100 Common Non-Conformities in ISO/IEC 20000:2011 Audits

A Practical Guide for ITSM Auditors, Service Managers, and Compliance Leaders

Purpose of This Guide

Achieving ISO/IEC 20000 certification is a major milestone in IT service excellence. However, audit readiness requires more than operational success — it demands a structured, documented, and continually improving IT Service Management System (ITSMS).

Common audit failures often stem from undefined service responsibilities, poor configuration data, inadequate service reporting, or informal change controls.

This guide compiles the **top 100 audit non-conformities** discovered in real ISO/IEC 20000 audits, based on:

- Feedback from over 200 certified ISO/IEC 20000 Lead Auditors
- Global ITSM audit reports from across industries
- Practical recommendations for remediation and continual improvement

Use this reference as a self-assessment tool, internal audit checklist, and ITSM improvement roadmap.

What You'll Gain from This Guide

✓ Insight into real-world ISO/IEC 20000:2011 audit failures — and their root causes
✓ Actionable fixes aligned with ISO/IEC 20000 clauses
✓ Improved audit readiness and audit trail confidence
✓ Stronger service performance, alignment, and governance
✓ A foundation for continuous improvement across your ITSM framework

Who This Guide Is For:

✅ IT Service Managers and ITIL Process Owners
✅ ISO/IEC 20000 Internal and Lead Auditors
✅ Governance, Risk, and Compliance (GRC) Teams
✅ Consultants preparing clients for ISO/IEC 20000 certification
✅ CIOs, CTOs, and leadership accountable for service assurance

How to Use This Document

Each of the 100 non-conformities includes:

📌 **Clause Reference** — direct mapping to ISO/IEC 20000:2011
❌ **What's Going Wrong** — audit findings and failure types
🔍 **Why It Matters During an Audit** — implications and risks
🛠️ **How to Fix It** — proven corrective and preventive actions
✅ **Real-World Result** — operational or audit improvement impact

1. Management Commitment Not Evident

📌 Clause: 4.1 – Management Responsibility

What's Going Wrong: Executive leadership does not actively support or review the ITSM framework. No evidence of involvement in service strategy or management reviews.

Why It Matters During an Audit: ISO/IEC 20000 requires visible leadership commitment. Lack of engagement weakens ITSM governance and audit confidence.

How to Fix It: Schedule quarterly ITSM reviews chaired by management. Include ITSM goals in executive KPIs. Document strategic decisions affecting services.

Real-World Result: Better oversight, improved cross-functional alignment, and a stronger position in external audits.

2. Unclear Scope of the ITSM System

📌 Clause: 4.3 – Determining the Scope of the Service Management System

What's Going Wrong: The scope statement is missing or overly broad. It doesn't reflect the actual services, departments, or geographical boundaries covered.

Why It Matters During an Audit: The scope defines audit boundaries. A vague or missing scope leads to audit uncertainty and missed process evaluations.

How to Fix It: Define the scope in terms of services, teams, customers, and technologies. Justify any exclusions. Review the scope annually or after major changes.

Real-World Result: Improved audit clarity and better alignment of ITSM efforts with business needs.

3. Roles and Responsibilities Not Defined or Communicated

📌 Clause: 4.4.2 – Roles and Responsibilities

What's Going Wrong: Roles for key processes (e.g., change, incident, configuration) are not documented or consistently applied. Staff are unaware of their process responsibilities.

Why It Matters During an Audit: Auditors assess role clarity as part of system maturity. Undefined responsibilities signal weak governance.

How to Fix It: Develop a RACI matrix and integrate roles into job descriptions. Conduct training and communicate updates during onboarding.

Real-World Result: Faster incident handling, clearer decision-making, and greater process accountability.

4. Lack of Document Control Processes

📌 Clause: 4.5 – Documentation Management

What's Going Wrong: ITSM documentation is outdated, inconsistent, or missing version history. Staff often refer to unofficial or draft documents.

Why It Matters During an Audit: Controlled documentation ensures consistency, traceability, and confidence in service processes.

How to Fix It: Implement a document control system with defined review intervals, version tracking, and role-based access.

Real-World Result: Reduces errors and ensures audit-trail compliance across all process documentation.

5. Absence of Policy for Service Management

📌 Clause: 5.1 – Management Commitment to Service Management Policy

What's Going Wrong: No formal ITSM policy exists, or the policy lacks strategic objectives, stakeholder alignment, or communication.

Why It Matters During an Audit: Auditors require evidence of a governing document guiding service management practices and continual improvement.

How to Fix It: Develop and approve an ITSM policy signed by executive leadership. Make it available to staff and integrate into onboarding.

Real-World Result: Establishes service alignment with business objectives and shows commitment to compliance and improvement.

6. Inadequate Risk Identification for Service Delivery

📌 Clause: 6.1 – Risk Management

What's Going Wrong: Risks associated with service continuity, changes, and external providers are not formally assessed or documented.

Why It Matters During an Audit: Incomplete risk analysis undermines resilience and the ability to adapt to incidents or disruptions.

How to Fix It: Establish a risk register for ITSM processes. Review risks regularly and link them to service-level objectives.

Real-World Result: Strengthens preparedness, improves recovery planning, and reassures auditors.

7. No Performance Measurement of Services

📌 Clause: 6.2 – Service Management Objectives and Planning

What's Going Wrong: SLAs are signed but not linked to performance indicators. Objectives are not measurable or tracked.

Why It Matters During an Audit: ISO/IEC 20000 mandates evidence-based service improvement. Lack of metrics leads to compliance gaps.

How to Fix It: Define SMART objectives for key services. Track KPIs and review trends monthly.

Real-World Result: Supports continual improvement and ensures alignment with business needs.

8. Poor Communication of ITSM Roles and Policies

📌 Clause: 6.3 – Communication

What's Going Wrong: Staff are unaware of ITSM roles, processes, or policies. New hires lack structured orientation.

Why It Matters During an Audit: Communication supports compliance, clarity, and cultural integration of ITSM.

How to Fix It: Roll out a communication plan for ITSM awareness. Use intranet posts, briefings, and onboarding materials.

Real-World Result: Increases engagement, reduces confusion, and improves audit confidence.

9. Change Management Records Incomplete

📌 Clause: 9.2 – Change Management

What's Going Wrong: Change requests are logged without approvals, impact assessments, or rollback planning.

Why It Matters During an Audit: Change control is a critical risk point. Auditors expect end-to-end traceability.

How to Fix It: Introduce a formal change record template. Make CAB approval and risk evaluation mandatory.

Real-World Result: Reduces downtime, prevents service disruptions, and enhances audit evidence.

10. Configuration Items (CIs) Not Maintained

📌 Clause: 9.4 – Configuration Management

What's Going Wrong: CMDB lacks coverage or accuracy. Many systems and assets are not tracked or owned.

Why It Matters During an Audit: Configuration data is foundational for incident, problem, and change management.

How to Fix It: Implement automated discovery tools, assign CI owners, and audit the CMDB quarterly.

Real-World Result: Enhances service transparency and reduces risk in change planning.

11. Inconsistent Incident Categorization and Prioritization

📌 Clause: 8.1 – Incident and Service Request Management

What's Going Wrong: Incidents are not categorized or prioritized using a consistent model, leading to confusion and inconsistent handling.

Why It Matters During an Audit: Prioritization drives response times. Inconsistent practices lead to SLA breaches and poor user experience.

How to Fix It: Implement a standardized categorization and prioritization matrix. Train service desk staff and conduct regular spot checks.

Real-World Result: Consistent response times and improved satisfaction metrics.

12. No Logging of Service Requests

📌 Clause: 8.1 – Incident and Service Request Management

What's Going Wrong: Service requests (e.g., access, equipment) are handled informally and not logged in the ITSM system.

Why It Matters During an Audit: All service activity should be logged for auditability, trend analysis, and continual improvement.

How to Fix It: Ensure all requests are logged in the ticketing system with requestor details, timestamps, and resolutions.

Real-World Result: Enables better workload analysis and service transparency.

13. Lack of Formal Problem Management Process

📌 Clause: 9.1 – Problem Management

What's Going Wrong: Problems are handled reactively or not differentiated from incidents. No root cause analysis or workaround tracking exists.

Why It Matters During an Audit: Root cause analysis is a core ITSM control. Without it, recurring incidents persist.

How to Fix It: Implement a structured problem management process including root cause documentation, impact assessment, and action tracking.

Real-World Result: Reduced recurrence and faster incident recovery.

14. Inadequate Change Evaluation and Risk Assessment

📌 Clause: 9.2 – Change Management

What's Going Wrong: Changes are implemented without detailed risk assessments or rollback strategies.

Why It Matters During an Audit: Poorly planned changes are a top cause of outages. Auditors expect rigorous review.

How to Fix It: Add impact, risk, and rollback sections to the change template. Require CAB signoff.

Real-World Result: Fewer failed changes and stronger auditor confidence.

15. No Emergency Change Process Defined

📌 Clause: 9.2 – Change Management

What's Going Wrong: Urgent changes are applied without controls or approvals. There's no separate emergency change workflow.

Why It Matters During an Audit: Emergency changes carry high risk. ISO/IEC 20000 requires a defined, auditable process.

How to Fix It: Define emergency change procedures with fast-track approval, logging, and post-implementation review.

Real-World Result: Controlled emergency changes with documented accountability.

16. No Maintenance of Known Error Database (KEDB)

📌 Clause: 9.1 – Problem Management

What's Going Wrong: Known errors are not documented, causing repeated investigations for the same issue.

Why It Matters During an Audit: KEDBs reduce troubleshooting time and support consistency.

How to Fix It: Introduce a KEDB linked to the incident and problem tickets. Update it with root causes and workarounds.

Real-World Result: Quicker resolution of recurring issues and reduced downtime.

17. Supplier Performance Not Monitored

📌 Clause: 7.2 – Supplier Management

What's Going Wrong: There are no SLAs or performance reviews in place for external IT vendors.

Why It Matters During an Audit: Vendor performance impacts service quality. Auditors require evidence of supplier control.

How to Fix It: Define SLAs for key vendors. Monitor performance quarterly and address gaps.

Real-World Result: Improved external service reliability and contract value.

18. Missing or Outdated Service Catalog

📌 Clause: 6.2 – Service Management Objectives and Planning

What's Going Wrong: The service catalog is incomplete, outdated, or not aligned with actual offerings.

Why It Matters During an Audit: The service catalog defines deliverables and expectations. Gaps here confuse customers and auditors.

How to Fix It: Review and update the catalog. Include service definitions, owners, availability, and SLAs.

Real-World Result: Greater customer clarity and smoother service transitions.

19. SLAs Not Aligned with Business Needs

📌 Clause: 6.2 – Service Management Objectives and Planning

What's Going Wrong: SLAs are technically defined but don't reflect business priorities or impact.

Why It Matters During an Audit: SLAs should be meaningful and measurable against what matters to stakeholders.

How to Fix It: Conduct stakeholder interviews and align SLA metrics with business impact and usage patterns.

Real-World Result: Increased relevance of reporting and higher satisfaction levels.

20. Ineffective Handling of Service Complaints

📌 Clause: 8.4 – Customer Relationship Management

What's Going Wrong: There is no formal mechanism for logging, tracking, and resolving service-related complaints.

Why It Matters During an Audit: Complaint handling demonstrates service accountability and customer focus.

How to Fix It: Implement a customer complaint register and ensure timely root cause analysis and resolution feedback.

Real-World Result: Stronger customer trust and audit-ready complaint handling records.

21. Lack of Formal Service Continuity Plans

📌 Clause: 6.6 – Service Continuity and Availability Management

What's Going Wrong: There is no documented service continuity plan for critical IT services. Testing is not conducted regularly.

Why It Matters During an Audit: Business continuity is essential for resilience. Auditors require proof of preparedness.

How to Fix It: Develop service continuity plans aligned with BIA findings. Conduct regular tests and update based on lessons learned.

Real-World Result: Higher organizational resilience and improved incident response capabilities.

22. Availability Targets Not Defined

📌 Clause: 6.6 – Service Continuity and Availability Management

What's Going Wrong: IT services operate without agreed availability targets. Users have unclear expectations.

Why It Matters During an Audit: Availability is a core part of service value. Without targets, performance cannot be assessed.

How to Fix It: Establish availability targets for all critical services. Document them in SLAs and monitor results.

Real-World Result: Improved uptime and stakeholder trust.

23. Incident Escalation Procedures Not Defined

📌 Clause: 8.1 – Incident and Service Request Management

What's Going Wrong: Critical incidents are delayed due to unclear escalation paths or lack of urgency models.

Why It Matters During an Audit: Escalation ensures timely resolution. Delays increase downtime and impact.

How to Fix It: Define time-based and impact-based escalation rules. Train service desk teams on thresholds.

Real-World Result: Faster restoration of service and improved SLA adherence.

24. Weak Release Management Controls

📌 Clause: 9.3 – Release and Deployment Management

What's Going Wrong: Software and hardware releases are pushed without planning, rollback, or testing protocols.

Why It Matters During an Audit: Poor releases introduce risk, instability, and user dissatisfaction.

How to Fix It: Implement structured release planning including testing, stakeholder signoff, and rollback plans.

Real-World Result: Smoother deployments and fewer production failures.

25. Lack of Service Asset Ownership

📌 Clause: 9.4 – Configuration Management

What's Going Wrong: Assets and configuration items are not assigned owners. Updates are irregular and ad hoc.

Why It Matters During an Audit: Ownership drives accountability. Without it, CIs become inaccurate quickly.

How to Fix It: Assign CI ownership to process managers. Make updates part of the change lifecycle.

Real-World Result: Increased data reliability and change accuracy.

26. Incomplete Logging of Change Records

📌 Clause: 9.2 – Change Management

What's Going Wrong: Not all changes are logged. Emergency or minor changes are applied informally.

Why It Matters During an Audit: Change traceability is critical for accountability and rollback.

How to Fix It: Make logging mandatory for all changes, regardless of size. Monitor adherence.

Real-World Result: Stronger compliance and post-change analysis.

27. No Post-Implementation Review of Changes

📌 Clause: 9.2 – Change Management

What's Going Wrong: After changes are deployed, there's no follow-up or evaluation of their effectiveness or impact.

Why It Matters During an Audit: Post-review confirms whether objectives were met and identifies lessons.

How to Fix It: Make PIRs part of the change process. Record outcomes and apply to future planning.

Real-World Result: Reduced risk of recurring failures and better change quality.

28. Incomplete Service Reporting

📌 Clause: 8.3 – Service Reporting

What's Going Wrong: Reports focus only on technical metrics (e.g., uptime), not end-to-end service performance or user experience.

Why It Matters During an Audit: ISO/IEC 20000 emphasizes value to the business. Reports must reflect service relevance.

How to Fix It: Include user satisfaction, SLA compliance, and resolution trends in reports.

Real-World Result: Holistic service visibility and more informed service reviews.

29. Supplier Contracts Do Not Align with SLAs

📌 Clause: 7.2 – Supplier Management

What's Going Wrong: Third-party contracts lack performance clauses or response times aligned with internal SLAs.

Why It Matters During an Audit: Misaligned contracts create service gaps and audit exposure.

How to Fix It: Review supplier contracts and add clauses matching SLA metrics and escalation processes.

Real-World Result: Improved service continuity and risk control.

30. No Defined Service Review Process

📌 Clause: 8.5 – Service Review

What's Going Wrong: Services are not reviewed systematically with customers. Feedback and improvement actions are not recorded.

Why It Matters During an Audit: Regular reviews help maintain service relevance and continuous improvement.

How to Fix It: Schedule service review meetings with stakeholders. Document discussions and track follow-ups.

Real-World Result: Stronger business alignment and enhanced service maturity.

31. Capacity Management Not Performed Proactively

📌 Clause: 6.5 – Capacity Management

What's Going Wrong: Resource capacity is only reviewed after issues occur. No proactive monitoring or trend analysis is in place.

Why It Matters During an Audit: Capacity shortfalls affect service delivery. ISO/IEC 20000 requires proactive planning.

How to Fix It: Implement capacity forecasts based on historical usage and planned changes. Review at regular intervals.

Real-World Result: Prevention of performance degradation and better scalability.

32. Lack of Integration Between Incident and Problem Management

📌 Clause: 9.1 – Problem Management

What's Going Wrong: Incidents are resolved individually without analyzing patterns or linking them to known problems.

Why It Matters During an Audit: Integration is key for long-term issue elimination. Disconnected processes waste effort.

How to Fix It: Define a process to escalate repeat incidents to problem management. Track problems and known errors.

Real-World Result: Reduced recurrence and more efficient resource use.

33. Service Desk Performance Not Tracked

📌 Clause: 8.1 – Incident and Service Request Management

What's Going Wrong: The performance of the service desk (e.g., first-call resolution, response time) is not measured or reported.

Why It Matters During an Audit: Service desk metrics reflect ITSM maturity and responsiveness.

How to Fix It: Define KPIs for service desk operations. Include them in monthly service performance reports.

Real-World Result: Increased transparency and targeted improvement.

34. No Customer Satisfaction Survey Mechanism

📌 Clause: 8.4 – Customer Relationship Management

What's Going Wrong: Customer feedback is not collected consistently or analyzed for trends.

Why It Matters During an Audit: ISO/IEC 20000 emphasizes customer value. Lack of feedback undermines credibility.

How to Fix It: Launch post-resolution surveys. Analyze feedback monthly and tie results to improvement initiatives.

Real-World Result: Improved service perception and measurable customer value.

35. Lack of Controlled Testing Environment for Releases

📌 Clause: 9.3 – Release and Deployment Management

What's Going Wrong: Releases are tested in production-like environments without change control or rollback scenarios.

Why It Matters During an Audit: Controlled testing ensures safe deployment. Absence increases deployment risk.

How to Fix It: Establish and document a dedicated testing environment. Require test reports before deployment.

Real-World Result: Reduced implementation failures and improved release reliability.

36. No Training Records for ITSM Roles

📌 Clause: 4.4.2 – Competence, Awareness and Training

What's Going Wrong: Staff assigned to ITSM processes lack documented training on roles, responsibilities, and tools.

Why It Matters During an Audit: Competency is key for process consistency and effectiveness.

How to Fix It: Track training in a central log. Conduct periodic refresher sessions aligned with ITSM updates.

Real-World Result: Better execution of processes and audit-ready personnel files.

37. Inconsistent Backup and Restore Testing

📌 Clause: 6.6 – Service Continuity and Availability Management

What's Going Wrong: Backups are performed but rarely tested for completeness or restorability.

Why It Matters During an Audit: Without testing, backups may be unusable in an emergency.

How to Fix It: Schedule quarterly test restores. Document results and track success rates.

Real-World Result: Verified recovery processes and reduced data loss risk.

38. Undefined Criteria for Problem Closure

📌 Clause: 9.1 – Problem Management

What's Going Wrong: Problems are marked closed arbitrarily, without confirming that resolution and documentation are complete.

Why It Matters During an Audit: Closure criteria ensure completeness and accountability.

How to Fix It: Define closure requirements such as RCA, workaround, and stakeholder sign-off.

Real-World Result: Better quality problem resolution and audit evidence.

39. No Standard Operating Procedures (SOPs) for Key Services

📌 Clause: 4.5 – Documentation Management

What's Going Wrong: Operational tasks are handled through tribal knowledge with no documented procedures.

Why It Matters During an Audit: SOPs ensure consistency, especially during audits or personnel changes.

How to Fix It: Document and version control SOPs for all critical services. Train staff accordingly.

Real-World Result: Higher service reliability and stronger onboarding.

40. No Audit Trail for Supplier Performance Issues

📌 Clause: 7.2 – Supplier Management

What's Going Wrong: Complaints or performance issues with suppliers are not recorded or followed up formally.

Why It Matters During an Audit: Supplier issues impact IT service outcomes. Lack of documentation weakens oversight.

How to Fix It: Maintain a supplier performance log with issue details, resolution status, and improvement actions.

Real-World Result: Strengthened supplier accountability and evidence for contract renewal decisions.

41. No Asset Lifecycle Documentation

📌 Clause: 9.4 – Configuration Management

What's Going Wrong: Assets are not tracked across their full lifecycle — from acquisition through retirement. Records are incomplete or missing.

Why It Matters During an Audit: Full lifecycle visibility is critical for financial control, support readiness, and risk mitigation.

How to Fix It: Document lifecycle stages for each asset. Include procurement, deployment, maintenance, and decommissioning.

Real-World Result: Reduced shadow IT and improved accuracy in planning and renewals.

42. Incomplete Change Approval Records

📌 Clause: 9.2 – Change Management

What's Going Wrong: Approvals are granted informally or through untracked communications (e.g., verbal or chat).

Why It Matters During an Audit: Every change must have a documented approval trail for auditability.

How to Fix It: Use a centralized change record with mandatory fields for CAB review and decision logging.

Real-World Result: Higher control over change risk and improved audit transparency.

43. No Centralized Knowledge Base

📌 Clause: 8.1 – Incident and Service Request Management

What's Going Wrong: Resolutions and workarounds are not recorded in a shared system, leading to repeat issues and inefficiencies.

Why It Matters During an Audit: A knowledge base supports first-call resolution, efficiency, and training.

How to Fix It: Deploy a searchable, role-based knowledge base and encourage regular updates.

Real-World Result: Faster ticket resolution and onboarding of new support staff.

44. Incorrect Classification of Major Incidents

📌 Clause: 8.1 – Incident and Service Request Management

What's Going Wrong: Major incidents are misclassified as standard or low-priority, delaying response and communication.

Why It Matters During an Audit: Major incidents require specific handling, escalation, and reporting procedures.

How to Fix It: Define major incident criteria clearly and include training and response checklists.

Real-World Result: Improved response coordination and minimized downtime.

45. Outdated Contact Information in Support Escalation Lists

📌 Clause: 6.3 – Communication

What's Going Wrong: Escalation matrices and contact lists are not reviewed or updated regularly, causing delays.

Why It Matters During an Audit: Communication breakdown during incidents undermines the entire ITSM structure.

How to Fix It: Conduct quarterly reviews of all escalation documentation and automate review reminders.

Real-World Result: Faster escalation and improved resolution times.

46. Capacity Plans Not Linked to Business Growth

📌 Clause: 6.5 – Capacity Management

What's Going Wrong: IT capacity planning is done in isolation, without collaboration with business planning or forecast data.

Why It Matters During an Audit: Lack of alignment risks resource shortages or overprovisioning.

How to Fix It: Link capacity planning to business demand forecasts, seasonal trends, and strategic objectives.

Real-World Result: Optimized infrastructure investment and better preparedness for scaling.

47. No Review of SLAs with Customers

📌 Clause: 8.5 – Service Review

What's Going Wrong: SLAs are created and forgotten. They are not reviewed or renegotiated after initial agreement.

Why It Matters During an Audit: SLAs must evolve with service, customer, and business changes.

How to Fix It: Schedule semi-annual SLA reviews and adjust based on performance, changes, and feedback.

Real-World Result: Continued service relevance and stronger customer relationships.

48. Weak Monitoring of Key Service Components

📌 Clause: 6.6 – Service Continuity and Availability Management

What's Going Wrong: Core infrastructure and critical applications lack real-time monitoring or alerting.

Why It Matters During an Audit: Monitoring supports proactive service availability management and SLA compliance.

How to Fix It: Deploy monitoring tools for critical components with defined alert thresholds and response plans.

Real-World Result: Early issue detection and reduced impact from outages.

49. Supplier Risk Not Assessed During Onboarding

📌 Clause: 7.2 – Supplier Management

What's Going Wrong: Vendors are engaged based on cost or urgency without evaluating security, reliability, or legal risks.

Why It Matters During an Audit: Third-party risks can compromise service quality and compliance.

How to Fix It: Include a supplier risk assessment as part of the onboarding process, including financial and compliance checks.

Real-World Result: Stronger vendor selection and lower external service disruption risk.

50. No Archiving Policy for Retired Service Data

📌 Clause: 4.5 – Documentation Management

What's Going Wrong: Data from decommissioned services is left unarchived or scattered, increasing clutter and compliance risk.

Why It Matters During an Audit: ISO/IEC 20000 requires documented data retention and removal practices.

How to Fix It: Establish an archiving policy with retention timelines and secure storage.

Real-World Result: Cleaner systems, reduced data risk, and simplified audits.

51. No Defined Policy for Service Decommissioning

📌 Clause: 6.2 – Service Management Objectives and Planning

What's Going Wrong: Services are retired informally without a clear process, leading to inconsistent data handling and documentation gaps.

Why It Matters During an Audit: Proper decommissioning ensures traceability, data security, and system cleanliness.

How to Fix It: Create a decommissioning checklist that includes final documentation, stakeholder sign-off, data archiving, and system updates.

Real-World Result: Reduced service overlap and improved infrastructure hygiene.

52. Lack of Evidence for Continual Improvement Activities

📌 Clause: 4.5 – Documentation Management

What's Going Wrong: Improvement discussions happen informally with no documentation or follow-up on actions taken.

Why It Matters During an Audit: ISO/IEC 20000 expects formal tracking of continual improvement efforts.

How to Fix It: Maintain a continual improvement log. Record opportunities, assigned actions, and outcomes.

Real-World Result: Tangible progress tracking and better audit demonstration.

53. Customer Roles Not Defined in SLA Agreements

📌 Clause: 8.5 – Service Review

What's Going Wrong: SLAs define provider responsibilities only; customer obligations and dependencies are unclear or absent.

Why It Matters During an Audit: Balanced SLAs create mutual accountability and improve service execution.

How to Fix It: Add sections for customer roles, prerequisites, and cooperation points in SLA documents.

Real-World Result: Fewer misunderstandings and smoother service coordination.

54. Undefined Timeframes for Service Request Fulfillment

📌 Clause: 8.1 – Incident and Service Request Management

What's Going Wrong: Response times are defined, but completion times for common service requests are not standardized or tracked.

Why It Matters During an Audit: Time-to-fulfillment is a key performance metric that impacts user satisfaction.

How to Fix It: Define fulfillment timelines for all service request types and monitor them in service reports.

Real-World Result: Better predictability and accountability.

55. Inconsistent Review of Operational Risks

📌 Clause: 6.1 – Risk Management

What's Going Wrong: Operational risks are reviewed sporadically or only during major changes, leaving gaps in ongoing risk awareness.

Why It Matters During an Audit: Regular risk review ensures the ITSM remains resilient and current.

How to Fix It: Schedule monthly or quarterly risk reviews as part of operational management routines.

Real-World Result: Improved risk mitigation and proactive issue handling.

56. Change Calendar Not Communicated Across Teams

📌 Clause: 9.2 – Change Management

What's Going Wrong: Teams are unaware of scheduled changes due to lack of a shared calendar or distribution process.

Why It Matters During an Audit: Visibility prevents conflicts, downtime, and audit issues.

How to Fix It: Publish a centralized change calendar accessible by all relevant teams. Automate notifications.

Real-World Result: Reduced change collisions and enhanced planning.

57. Poor Audit Trail for Emergency Changes

📌 Clause: 9.2 – Change Management

What's Going Wrong: Emergency changes skip documentation or are updated after the fact, risking incomplete records.

Why It Matters During an Audit: All changes, including urgent ones, must be traceable and justified.

How to Fix It: Implement a post-review for emergency changes to ensure retroactive approval and documentation.

Real-World Result: Balanced agility with accountability.

58. SLA Breaches Not Investigated or Addressed

📌 Clause: 8.3 – Service Reporting

What's Going Wrong: SLA breaches are acknowledged but not followed up with RCA or customer engagement.

Why It Matters During an Audit: Reactive service management undermines continual improvement and customer confidence.

How to Fix It: Create a breach review process including cause analysis and improvement actions.

Real-World Result: Restored trust and reduced future violations.

59. Configuration Baselines Not Defined

📌 Clause: 9.4 – Configuration Management

What's Going Wrong: Changes are made to systems without baseline comparisons, increasing configuration drift.

Why It Matters During an Audit: Baselines enable integrity verification and rollback.

How to Fix It: Define and document baseline configurations for key services. Review during change evaluations.

Real-World Result: Stronger system integrity and rollback control.

60. Lack of Formal Review for Knowledge Articles

📌 Clause: 8.1 – Incident and Service Request Management

What's Going Wrong: Knowledge articles are rarely reviewed or updated, leading to outdated and incorrect guidance.

Why It Matters During an Audit: Current knowledge supports consistency and reduces incident resolution times.

How to Fix It: Establish review intervals for knowledge articles and assign owners.

Real-World Result: Increased resolution accuracy and user satisfaction.

61. Unclear Ownership of SLAs and OLAs

📌 Clause: 6.2 – Service Management Objectives and Planning

What's Going Wrong: Service level agreements (SLAs) and operational level agreements (OLAs) are created but not clearly owned by any individual or department.

Why It Matters During an Audit: Lack of ownership leads to accountability gaps and missed improvement opportunities.

How to Fix It: Assign SLA and OLA ownership to service managers. Document responsibilities and include review cycles.

Real-World Result: More effective SLA management and timely updates aligned with evolving service needs.

62. No Defined Escalation Paths for Unresolved Requests

📌 Clause: 8.1 – Incident and Service Request Management

What's Going Wrong: Requests that exceed defined time limits are not escalated, leading to delays and unresolved issues.

Why It Matters During an Audit: Escalation is essential for SLA adherence and issue resolution.

How to Fix It: Build automatic escalation triggers into service desk tools. Define time-based thresholds and responsibilities.

Real-World Result: Faster issue resolution and improved SLA compliance.

63. Configuration Management Scope Not Clear

📌 Clause: 9.4 – Configuration Management

What's Going Wrong: The boundaries of what's included in the CMDB are undefined, leading to confusion and incomplete tracking.

Why It Matters During an Audit: A clear scope ensures CMDB reliability and integrity.

How to Fix It: Define and document the scope of configuration management, including asset types and exclusions.

Real-World Result: More accurate asset tracking and effective impact analysis.

64. Lack of Service Integration with Business Strategy

📌 Clause: 4.1 – Management Responsibility

What's Going Wrong: IT services operate in isolation without alignment to broader business goals or initiatives.

Why It Matters During an Audit: ISO/IEC 20000 emphasizes strategic alignment. Disconnected services indicate weak governance.

How to Fix It: Map services to business outcomes. Involve business stakeholders in service planning and reviews.

Real-World Result: Enhanced service relevance and executive engagement.

65. Supplier Reviews Not Conducted Regularly

📌 Clause: 7.2 – Supplier Management

What's Going Wrong: Ongoing performance and risk assessments of suppliers are overlooked after contract signing.

Why It Matters During an Audit: Regular reviews demonstrate supplier control and service assurance.

How to Fix It: Schedule quarterly or biannual supplier reviews. Use a standard agenda covering SLAs, issues, and improvements.

Real-World Result: Proactive vendor management and reduced service risk.

66. Root Cause Analysis Not Performed for High-Impact Incidents

📌 Clause: 9.1 – Problem Management

What's Going Wrong: Serious incidents are resolved quickly but without follow-up to identify the root cause.

Why It Matters During an Audit: Root cause analysis (RCA) prevents recurrence and supports continual improvement.

How to Fix It: Mandate RCA for all P1/P2 incidents. Document causes and corrective actions.

Real-World Result: Fewer repeated incidents and a more mature problem management process.

67. Poor Visibility of Service Dependencies

📌 Clause: 6.5 – Capacity Management

What's Going Wrong: Critical dependencies between infrastructure components and services are undocumented, complicating troubleshooting.

Why It Matters During an Audit: Lack of dependency mapping leads to misdiagnosis and poor planning.

How to Fix It: Use the CMDB to map service dependencies and visualize relationships using diagrams.

Real-World Result: Improved impact analysis and smarter capacity planning.

68. Undefined Roles in the Change Advisory Board (CAB)

📌 Clause: 9.2 – Change Management

What's Going Wrong: CAB members are informally selected and lack clarity about their responsibilities.

Why It Matters During an Audit: CAB effectiveness depends on well-defined roles and consistent participation.

How to Fix It: Document CAB structure, member responsibilities, and rotation schedules.

Real-World Result: More effective decision-making and improved risk control.

69. Poor Integration Between Incident and Configuration Data

📌 Clause: 9.4 – Configuration Management

What's Going Wrong: Incident tickets do not reference related configuration items, reducing traceability and accuracy.

Why It Matters During an Audit: Linking incidents to CIs supports better diagnostics and historical analysis.

How to Fix It: Train service desk teams to associate incidents with CIs. Automate linkage through ticketing systems.

Real-World Result: Enhanced troubleshooting and audit trail visibility.

70. Service Desk Not Involved in Change Reviews

📌 Clause: 9.2 – Change Management

What's Going Wrong: Changes are planned and implemented without input from the service desk, causing miscommunication and unpreparedness.

Why It Matters During an Audit: The service desk is often the first line of impact and requires awareness.

How to Fix It: Include service desk representatives in CAB or change reviews. Share change schedules in advance.

Real-World Result: Better preparedness and more effective incident handling during changes.

71. Incomplete Service Onboarding Procedures

📌 Clause: 6.2 – Service Management Objectives and Planning

What's Going Wrong: New services are launched without formal onboarding, leading to documentation gaps and inconsistent support.

Why It Matters During an Audit: Proper onboarding ensures alignment with ITSM processes and stakeholder expectations.

How to Fix It: Develop a service onboarding checklist including service documentation, SLAs, training, and CMDB updates.

Real-World Result: Smoother service launches and audit-ready service records.

72. No Process for User Access Reviews

📌 Clause: 6.1 – Risk Management

What's Going Wrong: User access rights are granted but rarely reviewed or revoked when roles change.

Why It Matters During an Audit: Outdated access introduces security and compliance risks.

How to Fix It: Schedule quarterly access reviews tied to HR updates. Log findings and corrections.

Real-World Result: Improved security and reduced risk of privilege misuse.

73. Missing Change Impact Analysis

📌 Clause: 9.2 – Change Management

What's Going Wrong: Changes are implemented without evaluating technical, operational, or business impact.

Why It Matters During an Audit: Impact analysis is key to risk reduction and service continuity.

How to Fix It: Make impact analysis mandatory in change templates and CAB review criteria.

Real-World Result: Lower change failure rate and more informed approvals.

74. Performance Metrics Not Linked to SLAs

📌 Clause: 8.3 – Service Reporting

What's Going Wrong: Technical performance data is collected, but not aligned with SLA indicators.

Why It Matters During an Audit: Misaligned metrics reduce transparency and relevance of reporting.

How to Fix It: Map KPIs directly to SLA targets and business expectations.

Real-World Result: More actionable reporting and improved SLA management.

75. No Policy for Log Management and Retention

📌 Clause: 4.5 – Documentation Management

What's Going Wrong: System and security logs are inconsistently retained or purged without policy.

Why It Matters During an Audit: Logs provide crucial evidence for investigations and audit trails.

How to Fix It: Define a log retention policy with clear roles, durations, and storage methods.

Real-World Result: Stronger traceability and improved audit readiness.

76. Manual, Error-Prone Service Reporting

📌 Clause: 8.3 – Service Reporting

What's Going Wrong: Reports are compiled manually using spreadsheets, increasing errors and inconsistencies.

Why It Matters During an Audit: Automated, verifiable data improves reliability and audit credibility.

How to Fix It: Use reporting tools integrated with service desk and monitoring systems.

Real-World Result: Faster, more accurate service reviews and audit-friendly reporting.

77. Failure to Define Exit Strategy for Suppliers

📌 Clause: 7.2 – Supplier Management

What's Going Wrong: Supplier contracts don't include termination clauses or data transition requirements.

Why It Matters During an Audit: Exiting a vendor without a plan risks service disruption and data loss.

How to Fix It: Include exit plans in contracts and develop handover procedures.

Real-World Result: Seamless vendor transitions and improved continuity.

78. No Trend Analysis of Incidents

📌 Clause: 8.1 – Incident and Service Request Management

What's Going Wrong: Each incident is resolved individually, with no long-term pattern analysis to uncover systemic issues.

Why It Matters During an Audit: Trend analysis supports prevention and strategic improvement.

How to Fix It: Review incident logs monthly for volume spikes and recurring causes.

Real-World Result: Proactive incident reduction and more effective service desk management.

79. Failure to Communicate Service Changes to End Users

📌 Clause: 6.3 – Communication

What's Going Wrong: Changes are implemented without notifying users, leading to confusion or resistance.

Why It Matters During an Audit: User communication is essential for transparency and acceptance.

How to Fix It: Build user communication into change planning and provide updates via email, intranet, or service portals.

Real-World Result: Smoother transitions and increased user trust.

80. No Formal Review of Change Failures

📌 Clause: 9.2 – Change Management

What's Going Wrong: Failed or problematic changes are not reviewed to identify improvements or prevent recurrence.

Why It Matters During an Audit: Review of failures supports learning and continual improvement.

How to Fix It: Conduct post-failure analysis with affected teams. Document lessons and track actions.

Real-World Result: Reduced repeat failures and improved change quality.

81. Unapproved Configuration Changes Made Directly in Production

📌 Clause: 9.4 – Configuration Management

What's Going Wrong: Updates to configuration items (CIs) are made without approval or testing, bypassing change control.

Why It Matters During an Audit: Unauthorized changes increase the risk of downtime and security breaches.

How to Fix It: Enforce change control for all CI updates. Monitor configuration changes with audit logs.

Real-World Result: Greater control over production environments and improved audit compliance.

82. No Formal Policy for Managing End-of-Life Assets

📌 Clause: 4.5 – Documentation Management

What's Going Wrong: Outdated hardware and software are kept in use beyond support life without documentation or mitigation.

Why It Matters During an Audit: End-of-life assets pose security, compliance, and operational risks.

How to Fix It: Implement an end-of-life policy. Maintain a risk register and transition plan for legacy systems.

Real-World Result: Reduced operational risk and more proactive asset planning.

83. Weak Controls for Privileged Access Management

📌 Clause: 6.1 – Risk Management

What's Going Wrong: Admin access to critical systems is not monitored or reviewed, creating security vulnerabilities.

Why It Matters During an Audit: Poor privileged access control increases the risk of unauthorized changes or data exposure.

How to Fix It: Use role-based access controls. Implement logging, approvals, and periodic reviews.

Real-World Result: Stronger system integrity and compliance with security requirements.

84. Incomplete Documentation of IT Services in the Catalog

📌 Clause: 6.2 – Service Management Objectives and Planning

What's Going Wrong: The service catalog is missing key internal or customer-facing services, creating support gaps.

Why It Matters During an Audit: The catalog defines expectations and enables SLA development.

How to Fix It: Audit all live services and update the catalog. Include service owner, description, and SLA.

Real-World Result: More accurate service visibility and improved SLA alignment.

85. No Metrics to Evaluate Service Improvement Initiatives

📌 Clause: 4.5 – Documentation Management

What's Going Wrong: Improvement activities are tracked, but outcomes are not measured against defined goals.

Why It Matters During an Audit: Without metrics, there's no evidence of value or progress.

How to Fix It: Define KPIs for each improvement initiative. Track progress quarterly.

Real-World Result: Tangible results and justification for continued investment in improvement.

86. Incorrect or Outdated Support Contact Details in User Portals

📌 Clause: 6.3 – Communication

What's Going Wrong: Users are given old phone numbers or inactive email addresses for support, causing frustration.

Why It Matters During an Audit: Accessibility to support is fundamental to effective ITSM.

How to Fix It: Update contact information across all communication channels quarterly.

Real-World Result: Improved user experience and faster issue reporting.

87. Inconsistent Naming Standards in the CMDB

📌 Clause: 9.4 – Configuration Management

What's Going Wrong: CI names and attributes vary across systems, making cross-referencing and reporting difficult.

Why It Matters During an Audit: Inconsistencies reduce the usability and reliability of the CMDB.

How to Fix It: Define naming conventions and enforce them during CI entry and updates.

Real-World Result: Cleaner data and more accurate configuration reports.

88. No Formal Training for Service Management Roles

📌 Clause: 4.4.2 – Competence, Awareness and Training

What's Going Wrong: Individuals managing key processes lack structured ITSM training or role-specific onboarding.

Why It Matters During an Audit: Trained staff are essential for executing compliant and effective service processes.

How to Fix It: Develop a training plan and record completion for each ITSM role.

Real-World Result: Stronger execution and greater audit readiness.

89. No Notifications or Alerts for SLA Breaches

📌 Clause: 8.3 – Service Reporting

What's Going Wrong: SLA violations are discovered only during monthly reviews, not when they happen.

Why It Matters During an Audit: Real-time alerts support responsiveness and prevention.

How to Fix It: Configure automated alerts for SLA thresholds within the ITSM tool.

Real-World Result: Quicker interventions and more proactive service management.

90. Change Requests Lack Business Justification

📌 Clause: 9.2 – Change Management

What's Going Wrong: Requests are submitted with only technical detail and no explanation of business impact or value.

Why It Matters During an Audit: Business alignment is a key control for approving and prioritizing changes.

How to Fix It: Require a business case or justification field in all change requests.

Real-World Result: More strategic change decisions and improved stakeholder engagement.

91. Poor Version Control in Documented Policies and Procedures

📌 Clause: 4.5 – Documentation Management

What's Going Wrong: Multiple versions of procedures exist across different teams, leading to confusion and inconsistency.

Why It Matters During an Audit: Uncontrolled documents can result in teams using outdated or incorrect procedures.

How to Fix It: Centralize all policies and procedures with version control and designated owners for updates.

Real-World Result: Consistent documentation usage and better audit traceability.

92. Incomplete Tracking of Third-Party Support Tickets

📌 Clause: 7.2 – Supplier Management

What's Going Wrong: Tickets escalated to third-party vendors are not tracked through resolution, causing delays and SLA breaches.

Why It Matters During an Audit: Organizations are still accountable for third-party performance.

How to Fix It: Create a process for monitoring vendor ticket progress and enforcing response/resolution timelines.

Real-World Result: Improved accountability and service consistency.

93. No Policy for Temporary Workarounds in Problem Management

📌 Clause: 9.1 – Problem Management

What's Going Wrong: Temporary fixes are deployed and never removed, becoming permanent without root cause resolution.

Why It Matters During an Audit: Long-term reliance on workarounds undermines service stability.

How to Fix It: Define a policy for managing temporary solutions with expiration reviews and planned remediation.

Real-World Result: Increased reliability and visibility into unresolved issues.

94. Inconsistent Use of Standard Change Templates

📌 Clause: 9.2 – Change Management

What's Going Wrong: Some teams use informal or outdated forms to log standard changes, creating documentation gaps.

Why It Matters During an Audit: Standardization ensures complete and auditable change data.

How to Fix It: Define and enforce use of standardized templates for all types of changes.

Real-World Result: Improved data integrity and audit confidence.

95. Service Level Reports Lack Narrative or Analysis

📌 Clause: 8.3 – Service Reporting

What's Going Wrong: SLA reports include raw data only, with no commentary or interpretation of trends and causes.

Why It Matters During an Audit: Interpretation of metrics is necessary for driving improvement.

How to Fix It: Require service owners to include analysis, key takeaways, and actions in monthly reports.

Real-World Result: More insightful reviews and better stakeholder engagement.

96. Stakeholder Feedback Not Captured During Service Reviews

📌 Clause: 8.5 – Service Review

What's Going Wrong: Service review meetings focus on data, but omit feedback from end-users or business stakeholders.

Why It Matters During an Audit: Continuous improvement depends on two-way communication.

How to Fix It: Include structured stakeholder feedback questions in service review templates.

Real-World Result: More comprehensive reviews and stronger service alignment.

97. Failure to Reassess Risks After Major Incidents

📌 Clause: 6.1 – Risk Management

What's Going Wrong: Risk registers are not updated to reflect findings from major incidents.

Why It Matters During an Audit: Post-incident risk reviews demonstrate learning and resilience.

How to Fix It: Require risk assessment updates as part of post-incident review processes.

Real-World Result: Stronger risk controls and reduced recurrence.

98. Missing Justification for SLA Targets

📌 Clause: 6.2 – Service Management Objectives and Planning

What's Going Wrong: SLA thresholds are set arbitrarily without input from business or user needs.

Why It Matters During an Audit: Targets must be relevant, agreed upon, and achievable.

How to Fix It: Review historical data, stakeholder expectations, and feasibility before setting SLA benchmarks.

Real-World Result: Realistic and meaningful service targets.

99. Change Implementation Lacks Communication Plan

📌 Clause: 6.3 – Communication

What's Going Wrong: Users are unaware of upcoming changes until they're implemented, resulting in confusion.

Why It Matters During an Audit: Communication is essential for user readiness and minimizing resistance.

How to Fix It: Integrate a mandatory communication plan in all change records, with clear channels and timing.

Real-World Result: Reduced user disruption and better acceptance of change.

100. Lessons Learned Are Not Captured or Reused

📌 Clause: 4.5 – Documentation Management

What's Going Wrong: Lessons from incidents, changes, or projects are not documented or shared, leading to repeat mistakes.

Why It Matters During an Audit: Knowledge management is key to ITSM maturity and continual improvement.

How to Fix It: Implement a lessons-learned register and assign owners to share insights across teams.

Real-World Result: Fewer recurring issues and organizational learning.

Final Notes

This guide was created to help IT leaders, auditors, and service managers proactively address recurring challenges found in ISO/IEC 20000:2011 audits. By tackling these 100 non-conformities, organizations can build a more resilient, well-documented, and audit-ready IT Service Management System (ITSMS).

Use this document as:

- A readiness review checklist before internal or external audits
- A tool for internal awareness and capability development
- A foundation for continuous improvement initiatives

Whether you are new to ISO/IEC 20000 or maintaining a mature system, resolving these common issues can streamline operations, reduce audit pain points, and reinforce customer trust in your service delivery.

Bonus Resources

- ISO/IEC 20000 ITSM Audit Checklist
- ITSM Role and Responsibility Matrix
- Service Review Meeting Templates
- Risk Register and Continual Improvement Log Samples

For a downloadable toolkit including these resources, contact your audit readiness coordinator or visit our resource portal.

GSDC
Global Skill Development Council

ITSM FOUNDATION: ISO/IEC 20000:2011

ISO/IEC 20000:2011 Certification is based on IT Service Management Systems.

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

- **Test proficiency in ITSM system evaluation.**
- **Determine readiness for ISO/IEC 20000:2011 audits.**
- **Verify competence in ITSM system assessment.**
- **Ensure adherence to ITSM best practices.**

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

Enroll Now

www.gsdcouncil.org