100 Common Non-Conformities in ISO 22301:2019 Audits

A Practical Guide for Lead Auditors, Continuity Managers, and Resilience Professionals

Purpose of This Guide

Achieving **ISO 22301 certification** is a major step toward organizational resilience — but many teams underestimate what it takes to stay compliant.

Common audit failures often stem from incomplete impact analysis, missing documentation, untested continuity strategies, or poor internal awareness of responsibilities.

This guide is built to help you proactively identify and correct the **top 100 ISO 22301 audit non-conformities**, compiled from:

- 200+ interviews with certified ISO 22301 Lead Auditors
- Real-world business continuity audit reports across industries
- Practical field-tested recommendations for corrective action

Use this resource as your **go-to audit preparation and review manual** — whether you're leading a BCMS implementation, supporting internal audits, or seeking lead auditor certification.

What You'll Gain from This Guide

✓ Understand exactly what goes wrong in ISO 22301 audits — and why
✓ Fix the most common BCMS gaps before they become findings
✓ Align your practices with the ISO 22301:2019 standard clause-by-clause
✓ Improve audit readiness, documentation, and stakeholder engagement
✓ Support continual improvement and resilience maturity

This Guide Is Perfect For:

- ✅ Business Continuity & Resilience Managers
- ✅ ISO 22301 Internal and Lead Auditors
- ✅ Risk, Compliance, and Governance Teams
- ✅ Consultants preparing clients for certification
- ✅ Executives and operational leaders accountable for BCM

How to Use This Document

Each of the 100 non-conformities is broken down by:

- 📌 **Clause Reference** — mapped directly to ISO 22301:2019
- ❌ **What's Going Wrong** — typical audit findings and gaps
- 🔍 **Why It Matters During an Audit** — implications and context
- 🛠 **How to Fix It** — practical, actionable guidance
- ✅ **Real-World Result** — what compliance and improvement look like in action

1. Business Impact Analysis (BIA) Not Performed or Incomplete

📌 Clause: 8.2.2 – Business Impact Analysis

What's Going Wrong: Organizations fail to conduct a structured BIA or do not cover all relevant business functions. Critical parameters such as Maximum Acceptable Outage (MAO), Recovery Time Objectives (RTOs), and dependencies are either undefined or insufficiently documented.

Why It Matters During an Audit: A well-documented BIA is essential to prioritize continuity strategies. Absence of it results in weak planning foundations and misalignment between recovery capabilities and business priorities.

How to Address It: Perform BIAs across all critical departments and services. Define MAOs, RTOs, interdependencies, and resource needs. Involve relevant process owners during assessment. Review and update the BIA periodically or after significant changes.
Expected Result: A complete and current BIA ensures that continuity plans are risk-based, priority-aligned, and auditable.

2. Inadequate or Missing Business Continuity Strategy

📌 Clause: 8.3.1 – Business Continuity Strategy

What's Going Wrong: Organizations proceed directly to response plans without establishing a documented strategy that defines how continuity will be maintained or restored under disruptive conditions.
Why It Matters During an Audit: Auditors expect a documented strategy outlining how recovery objectives will be achieved. Without this, continuity measures may appear disconnected and unjustified.
How to Address It: Define continuity strategies for people, facilities, technology, suppliers, and infrastructure. Align strategies with BIA

outcomes and risk assessments. Document rationale, dependencies, and assumptions. Review strategy at management reviews or after major operational changes.
Expected Result: A comprehensive and tested strategy supports effective planning and satisfies key audit expectations.

3. Continuity Plans Not Tailored to Business Needs

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Continuity plans are generic, outdated, or not aligned with specific business functions. Roles, responsibilities, contact lists, and operational procedures are often absent or irrelevant.
Why It Matters During an Audit: Auditors assess whether plans are actionable and applicable. Poorly tailored documents undermine the reliability of continuity response efforts.
How to Address It: Develop department-specific continuity plans based on the BIA and risk findings. Include step-by-step procedures, key contacts, and recovery teams. Ensure plans are accessible, current, and reviewed periodically. Validate plan effectiveness through exercises.
Expected Result: Customized plans ensure that recovery actions are aligned with real operational requirements.

4. Testing and Exercises Not Conducted or Documented

📌 Clause: 8.5 – Exercising and Testing

What's Going Wrong: Organizations either neglect regular testing or rely solely on informal discussions without documentation or defined objectives.
Why It Matters During an Audit: Testing verifies the effectiveness and

practicality of continuity arrangements. Lack of testing is viewed as a major gap in system assurance.

How to Address It: Establish an annual testing schedule with defined scope and objectives. Include simulations, technical recovery exercises, and role-based rehearsals. Record results, identify improvement areas, and assign corrective actions. Retest critical failures and track resolution.

Expected Result: Structured and recorded testing improves response capability and system credibility during audits.

5. Leadership Not Demonstrating Commitment to the BCMS

📌 Clause: 5.1 – Leadership and Commitment

What's Going Wrong: Top management is not actively involved in the BCMS lifecycle. No records exist of resource allocation, decision-making involvement, or strategic oversight.

Why It Matters During an Audit: Auditors evaluate leadership participation as a key determinant of BCMS effectiveness. Lack of involvement is a governance deficiency.

How to Address It: Engage management in setting objectives and approving policies. Ensure management attends reviews and receives BCMS performance updates. Allocate appropriate resources to maintain and improve continuity capability. Link BCMS performance to organizational goals.

Expected Result: Demonstrated management involvement enhances accountability and reinforces continuity as a strategic priority.

6. Risk Assessment Not Conducted or Not Linked to BIA

📌 Clause: 8.2.3 – Risk Assessment

What's Going Wrong: Risks to business continuity are assessed separately from the BIA, or not assessed at all. Scenarios are often overly generic and do not include operational dependencies.
Why It Matters During an Audit: ISO 22301 requires risks to be evaluated in the context of their potential impact on business operations. A disconnected risk assessment reduces the validity of the continuity strategy.
How to Address It: Conduct a formal risk assessment focusing on threats to business continuity. Align identified risks with BIA findings. Assign likelihood and impact values to determine treatment priorities. Review assessments periodically and after significant changes.
Expected Result: Integrated risk and impact assessments provide a coherent basis for continuity planning and mitigation.

7. Inadequate Document Control of BCMS Records

📌 Clause: 7.5 – Documented Information

What's Going Wrong: Documents related to the BCMS (e.g., policies, plans, test records) are not formally managed. Version control, approval history, and document accessibility are inconsistent.
Why It Matters During an Audit: Effective documentation control is critical to ensuring that only current, approved documents are in use — a core requirement of ISO 22301.
How to Address It: Maintain BCMS documentation in a centralized, access-controlled repository. Apply versioning, approval, and review mechanisms. Ensure documents are readily available to those who need them. Define retention and disposal criteria.
Expected Result: Controlled documentation strengthens audit reliability and supports operational clarity during incidents.

8. No Evidence of Corrective Action Following Tests or Incidents

📌 Clause: 10.2 – Nonconformity and Corrective Action

What's Going Wrong: Post-incident or post-exercise reviews do not result in formal corrective actions. Observations are informally discussed but not tracked or closed.

Why It Matters During an Audit: Corrective action processes are essential to demonstrate that the BCMS is continuously improving based on real feedback.

How to Address It: Log all identified issues in a corrective action register. Define root causes, responsible parties, and deadlines. Monitor and verify implementation. Present corrective action trends during management review.

Expected Result: Structured corrective action processes foster accountability, learning, and audit assurance.

9. Lack of Stakeholder Awareness of Continuity Roles

📌 Clause: 7.3 – Awareness

What's Going Wrong: Employees and continuity team members are unaware of their responsibilities during disruptions. Awareness training is either not conducted or not role-specific.

Why It Matters During an Audit: Auditors may interview staff to confirm awareness. Poor knowledge reflects inadequate communication and weakens the BCMS response capability.

How to Address It: Conduct periodic awareness sessions for all personnel involved in continuity. Tailor training content to specific roles and response expectations. Maintain attendance records and update materials annually. Test awareness during continuity exercises.

Expected Result: Informed stakeholders respond more effectively and reduce delays or confusion during incidents.

10. Business Continuity Policy Not Fit for Purpose

📌 Clause: 5.2 – Business Continuity Policy

What's Going Wrong: The policy is overly generic, lacks measurable objectives, or is not communicated to relevant stakeholders.
Why It Matters During an Audit: A policy establishes the BCMS framework. An irrelevant or inaccessible policy raises concerns about leadership commitment and system intent.
How to Address It: Draft a policy that reflects the organization's strategic direction, risk appetite, and continuity goals. Obtain executive approval and review annually. Communicate the policy through induction, training, and documentation platforms. Make it accessible to all relevant personnel.
Expected Result: A relevant, well-communicated policy clarifies expectations and reinforces organizational commitment.

11. Lack of Integration Between the BCMS and Organizational Context

📌 Clause: 4.1 – Understanding the Organization and Its Context

What's Going Wrong: The BCMS is implemented as a standalone program without being aligned with the organization's broader context, including internal and external issues that influence business continuity.
Why It Matters During an Audit: ISO 22301 requires the BCMS to reflect the unique environment in which the organization operates. A generic approach weakens its relevance and strategic value.
How to Address It: Document the organization's context, including economic, legal, and operational factors. Ensure this context influences

objectives, strategies, and risk assessments. Review the context annually or when significant changes occur.
Expected Result: A BCMS that reflects the real-world environment is more resilient, practical, and aligned with audit expectations.

12. Failure to Identify Relevant Interested Parties and Their Requirements

📌 Clause: 4.2 – Understanding the Needs and Expectations of Interested Parties

What's Going Wrong: Organizations do not maintain a register of interested parties or fail to identify their business continuity-related requirements, such as legal obligations, contractual commitments, or customer expectations.
Why It Matters During an Audit: The BCMS must be built on a clear understanding of stakeholder expectations. Failure to do so leads to compliance gaps and audit findings.
How to Address It: Identify all relevant interested parties (e.g., customers, regulators, suppliers). Document their expectations. Link requirements to plans, policies, and procedures. Update regularly as stakeholders or relationships evolve.
Expected Result: A well-maintained stakeholder requirements register supports compliance and enhances audit readiness.

13. Scope of the BCMS Is Not Clearly Defined or Documented

📌 Clause: 4.3 – Determining the Scope of the BCMS

What's Going Wrong: The scope statement is either missing, too broad, or too narrow. It may not reflect actual organizational functions, geographical locations, or activities covered by the BCMS.

Why It Matters During an Audit: Auditors rely on the scope to assess relevance and completeness. A poorly defined scope may misrepresent the system’s coverage.

How to Address It: Clearly define the scope in terms of locations, processes, products/services, and activities. Justify any exclusions. Ensure consistency with policies, risk assessments, and continuity plans.

Expected Result: A precise scope ensures clarity, improves audit efficiency, and avoids misalignment in system implementation.

14. No Records of BCMS Objectives or KPIs

📌 Clause: 6.2 – Business Continuity Objectives and Planning to Achieve Them

What’s Going Wrong: Objectives exist only in policy statements and are not translated into measurable goals or tracked through performance indicators.

Why It Matters During an Audit: Auditors expect documented objectives and evidence of performance monitoring. Without these, the system lacks direction and accountability.

How to Address It: Set SMART (Specific, Measurable, Achievable, Relevant, Time-bound) objectives. Define KPIs aligned with continuity goals. Assign ownership and review progress periodically.

Expected Result: Measurable objectives support strategic improvement and demonstrate ongoing performance during audits.

15. Business Continuity Roles and Responsibilities Not Defined

📌 Clause: 5.3 – Organizational Roles, Responsibilities and Authorities

What's Going Wrong: Roles for implementing and maintaining the BCMS are not formally assigned. Teams are unclear on their responsibilities during planning, testing, or actual incidents.
Why It Matters During an Audit: Undefined roles hinder effective BCMS operation and confuse accountability, both of which are critical audit concerns.
How to Address It: Document BCMS roles and responsibilities. Assign them through job descriptions, RACI matrices, or response plans. Communicate and review these roles regularly.
Expected Result: Defined and communicated responsibilities support operational efficiency and audit transparency.

16. No Documented Criteria for Acceptable Risk or Recovery Levels

📌 Clause: 6.1 – Actions to Address Risks and Opportunities

What's Going Wrong: Organizations do not define acceptable levels of risk or recovery (e.g., RTOs, MAOs), leading to unclear thresholds for decision-making.
Why It Matters During an Audit: The lack of predefined tolerances undermines planning quality and impedes consistent response and recovery decisions.
How to Address It: Establish risk acceptance criteria, including thresholds for disruption impacts and acceptable downtimes. Reference these criteria in risk assessments and recovery plans.
Expected Result: Defined thresholds enable better prioritization and strengthen system credibility during audits.

17. Communication Procedures During Disruptions Are Undefined or Ineffective

📌 Clause: 8.4.3 – Communication

What's Going Wrong: Communication protocols during incidents are informal or incomplete. Teams do not know who to contact, how to escalate issues, or how to communicate with external stakeholders.
Why It Matters During an Audit: Auditors expect formal procedures that ensure timely and accurate communication before, during, and after disruptions.
How to Address It: Develop internal and external communication plans, including roles, escalation paths, message templates, and contact directories. Test these during exercises.
Expected Result: Effective communication procedures reduce chaos during disruptions and demonstrate control to auditors.

18. Business Continuity Plans Not Aligned With Risk and Impact Data

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Plans are developed without considering BIA and risk assessment outcomes. There is a misalignment between documented risks, priorities, and the content of continuity procedures.
Why It Matters During an Audit: Plans must be directly informed by risk and impact assessments. If not, auditors may question their validity and effectiveness.
How to Address It: Use BIA and risk outputs as inputs for planning. Include response strategies that match critical process needs and impact durations. Review alignment annually.
Expected Result: Integrated planning reinforces continuity effectiveness and strengthens audit defensibility.

19. No Formal Review of the BCMS Context, Scope, or Risks

📌 Clause: 9.3.2 – Management Review Inputs

What's Going Wrong: Management reviews exclude updates to the organization's context, stakeholder needs, risk profile, or changes in BCMS scope.
Why It Matters During an Audit: ISO 22301 mandates these inputs as part of the management review process. Omissions reduce strategic oversight and adaptability.
How to Address It: Include context, scope, risk trends, and stakeholder expectations as fixed agenda items in management reviews. Retain minutes and action logs.
Expected Result: Comprehensive reviews ensure the BCMS remains aligned, relevant, and effective over time.

20. Records of Internal Audits Are Incomplete or Missing

📌 Clause: 9.2 – Internal Audit

What's Going Wrong: Internal audits are conducted but lack complete documentation. Checklists, findings, evidence, or follow-up actions are missing.
Why It Matters During an Audit: Auditors require complete internal audit records to validate the system's health and identify how nonconformities are addressed.
How to Address It: Maintain audit plans, checklists, auditor qualifications, findings, and evidence logs. Track follow-up actions and verify effectiveness. Schedule audits annually or per risk level.
Expected Result: Properly documented internal audits enhance transparency and help preempt external audit findings.

21. Lack of Evaluation of the Effectiveness of Business Continuity Measures

📌 Clause: 9.1 – Monitoring, Measurement, Analysis and Evaluation

What's Going Wrong: Organizations may monitor activities or conduct tests but fail to evaluate whether continuity strategies are effective in meeting defined objectives.
Why It Matters During an Audit: ISO 22301 requires not just testing, but an evaluation of how effective the BCMS is in achieving its intended outcomes.
How to Address It: Establish clear performance indicators related to continuity readiness. Measure against objectives. Evaluate test outcomes and incident responses for alignment with strategic goals.
Expected Result: Evaluation of performance supports continual improvement and helps demonstrate value and effectiveness to auditors.

22. No Management Review of BCMS Performance

📌 Clause: 9.3.1 – Management Review

What's Going Wrong: Top management does not review the BCMS at planned intervals. If reviews are conducted, they often exclude critical input elements or lack documented outputs.
Why It Matters During an Audit: Management review is essential for oversight and improvement. Its absence suggests disengagement from the continuity process.
How to Address It: Conduct formal management reviews at defined intervals. Include all ISO-required inputs and record decisions, actions, and assigned responsibilities.
Expected Result: Documented reviews confirm leadership involvement and support audit verification of strategic alignment.

23. Incomplete Training or Competence Records for BCMS Roles

📌 Clause: 7.2 – Competence

What's Going Wrong: Staff involved in BCMS responsibilities are not adequately trained, or there is no record of competence evaluation for critical roles.
Why It Matters During an Audit: Competence is a compliance requirement. Auditors must verify that personnel understand their roles and have been trained appropriately.
How to Address It: Identify competence requirements for each BCMS-related role. Provide appropriate training. Maintain records of attendance, assessments, and performance validation.
Expected Result: A competent workforce ensures effective execution of continuity procedures and enhances audit confidence.

24. BCMS Documentation Not Reviewed or Updated Periodically

📌 Clause: 7.5.2 – Creating and Updating

What's Going Wrong: Key documents such as policies, procedures, and plans are outdated or lack version control. Revisions do not reflect organizational or operational changes.
Why It Matters During an Audit: Up-to-date documentation is fundamental for demonstrating that the BCMS remains current and relevant.
How to Address It: Implement a review cycle for all BCMS documents. Assign document owners and record changes with version history. Use a document control register.
Expected Result: Regularly maintained documentation provides clarity and ensures alignment with the current business environment.

25. Poor Definition of Incident Response and Escalation Procedures

📌 Clause: 8.4.4 – Incident Response Structure

What's Going Wrong: Response roles and escalation criteria are not defined. Employees are unsure of who takes control during a disruption or how incidents should be escalated.
Why It Matters During an Audit: Incident response procedures are vital to minimizing impact. A lack of defined escalation processes compromises response coordination.
How to Address It: Define roles, response teams, escalation thresholds, and decision-making authority. Incorporate into continuity plans and test during exercises.
Expected Result: Clearly defined response procedures enhance speed and coordination during real incidents and support compliance.

26. Supplier and Third-Party Risks Not Considered in the BCMS

📌 Clause: 8.2.3 – Risk Assessment and 8.4.6 – Coordination with External Parties

What's Going Wrong: Third-party service dependencies (e.g., cloud, logistics, power) are not assessed for continuity risk or addressed in plans.
Why It Matters During an Audit: External party disruptions can significantly impact operations. ISO 22301 expects these to be addressed in both risk and strategy.
How to Address It: Identify all critical external providers. Assess their impact, review their continuity capabilities, and integrate responses into internal plans.
Expected Result: Addressing third-party risk supports continuity assurance and reflects thorough planning practices.

27. No Defined Process for Continual Improvement of the BCMS

📌 Clause: 10.1 – Continual Improvement

What's Going Wrong: Improvements are only made reactively after incidents. There is no systematic process to identify and implement ongoing enhancements.
Why It Matters During an Audit: ISO 22301 requires a culture of continual improvement based on performance monitoring, audit results, and feedback.
How to Address It: Establish a continual improvement log. Include opportunities identified from reviews, audits, tests, or suggestions. Track progress and implementation.
Expected Result: A documented improvement process reinforces maturity and strengthens audit outcomes.

28. Inadequate Awareness Campaigns for Employees Not Directly Involved in the BCMS

📌 Clause: 7.3 – Awareness

What's Going Wrong: Only designated continuity team members receive communication or training. General staff lack basic awareness of the BCMS or response expectations.
Why It Matters During an Audit: ISO 22301 requires that all personnel understand how disruptions might affect them and what is expected.
How to Address It: Provide BCMS orientation for all employees. Distribute awareness materials and conduct periodic refresher sessions. Test awareness during drills.
Expected Result: An informed workforce contributes to effective response and audit demonstration of broad engagement.

29. Recovery Resources Not Clearly Identified or Allocated

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Recovery plans exist but do not detail the physical, technological, or human resources needed to resume operations.
Why It Matters During an Audit: Plans must be actionable, and recovery cannot occur without predefined, available resources.
How to Address It: List all required resources per plan. Include IT systems, facilities, personnel, equipment, and external services. Validate availability through testing.
Expected Result: Clear identification and allocation of resources enhance response readiness and audit credibility.

30. Lack of Review and Updating Following Disruptions or Exercises

📌 Clause: 10.2 – Nonconformity and Corrective Action

What's Going Wrong: After real events or drills, plans and procedures are not updated to reflect lessons learned. Reviews are informal or undocumented.
Why It Matters During an Audit: Post-incident or post-test evaluation is essential to drive learning. Failure to update the BCMS reduces its effectiveness and compliance.
How to Address It: Conduct structured debriefs after every event or exercise. Record findings, assign corrective actions, and revise plans as needed.
Expected Result: A feedback loop that drives improvement and reinforces audit assurance through traceable updates.

31. Failure to Ensure BCMS Is Aligned with Organizational Objectives

📌 Clause: 5.1 – Leadership and Commitment

What's Going Wrong: The BCMS is implemented as a parallel system without direct alignment to the organization's mission, strategic direction, or operational goals.
Why It Matters During an Audit: ISO 22301 requires leadership to ensure the BCMS supports the organization's objectives. Lack of integration can render the system ineffective or siloed.
How to Address It: Link BCMS priorities to business goals. Ensure continuity risks and opportunities are reflected in organizational strategy. Involve executives in BCMS development and review.
Expected Result: Strategic alignment enhances system relevance, improves engagement, and satisfies auditor expectations.

32. Incomplete or Missing Business Continuity Procedures

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Organizations maintain summary-level plans but do not include detailed step-by-step procedures for critical operations.
Why It Matters During an Audit: ISO 22301 mandates procedures that guide recovery efforts clearly and practically. Without these, response efforts may fail.
How to Address It: Develop comprehensive operational procedures for all critical processes. Include who, what, when, and how tasks are to be executed. Validate through testing.
Expected Result: Detailed procedures improve clarity during response, increase personnel confidence, and meet audit standards.

33. Lack of Objective Evidence of Business Continuity Testing Results

📌 Clause: 8.5 – Exercising and Testing

What's Going Wrong: While exercises may be conducted, there are no records of objectives, results, gaps identified, or actions taken.
Why It Matters During an Audit: ISO 22301 requires documented evidence of testing effectiveness and follow-up. Absence of records raises concerns about system integrity.
How to Address It: For each exercise, define objectives, scope, participants, outcomes, and post-test analysis. Log observations and corrective actions. Retain as part of audit documentation.
Expected Result: Documented testing evidence demonstrates operational maturity and continuous improvement.

34. Communications Strategy Not Tested During Exercises

📌 Clause: 8.5 – Exercising and Testing

What's Going Wrong: Continuity testing focuses on technical recovery but overlooks validation of communication plans and escalation procedures.
Why It Matters During an Audit: Communications are critical during disruption. If not tested, their reliability remains unproven.
How to Address It: Incorporate internal and external communication scenarios in all major exercises. Simulate stakeholder outreach, media statements, and internal alerts.
Expected Result: Tested communications enhance crisis coordination and fulfill critical audit and continuity criteria.

35. No Process to Monitor Changes That Impact the BCMS

📌 Clause: 6.3 – Planning Changes to the BCMS

What's Going Wrong: Organizational changes such as restructuring, new technologies, or third-party transitions are not assessed for their impact on the BCMS.
Why It Matters During an Audit: ISO 22301 requires that changes be planned and evaluated for continuity impact. Failure to do so compromises the system's adaptability.
How to Address It: Implement a change management procedure including BCMS impact analysis. Update risk assessments, plans, and resource requirements accordingly.
Expected Result: Structured change monitoring ensures system relevance and operational continuity during transformation.

36. Roles in Incident Management Team Not Formally Assigned

📌 Clause: 8.4.4 – Incident Response Structure

What's Going Wrong: There is no documented assignment of key roles such as incident commander, communications lead, or recovery coordinator.
Why It Matters During an Audit: ISO 22301 requires a defined and documented response structure. Unclear roles delay decisions and weaken response capability.
How to Address It: Assign formal roles and responsibilities within the incident management structure. Define authorities, decision protocols, and deputies.
Expected Result: A clearly documented response structure improves decision-making and ensures system accountability.

37. Training Programs Not Tailored to Specific Continuity Roles

📌 Clause: 7.2 – Competence

What's Going Wrong: Training is generic and does not reflect role-specific expectations, particularly for those in recovery, response, or testing roles.
Why It Matters During an Audit: ISO 22301 expects personnel to be trained according to their roles. Generic training fails to ensure effective capability.
How to Address It: Develop training modules based on defined BCMS responsibilities. Deliver practical instruction and evaluate effectiveness. Document training outcomes.
Expected Result: Role-specific training supports competence and reinforces operational readiness in audits.

38. No Consistent Methodology for Impact and Risk Evaluation

📌 Clause: 8.2.2 and 8.2.3 – Business Impact Analysis and Risk Assessment

What's Going Wrong: Different departments use inconsistent methods for assessing impacts and risks, leading to misaligned recovery priorities.
Why It Matters During an Audit: Uniformity is essential for comparing and prioritizing risk and recovery strategies across the organization.
How to Address It: Adopt a standardized evaluation methodology. Use common scoring systems, definitions, and criteria for all assessments. Train stakeholders accordingly.
Expected Result: A unified approach improves consistency, transparency, and audit traceability.

39. Third Parties Not Informed of Their Role in Continuity

📌 Clause: 8.4.6 – Coordination with External Parties

What's Going Wrong: Vendors and service providers involved in critical processes are unaware of their role in business continuity arrangements or expectations during disruption.
Why It Matters During an Audit: External dependencies must be coordinated and documented. Lack of engagement introduces continuity and compliance risk.
How to Address It: Communicate continuity expectations to third parties. Include roles in contracts or service level agreements. Test vendor response capabilities.
Expected Result: Informed and engaged third parties support uninterrupted service delivery and reinforce BCMS integrity.

40. Recovery Time Objectives (RTOs) Not Validated Through Testing

📌 Clause: 8.2.2 and 8.5 – Business Impact Analysis and Exercising

What's Going Wrong: RTOs are defined during planning but are not tested in practice. This creates a risk that assumptions do not hold in real-world scenarios.
Why It Matters During an Audit: RTOs must be realistic and achievable. Auditors expect proof of validation through live or simulated tests.
How to Address It: Design exercises to test the organization's ability to meet declared RTOs. Monitor performance and adjust targets if necessary.
Expected Result: Validated RTOs build confidence in the BCMS and demonstrate evidence-based planning to auditors.

41. No Traceability Between Continuity Objectives and Performance Data

📌 Clause: 6.2 and 9.1 – Objectives and Monitoring

What's Going Wrong: Continuity objectives are defined, but there is no structured monitoring of whether they are being achieved, nor is there data to support progress.
Why It Matters During an Audit: ISO 22301 requires not only setting objectives, but tracking their effectiveness through measurable outcomes.
How to Address It: Develop KPIs linked to each BCMS objective. Collect and review relevant data regularly. Report on progress during management reviews.
Expected Result: Demonstrated alignment between objectives and performance enhances audit transparency and supports continuous improvement.

42. Lack of Defined Metrics for BCMS Performance

📌 Clause: 9.1 – Monitoring, Measurement, Analysis and Evaluation

What's Going Wrong: The organization has no defined metrics for assessing the health or performance of the BCMS. Evaluation is based on anecdotal or qualitative feedback only.
Why It Matters During an Audit: Auditors require objective evidence of system effectiveness. The absence of metrics impairs system visibility and oversight.
How to Address It: Define a set of BCMS metrics (e.g., plan update frequency, exercise success rate, corrective actions closed, BIA coverage). Collect and analyze data periodically.
Expected Result: Quantitative metrics enable data-driven management and improve audit defensibility.

43. No Plan for Testing Resource Failover or Alternate Sites

📌 Clause: 8.5 – Exercising and Testing

What's Going Wrong: Recovery plans include backup facilities or systems, but their functionality has never been tested under simulated failover conditions.
Why It Matters During an Audit: ISO 22301 requires that recovery capabilities are tested, not assumed. Unvalidated resources may fail during real events.
How to Address It: Design and execute scenario-based tests to validate use of backup sites, cloud environments, or manual workarounds. Include results in testing logs.
Expected Result: Tested fallback solutions provide assurance of operational resilience and auditor confidence.

44. Inadequate Control Over Changes to BCMS Documentation

📌 Clause: 7.5.3 – Control of Documented Information

What's Going Wrong: Changes to plans or policies are not reviewed or approved before implementation. Historical versions are not maintained, leading to confusion.
Why It Matters During an Audit: ISO 22301 mandates control over documented information. Lack of version control can lead to errors and noncompliance.
How to Address It: Apply document control policies including versioning, approval workflows, and archive requirements. Use a centralized repository.
Expected Result: Controlled documentation ensures accuracy, avoids ambiguity, and satisfies auditors.

45. Lessons Learned Not Captured Following Disruptions or Tests

📌 Clause: 10.2 – Nonconformity and Corrective Action

What's Going Wrong: Exercises and incidents are not followed by formal debriefs or reports. Opportunities for improvement are missed.
Why It Matters During an Audit: Capturing and acting on lessons learned is central to ISO 22301's continual improvement model.
How to Address It: Conduct structured reviews after each event. Document findings, assign actions, and track implementation. Feed outcomes into risk assessments and planning updates.
Expected Result: A formalized learning process strengthens resilience and provides a defensible audit trail.

46. Internal Audit Scope Does Not Fully Cover the BCMS

📌 Clause: 9.2.2 – Internal Audit Programme

What's Going Wrong: Internal audits focus narrowly on documentation or selected departments and fail to evaluate the BCMS in its entirety.
Why It Matters During an Audit: Auditors expect comprehensive internal reviews that assess the full scope of the BCMS. Gaps raise concerns about oversight.
How to Address It: Define the full scope of the BCMS, including processes, departments, and interfaces. Ensure audit plans rotate through the full system over a set cycle.
Expected Result: A complete audit programme supports system integrity and demonstrates proactive governance.

47. No Formal Mechanism for Reviewing Risk and Impact Trends

📌 Clause: 6.1 and 8.2.3 – Risks and Business Impacts

What's Going Wrong: Risk assessments and BIAs are conducted but are not reviewed over time for changes or emerging trends.
Why It Matters During an Audit: Ongoing evaluation is necessary to ensure the BCMS remains current with organizational and external developments.
How to Address It: Schedule periodic reviews of BIA and risk data. Identify trend indicators (e.g., frequency, severity, recurrence). Update planning assumptions accordingly.
Expected Result: Dynamic risk and impact review processes improve system responsiveness and risk management maturity.

48. No Contingency Planning for Key Personnel Unavailability

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Continuity plans rely on specific individuals without planning for their unavailability during a crisis.
Why It Matters During an Audit: ISO 22301 emphasizes continuity of operations, not individuals. Relying on single points of failure is a risk.
How to Address It: Identify key personnel in each plan. Assign alternates and cross-train staff. Document backup roles and responsibilities.
Expected Result: Built-in redundancy strengthens the reliability of continuity procedures and meets auditor expectations.

49. External Parties Not Included in Continuity Exercises

📌 Clause: 8.5 and 8.4.6 – Testing and Coordination with External Parties

What's Going Wrong: Vendors and partners providing critical services are not involved in tests or simulations, even when their performance affects recovery.
Why It Matters During an Audit: ISO 22301 requires that external dependencies be tested for continuity reliability. Exclusion signals a gap in planning and coordination.
How to Address It: Invite external providers to participate in exercises. Share objectives in advance and capture their performance during the activity.
Expected Result: Coordinated testing improves recovery effectiveness and fulfills compliance obligations.

50. Top Management Not Involved in BCMS Reviews or Decision-Making

📌 Clause: 5.1 and 9.3 – Leadership and Management Review

What's Going Wrong: Senior leadership is not actively engaged in the BCMS. They do not attend reviews or make informed decisions based on BCMS outcomes.
Why It Matters During an Audit: ISO 22301 requires active leadership support. Lack of involvement indicates weak governance and commitment.
How to Address It: Schedule regular leadership briefings. Include BCMS updates in strategic reviews. Ensure executive presence in management reviews and exercises.
Expected Result: Active executive involvement enhances alignment, resource allocation, and audit credibility.

51. Failure to Communicate BCMS Policy Across the Organization

📌 Clause: 5.2.2 – Communicating the Business Continuity Policy

What's Going Wrong: The BCMS policy is documented but not distributed or explained to staff. Employees are unaware of its existence or purpose.
Why It Matters During an Audit: ISO 22301 requires that the policy be communicated and understood by all relevant personnel. Lack of awareness undermines implementation.
How to Address It: Distribute the policy through onboarding, intranet, training, and internal communications. Verify understanding through feedback or awareness checks.
Expected Result: An informed workforce supports the organization's continuity vision and improves audit response.

52. Business Continuity Planning Excludes Non-IT Functions

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Continuity plans are focused exclusively on IT or data recovery, omitting other critical areas like HR, finance, supply chain, or facilities.
Why It Matters During an Audit: ISO 22301 covers all critical business functions. A narrow focus signals an incomplete BCMS.
How to Address It: Identify all critical processes across the organization. Develop continuity plans specific to each function. Ensure cross-functional coordination.
Expected Result: Comprehensive planning enhances coverage and ensures operational continuity beyond IT systems.

53. Inadequate Identification of Legal and Regulatory Requirements

📌 Clause: 4.2 and 6.1.3 – Interested Parties and Compliance Obligations

What's Going Wrong: Organizations do not maintain a current list of business continuity-related legal, regulatory, or contractual obligations.
Why It Matters During an Audit: Compliance is a core component of the BCMS. Gaps in identification may result in missed requirements and findings.
How to Address It: Maintain a compliance register including applicable laws, standards, industry guidelines, and customer-specific requirements. Review regularly.
Expected Result: Proper identification supports legal compliance and strengthens audit preparedness.

54. Plans Do Not Include Resource Mobilization Procedures

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Plans fail to address how critical resources (e.g., equipment, personnel, data) will be accessed, mobilized, or deployed during a disruption.
Why It Matters During an Audit: Plans must be actionable. Missing resource procedures reduce their utility and raise auditor concerns.
How to Address It: Include logistics for accessing backup systems, temporary facilities, alternative suppliers, and emergency contacts. Define roles and responsibilities.
Expected Result: Well-structured plans enable efficient recovery execution and improve audit assurance.

55. Business Continuity Objectives Are Not Monitored or Reviewed

📌 Clause: 6.2 and 9.3.2 – Objectives and Management Review Inputs

What's Going Wrong: Objectives are set at system launch but never re-evaluated. No monitoring data is used to assess whether they remain relevant or achieved.
Why It Matters During an Audit: Objectives must drive system performance and be reviewed to ensure continued relevance and achievement.
How to Address It: Monitor objective-related metrics regularly. Include them as a standing item in management reviews. Adjust objectives as the organization evolves.
Expected Result: Continuously monitored objectives reinforce system performance and strategic relevance.

56. Outsourced Functions Not Included in BCMS Scope

📌 Clause: 4.3 and 8.4.6 – BCMS Scope and External Coordination

What's Going Wrong: Functions outsourced to third parties (e.g., call centers, data hosting, manufacturing) are not covered within the scope of the BCMS.
Why It Matters During an Audit: If outsourced functions are critical to service delivery, their exclusion may invalidate the continuity posture.
How to Address It: Reassess BCMS scope to include all critical outsourced services. Coordinate continuity arrangements with vendors and monitor their capabilities.
Expected Result: A comprehensive scope enhances risk management and satisfies auditors that no critical dependencies are overlooked.

57. Exercise Results Are Not Reviewed by Top Management

📌 Clause: 9.3.2 – Management Review Inputs

What's Going Wrong: Post-exercise reports are generated but never escalated to top management for review, approval, or strategic input.
Why It Matters During an Audit: Management review must include evaluation of exercise results to ensure organizational learning and strategic decision-making.
How to Address It: Include summaries of testing and exercising in review meetings. Use these to drive improvements and allocate necessary resources.
Expected Result: Management-level review reinforces oversight and prioritizes business continuity within the broader organizational agenda.

58. Continuity Plans Lack Defined Recovery Timeframes

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Recovery timelines are omitted or undefined in business continuity plans, creating ambiguity in expectations.
Why It Matters During an Audit: Recovery Time Objectives (RTOs) and deadlines are essential for coordinated and timely restoration efforts.
How to Address It: Incorporate RTOs, Maximum Tolerable Periods of Disruption (MTPDs), and sequencing into all plans. Align with BIA data.
Expected Result: Defined timeframes improve coordination, decision-making, and performance during recovery.

59. Incident Logs and Response Actions Not Retained

📌 Clause: 7.5.1 and 10.2 – Documented Information and Corrective Action

What's Going Wrong: Organizations do not retain documentation related to incident occurrences, decisions taken, or corrective actions performed.
Why It Matters During an Audit: Records are necessary to demonstrate

incident handling, learning, and compliance with the standard.
How to Address It: Log all incidents, decisions made, communications sent, and actions implemented. Maintain records per your document control policy.
Expected Result: Complete records support accountability and provide essential evidence for both internal and external audits.

60. Continuity Responsibilities Are Not Reflected in Job Descriptions

📌 Clause: 5.3 – Roles and Responsibilities

What's Going Wrong: BCMS responsibilities are assigned informally or verbally, with no mention in job descriptions, contracts, or organizational charts.
Why It Matters During an Audit: ISO 22301 requires defined and documented roles. Absence of formalization may lead to role confusion or missed duties.
How to Address It: Update job descriptions to reflect continuity responsibilities. Include expectations in performance reviews and training plans.
Expected Result: Documented responsibilities enhance accountability and ensure continuity is embedded into daily roles.

61. Post-Incident Communication Not Planned or Documented

📌 Clause: 8.4.3 – Communication

What's Going Wrong: Organizations fail to define how communication will be handled after the initial response phase. Stakeholder updates and status notifications are not addressed.
Why It Matters During an Audit: ISO 22301 requires structured

communication before, during, and after disruptive events. Lack of planning compromises transparency and stakeholder trust.

How to Address It: Develop a post-incident communication plan detailing timing, responsibilities, and channels for both internal and external communications.

Expected Result: Effective post-incident communication enhances reputation management and audit compliance.

62. Lack of Competency Validation for BCMS-Critical Roles

📌 Clause: 7.2 – Competence

What's Going Wrong: Personnel are assigned to continuity roles without verification that they have the required skills or experience to fulfill those duties.

Why It Matters During an Audit: ISO 22301 requires organizations to ensure competence, not just provide training. Auditors look for validation mechanisms.

How to Address It: Define competency criteria for each role. Use assessments, simulations, or certifications to confirm capability.

Expected Result: Validated competencies ensure operational readiness and audit defensibility.

63. Business Continuity Not Considered in Organizational Projects or Change Initiatives

📌 Clause: 6.3 – Planning Changes to the BCMS

What's Going Wrong: Project teams implement new systems, processes, or structures without assessing the impact on business continuity arrangements.

Why It Matters During an Audit: ISO 22301 requires that changes be evaluated for BCMS impact. Oversights may leave gaps in recovery capabilities.
How to Address It: Integrate BCMS review into change management and project planning. Involve BCMS stakeholders in impact analysis.
Expected Result: Proactive continuity integration ensures the BCMS remains current and effective amid organizational evolution.

64. Lack of Defined Criteria for Activation of Continuity Plans

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Plans do not define under what conditions they should be activated, leaving decisions open to individual interpretation.
Why It Matters During an Audit: Clear activation criteria enable timely, decisive action and reduce confusion during critical moments.
How to Address It: Document trigger points, thresholds, or escalation protocols that guide activation decisions. Train stakeholders accordingly.
Expected Result: Defined activation criteria support swift and consistent decision-making in emergencies.

65. Roles in Communications Management Not Clearly Assigned

📌 Clause: 8.4.3 – Communication

What's Going Wrong: Communication during disruptions is handled inconsistently. There is no designated spokesperson or chain of responsibility.
Why It Matters During an Audit: ISO 22301 requires planned, authorized communications. Lack of structure risks misinformation and reputational damage.

How to Address It: Assign specific roles for internal, media, regulatory, and customer communication. Document contact points and protocols.
Expected Result: Designated communication roles ensure clarity, authority, and compliance during disruptions.

66. Exercises Are Not Evaluated for Effectiveness

📌 Clause: 8.5 – Exercising and Testing

What's Going Wrong: Exercises are conducted but without post-test evaluation or analysis of what worked, what failed, and what should change.
Why It Matters During an Audit: ISO 22301 emphasizes the importance of learning through evaluation. Without it, exercises yield limited value.
How to Address It: Use post-exercise reviews, feedback forms, and debrief sessions to assess outcomes. Document findings and link to corrective actions.
Expected Result: Evaluated exercises reinforce learning and demonstrate system improvement to auditors.

67. Incident Management Structure Not Maintained or Updated

📌 Clause: 8.4.4 – Incident Response Structure

What's Going Wrong: The incident response structure was established at system launch but has not been updated to reflect organizational or personnel changes.
Why It Matters During an Audit: An outdated structure leads to confusion and weakens response coordination.
How to Address It: Review and update the structure regularly. Ensure alignment with organizational charts and operational roles.

Expected Result: An up-to-date response structure supports coordination and satisfies auditor expectations.

68. No Provisions for Coordinating with Public Authorities During Disruption

📌 Clause: 8.4.6 – Coordination with Relevant Interested Parties

What's Going Wrong: Organizations overlook the role of external authorities such as emergency services, regulators, or public health bodies in their plans.
Why It Matters During an Audit: ISO 22301 requires coordination with external parties. Gaps may cause delays or noncompliance during real events.
How to Address It: Identify relevant external agencies. Define communication protocols and responsibilities. Include coordination in exercises where possible.
Expected Result: Clear external coordination ensures legal compliance and strengthens response capabilities.

69. Lack of Awareness of BCMS Among Senior Executives

📌 Clause: 5.1 and 7.3 – Leadership and Awareness

What's Going Wrong: Senior leaders endorse the BCMS in principle but cannot articulate its scope, structure, or current priorities when questioned.
Why It Matters During an Audit: ISO 22301 requires active leadership engagement. Auditor interviews may reveal disengagement.
How to Address It: Provide regular briefings to senior executives. Ensure involvement in reviews, exercises, and key decisions.

Expected Result: Informed leadership demonstrates governance maturity and improves audit confidence.

70. Failure to Consider Seasonal or Time-Based Risks in Risk Assessments

📌 Clause: 8.2.3 – Risk Assessment

What's Going Wrong: Risk assessments consider only general threats and fail to factor in seasonal factors (e.g., monsoons, year-end demand spikes, flu season).
Why It Matters During an Audit: ISO 22301 expects context-aware assessments. Ignoring seasonal variables leads to gaps in preparation.
How to Address It: Incorporate time-based risks into risk assessments. Include mitigation and readiness planning where appropriate.
Expected Result: Contextualized risk assessments improve realism, enhance planning quality, and reduce audit exposure.

71. Backup and Recovery Procedures Not Integrated into Continuity Plans

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: IT backup and recovery processes exist but are not referenced or linked in business continuity plans, resulting in disconnected response efforts.
Why It Matters During an Audit: ISO 22301 requires cohesive planning. Separation of IT disaster recovery from broader continuity efforts creates coordination gaps.
How to Address It: Link IT recovery procedures to relevant business continuity plans. Ensure synchronization of timelines, roles, and resource

dependencies.
Expected Result: Integrated planning improves recovery efficiency and demonstrates alignment between IT and business continuity frameworks.

72. Key Continuity Roles Not Involved in Exercises

📌 Clause: 8.5 – Exercising and Testing

What's Going Wrong: Individuals identified as essential to recovery efforts are not included in tests or simulations, leaving their preparedness unverified.
Why It Matters During an Audit: Exercises must test actual response capabilities. Excluding key personnel creates uncertainty and audit concerns.
How to Address It: Involve all critical role-holders in at least one annual exercise. Evaluate individual and team performance. Address skill or coordination gaps.
Expected Result: Inclusive testing validates readiness and improves coordination across the recovery structure.

73. No Record of Communications With External Stakeholders During Incidents

📌 Clause: 8.4.3 – Communication

What's Going Wrong: External communications during disruptions are handled informally, and no records are kept of messages shared or stakeholder engagement.
Why It Matters During an Audit: ISO 22301 emphasizes traceability. Lack of documented communications weakens post-incident analysis and legal defensibility.

How to Address It: Maintain communication logs, including recipient, date, time, method, and content summaries. Include copies of emails or press statements where applicable.
Expected Result: Documented external communication ensures transparency, supports compliance, and strengthens audit credibility.

74. Exercise Scenarios Not Based on Realistic or High-Risk Events

📌 Clause: 8.5 – Exercising and Testing

What's Going Wrong: Testing focuses on low-impact or generic scenarios that do not reflect actual risks faced by the organization.
Why It Matters During an Audit: ISO 22301 requires that exercises reflect realistic conditions. Inadequate scenarios provide little value.
How to Address It: Select scenarios based on BIA and risk assessments. Prioritize high-risk, high-impact events for testing. Rotate scenarios annually.
Expected Result: Risk-aligned exercises improve system relevance and audit recognition of effective preparedness.

75. Internal Audit Results Are Not Communicated to Process Owners

📌 Clause: 9.2.2 – Internal Audit

What's Going Wrong: Internal audit findings are filed centrally but not shared with those responsible for implementing changes or improvements.
Why It Matters During an Audit: ISO 22301 requires communication of audit results to relevant stakeholders. Lack of awareness hinders resolution of issues.
How to Address It: Distribute findings to all applicable process owners. Assign responsibilities for corrective actions and follow up on

implementation.
Expected Result: Transparent audit communication improves responsiveness and supports continual improvement.

76. Recovery Strategies Lack Prioritization Among Critical Functions

📌 Clause: 8.3.1 – Business Continuity Strategy

What's Going Wrong: All functions are assigned equal importance in plans without considering their true criticality or recovery urgency.
Why It Matters During an Audit: ISO 22301 expects prioritization based on BIA results. Equal treatment may overload recovery resources.
How to Address It: Categorize functions based on impact and time sensitivity. Sequence recovery strategies accordingly. Communicate prioritization in plans.
Expected Result: Clear prioritization supports efficient recovery and audit demonstration of resource management.

77. No Testing of Manual Workarounds in the Event of System Failure

📌 Clause: 8.5 – Exercising and Testing

What's Going Wrong: Plans include manual alternatives to systems but these are not tested, leaving usability and effectiveness unknown.
Why It Matters During an Audit: Assumptions about manual workarounds must be validated. Otherwise, they may fail under pressure.
How to Address It: Include manual process testing in exercises. Validate instructions, duration, and resource needs. Adjust plans as needed.
Expected Result: Verified alternatives strengthen resilience and improve audit confidence in business continuity arrangements.

78. Contracts With Critical Vendors Do Not Include Continuity Requirements

📌 Clause: 8.4.6 – Coordination with External Parties

What's Going Wrong: Contracts with key suppliers or partners do not include clauses related to continuity responsibilities or expectations.
Why It Matters During an Audit: ISO 22301 requires that external dependencies be coordinated and controlled. Lack of contractual obligations reduces enforceability.
How to Address It: Add continuity expectations to contracts or SLAs, including recovery capabilities, participation in exercises, and notification requirements.
Expected Result: Clear contractual obligations support compliance and promote aligned recovery with third parties.

79. BCMS Scope Statement Not Reviewed as Business Evolves

📌 Clause: 4.3 – Determining the Scope of the BCMS

What's Going Wrong: The scope was defined during implementation but has not been reviewed despite changes in operations, geography, or service offerings.
Why It Matters During an Audit: An outdated scope leads to coverage gaps or misalignment with current risk exposure.
How to Address It: Reevaluate the BCMS scope annually or when significant organizational changes occur. Update documentation and communicate changes.
Expected Result: A current scope supports relevance, resource alignment, and audit clarity.

80. BIA and Risk Assessment Not Reviewed Together for Consistency

📌 Clause: 8.2.2 and 8.2.3 – BIA and Risk Assessment

What's Going Wrong: Risk and impact assessments are conducted in isolation. Inconsistencies exist between criticality ratings and risk prioritization.

Why It Matters During an Audit: ISO 22301 expects a cohesive understanding of impact and risk. Misalignment compromises planning validity.

How to Address It: Review BIA and risk findings side-by-side. Adjust for alignment and validate prioritization logic across departments.

Expected Result: Consistent assessments ensure accurate recovery strategies and audit defensibility.

81. Evidence of Top Management Involvement in BCMS Not Retained

📌 Clause: 5.1 – Leadership and Commitment

What's Going Wrong: While management supports the BCMS verbally, there is no documented evidence of their participation in reviews, decision-making, or resourcing.

Why It Matters During an Audit: ISO 22301 requires demonstrable leadership commitment. Absence of records undermines governance claims.

How to Address It: Record meeting attendance, approvals, and resource allocations tied to BCMS activities. Include top management in documented reviews.

Expected Result: Documented involvement reinforces governance credibility and satisfies auditor expectations.

82. Training Plans for Business Continuity Are Not Reviewed or Updated

📌 Clause: 7.2 – Competence

What's Going Wrong: Training plans are static and do not reflect evolving risks, personnel changes, or improvements from past exercises.
Why It Matters During an Audit: ISO 22301 requires training to be relevant and effective. Outdated plans reduce preparedness.
How to Address It: Review training needs annually or after major changes. Update content based on lessons learned and new threats. Track completions and outcomes.
Expected Result: Current, role-specific training supports effective performance and readiness during audits or actual disruptions.

83. Business Continuity Planning Does Not Account for Data Protection Requirements

📌 Clause: 4.2 and 6.1.3 – Interested Parties and Legal Requirements

What's Going Wrong: Plans focus on recovery logistics but overlook obligations related to data privacy, retention, or legal protections during recovery.
Why It Matters During an Audit: Data handling is a legal and stakeholder expectation. Noncompliance can trigger regulatory penalties and audit findings.
How to Address It: Identify applicable data regulations (e.g., GDPR). Align continuity procedures with data protection requirements. Include safeguards in recovery workflows.
Expected Result: Aligned planning ensures legal compliance and enhances organizational trust and audit outcomes.

84. No Mechanism for Updating Plans Following Organizational Restructuring

📌 Clause: 6.3 – Planning Changes

What's Going Wrong: Organizational changes such as mergers, acquisitions, or departmental restructuring are not followed by a review of continuity documentation.
Why It Matters During an Audit: ISO 22301 requires changes to be reflected in the BCMS. Outdated plans lead to ineffective or inaccurate response.
How to Address It: Include BCMS updates as part of organizational change protocols. Notify BCMS owners when operational changes are approved.
Expected Result: Accurate, updated documentation ensures system integrity and audit compliance.

85. Lack of Role Redundancy in Continuity Plans

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Plans assign recovery actions to individuals without identifying alternates or deputies, increasing single-point-of-failure risk.
Why It Matters During an Audit: Continuity depends on role coverage during disruptions. ISO 22301 emphasizes reliability over individuals.
How to Address It: Assign backups for all critical roles. Include alternates in training and exercises. Document both primary and secondary responsibilities.
Expected Result: Built-in redundancy supports continuity execution and strengthens audit assurance.

86. Supplier Continuity Capabilities Not Assessed or Verified

📌 Clause: 8.4.6 – Coordination with External Parties

What's Going Wrong: Organizations rely on critical suppliers but do not request or review their continuity capabilities or plans.
Why It Matters During an Audit: ISO 22301 expects risk-based management of dependencies. Unverified supplier resilience exposes the organization to disruption.
How to Address It: Request supplier continuity documentation or certifications. Assess based on criticality. Include reviews in procurement or audit cycles.
Expected Result: Supplier assurance supports operational reliability and strengthens external compliance posture.

87. Lessons Learned Are Not Used to Update Training Content

📌 Clause: 7.2 and 10.2 – Competence and Corrective Action

What's Going Wrong: Training programs are not revised after incidents or exercises, missing the opportunity to address identified weaknesses.
Why It Matters During an Audit: ISO 22301 emphasizes continual improvement. Static training indicates low system maturity.
How to Address It: Use findings from exercises and incidents to revise training content. Emphasize real-world examples and specific learning points.
Expected Result: Updated training enhances organizational capability and demonstrates a responsive improvement culture.

88. Communication Equipment and Channels Not Tested Under Disruption Conditions

📌 Clause: 8.4.3 – Communication

What's Going Wrong: Communication tools (e.g., satellite phones, emergency apps, mass notification systems) are not tested in realistic conditions.
Why It Matters During an Audit: ISO 22301 requires validation of tools and procedures. Untested equipment may fail when needed.
How to Address It: Simulate communication use under stress (e.g., loss of power, remote work). Test accessibility and reliability across platforms.
Expected Result: Verified communication tools increase preparedness and demonstrate operational realism during audits.

89. Business Continuity Documentation Not Version Controlled

📌 Clause: 7.5.3 – Control of Documented Information

What's Going Wrong: Policies and plans are edited without maintaining version histories, approval dates, or previous revisions.
Why It Matters During an Audit: ISO 22301 mandates document control. Lack of versioning impairs traceability and increases error risk.
How to Address It: Implement version control policies. Track authorship, review, and approval metadata. Use document management systems where feasible.
Expected Result: Controlled documentation supports compliance, auditability, and consistent execution.

90. Post-Incident Reviews Are Not Conducted in a Timely Manner

📌 Clause: 10.2 – Nonconformity and Corrective Action

What's Going Wrong: Reviews of incidents are delayed or skipped, resulting in poor recollection of events and missed learning opportunities.
Why It Matters During an Audit: ISO 22301 emphasizes rapid review for effective corrective action. Delays reduce insight and accountability.
How to Address It: Set deadlines for initiating post-incident reviews (e.g., within 7 days). Use structured templates for consistency.
Expected Result: Timely reviews lead to actionable insights and demonstrable improvement, strengthening audit confidence.

91. No Identification of Interdependencies Between Business Functions

📌 Clause: 8.2.2 – Business Impact Analysis

What's Going Wrong: The BIA is conducted in silos, with no assessment of how disruption in one process may affect others across departments.
Why It Matters During an Audit: ISO 22301 requires a holistic view of impacts. Unrecognized interdependencies reduce planning accuracy and increase risk.
How to Address It: Include cross-functional workshops during the BIA process. Map dependencies between processes, systems, and third parties.
Expected Result: Awareness of interdependencies enhances response coordination and supports auditor confidence in planning integrity.

92. Business Continuity Policy Not Reviewed at Planned Intervals

📌 Clause: 5.2.1 – Establishing the Business Continuity Policy

What's Going Wrong: The policy remains unchanged for several years, despite changes in risk environment, leadership, or business strategy.
Why It Matters During an Audit: ISO 22301 expects the policy to remain

relevant and aligned. Lack of review indicates passive governance.
How to Address It: Review the policy annually or when major changes occur. Update language, references, and alignment with strategic direction.
Expected Result: A current policy reflects leadership oversight and reinforces organizational commitment.

93. Incident Escalation Procedures Lack Specific Thresholds

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Escalation procedures exist in name only, with no clearly defined criteria or conditions that trigger upward communication.
Why It Matters During an Audit: ISO 22301 emphasizes structured escalation. Vague procedures result in delays or inconsistent responses.
How to Address It: Define quantitative or qualitative thresholds for escalation (e.g., downtime duration, financial impact). Include responsible contacts.
Expected Result: Clear escalation improves decision-making speed and coordination, and supports audit validation.

94. Strategic Suppliers Are Not Participating in Continuity Reviews

📌 Clause: 8.4.6 – Coordination with External Parties

What's Going Wrong: Critical vendors are excluded from planning, testing, or strategy discussions, limiting integration and risk awareness.
Why It Matters During an Audit: ISO 22301 requires coordination with third parties. Isolation weakens continuity assurance.
How to Address It: Invite key suppliers to continuity briefings or exercises. Share requirements and assess response capabilities.

Expected Result: Active supplier involvement strengthens system resilience and ensures regulatory and contractual alignment.

95. No Distinction Between Crisis Management and Business Continuity Plans

📌 Clause: 8.4.2 and 8.4.4 – Plans and Incident Response

What's Going Wrong: Crisis management (strategic decisions, stakeholder management) and business continuity (operational recovery) are combined into a single, unclear plan.
Why It Matters During an Audit: ISO 22301 distinguishes between tactical and strategic response layers. Combined plans confuse roles and responsibilities.
How to Address It: Develop separate crisis management and continuity plans. Define ownership, escalation levels, and communication boundaries.
Expected Result: Clear structure ensures effective strategic response and operational execution during disruptions.

96. Inconsistent Format and Structure of Continuity Documents Across Departments

📌 Clause: 7.5 – Documented Information

What's Going Wrong: Different teams use varied formats and terminology in their continuity documentation, creating inconsistency.
Why It Matters During an Audit: Standardization supports clarity and ensures documents can be interpreted during crisis conditions.
How to Address It: Create standardized templates for continuity documents. Enforce formatting and terminology guidelines.

Expected Result: Consistent documentation improves usability and meets ISO documentation requirements.

97. Recovery Procedures Do Not Address Partial Disruptions

📌 Clause: 8.4.2 – Business Continuity Plans and Procedures

What's Going Wrong: Plans assume total loss scenarios but do not include actions for localized or partial failures, which are more common.
Why It Matters During an Audit: ISO 22301 expects practical, scalable response capabilities. Overlooking partial scenarios is a gap.
How to Address It: Include tiered response strategies based on incident severity. Address local, regional, and complete outages.
Expected Result: Scalable plans enhance resilience and readiness for real-world conditions.

98. No Integration of BCMS KPIs Into Broader Performance Management

📌 Clause: 6.2 and 9.1 – Objectives and Monitoring

What's Going Wrong: BCMS metrics are tracked separately but are not aligned with organizational KPIs or management dashboards.
Why It Matters During an Audit: ISO 22301 encourages integration with business performance to ensure continuity is embedded in culture.
How to Address It: Incorporate continuity KPIs into enterprise performance systems. Report metrics in governance meetings.
Expected Result: Integrated monitoring increases visibility, accountability, and supports a culture of resilience.

99. No Consideration of Environmental Events in Risk Scenarios

📌 Clause: 8.2.3 – Risk Assessment

What's Going Wrong: Natural and environmental threats (e.g., climate change, floods, heatwaves) are not assessed in continuity planning.
Why It Matters During an Audit: ISO 22301 expects context-aware planning. Environmental threats are increasingly material.
How to Address It: Add environmental risks to your risk register. Assess based on location, infrastructure, and dependencies.
Expected Result: Comprehensive risk coverage improves system relevance and aligns with ESG and sustainability objectives.

100. Business Continuity Governance Structure Not Formalized

📌 Clause: 5.3 – Roles, Responsibilities, and Authorities

What's Going Wrong: BCMS governance exists informally but lacks a defined structure, charters, or decision-making framework.
Why It Matters During an Audit: ISO 22301 requires clear governance. Informality signals weak oversight and authority ambiguity.
How to Address It: Define the BCMS governance model. Assign roles, establish reporting lines, and formalize decision-making protocols.
Expected Result: Formal governance ensures accountability, supports continuity maturity, and satisfies auditor expectations.

Building a Robust and Audit-Ready BCMS

Achieving and maintaining ISO 22301:2019 certification is more than fulfilling an audit checklist — it represents an organization’s commitment to operational resilience, risk awareness, and stakeholder trust.

The ability to effectively respond to disruptions, recover critical operations, and safeguard continuity is a strategic advantage in today’s volatile environment.

By addressing the 100 most common audit non-conformities outlined in this guide, your organization takes a significant step toward building a mature, auditable, and sustainable Business Continuity Management System (BCMS).

These observations, derived from actual audit findings and the insights of certified lead auditors, provide a clear and practical path for continuous improvement.

Key takeaways:

- **Continual Improvement Is a Requirement, Not a Recommendation**
  Regular testing, reviews, training, and corrective actions are fundamental to maintaining BCMS relevance and audit readiness.
- **Documentation and Traceability Matter**
  Accurate, version-controlled, and accessible documentation is essential for demonstrating compliance and for effective incident response.
- **Leadership and Integration Drive Success**
  An effective BCMS requires top management involvement, alignment with business strategy, and cross-functional coordination.

- **Risk-Based Thinking Is Core**
  ISO 22301 is built on the principle of understanding and addressing risk. Integrating BIA, risk assessment, and strategic planning ensures a robust response framework.

This guide should be used not only as an audit preparation tool, but also as a blueprint for elevating resilience, ensuring regulatory alignment, and embedding continuity into your organizational culture.

Stay proactive. Stay prepared. Let your continuity capabilities reflect your commitment to stability, trust, and operational excellence.

GSDC
Global Skill Development Council

CERTIFIED ISO 22301:2019 LEAD AUDITOR

Get global recognition and stand out as a leader in the field of Lead Auditor.

ABOUT GSDC CERTIFICATION

LIFETIME VALIDITY

GSDC Certification is an globally accreditted certification with lifetime validity.

EBOOK

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

CREATED BY EXPERTS

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

LEARNING MATERIALS

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

LEARNING OBJECTIVE

- **Establish credibility as a trusted business continuity management auditor**
- **Enhance career opportunities in auditing.**
- **Demonstrate commitment to organizational resilience and continuity**
- **Proficiency in planning and executing ISO 22301 audits**

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

Enroll Now

www.gsdcouncil.org