm BCMS scope	Define products, services, sites, departments and boundaries covered.
Step 2	Set governance	Assign BCMS owner, response team, roles and reporting channels.
Step 3	Identify requirements	Determine interested parties, legal, regulatory, customer and contractual obligations.
Step 4	Conduct BIA	Identify priority activities, impacts, RTOs, MTPDs, dependencies and minimum resources.
Step 5	Assess continuity risks	Evaluate disruption scenarios and existing controls.
Step 6	Select strategies	Choose continuity and recovery strategies aligned with BIA and risks.
Step 7	Create plans	Prepare business continuity, incident response, crisis communication and recovery procedures.
Step 8	Train and communicate	Make people aware of roles, escalation and continuity procedures.
Step 9	Exercise and audit	Test plans, complete internal audit and conduct management review.
Step 10	Improve	Close actions, update documents and prepare for certification assessment.

6. CLAUSE 4 - CONTEXT OF THE ORGANIZATION

Clause 4 requires the organization to understand its context and determine the scope of the BCMS. This should include internal and external issues that affect continuity capability and the expectations of interested parties.

Implementation actions

- Define the organization, sites, functions, services and boundaries under the BCMS.
- Identify internal issues such as staffing, systems, infrastructure, culture, processes and dependencies.
- Identify external issues such as regulatory requirements, market expectations, supplier risk, geography, climate, utilities and emergency services.
- Identify interested parties and determine which requirements are relevant to continuity.
- Prepare a scope statement that is clear enough for certification assessment.

Evidence to retain	Examples
Context analysis	SWOT, PESTLE, risk context summary, business environment review
Interested party register	Customers, regulators, employees, suppliers, owners, insurers, emergency services
Scope statement	Sites, business units, products/services, exclusions and justification
Process/dependency map	Critical functions, supporting services, outsourced processes

7. CLAUSE 5 - LEADERSHIP

Leadership is essential for business continuity because continuity arrangements require resources, decision-making authority and organization-wide coordination. Top management should ensure the BCMS is aligned with strategic direction and that responsibilities are clear.

Leadership requirement	Practical evidence
BCMS policy	Approved policy showing commitment to continuity, improvement and applicable requirements.
Roles and authorities	BCMS owner, incident response roles, crisis management team, plan owners, deputies.
Resource commitment	Budget, tools, alternate arrangements, training time and testing resources.
Communication	Awareness messages, leadership briefings, escalation protocols and reporting lines.
Review and oversight	Management review, objectives review, action tracking and approval of continuity strategies.

Implementation note: Management commitment should be visible in approvals, communication, resource allocation and participation in exercises or review meetings. The BCMS should not be seen only as an administrative document set.

8. CLAUSE 6 - PLANNING

Planning covers actions to address risks and opportunities, business continuity objectives and controlled change. Objectives should be measurable and relevant to continuity performance.

Planning area	What to define	Example KPI or evidence
Risks and opportunities	Risks to BCMS effectiveness and improvement opportunities.	Risk register, action plan, review records
BC objectives	Measurable targets aligned with continuity needs.	Exercise completion rate, plan review status, RTO test success
Change planning	Method to update BCMS when services, sites, systems or suppliers change.	Change checklist, management review, document updates
Action tracking	Responsibilities, dates, resources and verification.	BCMS action log, CAPA log

Examples of business continuity objectives

- Complete BIA review for all priority activities annually.
- Exercise high-priority business continuity plans at least once per year.
- Verify call tree accuracy every quarter.
- Restore critical systems within approved RTO during test conditions.
- Close exercise findings within the agreed action timeline.

9. CLAUSE 7 - SUPPORT

The BCMS requires support in the form of resources, competence, awareness, communication and controlled documented information.

Support area	Implementation requirement
Resources	Determine people, technology, facilities, tools, suppliers and finances required for continuity arrangements.
Competence	Ensure individuals involved in BCMS and response activities are competent based on education, training or experience.
Awareness	Personnel should understand BCMS policy, their role, escalation process and the consequences of not following procedures.
Communication	Define what is communicated, when, to whom, by whom and through which channels during normal and disruption conditions.
Documented information	Control BCMS documents and records so that current versions are available when needed.

Typical support records

- BCMS competence matrix
- Training attendance and awareness records
- Communication plan and contact lists
- Document master list and revision history
- Supplier continuity agreements or service arrangements

10. CLAUSE 8 - OPERATION: BIA AND RISK ASSESSMENT

Clause 8 is the operational core of ISO 22301. It requires the organization to implement the processes needed to establish and maintain business continuity arrangements.

Business impact analysis

- Identify activities that support products and services.
- Assess impacts of disruption over time.
- Determine maximum tolerable period of disruption and recovery time objectives.
- Identify dependencies on people, systems, information, facilities, suppliers and equipment.
- Determine minimum resources needed for recovery.

Risk assessment

- Define risk criteria for disruption likelihood and impact.
- Identify threats such as cyber incidents, fire, power failure, supplier failure, loss of facility and people unavailability.
- Evaluate existing controls and decide treatment actions.
- Link treatments to continuity strategies and recovery plans.

BIA output	How it is used
Priority activities	Determines which processes need continuity arrangements first.
RTO and MTPD	Defines acceptable recovery timing.
Dependencies	Identifies resources and suppliers needed for recovery.
Minimum resources	Supports alternate work arrangements and recovery planning.

11. CLAUSE 8 - CONTINUITY STRATEGIES AND SOLUTIONS

Continuity strategies should be chosen based on BIA and risk assessment results. Strategies should be practical, approved, resourced and tested.

Continuity area	Possible strategies
People	Cross-training, deputies, emergency rosters, remote working, call tree, succession arrangements.
Facilities	Alternate site, shared workspace, remote work capability, mutual aid arrangements.
Technology	Backups, cloud recovery, redundant systems, failover, cyber incident recovery procedures.
Information	Offsite storage, secure access, document backup, protected records and emergency access rules.
Suppliers	Dual sourcing, supplier continuity commitments, stock buffers, service level agreements.
Equipment/materials	Spare parts, alternate equipment, emergency procurement, maintenance contracts.

Implementation note: A strategy is only effective when it is implemented. For example, an alternate site is not enough unless access, equipment, staff, communications and data availability have also been considered.

12. CLAUSE 8 - BUSINESS CONTINUITY PLANS AND PROCEDURES

Business continuity plans should be clear enough to be used under pressure. They should define who does what, when, how, and with which resources.

Plan component	Details to include
Activation criteria	When the plan is invoked and who has authority to activate it.
Roles and responsibilities	Incident leader, communication owner, recovery team, process owner and deputies.
Escalation and communication	Internal contacts, external contacts, emergency services, customer communication and media handling.
Recovery procedures	Step-by-step recovery for priority activities and supporting resources.
Resource requirements	People, facilities, systems, equipment, suppliers, information and records.
Stand-down and return to normal	Criteria for ending response and returning to normal operations.

Plans should be controlled documents. Contact lists may need more frequent review than other documents because they become outdated quickly.

13. EXERCISE AND TESTING

Exercises and tests verify whether continuity arrangements are suitable and effective. They also build confidence and awareness before an actual disruption occurs.

Exercise type	Purpose	Example
Tabletop exercise	Discuss response using a scenario.	Cyberattack, fire, supplier failure or building access loss.
Call tree test	Verify contact information and escalation speed.	Out-of-hours notification drill.
Technical recovery test	Confirm systems or data can be restored.	Backup restore, failover or disaster recovery test.
Functional exercise	Validate a department recovery procedure.	Manual processing or alternate work location test.
Full simulation	Test coordinated multi-team response.	Major disruption affecting people, site and systems.

Exercise records should include scenario, participants, timing, observations, performance against objectives, lessons learned, corrective actions and management review input.

14. CLAUSE 9 - PERFORMANCE EVALUATION

The organization must evaluate whether the BCMS is suitable, adequate and effective. Evidence comes from monitoring, exercises, internal audits, management reviews and incident outcomes.

Evaluation method	Expected evidence
Monitoring and measurement	BCMS KPIs, plan review status, exercise completion, action closure status.
Exercise evaluation	Exercise reports, results against objectives, corrective action records.
Internal audit	Audit programme, audit plan, audit checklist, findings and audit report.
Management review	Review agenda, inputs, decisions, actions and opportunities for improvement.
Incident review	Post-incident report, lessons learned, communication review and plan updates.

Useful BCMS KPIs

- Percentage of continuity plans reviewed on time
- Exercise completion rate
- Critical contact list accuracy
- Corrective action closure time
- Recovery test results against RTO
- Number of overdue BCMS actions

15. CLAUSE 10 - IMPROVEMENT

Improvement is driven by nonconformities, corrective actions, exercise results, internal audits, management review, changes in the organization and actual incidents.

Improvement trigger	Action required
Exercise failure	Analyze why the plan or resource did not perform as expected.
Audit finding	Correct the issue and verify effectiveness.
Incident lesson	Update plans, controls, contact lists, training or strategy.
Business change	Update BIA, risk assessment, scope or recovery procedures.
Supplier change	Review dependencies, service levels and alternate arrangements.

Corrective action should include the issue, cause, correction, root cause analysis, action owner, target date, completion evidence and effectiveness verification.

Implementation note: Continual improvement does not mean changing plans without reason. It means using evidence to improve continuity capability and reduce the likelihood or impact of future disruption.

16. DOCUMENTED INFORMATION TOOLKIT

Document / record	Purpose
BCMS scope	Defines the boundaries and applicability of the BCMS.
BCMS policy	States management commitment and direction.
Business continuity objectives	Defines measurable continuity goals.
BIA procedure and records	Shows how impacts, RTOs and priorities are determined.
Risk assessment procedure and register	Shows disruption risks and treatment decisions.
Continuity strategies and solutions	Documents selected arrangements and resources.
Business continuity plans	Provides response and recovery instructions.
Communication plan	Defines internal and external communication during disruption.
Exercise and test records	Demonstrates validation of continuity arrangements.
Internal audit and management review records	Provides performance evaluation evidence.
Corrective action register	Tracks issues, causes, actions and effectiveness.

Implementation note: The organization should avoid creating documents only for certification. Documents should be practical, controlled, used by process owners and updated after exercises or changes.

17. CERTIFICATION-READINESS CHECKLIST

No.	Readiness question	Status
1	BCMS scope approved and controlled	Yes / No
2	BCMS policy approved and communicated	Yes / No
3	Interested parties and requirements identified	Yes / No
4	Business impact analysis completed	Yes / No
5	Continuity risk assessment completed	Yes / No
6	RTOs, MTPDs and dependencies defined	Yes / No
7	Continuity strategies selected and resourced	Yes / No
8	Business continuity plans approved and available	Yes / No
9	Communication and escalation process tested	Yes / No
10	Exercise or test completed and recorded	Yes / No
11	Internal audit completed	Yes / No
12	Management review completed	Yes / No
13	Corrective actions closed or controlled	Yes / No

18. 90-DAY IMPLEMENTATION PLANNER

Timeline	Focus area	Key outputs
Days 1-15	Project start and scope	BCMS team, project plan, scope, policy draft, document structure.
Days 16-30	Context and requirements	Interested party register, legal/contractual requirements, communication needs.
Days 31-45	BIA	BIA records, prioritized activities, RTO/MTPD, dependencies, resource needs.
Days 46-60	Risk assessment and strategies	Risk register, treatment plan, continuity strategies, resource approvals.
Days 61-75	Plans and training	BCP, incident response procedure, call tree, communication plan, awareness records.
Days 76-85	Exercise and evaluation	Exercise report, findings, corrective action plan, updated procedures.
Days 86-90	Internal audit and management review	Internal audit report, management review minutes, action closure plan.

Before Stage 1

- Confirm the BCMS scope and mandatory documented information.
- Complete BIA and risk assessment records.
- Ensure business continuity plans are approved and accessible.
- Prepare evidence of exercises, internal audit and management review.

19. FREQUENTLY ASKED QUESTIONS

Is ISO 22301 only for large organizations?

No. It can be applied by organizations of any size. The depth of the BCMS should match the organization's context, activities and risks.

Can ISO 22301 be integrated with ISO 9001 or ISO 27001?

Yes. It uses a management system structure that supports integration with other ISO standards.

Is a business continuity plan enough for certification?

No. Certification requires a managed system including context, leadership, planning, support, operation, evaluation and improvement.

How often should plans be tested?

Plans should be exercised at planned intervals and after significant changes. High-risk or priority activities may need more frequent testing.

What is the difference between BIA and risk assessment?

BIA looks at the impact of disruption over time and recovery priorities. Risk assessment looks at threats and scenarios that could cause disruption.

What should be ready for certification assessment?

Scope, policy, objectives, BIA, risk assessment, continuity plans, exercise records, internal audit, management review and corrective action evidence should be available.

Certification note: Pacific Certifications can conduct certification assessment activities once the organization has implemented the BCMS and retained sufficient evidence of operation.