GSDC
Global Skill Development Council

ISO 22301

LEAD AUDITOR CHEAT SHEET

www.gsdcouncil.org

What Is ISO 22301?

ISO 22301:2019 is the international standard for Business Continuity Management Systems (BCMS). It gives organizations a framework to prepare for, respond to, and recover from disruptive incidents — protecting people, operations, reputation, and revenue when things go wrong.

A Lead Auditor's job is to assess whether an organization's BCMS is properly implemented, effectively maintained, and genuinely capable of delivering business continuity when it matters most.

Scope

Define BCMS boundaries and context

Risk Assessment

Identify threats and impacts

Controls

Verify continuity plans and procedures

Audit Evidence

Assess implementation and effectiveness

ISO 22301 Standard Structure at a Glance

Clause	Title	What It Covers
1	Scope	What the standard applies to
2	Normative References	Referenced standards
3	Terms and Definitions	Key terminology
4	Context of the Organization	Internal/external issues, interested parties, scope
5	Leadership	Top management commitment, BC policy, roles
6	Planning	Risks, opportunities, BC objectives
7	Support	Resources, competence, awareness, communication, documentation
8	Operation	BIA, risk assessment, BC strategy, BCPs, exercises
9	Performance Evaluation	Monitoring, internal audit, management review
10	Improvement	Nonconformity, corrective action, continual improvement

Clauses 4–10 are auditable. Clauses 1–3 are informational.

Key Terms Every Lead Auditor Must Know

www.gsdcouncil.orgTerm	Definition
BCMS	Business Continuity Management System — the overall framework of policies, plans, and processes
Business Continuity	The capability of an organization to continue delivering products and services during a disruption
Disruption	Any incident — planned or unplanned — that interrupts normal business operations
Critical Activity	An activity that must be performed to deliver key products and services
BIA	Business Impact Analysis — identifies critical activities and the impact of disruption over time
RTO	Recovery Time Objective — maximum time to restore a critical activity after disruption
RPO	Recovery Point Objective — maximum acceptable data loss measured in time
MTPD	Maximum Tolerable Period of Disruption — longest time a disruption can last before unacceptable consequences
MBCO	Minimum Business Continuity Objective — minimum level of service acceptable during recovery
BC Plan (BCP)	Documented procedures to respond to and recover from a disruption
Incident	A situation that might be or could lead to a disruption
Exercise	A process to test, practice, or validate BC procedures
Interested Party	A person or organization that can affect or be affected by the BCMS
Nonconformity	Failure to meet a requirement of ISO 22301

The Audit Process — Step by Step

1

Stage 1 — Audit Initiation

- Confirm audit objectives, scope, and criteria
- Review previous audit reports and findings
- Assess organizational context and BC risk profile
- Appoint audit team and confirm independence
- Issue formal notification to auditee

2

Stage 2 — Document Review

- Review BCMS documentation before the on-site audit
- Check for completeness of required documented information
- Identify potential gaps or areas requiring focus
- Prepare audit plan and checklists

3

Stage 3 — Opening Meeting

- Introduce the audit team
- Confirm scope, objectives, and methodology
- Agree on logistics — time, access, guides
- Explain the grading system and reporting process
- Invite auditee questions

4

Stage 4 — On-Site Audit

- Conduct interviews with key personnel
- Review documented information and records
- Observe processes and facilities
- Verify that documented procedures reflect actual practice
- Record findings with objective evidence

The Audit Process — Stages 5 to 8

1

Stage 5 — Audit Team Meeting

- Consolidate findings across the team
- Classify findings — Conformant, NC, OFI
- Agree on major vs minor nonconformities
- Prepare audit report summary

2

Stage 6 — Closing Meeting

- Present findings to auditee and management
- Explain each nonconformity clearly with evidence
- Allow auditee to respond and clarify
- Confirm next steps and corrective action timelines
- Confirm report distribution and follow-up process

3

Stage 7 — Audit Report

- Document all findings with clause references
- Include objective evidence for each nonconformity
- Record strengths and opportunities for improvement
- Distribute report to agreed parties within agreed timeframe

4

Stage 8 — Corrective Action Follow-Up

- Review corrective action plans submitted by auditee
- Verify root cause analysis has been performed
- Confirm actions address the root cause not just the symptom
- Verify effectiveness before closing nonconformities

Audit Finding Classifications

Classification	Definition	Action Required
Major NC	Complete absence of a required element or systematic failure that significantly impacts BCMS effectiveness	Immediate corrective action required — must be resolved before certification
Minor NC	Isolated lapse or partial implementation of a requirement	Corrective action required within agreed timeframe
Observation	Not yet a nonconformity but could become one if not addressed	Monitoring recommended
OFI	Opportunity for Improvement — no nonconformity but enhancement is possible	Suggested improvement — not mandatory
Conformant	Requirement is fully met with adequate objective evidence	No action required

Clause-by-Clause Audit Focus Areas

Clause 4 — Context

- Is there a documented context analysis covering internal AND external factors?
- Are interested parties and their requirements formally identified?
- Is the scope clearly defined, documented, and justified?
- Does the scope cover all relevant locations, activities, and services?

Clause 5 — Leadership

- Can top management demonstrate genuine, active commitment?
- Is the BC Policy approved, current, communicated, and accessible?
- Are roles, responsibilities, and authorities clearly defined and understood?
- Is a competent, formally appointed person responsible for the BCMS?

Clause 6 — Planning

- Are BCMS-specific risks and opportunities identified and treated?
- Are BC objectives measurable, monitored, and aligned with the BC policy?
- Do plans to achieve objectives include owners, timelines, and resources?

Clause 7 — Support

- Are resource needs formally assessed and adequately provided?
- Is competence defined, evidenced, and gaps addressed?
- Do staff know the BC policy, their role, and consequences of non-conformance?
- Is there a documented communication plan covering internal and external needs?
- Is document control consistently applied across all BCMS documentation?

Clause-by-Clause Audit Focus Areas (Continued)

1

Clause 8 — Operation *(Most Audited Clause)*

- Is the BIA methodology documented and consistently applied?
- Are ALL critical activities identified with RTOs, RPOs, and dependencies?
- Is the BC strategy based on BIA and risk assessment outputs?
- Are BCPs complete, accessible, and aligned with BIA outputs?
- Is there a clear incident response and escalation structure?
- Is there a tested crisis communication plan?
- Is an exercise programme established and followed?
- Are exercise results documented and used to improve plans?

2

Clause 9 — Performance Evaluation

- Are BCMS metrics defined, monitored, and reported?
- Is the internal audit programme risk-based and consistently implemented?
- Are auditors independent and competent?
- Does management review happen at planned intervals with required inputs?
- Do management reviews produce documented outputs and action items?

3

Clause 10 — Improvement

- Are nonconformities reacted to promptly with containment actions?
- Is root cause analysis always performed — not just symptom fixing?
- Are corrective actions tracked, verified for effectiveness, and closed properly?
- Is there evidence of continual improvement over time — not just on paper?

BIA Audit Quick Reference

> The BIA is the foundation of the entire BCMS — audit it thoroughly.

What to Check	What Good Looks Like	Common Gap
BIA methodology	Documented, consistent, repeatable process	No methodology documented
Critical activities	All key activities identified and prioritized	Significant functions missing
Impact assessment	Financial, operational, regulatory, reputational impacts assessed over time	Only financial impacts considered
RTOs	Defined for every critical activity	RTOs missing or not aligned with BCPs
RPOs	Defined for systems and data where relevant	RPOs not defined or not tested
MTPD	Maximum tolerable disruption period defined	MTPD not considered or confused with RTO
Dependencies	People, technology, facilities, suppliers, utilities mapped	Dependencies not mapped
Minimum resources	Resources needed for recovery specified	No minimum resource requirements
BIA currency	Reviewed and updated at planned intervals	BIA several years out of date
BIA approval	Formally approved by appropriate authority	No approval records

BC Plan Audit Quick Reference

Check every BCP against this list.

Element	Present?	Aligned with BIA?
Scope and purpose of the plan	□ Yes □ No	□ Yes □ No
Activation criteria and triggers	□ Yes □ No	□ Yes □ No
Roles and responsibilities	□ Yes □ No	□ Yes □ No
Escalation and decision authority	□ Yes □ No	□ Yes □ No
Internal communication procedures	□ Yes □ No	□ Yes □ No
External communication procedures	□ Yes □ No	□ Yes □ No
Step-by-step recovery procedures	□ Yes □ No	□ Yes □ No
Recovery timelines aligned to RTOs	□ Yes □ No	□ Yes □ No
Resource requirements for recovery	□ Yes □ No	□ Yes □ No
Contact lists — internal and external	□ Yes □ No	□ Yes □ No
Offline/accessible copy available	□ Yes □ No	N/A
Last review date	□ Current □ Outdated	N/A
Personnel briefed on their role	□ Yes □ No	N/A

Exercise Programme Audit Quick Reference

What to Check	What Good Looks Like
Exercise programme documented	Formal schedule with types, frequency, and objectives
Variety of exercise types	Mix of tabletop, simulation, and operational testing
Exercise objectives defined	Clear goals for each exercise linked to BC plan elements
Exercise reports produced	Documented findings, lessons learned, and improvement actions
Corrective actions tracked	Actions from exercises assigned, followed up, and closed
All BCPs tested over time	No plans that have never been exercised
Key personnel participate	Relevant staff involved — not just BC managers
Results feed into plan improvement	BCPs updated following exercise findings

Interview Questions for Key Roles

For Top Management

- How do you demonstrate your commitment to business continuity?
- When did you last review the BCMS performance?
- What resources have you allocated to business continuity this year?
- What are the organization's BC objectives and are they being achieved?

For BC Manager / BCMS Owner

- Walk me through how the BIA was conducted.
- How are RTOs determined and who approves them?
- When were BCPs last reviewed and what triggered the review?
- Describe the last BC exercise — what did you find and what changed?
- How do you monitor BCMS performance?

For Department Heads / Critical Activity Owners

- What is your critical activity and what is its RTO?
- Have you seen and practiced your BC plan?
- What would you do if a disruption occurred right now?
- Who do you contact first during an incident?

For General Staff

- Are you aware of the organization's BC policy?
- Do you know what to do if there is a disruption to your work area?
- Have you participated in any BC awareness training or exercises?
- Where would you find the BC plan for your area?

Objective Evidence — What to Ask For

Requirement	Documents / Evidence to Request
Context analysis	PESTLE analysis, SWOT, context register
Interested parties	Stakeholder register, legal/regulatory obligations list
BC Policy	Current signed policy document
BIA	BIA methodology, BIA report with RTOs and RPOs
Risk assessment	Risk register, risk treatment plan
BC strategy	BC strategy document with approval evidence
BCPs	All current BCP documents
Exercise programme	Exercise schedule, exercise reports, corrective actions
Training and awareness	Training records, awareness campaign evidence
Internal audit	Audit programme, audit reports, corrective action records
Management review	Meeting minutes, action trackers
Corrective actions	Corrective action register with root cause analysis
Document control	Document register, version history, approval records

Major vs Minor Nonconformity — Decision Guide

Classify as MAJOR when:

- A required element is completely absent
- A process exists on paper but is not implemented in practice
- The same nonconformity has recurred across multiple audit cycles
- The finding directly undermines the organization's ability to respond to a disruption
- Critical BCPs do not exist, are inaccessible, or have never been tested
- Top management shows no evidence of BCMS involvement or commitment

Classify as MINOR when:

- A process is implemented but has an isolated gap or lapse
- Documentation is incomplete but the underlying activity is happening
- A requirement is partially met but not fully conformant
- The finding has limited impact on overall BCMS effectiveness

Common Audit Mistakes to Avoid

→ Accepting documents at face value without verifying they reflect actual practice

→ Only interviewing BC managers — always talk to operational staff and senior leadership

→ Forgetting to check whether BCPs are accessible offline during an actual incident

→ Not verifying that RTOs in BCPs match what the BIA established

→ Closing corrective actions based on implementation alone without checking effectiveness

→ Treating the audit as a document review rather than a system effectiveness assessment

→ Missing the thread — always trace from BIA outputs through to strategy and into BCPs

→ Failing to check whether previous audit findings have been genuinely resolved

Corrective Action Quality Check

Before accepting a corrective action plan, verify it includes:

□ ⍰ Clear description of the nonconformity being addressed

□ ⍰ Root cause analysis — not just symptom description

□ ⍰ Specific actions planned — not vague commitments

□ ⍰ Named responsible owner for each action

□ ⍰ Realistic target completion dates

□ ⍰ How effectiveness will be verified

□ ⍰ Whether similar issues could exist elsewhere in the BCMS

□ ⍰ Any changes needed to documented information or processes

ISO 22301 Mandatory Documented Information

The standard requires these as a minimum.

#	Required Documented Information	Clause
1	Scope of the BCMS	4.3
2	Business Continuity Policy	5.2
3	BC Objectives	6.2
4	Business Impact Analysis	8.2
5	Risk Assessment	8.2
6	Business Continuity Strategy	8.3
7	Business Continuity Plans	8.4
8	Exercise Programme and Results	8.5
9	Monitoring and Measurement Results	9.1
10	Internal Audit Programme and Reports	9.2
11	Management Review Records	9.3
12	Nonconformities and Corrective Actions	10.1
13	Competence Records	7.2
14	Communication Plan	7.4

Audit Report Structure

A well-structured ISO 22301 audit report should include:

01

Cover Page

Organization name, audit date, audit type, standard, lead auditor

02

Executive Summary

High-level overview of findings and overall BCMS maturity

03

Audit Details

Scope, objectives, criteria, audit team, auditees interviewed

04

Documents Reviewed

List of documented information reviewed

05

Findings by Clause

Each finding with clause reference, description, and objective evidence

06

Nonconformity Summary

Table of all NCs classified as major or minor

07

Opportunities for Improvement

Listed OFIs with recommendations

08

Strengths Observed

Positive findings worth acknowledging

09

Overall Conclusion

Auditor's overall assessment of BCMS conformance

10

Corrective Action Requirements

What needs to be addressed and by when

11

Sign-Off

Lead auditor and auditee signatures

Audit Timing Guide

Audit Activity	Suggested Time Allocation
Document review (pre-audit)	1–2 days
Opening meeting	30–60 minutes
Clause 4 and 5 audit	1–2 hours
Clause 6 and 7 audit	2–3 hours
Clause 8 audit (BIA, strategy, BCPs, exercises)	4–6 hours
Clause 9 and 10 audit	2–3 hours
Audit team consolidation meeting	1–2 hours
Closing meeting	60–90 minutes
Audit report writing	1–2 days

🗒 Times vary based on organization size, scope, and complexity.

Lead Auditor Reminders

Your role is to find objective evidence — **not to consult or advise during the audit**

Stay professional and neutral — **findings must be evidence-based, not opinion-based**

Always give the auditee the opportunity to provide evidence **before recording a nonconformity**

Keep findings factual — describe what was found, what was missing, and **which clause it relates to**

A strong BCMS is one that **works in practice** — documentation alone is never enough

The audit is a snapshot — **be fair, be thorough, and be consistent**