GSDC
Global Skill Development Council

ISO 22301

TOP 100 COMMON ISMS AUDIT NON-CONFORMITIES LIST

www.gsdcouncil.org

How to Use This List

This list covers the most frequently identified non-conformities during ISO 22301:2019 Business Continuity Management System (BCMS) audits across industries. Use it to prepare for audits, strengthen your BCMS before an external assessment, or guide corrective action planning after findings are raised.

Each non-conformity is mapped to its relevant ISO 22301:2019 clause for quick reference.

Audit Preparation

Use this list to anticipate findings before an external assessment takes place.

BCMS Strengthening

Identify and close gaps in your system before auditors arrive.

Corrective Action

Guide corrective action planning after findings are raised during an audit.

CLAUSE 4 — Context of the Organization

(10 Common Non-Conformities)

NC 1 — Clause 4.1

The organization has not formally documented its internal and external context. There is no evidence of a structured analysis identifying issues that could affect the BCMS and its intended outcomes.

NC 2 — Clause 4.1

The context analysis exists but has never been reviewed or updated. It reflects the organization's situation from several years ago and does not account for significant changes in the business environment.

NC 3 — Clause 4.1

External factors such as regulatory changes, supply chain dependencies, and geopolitical risks have not been considered in the context analysis.

NC 4 — Clause 4.2

Interested parties have not been formally identified. There is no stakeholder register or equivalent documented information showing who the relevant interested parties are and what their requirements mean for the BCMS.

NC 5 — Clause 4.2

Legal, regulatory, and contractual obligations relevant to business continuity have not been captured or linked to BCMS requirements. The organization cannot demonstrate awareness of its compliance obligations.

CLAUSE 4 — Context of the Organization (continued)

NC 6 — Clause 4.2

Interested party requirements are documented but have not been reviewed following regulatory changes or new contractual commitments.

NC 7 — Clause 4.3

The BCMS scope is either not documented or is too vague to determine what products, services, locations, and activities are included or excluded.

NC 8 — Clause 4.3

The scope excludes significant operational areas without documented justification. Exclusions appear to have been made to reduce audit burden rather than based on legitimate applicability criteria.

NC 9 — Clause 4.3

The scope document is not available to relevant personnel and is not maintained as controlled documented information.

NC 10 — Clause 4.4

The interactions between BCMS processes are not defined or mapped. The organization cannot demonstrate that the BCMS functions as an integrated system rather than a collection of isolated documents.

CLAUSE 5 — Leadership

(10 Common Non-Conformities)

NC 11 — Clause 5.1

Top management cannot demonstrate active commitment to the BCMS. Management review meetings are infrequent, poorly attended by senior leadership, and do not result in meaningful decisions or resource commitments.

NC 12 — Clause 5.1

Business continuity has not been integrated into the organization's strategic planning or business processes. The BCMS operates as a standalone compliance exercise rather than a core business function.

NC 13 — Clause 5.1

There is no evidence that top management has communicated the importance of effective business continuity management to the organization. Awareness among senior leaders is limited.

NC 14 — Clause 5.2

A Business Continuity Policy does not exist or has not been formally approved and signed by top management.

NC 15 — Clause 5.2

The BC Policy exists but does not include a commitment to satisfy applicable requirements or a commitment to continual improvement of the BCMS.

CLAUSE 5 — Leadership (continued)

NC 16 — Clause 5.2

The BC Policy has not been communicated to all relevant personnel. Many employees are unaware the policy exists or cannot locate it.

NC 17 — Clause 5.2

The BC Policy has not been reviewed since its initial creation. It does not reflect the organization's current context, scope, or strategic direction.

NC 18 — Clause 5.3

Roles, responsibilities, and authorities for the BCMS are not clearly defined or documented. It is unclear who is responsible for maintaining and improving the BCMS.

NC 19 — Clause 5.3

A competent person has not been formally appointed with responsibility for the BCMS. The role is informally assigned without documented authority or accountability.

NC 20 — Clause 5.3

BC roles and responsibilities are defined in documentation but are not understood by the personnel assigned to them. Interviews confirm that staff are unaware of their specific BC responsibilities.

CLAUSE 6 — Planning

(10 Common Non-Conformities)

NC 21 — Clause 6.1

The organization has not determined the risks and opportunities that need to be addressed to ensure the BCMS can achieve its intended outcomes.

NC 22 — Clause 6.1

A risk register exists but it is not specific to the BCMS. Generic organizational risks have been listed without considering their impact on business continuity specifically.

NC 23 — Clause 6.1

Actions to address identified risks and opportunities are not planned, assigned, or tracked. The risk register is a static document with no associated treatment or follow-up activity.

NC 24 — Clause 6.1

The effectiveness of actions taken to address BCMS risks and opportunities is not evaluated. There is no evidence that risk treatment measures are working as intended.

NC 25 — Clause 6.2

Business continuity objectives have not been established at relevant functions and levels within the organization.

CLAUSE 6 — Planning (continued)

NC 26 — Clause 6.2

BC objectives are documented but are not measurable. They are stated in broad terms with no associated metrics, targets, or KPIs.

NC 27 — Clause 6.2

BC objectives are not monitored or reported on. There is no evidence that progress toward achieving objectives is tracked.

NC 28 — Clause 6.2

BC objectives are not aligned with the BC policy. The policy commits to specific outcomes that are not reflected in the defined objectives.

NC 29 — Clause 6.2

Plans to achieve BC objectives do not include defined timelines, responsible owners, or resource requirements.

NC 30 — Clause 6.2

BC objectives have not been updated to reflect changes in the organization's context, risk profile, or strategic direction.

CLAUSE 7 — Support

(15 Common Non-Conformities)

NC 31 — Clause 7.1

The organization has not formally determined the resources needed for the BCMS. There is no resource plan, budget allocation, or evidence that resource adequacy has been assessed.

NC 32 — Clause 7.1

Resources allocated to the BCMS are clearly insufficient given the scope and complexity of the organization's operations. Key BC roles are unfilled or assigned as secondary duties with no dedicated time.

NC 33 — Clause 7.2

Competency requirements for personnel with BCMS responsibilities have not been defined. There are no job descriptions, competency frameworks, or role profiles that specify what knowledge and skills are required.

NC 34 — Clause 7.2

Personnel assigned to BC roles do not have the necessary competence. There is no evidence of relevant training, qualifications, or experience for key BCMS roles.

NC 35 — Clause 7.2

Competency gaps have been identified but no actions have been taken to address them. Training plans exist on paper but have not been implemented.

CLAUSE 7 — Support (continued)

NC 36 — Clause 7.2

Records of training, education, and experience are not maintained or are incomplete. The organization cannot demonstrate that its people are competent to perform their BCMS roles.

NC 37 — Clause 7.3

Personnel awareness of the BC policy is very low. Staff interviewed during the audit cannot describe the policy, its purpose, or their role in supporting it.

NC 38 — Clause 7.3

Personnel are unaware of their specific responsibilities during a business continuity incident. Awareness training has not been conducted or has not been effective.

NC 39 — Clause 7.3

The consequences of not conforming to BCMS requirements have not been communicated to personnel. There is no evidence of awareness campaigns, briefings, or communications covering this.

NC 40 — Clause 7.4

A communication plan for the BCMS does not exist. The organization has not determined what needs to be communicated, to whom, when, and through what channels during normal operations or an incident.

CLAUSE 7 — Support (continued)

NC 41 — Clause 7.4

Communication procedures have not been tested as part of BC exercises. It is unknown whether the communication plan would work effectively during a real incident.

NC 42 — Clause 7.4

External communication procedures are inadequate. There is no documented process for communicating with regulators, customers, suppliers, or media during a disruption.

NC 43 — Clause 7.5

Required documented information is missing. Key BCMS documents — such as the BIA, BC strategy, or BCPs — are not documented or cannot be located.

NC 44 — Clause 7.5

Document control is poor. Documents are not version controlled, approval records are missing, and outdated versions are in circulation alongside current ones.

NC 45 — Clause 7.5

Documented information is not adequately protected. BC plans and sensitive recovery information are stored without appropriate access controls or backup arrangements.

CLAUSE 8 — Operation

NC 46 — Clause 8.1

Operational processes for the BCMS have not been planned or documented. There is no evidence of controlled, repeatable processes supporting BC implementation.

NC 47 — Clause 8.1

Changes to operational processes are not managed. Significant organizational changes have been made without assessing their impact on the BCMS or updating related documentation.

NC 48 — Clause 8.1

Outsourced processes and third-party dependencies are not identified or controlled within the BCMS. Suppliers critical to business continuity have not been assessed or included in BC planning.

NC 49 — Clause 8.2

A Business Impact Analysis (BIA) has not been conducted. The organization has no documented understanding of which activities are critical, what their dependencies are, or what the impact of disruption would be over time.

CLAUSE 8 — Operation (continued)

NC 50 — Clause 8.2

The BIA methodology is not documented. It is unclear how critical activities were identified, how impact was assessed, or how recovery priorities were determined.

NC 51 — Clause 8.2

Recovery Time Objectives (RTOs) have not been defined for critical activities. The organization cannot demonstrate what timeframes it is working to restore operations within.

NC 52 — Clause 8.2

Recovery Point Objectives (RPOs) have not been defined for systems and data where data loss could occur. The organization has not determined what level of data loss is acceptable.

NC 53 — Clause 8.2

The BIA does not cover all critical activities. Significant functions have been omitted without documented justification.

NC 54 — Clause 8.2

Dependencies — including people, technology, facilities, utilities, and suppliers — have not been mapped in the BIA. Recovery plans cannot be effective without understanding what each critical activity depends on.

NC 55 — Clause 8.2

Minimum resource requirements for recovery have not been identified. The BIA does not specify what people, equipment, systems, or space are needed to recover within RTOs.

CLAUSE 8 — Operation (continued)

NC 56 — Clause 8.2

The BIA has not been reviewed or updated for several years. It does not reflect significant changes to the organization's operations, structure, or systems.

NC 57 — Clause 8.2

The risk assessment for BC threats is superficial. Threats are listed without meaningful assessment of likelihood or impact, and treatment actions are not defined.

NC 58 — Clause 8.2

The risk assessment does not consider the full range of plausible disruption scenarios — including cyber incidents, supply chain failures, pandemics, and utility outages.

NC 59 — Clause 8.2

Risk treatment options have not been evaluated or selected. The organization has identified risks but has taken no documented action to reduce, transfer, or accept them.

NC 60 — Clause 8.3

A BC strategy has not been developed. The organization moves directly from BIA and risk assessment to BCPs without a documented strategic framework linking them.

CLAUSE 8 — Operation (continued)

NC 61 — Clause 8.3

The BC strategy does not address all critical activities identified in the BIA. Some activities have no recovery strategy defined.

NC 62 — Clause 8.3

Recovery strategies are not feasible within the defined RTOs. The plans describe recovery approaches that would realistically take far longer than the RTO allows.

NC 63 — Clause 8.3

Alternative strategies have not been considered or evaluated. The organization has adopted a single recovery approach without assessing whether it is the most effective or resilient option.

NC 64 — Clause 8.3

The BC strategy has not been formally approved by top management. There is no evidence of sign-off or authorization for the chosen recovery approach.

NC 65 — Clause 8.4

Business Continuity Plans are not documented. The organization relies on informal knowledge rather than written, accessible procedures during a disruption.

CLAUSE 8 — Operation (continued)

NC 66 — Clause 8.4

BCPs exist but are incomplete. They lack defined roles, activation criteria, step-by-step recovery procedures, or contact lists needed to execute the plan during an incident.

NC 67 — Clause 8.4

BCPs are not accessible to the people who need them during an incident. Plans are stored only on systems that may themselves be unavailable during a disruption.

NC 68 — Clause 8.4

BCPs do not align with the BIA outputs. Recovery steps in the plans do not reflect the RTOs, RPOs, or resource requirements identified in the BIA.

NC 69 — Clause 8.4

There is no documented incident response structure. It is unclear how an incident is declared, who has authority to activate BCPs, and how escalation decisions are made.

NC 70 — Clause 8.4

A crisis communication plan does not exist or is inadequate. There are no pre-approved templates, contact lists, or communication protocols for managing internal and external communications during a disruption.

CLAUSE 8 — Operation (continued)

NC 71 — Clause 8.4

BCPs have not been reviewed or updated following incidents, exercises, or organizational changes. Plans are outdated and may no longer reflect how the organization operates.

NC 72 — Clause 8.4

Personnel named in BCPs are unaware of their role. Key individuals have not been briefed on the plan, have never practiced it, and cannot describe what they would do during activation.

NC 73 — Clause 8.5

A BC exercise programme has not been established. The organization has no scheduled or documented exercises to test the effectiveness of its plans and procedures.

NC 74 — Clause 8.5

Exercises are conducted but are not documented. There are no exercise reports, findings logs, or records of lessons learned that demonstrate the exercise took place and produced useful outputs.

NC 75 — Clause 8.5

Exercises are limited to tabletop discussions and have never included simulation or operational testing. The effectiveness of plans under real conditions has never been validated.

CLAUSE 9 — Performance Evaluation

(15 Common Non-Conformities)

NC 76 — Clause 9.1

The organization has not determined what needs to be monitored and measured within the BCMS. There are no defined metrics, indicators, or performance criteria for evaluating BCMS effectiveness.

NC 77 — Clause 9.1

BC objectives exist but are not monitored. There is no reporting on whether objectives are being achieved and no mechanism for escalating when they are not.

NC 78 — Clause 9.1

Monitoring data is collected but not analyzed or acted upon. Reports are produced but there is no evidence they are reviewed or used to drive decisions.

NC 79 — Clause 9.1

Records of monitoring and measurement results are not retained. The organization cannot demonstrate the BCMS performance over time.

NC 80 — Clause 9.1

Performance evaluation does not include assessment of the BCMS following real incidents. Actual events are not used as input to evaluate whether plans performed as expected.

CLAUSE 9 — Performance Evaluation (continued)

NC 81 — Clause 9.2

An internal audit programme for the BCMS has not been established. No internal audits of the BCMS have been conducted.

NC 82 — Clause 9.2

Internal audits are conducted but are not planned based on risk or the importance of processes. All areas receive the same audit frequency regardless of criticality or previous findings.

NC 83 — Clause 9.2

Internal auditors are not independent of the areas they audit. The same person responsible for maintaining BC documentation is conducting audits of that documentation.

NC 84 — Clause 9.2

Internal auditor competence has not been demonstrated. Auditors have no documented training, qualifications, or experience in BCMS auditing.

NC 85 — Clause 9.2

Internal audit results are not reported to top management. Findings are recorded but do not reach the level of leadership needed to drive corrective action.

CLAUSE 9 — Performance Evaluation (continued)

NC 86 — Clause 9.2

Nonconformities identified in previous internal audits have not been addressed. The same findings recur across multiple audit cycles with no evidence of effective corrective action.

NC 87 — Clause 9.3

Management reviews of the BCMS are not conducted at planned intervals. There is no evidence that top management regularly reviews the suitability, adequacy, and effectiveness of the BCMS.

NC 88 — Clause 9.3

Management review records are incomplete. Minutes do not show that required inputs — such as audit results, incident data, or performance against objectives — were considered.

NC 89 — Clause 9.3

Management review outputs do not include decisions on improvement actions or resource needs. Reviews are conducted but produce no documented outcomes or commitments.

NC 90 — Clause 9.3

Actions arising from management reviews are not tracked or followed up. Decisions made in review meetings are not implemented and their status is not monitored.

CLAUSE 10 — Improvement

(10 Common Non-Conformities)

NC 91 — Clause 10.1

When nonconformities occur, no immediate containment actions are taken. The organization does not have a defined process for reacting to and controlling nonconformities when they are identified.

NC 92 — Clause 10.1

Root cause analysis is not performed for nonconformities. Corrective actions address the symptom rather than the underlying cause, resulting in recurring findings.

NC 93 — Clause 10.1

Corrective action plans lack defined owners, timelines, or specific actions. They are too vague to be implemented effectively or verified for completion.

NC 94 — Clause 10.1

Corrective actions are not reviewed for effectiveness before being closed. Actions are marked complete based on implementation alone, without verifying that the nonconformity has been resolved and will not recur.

NC 95 — Clause 10.1

A corrective action register is not maintained. There is no central record of nonconformities, their root causes, actions taken, or closure status.

CLAUSE 10 — Improvement (continued)

NC 96 — Clause 10.1

The organization does not consider whether nonconformities in one area could exist elsewhere in the BCMS. Corrective actions are applied narrowly without assessing systemic implications.

NC 97 — Clause 10.1

Documented information related to nonconformities and corrective actions is not retained. The organization cannot demonstrate its history of corrective action or show that issues have been resolved.

NC 98 — Clause 10.2

There is no evidence of continual improvement in the BCMS over time. The same weaknesses are present year after year with no demonstrated progress.

NC 99 — Clause 10.2

Improvement opportunities identified through audits, exercises, and incidents are not captured or tracked. There is no improvement log or register where potential enhancements are recorded and prioritized.

NC 100 — Clause 10.2

The organization cannot demonstrate that improvements have been evaluated for effectiveness. Actions intended to improve the BCMS are implemented but their impact is never assessed.

Quick Reference Summary

Clause	Focus Area	No. of NCs in This List
4	Context of the Organization	10
5	Leadership	10
6	Planning	10
7	Support	15
8	Operation	30
9	Performance Evaluation	15
10	Improvement	10

Total	**100**

Top 10 Most Critical Non-Conformities to Watch For

These are the findings that most frequently result in **major non-conformities** during certification audits:

1. No documented BIA or BIA that is significantly out of date
2. RTOs not defined or not reflected in BCPs
3. BCPs not tested through a formal exercise programme
4. Top management not demonstrably involved in the BCMS
5. Internal audits not conducted or auditors not independent
6. BC plans not accessible during an incident scenario
7. No root cause analysis performed for nonconformities
8. Scope too narrow — critical areas excluded without justification
9. Awareness among staff critically low — people unaware of BC plans or their role
10. Management reviews not held or producing no documented outcomes

Tips for Auditors

- Always verify documented information against actual practice — **documents and reality often diverge**
- Interview a cross-section of staff, not just BC managers — **awareness gaps are one of the most common findings**
- Check that BCPs are accessible offline and in formats usable during a crisis
- Verify that RTOs in BCPs match the RTOs established in the BIA
- Follow the thread from BIA to strategy to plan — **gaps in this chain are extremely common**
- Ask to see the last exercise report and check whether findings were actioned
- Check the date on every key document — **outdated documentation is one of the top non-conformity sources**

GSDC
Global Skill Development Council

CERTIFIED ISO 22301:2019 LEAD AUDITOR

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING OBJECTIVE

- Gain insights into autonomous decision-making processes
- Apply knowledge using ready-to-implement templates
- Demonstrate ability to work with Agentic AI models
- Validate your skills wit

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org